

REFERENCE GUIDE FOR

INCLUSIVE INSTANT PAYMENT SYSTEM SCHEME RULES

Version 1.0 - October 2026

Copyright Notice

These materials are proprietary to AfricaNenda Foundation; no part of this material should be reproduced or published in any form by any means, electronic or mechanical, including photocopy or any information storage or retrieval system, nor should the material be disclosed to third parties without the express written authorization of AfricaNenda Foundation.

Contents

EXECUTIVE SUMMARY	4
1. INTRODUCTION	6
1.1. Background	6
1.2. Purpose and Scope	6
2. GUIDING APPROACH TO SCHEME RULES DEVELOPMENT	9
2.1. Design Principles	10
2.2. Scheme Rules Development and Maintenance	10
3. THE LEGAL FRAMEWORK OF INSTANT PAYMENT SCHEMES	16
3.1. Hierarchical Structure	17
3.2. International Standards: The PFMI's	17
3.3. National Laws and Regulations	18
3.4. Participation Agreements	19
3.5. Scheme Rules	19
3.6. Operational Guidelines	20
4. CORE COMPONENTS OF PARTICIPATION AGREEMENTS	21
5. CORE COMPONENTS OF THE SCHEME RULES	24
5.1. Strategic Objectives	25
5.2. Governance Framework	25
5.3. Scheme Participation Framework	32
5.4. Operational Rules	44
5.5. User Experience Guideline	74
5.6. Branding Guidelines	78
5.7. Compliance Monitoring Framework	80
6. PRICING POLICY	81
6.1. Core Principles for Inclusive Pricing	82
6.2. Pricing Models for Instant Payments	82
6.3. Key Elements to Consider in the Scheme Rules	86
7. EDUCATION AND AWARENESS FRAMEWORK	88
7.1. Purpose	89
7.2. Key Learning Areas	89
7.3. Delivery Channels and Methods	90
7.4. Institutional Responsibilities	91
8. CONCLUSION AND PATH FORWARD	92
9. ANNEXES	93

EXECUTIVE SUMMARY

This Reference Guide, developed by AfricaNenda Foundation, is a practical resource designed to help African countries establish and strengthen inclusive instant payment ecosystems. It provides a structured framework for developing scheme rules, offering the legal, operational, and governance foundations necessary to build secure, efficient, and accessible instant payment systems.

The Reference Guide addresses key areas such as scheme purpose, governance structures, participation criteria, transaction processing, settlement mechanisms, risk and compliance frameworks, dispute resolution, user experience, and pricing principles with the aim of enhancing understanding of key concepts, requirements, and best practices among all stakeholders while ensuring consistency and transparency in rule application across payment ecosystems.

This Reference Guide is principles-based rather than prescriptive, acknowledging the diversity of legal systems, market structures, and development stages across the continent. It provides options and considerations rather than mandates, enabling countries to make informed decisions aligned with their specific circumstances and policy objectives while maintaining adherence to international standards and best practices, such as the Principles for Financial Market Infrastructures (PFMIs) and ISO 20022, to support global interoperability.

The Reference Guide is intended for a broad audience, including central banks and regulators, scheme operators, financial institutions, fintechs, and technical advisors. Each stakeholder group will find clear guidance tailored to their respective roles, responsibilities, and compliance obligations within the IPS ecosystem. Each section provides both educational content and practical implementation guidance to support these diverse audiences.

By promoting transparency, consistency, and interoperability, the Reference Guide serves as a blueprint for building resilient and scalable instant payment systems across Africa, fostering broader participation and accelerating the continent's digital financial transformation.



**Executive
Summary**

1

INTRODUCTION

2

**Guiding Approach
to Scheme Rules
Development**

3

**The Legal
Framework of
Instant Payment
Schemes**

4

**Core Components
of Participation
Agreements**

5

**Core Components
of the Scheme
Rules**

6

Pricing Policy

7

**Education
and Awareness
Framework**

8

**Conclusion and
Path Forward**

9

Annexes



1.1

Background

In today's rapidly evolving financial technology landscape, instant payments have emerged as a transformative force, fundamentally reshaping how consumers and businesses transact globally. Defined as credit transfers that enable real-time movement of funds between parties, available 24/7/365, instant payment schemes mark a significant departure from traditional payment methods, which often involve processing delays ranging from several hours to multiple days.

This global shift toward instant payments is driven by a confluence of factors: advances in digital infrastructure, supportive regulatory frameworks, growing consumer demand for speed and convenience, and the widespread adoption of mobile technologies. Together, these elements have positioned instant payment schemes as a cornerstone of modern digital economies, enabling seamless, secure, and efficient transactions while also advancing financial inclusion and fostering innovation.

In Africa, where improving access to financial services remains both a challenge and a priority, well-designed instant payment system schemes hold the promise of delivering accessible, affordable, and efficient payment solutions—particularly for underserved and rural populations. These systems can catalyze economic development, enhance the delivery of both public and private services, and reduce reliance on cash-based transactions.

To support this transformation, AfricaNenda Foundation has developed the Reference Guide for Inclusive Instant Payment System Scheme Rules (hereinafter referred to as the “Reference Guide”). This Reference Guide is intended as a comprehensive and practical resource for African countries to help design, implement, and manage effective inclusive instant payment ecosystems. It is tailored to the needs of a broad range of stakeholders, including regulators, scheme operators, financial service providers, and technology partners.

Acknowledging the diversity of regulatory, technological, and market contexts across the continent, the Reference Guide offers a flexible and modular framework. This approach enables adaptation to local realities while fostering transparency, consistency, and interoperability across the broader African payments landscape.

The Reference Guide outlines the core components of IPS scheme rules, showcases international best practices, and provides actionable guidance to support the creation of inclusive, resilient, and secure instant payment systems.

1.2

Purpose and Scope

Purpose

The purpose of this Reference Guide is to support African countries in developing and enhancing instant payment infrastructures through a clear, comprehensive framework of scheme rules. It provides the foundational legal, operational, and governance provisions necessary to establish secure, efficient, and inclusive instant payment systems. The Reference Guide addresses both opportunities and challenges specific to the instant payments environment and offers actionable models for system implementation, management, and continuous evolution in diverse local contexts.

Primary Objectives

The Reference Guide is designed with the following key objectives:

- Provide clear, practical guidance for developing comprehensive instant payment scheme rules that balance innovation with risk management.
- Enhance understanding of key concepts, requirements, and best practices among diverse stakeholders.
- Ensure consistency and transparency in rule application across payment ecosystems.
- Create an adaptable blueprint that countries can customize to their specific circumstances.
- Enable cross-border interoperability through harmonized standards, while allowing flexibility for country-specific governance and regulatory requirements.

Scope

This Reference Guide covers the following areas essential to the design and implementation of inclusive instant payment scheme rules:

- Scheme business purpose
- Governance models and decision-making processes
- Participation criteria and onboarding procedures
- Transaction processing rules and standards
- Settlement models and mechanisms
- Risk management frameworks and requirements
- Compliance and regulatory considerations
- Dispute resolution and exception handling
- User experience guidelines and requirements
- Pricing principles and models

The following items fall outside the scope of this Reference Guide:

- Detailed technical specifications for system implementation
- Specific software or hardware recommendations
- Country-specific regulatory requirements (beyond principles)
- Vendor selection guidance

Target Audience

This Reference Guide is designed to serve multiple stakeholder groups involved in the development, implementation, and oversight of instant payment systems. **Each audience segment will utilize this document differently according to their specific roles and responsibilities within the payment ecosystem.**



Regulatory Authorities: This includes central banks and financial regulators tasked with overseeing national payment systems, formulating policy, and developing regulatory frameworks. These institutions require comprehensive guidance to foster secure, inclusive, and efficient instant payment schemes that align with international standards while addressing domestic priorities.



Payment System Operators/Managers: These are entities responsible for managing or operating instant payment infrastructure, whether central banks, industry associations, or dedicated operators. These institutions need detailed guidance on rule development, participant management, operational frameworks, and system modernization to ensure reliable, efficient, and inclusive payment services.



System Participants: Comprise financial institutions, payment service providers, and fintechs that participate in instant payment systems. These institutions need a clear understanding of operational requirements, compliance obligations, technical specifications, and implementation approaches to effectively integrate with and utilize instant payment infrastructure.



Technical Advisors: Consultants and advisors supporting the instant payment system implementation. These professionals can benefit from comprehensive reference materials that inform their advisory services and implementation support activities, enabling them to provide consistent, high-quality guidance aligned with international best practices and local requirements.



Executive
Summary

1

Introduction

2

GUIDING APPROACH TO SCHEME RULES DEVELOPMENT

3

The Legal
Framework of
Instant Payment
Schemes

4

Core Components
of Participation
Agreements

5

Core Components
of the Scheme
Rules

6

Pricing Policy

7

Education
and Awareness
Framework

8

Conclusion and
Path Forward

9

Annexes



2.1

Design Principles

The Reference Guide has been developed based on the following principles:

Principles-Based Methodology: The Reference Guide employs a principles-based approach that focuses on adaptable frameworks and guidelines rather than prescriptive requirements. This allows countries to tailor the rules to their specific situations while ensuring system integrity and interoperability through adherence to core principles and standards.

Flexible Guidance: The Reference Guide provides frameworks, options, and considerations rather than mandates. They outline the advantages and disadvantages of different approaches, allowing countries to make informed decisions based on their specific circumstances and policy objectives. This flexibility enables innovation while maintaining necessary controls and protections.

Implementation Neutrality: The Reference Guide remains neutral regarding specific technologies, vendors, and implementation models. They focus on functional requirements and operational considerations that can be implemented through various technical approaches, allowing countries to select technologies appropriate to their infrastructure, capabilities, and resources.

Alignment with International Standards: While tailored to African contexts, the Reference Guide refers to and aligns with relevant international standards such as the Principles for Financial Market Infrastructures (PFMI)¹ and ISO 20022. This alignment ensures that systems developed under this Reference Guide will be compatible with the global payment infrastructure while addressing unique national considerations.

2.2

Scheme Rules Development and Maintenance

Rules Development Methodology

Effective scheme rules require a systematic development approach to ensure they are comprehensive, clearly articulated, and aligned with the needs of all stakeholders. **This process should encompass the following key stages:**



Requirements Gathering: A thorough understanding of the scheme's objectives should be established by gathering input from a broad range of sources across diverse domains, including—but not limited to—operational and technical requirements, risk and security considerations, regulatory and compliance obligations, the capabilities of scheme participants, and customer experience expectations.

¹ CPMI-ISCO: [Principles for Financial Market Infrastructures](#), April 2012



Gap Analysis: A detailed gap analysis should be conducted to identify areas where rules are needed or where existing guidance is insufficient. This process should encompass a review of current rule frameworks and policies, comprehensive risk assessments, and an analysis of typical operational scenarios and potential failure experiences.



Benchmarking: A comparative analysis of similar rulebooks and best practices from other domestic and international payment systems should be undertaken to guide the rule design process. This analysis aims to identify successful approaches, avoid common pitfalls, and ensure that the resulting rules remain relevant while being appropriately tailored to the specific context and objectives of the scheme.



Rulebook Drafting: Rulebook drafting should follow standardized procedures to promote consistency, clarity, and ease of interpretation. This includes the consistent use of terminology and definitions, clear articulation of obligations and responsibilities, and the appropriate use of cross-references between rules and related supporting documents.



Legal Review: Each draft should undergo a thorough legal review to ensure the enforceability of the rules under applicable law, alignment with relevant regulatory requirements, and clear allocation of liability, along with well-defined dispute resolution mechanisms.



Stakeholder Consultation: Stakeholders should be given the opportunity to review and provide feedback on the draft rules through a formal consultation process, which typically includes comment periods ranging from 30 to 90 days, depending on the complexity of the proposed changes, and structured mechanisms for submitting, tracking, and responding to feedback to ensure transparency and inclusive participation.

Rules Structure and Organization

A well-organized rulebook is essential for promoting clarity, consistency, and ease of compliance. The structure should be logical and modular, enabling efficient navigation and targeted updates. **The following elements contribute to effective rule organization:**

A

Modular Organization: Rules should be divided into functional sections, each addressing a distinct operational area. This modularity allows easier understanding by topic, streamlined revisions without requiring changes to unrelated sections, and flexibility in adapting to evolving operational needs. An example of a modular structure is illustrated in the table below.

Table 1: Illustration of a Modular Structure

Module	Content Focus
Module 1: Definitions	Key terms used throughout the scheme rules
Module 2: Governance	Rule change procedures, decision-making bodies, and compliance responsibilities

Module	Content Focus
Module 3: Participation	Eligibility, onboarding, and suspension/termination rules
Module 4: Operational Rules	Transaction flow, cut-off times, service availability, and business rules
Module 5: Clearing & Settlement	Settlement model, liquidity requirements, and reconciliation
Module 6: Technical Standards	Messaging formats (e.g., ISO 20022) and API specifications
Module 7: Risk & Security	Fraud management, authentication, and business continuity
Module 8: Customer Protection	Dispute resolution, transparency, and refund rights

B Hierarchical Structure: A clearly defined hierarchy helps establish the relationship between high-level principles and detailed rules by using consistent numbering and labeling conventions, grouping related rules into coherent subsections, and maintaining traceability between overarching principles and specific obligations, thereby enhancing clarity, structure, and ease of reference throughout the rulebook.

Box 1: Operational Rules

Each module contains sections, sub-sections, and clauses, using a consistent numbering system to show rule relationships.

4.0 Operational Rules Overview

4.1 Transaction Lifecycle

4.1.1 Initiation

4.1.1.1 *Payments must be initiated via authenticated digital channels.*

4.1.1.2 *Each transaction must include a unique reference ID.*

4.1.2 Processing

4.1.2.1 *All payments must be processed within 10 seconds.*

4.1.2.2 *The system must ensure funds availability prior to authorization.*

4.1.3 Confirmation

4.1.3.1 *Both sender and receiver must receive confirmation of successful transfer.*

4.2 Operating Hours

4.2.1 *The IPS shall operate 24/7/365 without downtime.*

4.3 Exception Handling

4.3.1 *Timeouts exceeding 10 seconds shall trigger a transaction failure response.*

C **Definitional Framework:** A dedicated section for definitions provides standardized meanings for key terms and concepts. This enhances clarity and reduces the risk of misinterpretation or ambiguity across the rulebook.

D **Cross-Referencing System:** To avoid duplication and improve usability, the rulebook should include cross-references that link related provisions across different sections. This allows users to understand rule interdependencies and navigate complex topics more efficiently.

Box 2: Cross-referencing ensures coherence and avoids duplication.

Example:

Clause 4.1.2.2 (“The system must ensure funds availability...”) may include a reference:

“See also **Clause 5.1.3** on pre-funded settlement obligations and liquidity thresholds.”

In **Module 7: Risk & Security**, a rule may state:

“Participants must follow the encryption standards defined in **Clause 6.2.1**.”

In **Module 8: Customer Protection**, a rule might read:

“For dispute resolution timelines, refer to **Clause 4.3.2** under exception handling.”

E **Version Control and Documentation:** Clear version control mechanisms should be implemented to track the evolution of rules over time. This includes assigning unique version numbers, specifying effective dates for rule changes, and maintaining comprehensive change logs that summarize amendments, ensuring transparency and a clear record of rule modifications.

Table 2: Illustration: Version Control and Documentation

Version	Effective Date	Summary of Changes	Section(s) Affected	Approved By	Notes
1.0	01 Jan 2025	Initial release of the scheme rulebook	All sections	Scheme Governing Body	Foundational rulebook covering core areas
1.1	15 Mar 2025	Clarified participant onboarding requirements	Section 3: Participation	Rulemaking Committee	Responded to feedback from early adopters
1.2	01 Jul 2025	Updated message format to support ISO 20022 v2.1	Section 5: Technical Standards	Scheme Governing Body	Ensures compliance with regional standards

Version	Effective Date	Summary of Changes	Section(s) Affected	Approved By	Notes
1.3	01 Oct 2025	Added business continuity obligations for all participants	Section 4: Operational Rules	Risk Committee	Strengthens resilience and uptime policies
2.0	01 Jan 2026	Major revision: introduced real-time fraud detection rules	Sections 4, 6: Operations, Compliance	Full Board Approval	Marked as a major version due to scope

Rules Adoption and Implementation

Transitioning from rule development to operational implementation requires a structured and transparent implementation framework that promotes readiness, alignment, and compliance among all participants. **This process should include the following key stages:**

- A Formal Approval Processes:** Clearly defined governance procedures should guide rule adoption. This includes formal review stages, stakeholder consultations, voting mechanisms (if applicable), and proper documentation of decisions.
- B Notice Periods:** Adequate lead time should be provided between the publication and the effective date of new rules. Typical notice periods range from 3 to 12 months, depending on the complexity of the changes and the level of operational adjustment required.
- C Phased Implementation:** Where feasible, rule implementation may be conducted in phases, prioritizing components based on criticality, readiness, or difficulty. This allows stakeholders to gradually adapt and mitigate risk during deployment.
- D Educational Support and Capacity Building:** To ensure smooth adoption, the scheme operator should offer a variety of training and support resources, such as user guides and implementation manuals, workshops and webinars, as well as technical assistance and frequently asked questions (FAQs). These resources will help participants effectively navigate and adopt the scheme.
- E Compliance Verification Mechanisms:** Clear procedures should be established to verify compliance with the new rules. These procedures may include testing or certification requirements, formal attestation by participants, and an independent compliance committee (e.g., the EPC Dispute Resolution Committee (DRC)²) or audits, as appropriate, to ensure adherence to the established standards.
- F Transitional Provisions:** Temporary arrangements may be necessary to support participants during the transition. These arrangements could include grace periods for compliance, temporary waivers or alternative procedures, and pilot or soft-launch phases to ensure a smooth implementation of the new rules.

² European Payment Council: [EPC150-19 Approved Dispute Resolution Committee Mandate v2.6.pdf](#), November 2024.

Rules Maintenance and Evolution

To ensure that scheme rules remain relevant, effective, and aligned with evolving needs, a robust and transparent rules maintenance framework must be established. This framework should support continuous improvement through regular reviews, structured change management, and regulatory compliance. **Key elements include:**

A Regular Review Cycles: A schedule for periodic assessment should be established to evaluate the effectiveness and clarity of the rules. This should include an annual comprehensive review of the entire rulebook, along with more frequent, targeted reviews of specific sections based on operational feedback, incident reports, or stakeholder input.

B Change Request Procedures: Modifications to rules should follow standardized procedures to ensure consistency, transparency, and accountability throughout the change process. These procedures should include a clear justification for each proposed change, an assessment of its potential impact on operations, regulatory compliance, and scheme participants, as well as well-defined pathways for consultation and formal approval.

C Interpretation Mechanisms: Ambiguities or unforeseen situations should be addressed through formal interpretation processes that ensure clarity and consistency in rule application. These mechanisms should clearly define the authority responsible for interpreting the rules, outline the procedure for submitting interpretation requests, and establish requirements for documenting and, where applicable, publishing official interpretations to promote transparency and guidance for all stakeholders.



Executive
Summary

1

Introduction

2

Guiding Approach
to Scheme Rules
Development

3

THE LEGAL FRAMEWORK OF INSTANT PAYMENT SCHEMES

4

Core Components
of Participation
Agreements

5

Core Components
of the Scheme
Rules

6

Pricing Policy

7

Education
and Awareness
Framework

8

Conclusion and
Path Forward

9

Annexes



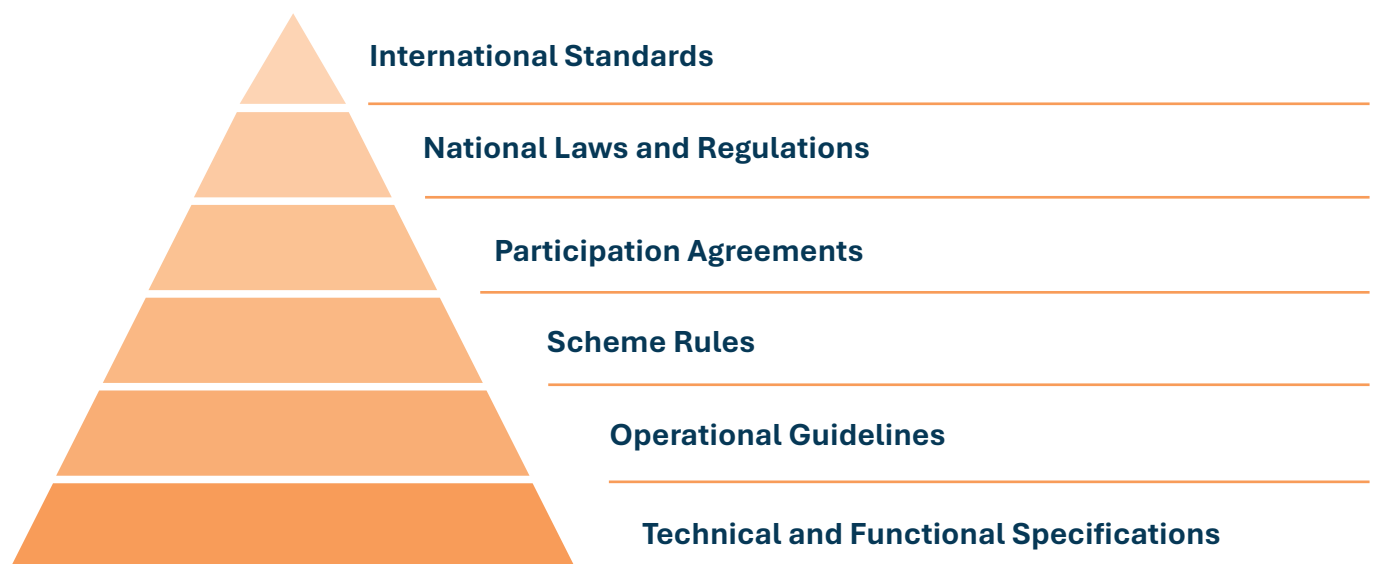
3.1

Hierarchical Structure

A sound legal framework is fundamental to the safe, efficient, and trustworthy operation of instant payment schemes. This framework provides the legal and institutional foundation that governs the rights, responsibilities, and interactions of all stakeholders involved. It ensures that instant payment schemes operate within a clearly defined structure that supports regulatory compliance, risk management, and operational consistency.

To achieve this, instant payment schemes typically adopt a tiered rule hierarchy that translates high-level legal and regulatory requirements into specific, enforceable rules and detailed operational guidance. These tiers range from international standards and national laws to participation agreements, core operational rules, and practical implementation guidelines, each playing a distinct but interconnected role in the scheme's overall governance and functionality.

Figure 1: The Legal Framework for Instant Payment Scheme



3.2

International Standards: The PFMI

The BIS Principles for Financial Market Infrastructures provide the global standards for designing and regulating financial market infrastructures, including instant payment systems. These principles ensure systems are safe, resilient, efficient, and transparent.

Regulators are expected to adopt and embed these principles into domestic regulatory frameworks, and system operators are expected to assess their systems against the PFMI to ensure alignment and compliance with global best practices.

The PFMI consists of 24 principles, of which 17 directly apply to payment systems, structured into the following categories:

- **General Organization:** Establish a sound legal basis, robust governance arrangements, and comprehensive risk management frameworks.
- **Credit and Liquidity Risk:** Maintain effective tools to monitor, manage, and contain credit and liquidity exposures to preserve financial stability.
- **Default Management:** Define clear procedures and rules to manage participant defaults without disrupting overall system operation.
- **Access Criteria:** Ensure fair and open access, while managing risks associated with different types of participants.
- **Settlement Finality:** Guarantee the irrevocability and finality of payments, ideally in central bank money.
- **Efficiency and Effectiveness:** Operate efficiently to meet market and participant needs at minimal cost.
- **Transparency:** Disclose rules, procedures, and performance data to promote informed decision-making and confidence among stakeholders.

In addition to the principles themselves, the PFMI outlines five key responsibilities for public authorities (e.g., central banks and market regulators) in charge of regulating and overseeing FMIs.

3.3 National Laws and Regulations

National laws and regulations governing payment systems provide the essential legal foundation for the effective operation of instant payment schemes. These legal instruments must align with international standards, such as the PFMI, while reflecting each country's unique legal, economic, and social environment.

National laws typically provide the legal foundation for the recognition and protection of payment systems. They define the oversight responsibilities of central banks or other designated regulatory authorities and set out the core principles governing system operation. These laws may include provisions related to, among others, settlement finality (see the EU Financial Settlement Directive³), recognition and use of financial instruments such as collateral, system resilience, licensing and designation of payment systems, eligibility criteria for participants, risk management obligations, consumer protection, data privacy, and enforcement mechanisms.

In addition to primary legislation, supplementary regulations issued by central banks or financial regulators offer detailed operational and compliance requirements. For instant payment systems, these regulations often include specific measures tailored to the unique features and risks of real-time payments, such as transaction speed, continuous availability, and fraud prevention. An example is the EU Regulation on Instant Credit Transfers, which sets mandatory requirements for euro-denominated instant payments within the European Union.⁴

3 Directive 98/26/EC of the European Parliament and of the Council on Settlement Finality in Payment and Securities Settlement Systems*. (2005). Uniform Law Review, 10(1–2), 390–404. <https://doi.org/10.1093/ulr/10.1-2.390>

4 [Regulation \(EU\) 2024/886 of the European Parliament and of the Council of 13 March 2024 amending Regulations \(EU\) No 260/2012 and \(EU\) 2021/1230 and Directives 98/26/EC and \(EU\) 2015/2366 as regards instant credit transfers in euro](#)

3.4

Participation Agreements

Participation agreements establish the contractual foundation between the scheme manager and all participants in the scheme. They play a crucial role in translating international standards and national regulations into specific, legally binding obligations that participants must fulfill to gain and maintain access to the scheme.

Typically, participation agreements include comprehensive contractual provisions that define the rights, responsibilities, liabilities, and dispute resolution procedures for both the scheme operator and participating institutions.

Beyond the bilateral relationship between each participant and the scheme manager, these agreements also establish a multilateral legal framework governing interactions among participants, including rules for cooperation, operational conduct, and liability allocation in case of disputes.

3.5

Scheme Rules

The scheme rules serve as the core operational framework of the instant payment systems. They operationalize the high-level requirements set out in international standards, national regulations, and participation agreements by defining detailed parameters and procedures that govern the day-to-day functioning of the scheme. **These rules typically cover the following key areas:**

A Governance Framework: Governance is defined as a “set of relationships between an FMI’s owners, board of directors (or equivalent), management, and other relevant parties, including participants, authorities, and other stakeholders (such as participants’ customers, other interdependent FMIs, and the broader market).”⁵

These rules establish the governance structure that defines how decisions are made, including the development, approval, review, and modification of rules over time. This governance structure ensures the scheme remains adaptable to changing participant needs and market dynamics while upholding alignment with higher-tier obligations. It also ensures the protection of the system’s integrity, stability, and long-term viability, with active involvement from stakeholders such as scheme operators, regulators, and participants, all of whom play a crucial role in the governance process.

B Participant Eligibility and Onboarding: The scheme rules should establish clear eligibility criteria and onboarding procedures for prospective participants, ensuring that only institutions meeting the necessary regulatory, financial, and operational standards are allowed to join the scheme. This process safeguards the reliability and efficiency of the system by maintaining high standards for participation.

5 CPMI-ISCO “[Principles for Financial Market Infrastructures](#)” April 2012.

C Payment Processing Rules: The scheme rules should provide comprehensive coverage of the entire payment process, addressing various key aspects such as the types of supported transactions, message formats and content standards, processing flows and timeframes, and transaction validation and authorization requirements. In addition, the rules define the settlement model, outlining the timing and finality of settlements, procedures for managing settlement risk, and protocols for handling exceptions, such as failed or rejected payments.

D Operational Resilience and Service Levels: Beyond payment processing, the scheme rules also cover broader operational requirements, including defined service levels and availability targets, business continuity and disaster recovery arrangements, and procedures for managing operational incidents. These procedures encompass communication protocols and escalation paths to ensure smooth and efficient operations in the event of disruptions.

E Risk Management and Compliance: The scheme's risk management approach is outlined through measures focused on fraud prevention, anti-money laundering (AML) and counter-terrorism financing (CTF) compliance, and cybersecurity safeguards. These measures are designed to ensure the security, integrity, and resilience of the scheme, protecting it against various threats.

F Dispute Resolution and Complaints Handling: Scheme rules also include provisions for resolving disputes, whether between participants or between participants and their customers. These procedures ensure fair handling of complaints and foster trust in the scheme.

3.6 Operational Guidelines

Operational guidelines provide practical, detailed instructions and best practices to support the day-to-day functioning of the payment system. While the core scheme rules define *what* must be done, operational guidelines focus on *how* to do it, offering actionable guidance that enables participants to implement requirements effectively and consistently.

These guidelines encompass a wide range of operational activities essential to the smooth functioning of the instant payment scheme. Key areas include transaction processing, settlement management, exception handling, user experience, marketing and branding, and customer service. They provide step-by-step procedures for routine tasks such as initiating and receiving payments, managing liquidity, reconciling transactions, and generating reports. Additionally, the guidelines offer practical direction for managing non-routine situations, such as handling transaction errors, investigating potential fraud, responding to customer complaints, and addressing system disruptions.

To support consistent application, the guidelines may include practical tools such as templates, checklists, and decision trees. Unlike higher-tier rules that are typically more rigid, operational guidelines are designed to be more flexible and adaptable, allowing participants to tailor their implementation based on internal capabilities while still achieving the intended outcomes of the scheme.



**Executive
Summary**

1

Introduction

2

**Guiding Approach
to Scheme Rules
Development**

3

**The Legal
Framework of
Instant Payment
Schemes**

4

CORE COMPONENTS OF PARTICIPATION AGREEMENTS

5

**Core Components
of the Scheme
Rules**

6

Pricing Policy

7

**Education
and Awareness
Framework**

8

**Conclusion and
Path Forward**

9

Annexes



Participation agreements form the contractual backbone of an instant payment scheme, defining the legal relationship between the system operator and participating institutions. **To ensure effective governance, operational clarity, and legal certainty, these agreements must comprehensively address the following key components:**

A

Rights and Obligations: Participation agreements should clearly articulate the respective rights and responsibilities of both the scheme operator and participants. These include provisions related to system access, compliance with scheme rules, service delivery standards, and operational conduct.

B

Liability and Risk Allocation: Robust liability clauses are essential to allocate responsibility for losses resulting from operational errors, participant misconduct, or external events. These provisions help to mitigate disputes and clarify expectations in the event of incidents or failures.

C

Confidentiality and Information Sharing: Confidentiality provisions should safeguard sensitive information while enabling necessary data sharing for operational, compliance, and supervisory purposes. These provisions should balance privacy with transparency and collaboration.

D

Change Management: Participation agreements must establish structured procedures for modifying terms and conditions. These should include notice periods, consultation processes, and mechanisms for participants to review or respond to material changes.

E

Compliance Monitoring and Enforcement: Effective participation agreements must include mechanisms for ongoing compliance monitoring and enforcement. Key elements include:

- **Monitoring Frameworks:** System operators should be empowered to verify compliance through participant reporting, audits, and performance assessments.
- **Enforcement Mechanisms:** Proportional enforcement tools designed to address varying degrees of non-compliance, ranging from minor to severe. These may include warning letters for minor breaches, financial penalties for moderate violations, mandatory remediation plans to address systemic issues, participation restrictions in response to serious concerns, and termination clauses for fundamental breaches of the scheme's rules.

F

Dispute Resolution and Governing Law: Effective dispute resolution mechanisms and clearly defined governing law provisions are essential to ensure that any conflicts arising under the agreement are resolved fairly, efficiently, and consistently. These provisions establish the legal foundation for managing disputes, including the use of arbitration under the UNCITRAL Rules⁶ and relevant laws as a final recourse. They also preserve each party's right to seek interim legal or injunctive relief when warranted.

G

Termination and Exit Provisions: Participation agreements must also provide a structured framework for both voluntary and involuntary termination of participation:

- **Voluntary Exit:** Provisions should outline notice periods (typically 90–180 days), final settlement requirements, data retention obligations, and communication responsibilities.

6 UNCITRAL: [UNCITRAL Arbitration Rules, Expedited Arbitration Rules and Rules on Transparency in Treaty-based Investor-State Arbitration](#); 2021

- **Involuntary Termination:** Grounds for termination should include material breaches of agreement, insolvency, persistent non-compliance, or regulatory sanctions.
- **Emergency Suspension:** The agreement should allow the scheme operator to temporarily suspend a participant's access in cases where continued participation poses a risk to system integrity. Such actions must follow governance oversight and due process.
- **Transitional Arrangements:** To minimize disruption, exit provisions should address the orderly transfer of customer accounts, open transactions, and obligations to other participants.

H

Additional Legal Considerations: Beyond the core provisions already mentioned, participation agreements should address several additional legal considerations to ensure comprehensive coverage of all potential issues.

- **Intellectual Property Rights:** Clear provisions should establish that intellectual property provided by either party remains vested in the original owner, with access granted under a limited license that expires upon termination. The agreement should address ownership of jointly created intellectual property and include warranties against third-party infringement claims.
- **Force Majeure:** Agreements should define force majeure events (such as natural disasters, pandemics, war, labor disputes, regulatory changes, and utility failures) and establish procedures for notification, relief from obligations, and potential termination if force majeure conditions persist beyond a specified period (typically 3 months).
- **Liability and Indemnity:** Agreements should include carefully crafted liability and indemnity provisions that allocate responsibility for losses resulting from breaches, negligence, or misconduct. These provisions may include limitations of liability for certain types of damages while ensuring accountability for direct losses caused by a party's actions or omissions.
- **Confidentiality:** Robust confidentiality provisions should protect sensitive information shared between parties while allowing for necessary disclosures for legal proceedings, regulatory filings, or other circumstances required by law. These provisions should survive termination of the agreement.



**Executive
Summary**

1

Introduction

2

**Guiding Approach
to Scheme Rules
Development**

3

**The Legal
Framework of
Instant Payment
Schemes**

4

**Core Components
of Participation
Agreements**

5

CORE COMPONENTS OF THE SCHEME RULES

6

Pricing Policy

7

**Education
and Awareness
Framework**

8

**Conclusion and
Path Forward**

9

Annexes

5.1

Strategic Objectives

The rules of an instant payment scheme should explicitly articulate the core business principles that underpin its design, governance, and operation. These principles serve to ensure that the scheme functions in a fair, transparent, and efficient manner, while aligning with the public interest and participants' needs (PFMIs, Principle 21). Embedding these principles within the scheme rules promotes coherence, accountability, and long-term viability. **The key business principles may include:**

A Inclusive Participation and Accessibility: Instant payment schemes should enable broad, non-discriminatory access for eligible institutions, regardless of size or market share. Participation criteria should be transparent and uniformly applied.

B Utility-Based Operating Model: The scheme should operate as a public utility serving the financial sector, prioritizing accessibility and public benefit over profit.

C Transparency and Public Availability: All core documents, including rules, technical specs, and use cases, should be publicly accessible and regularly updated.

D System Safety and Financial Stability: The scheme should be designed with robust controls to mitigate liquidity, operational, and business risks. As a critical financial infrastructure, it should uphold the stability and integrity of the broader financial system.

E Stakeholder-Inclusive Governance: Governance should reflect the interests of all stakeholders, participants, businesses, consumers, and governments.

F Transparent Decision-Making: Decision-making processes must be open and well-communicated. Clear communication protocols (e.g., notices, consultations, public updates) ensure stakeholders are informed and able to provide feedback.

The business object of the scheme, as reflected in the Articles of Association or equivalent founding documentation of the scheme's managing institution, must be explicitly defined and aligned with these foundational business principles.

5.2

Governance Framework

Governance Structure

The governance rules are primarily shaped by the choice between two main governance models (see *Annex 2 for international benchmarking*). Each model distributes responsibilities in distinct ways and requires structural arrangements to support effective oversight, clear accountability, and strong operational performance.

A

Integrated Scheme and Operator Model:

In this model, a single entity is responsible for both governing and operating the instant payment system. This integration enables streamlined decision-making, reduced coordination overhead, and faster implementation. However, it requires clear internal safeguards to prevent conflicts of interest between governance and operations.

Key governance considerations include:

- Transparent decision-making processes with adequate participant representation.
- Internal separation of governance and operational functions to mitigate conflicts.
- Oversight mechanisms to ensure accountability in both roles.
- Defined escalation procedures for resolving participant concerns.
- Periodic reviews of governance and operational effectiveness.

The integrated model benefits from simplicity and agility but demands strong internal governance to maintain neutrality and integrity.

B

Separated Scheme and Operator Model:

This model assigns governance and operational responsibilities to two distinct entities. The scheme manager governs the rulebook, compliance, and strategic direction, while the system operator handles technical implementation and operations.

This separation introduces checks and balances, enhancing transparency and stakeholder confidence. However, it requires robust coordination between entities. **Critical governance provisions in this model include:**

- Clearly defined roles and responsibilities through formal agreements.
- Established communication protocols and joint decision-making frameworks.
- Dispute resolution procedures between the scheme manager and system operator.
- Joint planning mechanisms for system changes and enhancements.
- Accountability structures to prevent gaps or overlaps in responsibilities.

A clear delineation of duties is essential to ensure effective cooperation and operational harmony:

i. Scheme Manager Responsibilities: The scheme manager holds authority over the strategic and rule-making aspects of the instant payment scheme. Governance rules should explicitly empower the scheme manager to:

- Define business rules, technical standards, and scheme policies.
- Set eligibility criteria and participation requirements.
- Determine funding and cost allocation mechanisms.
- Manage onboarding and certification of participants.
- Resolve escalated disputes through expert determination.
- Establish the long-term strategic roadmap for the scheme.
- Own scheme-related intellectual property, where applicable.

.....

ii. System Operator Responsibilities: The system operator is responsible for delivering the technical backbone of the scheme. While operating under the scheme manager's governance, the system operator ensures reliable and secure system performance. **Key responsibilities include:**

- Building and maintaining the payment infrastructure in line with scheme specifications.
 - Ensuring high availability and meeting performance benchmarks.
 - Implementing strong cybersecurity and data protection measures.
 - Coordinating updates and upgrades with the scheme manager.
 - Providing monitoring, incident response, and participant support.
 - Maintaining disaster recovery and continuity plans.
 - Supplying performance data and incident reports to the scheme manager and relevant stakeholders.
 - Conducting first-line investigations of disputes.
- _____

Governance Composition

A

Governing Board

The governing board should be the highest decision-making body of the instant payment system, responsible for setting strategic direction, approving scheme rules, and overseeing system operations.

- The board composition should balance representation across different participant categories while ensuring appropriate expertise in payment systems, risk management, technology, and regulatory compliance.
- Clear eligibility criteria should establish qualification requirements for board membership, including professional expertise, institutional representation, and absence of conflicts of interest.
- The board's authority and responsibilities should be formally documented, including decision-making procedures, reserved powers, and delegation frameworks for operational matters.

As part of sound governance practices, the terms of reference for the governing board (PFMIs, Principle 2) should be clearly stipulated in the Articles of Association of the Institution Managing the Schemes.

The board's composition should ensure a balanced representation across different participant categories, while also providing appropriate expertise in payment systems, risk management, technology, and regulatory compliance.

The board may delegate specific responsibilities to management as appropriate, while retaining ultimate authority and oversight.

B

Advisory Forums

Advisory forums serve as structured platforms for engaging scheme participants and other key stakeholders in the governance process. These forums provide input on rule development, operational improvements, market needs, and emerging risks. While they do not hold decision-making power, their insights help ensure that the scheme remains aligned with user expectations, industry trends, and practical realities.

Two key types of forums include:

- **Participants Forums**, composed of direct scheme participants such as banks, non-bank financial institutions, and payment service providers. These forums provide operational feedback, raise implementation challenges, and suggest enhancements based on real-world use.
- **End User Forums**, which represent consumer and business perspectives. They focus on user experience, accessibility, trust, and service quality.

Even within a bank-led model, it is critical to ensure inclusive governance. A notable example is the Central Bank of Brazil, which established a permanent advisory body (**Pix Forum**). This forum plays a key role in supporting the central bank by contributing to the development of rules and procedures that govern the Pix system. By incorporating a wide range of stakeholder perspectives, the Pix Forum helps ensure that decision-making is transparent, participatory, and reflective of the broader ecosystem's needs.⁷

C

Working Groups

To strengthen operational collaboration and ensure that the scheme remains responsive to participant needs, instant payment systems should establish dedicated **Participant Working Groups**. These groups offer structured platforms for participants to contribute expertise on technical, operational, legal, and business issues. They foster coordination among participants and address cross-cutting challenges that affect inter-participant operations and participant–customer interactions. **The core objectives of these working groups include:**

- Facilitating knowledge-sharing and collaboration among participants.
- Identifying and resolving technical, legal, and operational challenges.
- Advising on enhancements to the scheme and addressing emerging issues.
- Escalating material concerns and actionable recommendations to the governing body.

The number and scope of working groups may depend on the size, complexity, and maturity of the scheme, as well as the specific issues and priorities faced at a given time. **Example of working groups:**

- **Business Working Group:** Focuses on product design, pricing models, and marketing strategies to support adoption and customer engagement.
- **Operational Working Group:** Covers operations, technology, and information security, including incident handling, performance monitoring, and interoperability issues.

⁷ Banco Central do Brasil: https://www.bcb.gov.br/content/estabilidade/financeira/pix/Pix_Regulation/Resolution_BCB_1.pdf, August, 2020

- **Legal Working Group:** Addresses legal, risk, compliance, and data protection matters, helping ensure alignment with applicable regulations and scheme policies.
- **Ad Hoc Working Groups:** May be formed as needed to address specific topics or temporary issues requiring focused attention.

These groups should operate under clear terms of reference and maintain regular communication with the scheme's management to ensure their input informs decision-making and continuous improvement.

Principles for Effective Management

To ensure effective execution of strategic decisions and strong operational management, instant payment schemes should adopt a clear and accountable management framework. **Key principles include:**

- Leadership Structure and Accountability:** The scheme should have a well-defined leadership structure with clear accountability lines. The executive team should report directly to the governing board to ensure alignment with strategic objectives.
- Segregation of Duties:** In integrated models, it is crucial to maintain a clear separation between governance functions and operational responsibilities to prevent conflicts of interest and safeguard the integrity of the scheme.
- Performance Management:** A performance management framework should be in place to monitor the effectiveness of the management team, using KPIs aligned with the scheme's objectives and stakeholder expectations.
- Clear Decision-Making Processes:** The scheme should establish well-defined decision-making processes at all levels to ensure accountability and that decisions are made in the best interest of the scheme.
- Risk Management Framework:** A comprehensive framework for identifying, assessing, and managing various risks (operational, legal, financial, and reputational) must be implemented, including crisis management procedures.
- Cross-Functional Collaboration:** The scheme should encourage collaboration among different functions (leadership, operations, legal, technical, and compliance) to ensure that all perspectives are considered in decision-making.
- Stakeholder Engagement:** Regular communication with stakeholders, including participants, regulators, and consumers, is essential to ensure their needs and concerns are considered in strategic decisions.
- Continuous Improvement and Innovation:** The scheme should foster a culture of innovation and continuous improvement, responding to technological advancements and evolving market conditions.
- Internal and External Auditing:** Both internal and external auditing processes should be implemented to ensure compliance, identify inefficiencies, and assess the overall performance of the scheme.
- Succession Planning:** A well-defined succession plan for leadership roles and technical experts is crucial for the scheme's continuity and stability.

This structure ensures both operational efficiency and governance integrity.

Decision-Making Frameworks

A

Voting Mechanisms

Effective governance requires clear voting mechanisms that balance stakeholder interests and establish transparent decision procedures. **Different voting models may be appropriate for different decisions:**

- Simple majority voting for routine operational matters, qualified majority (e.g., two-thirds) for significant rule changes, and consensus approaches for fundamental system changes.
- Voting rights allocation should be carefully designed to prevent domination by larger participants while ensuring representation proportionate to participation levels and risk exposure. This may involve tiered voting rights, participant category representation requirements, or voting caps for individual institutions.

B

Rule Change Procedures

A structured rule change process enables the scheme to evolve in response to market needs, technological developments, and emerging risks. This process should balance the need for stability and predictability with the importance of continuous improvement and adaptation.

To ensure transparency, consistency, and operational stability, all rule changes within the instant payment scheme should be classified and managed based on both **impact level** and **subject matter category**.

(1) Classification by Impact

- **Major Changes:** Substantial modifications that may significantly affect system functionality, participant obligations, risk management, or user experience. These changes typically require broad consultation, formal approval processes, and sufficient notice prior to implementation.
- **Minor Changes:** Limited adjustments with minimal operational or compliance impact, such as editorial corrections, clarifications, or routine updates. These changes may follow a simplified approval and notification process.

(2) Categorization by Subject Matter

- **Technical Enhancements:** Updates to technical standards, message formats, system interfaces, or integration protocols that affect how participants connect and interact with the system.
- **Operational Adjustments:** Modifications to operational procedures, service levels, processing schedules, or performance expectations that govern day-to-day activities.
- **Risk and Security Updates:** Changes related to fraud prevention, cybersecurity requirements, business continuity, or other risk mitigation controls critical to the scheme's integrity.
- **Governance Modifications:** Adjustments to governance structures, such as decision-making procedures, voting mechanisms, representation rights, or participation categories.

- **Emergency Changes:** Urgent modifications required to address immediate threats, system failures, or regulatory demands. These changes may be fast-tracked but should still be subject to post-implementation review and communication.

(3) Change Management Process

A formalized change management process ensures that all rule changes are evaluated, approved, and implemented in a transparent, consistent, and timely manner.

The process includes the following key stages:

- **Initiation:** Rule changes may be proposed by the scheme manager, the system operator participants, or regulators. Each proposal must include a clear rationale, expected impact, and supporting documentation. Proposals are logged in a centralized change request register maintained by the scheme manager.
- **Preliminary Assessment:** The scheme manager conducts an initial assessment to:
 - Classify the change by impact level (major or minor).
 - Categorize it by subject matter (technical, operational, risk, governance, or emergency).
 - Determine whether immediate action is required (for emergency changes).
The outcome of this assessment determines the required pathway for consultation and approval.
- **Stakeholder Consultation:** For major changes, the scheme manager initiates a formal consultation with affected stakeholders, including participants, the system operator, and relevant regulators. Draft changes may be circulated for written feedback over a defined period (e.g., 2 to 4 weeks). Where relevant, technical or operational impact assessments may be conducted.
- **Review and Approval:** A designated scheme change advisory committee or governance body reviews the proposed change, stakeholder input, and supporting analysis. Approval follows a formal voting or consensus-based decision-making process. In urgent situations, emergency changes may be fast-tracked for immediate implementation. However, these changes must subsequently undergo formal review and approval by the appropriate governance body to ensure proper oversight and accountability.
- **Notification and Publication:** Once approved, the final rule change is documented and published through official scheme communication channels. Participants are provided with implementation timelines, technical specifications (if applicable), and any relevant training or guidance.
- **Implementation:** Participants implement the approved change within the agreed timeframe. The system operator supports implementation for system-level or technical changes. The scheme manager monitors readiness and compliance across the ecosystem.
- **Post-Implementation Review:** Following implementation, the scheme manager conducts a review to:
 - Assess whether the change achieved its intended objectives;
 - Identify any implementation issues or unintended consequences;
 - Gather feedback from participants and stakeholders;
 - Recommend any follow-up actions or additional clarifications;

5.3

Scheme Participation Framework

Core Principles

Instant payment schemes should adopt a clear set of core principles that serve as the foundation for defining participation, who is eligible to join, under what conditions, and with what responsibilities. These principles promote open and fair access (PFMIs, Principle 18) while supporting the development of inclusive, secure, and high-performing payment ecosystems. **The recommended core principles are:**

- **Balance:** Achieving the right equilibrium between broad access and effective risk management, ensuring that increased participation does not compromise system stability.
- **Security:** Safeguarding the integrity, confidentiality, and resilience of the payment system through strong data protection and cybersecurity measures.
- **Accessibility:** Enabling participation by a diverse range of financial service providers, including banks, fintechs, and other regulated entities, to promote innovation and financial inclusion (see **Annex 4 for related metrics**).
- **Fairness:** Ensuring all participants are treated equitably through transparent rules and non-discriminatory access to system functionalities.
- **Efficiency:** Designing participation processes and operational workflows that minimize complexity, reduce costs, and support the seamless flow of transactions.

Participant Classification

Instant payment systems generally define multiple categories of participants, each with distinct rights, obligations, and levels of system access. These classifications help ensure that the system remains both inclusive and operationally sound. **The main participant categories typically include:**

A

Core Participation Types

- **Direct Participants:** These entities establish a direct technical connection to the instant payment system and participate directly or indirectly in the settlement process. Direct participants are fully responsible for meeting all technical, operational, and compliance requirements defined by the scheme.

In some jurisdictions⁸, direct participants may be further categorized as:

- *Directly Connected Settling Participants (DCSPs) – with direct access to both the payment system and the settlement mechanism.*
- *Directly Connected Non-Settling Participants (DCNSPs) – with direct technical access but relying on a third party for settlement services.*

⁸ Pay UK: <https://www.wearepay.uk/wp-content/uploads/2023/02/Pay.UK-Faster-Payments-Service-Principles.pdf> Jan 2023.

- **Indirect Participants:** Indirect participants connect to the instant payment system through a direct participant, leveraging that relationship for both technical access and, potentially, settlement. While they are still subject to relevant rules and obligations, they typically face less demanding technical requirements.

B

Specialized Participation Roles

In addition to core participant types, instant payment schemes may recognize specialized roles that contribute to the ecosystem's functionality and innovation. These include:

- **Third-Party Payment Providers (TPPs):** These entities provide services such as payment initiation or account information access (as defined in Payment Service Directive⁹) to end-users, without necessarily holding or settling customer funds. TPPs play a key role in enabling innovative services and expanding the use cases of the instant payment system.
- **Technical Service Providers (TSPs):** TSPs offer technology infrastructure, integration services, or operational support to other participants. Although they do not process payments directly, they enhance system accessibility, particularly for smaller institutions, by offering shared technical platforms and reducing the complexity and cost of system participation.

Eligibility Criteria for Participation

A

Direct Participants

Eligibility for direct participation typically includes several categories of requirements.

- i. Legal status requirements generally mandate that participants be licensed financial institutions or regulated payment service providers authorized to provide payment services in the relevant jurisdiction.
- ii. Financial requirements include minimum capital standards, liquidity capacity relative to expected transaction volumes, and financial guarantee mechanisms where applicable.
- iii. Operational requirements typically include minimum technical capability standards, business continuity provisions, and customer service capabilities.
- iv. Compliance capabilities should include appropriate risk management systems, AML/CFT programs, and data protection measures.

Direct participants generally must also demonstrate the ability to meet the system's security standards and performance requirements.

⁹ [Directive \(EU\) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation \(EU\) No 1093/2010, and repealing Directive 2007/64/EC.](#)

B Indirect Participants

Indirect participation criteria typically focus on ensuring appropriate relationships with direct participants while maintaining system integrity.

- Legal status requirements usually parallel those for direct participants, requiring appropriate regulatory authorization to provide payment services.
- Indirect participants must establish contractual relationships with direct participants that clearly allocate responsibilities and liabilities.
- While technical requirements may be less stringent than for direct participants, indirect participants still must maintain appropriate security controls and operational capabilities relative to their transaction volumes.
- Compliance obligations generally include maintaining appropriate AML/CFT programs and data protection measures, though implementation may differ from direct participant requirements.

Participant Onboarding Process

The participant onboarding process should be transparent, objective, and efficient, ensuring that only qualified entities gain access to the instant payment system. A well-defined onboarding framework safeguards the integrity, security, and operational reliability of the system. **The process should include the following components:**

A Application and Eligibility Requirements: New applicants must submit all required documentation, which may include:

- License certificate
- Financial statements and evidence of solvency;
- Proof of operational readiness and internal capacity;
- Details of risk management, fraud prevention, and compliance programs.

The application process should be standardized, with published forms, instructions, and eligibility criteria.

B Assessment and Evaluation: The scheme manager should apply a consistent and objective methodology to evaluate applications. Evaluation criteria may include:

- Legal and regulatory standing;
- Financial health and institutional soundness;
- Technical and operational capabilities.

Clear timelines should be established for the assessment process to ensure predictability and fairness.

C Technical Certification: Applicants must demonstrate their ability to interface with the system by completing a technical certification process that covers:

- Conformance to message formats and protocols.
- Security architecture and authentication capabilities.
- Ability to send, receive, and reconcile payment messages accurately.

D

Testing and Validation: Before going live, applicants must undergo rigorous testing, including:

- End-to-end transaction simulations.
- Performance and stress testing.
- Validation of security and data protection controls.

_____ A successful testing phase is a prerequisite for production access.

E

Implementation and Go-Live Readiness: An implementation plan must be developed in coordination with the system operator, covering:

- Transition and cutover planning;
- Staff training and operational readiness;
- Communication strategies for customer awareness and support.

F

Ongoing Compliance and Reassessment: After onboarding, participants remain subject to ongoing compliance monitoring.

- Periodic reassessments should verify continued eligibility and operational conformity.
- Any material changes in the participant's business model, technical infrastructure, or risk posture must be reported and may trigger a revalidation process.

General Rights and Obligations

A well-functioning instant payment scheme requires clear allocation of rights and obligations among the system operator and scheme participants. These guidelines provide a generic framework that can be adapted to different institutional, regulatory, and market contexts.

A

System Manager/Operator

The system manager/operator is tasked with the management, operation, and oversight of the IPS infrastructure, playing a critical role in ensuring the system's stability, security, and equitable access for all participants.

i. Key Obligations of the System Operator/Manager Include:

- Operate and maintain the IPS in a secure, efficient, and reliable manner, aligned with the scheme rules and agreed service levels.
- Ensure fair and transparent access to all eligible participants without discrimination.
- Coordinate governance structures, including working groups and consultative forums.
- Provide technical support and operational assistance, including issue resolution.
- Communicate proactively, including advance notice of maintenance, upgrades, or rule changes.
- Monitor compliance, address violations in line with scheme procedures, and safeguard participant and customer confidentiality.

- Publish periodic system performance reports in anonymized form to inform participants.
- Exercise discretion under the scheme rules fairly, reasonably, and in line with the scheme's objectives.

ii. The Main Rights of the System Operator/Manager Include:

- Set and review participation fees, following consultation with participants.
- Share performance data with regulators and advisors for supervisory and policy purposes, while preventing commercial misuse of such data.
- Notify participants of material or repeated non-compliance, ensuring such communication is limited to the concerned party and preserves confidentiality.
- Limit liability for any loss or damage arising from actions or omissions made in good faith and within the framework of the scheme rules.

B

Participants

Participants' rights and obligations may vary based on their participation model (e.g., direct or indirect), but all are expected to uphold the rules and principles of the scheme.

i. Rights of Participants: Participants should be guaranteed the following rights:

Operational Rights:

- Submit transactions in accordance with the scheme rules and established parameters.
- Receive timely settlement for valid and properly submitted transactions.
- Access technical support, issue resolution services, and operational guidance.
- Receive advance notification of planned system changes or maintenance.
- Be treated equitably in transaction processing without preference or bias.

Governance Rights

- Participate in consultations related to rule changes and system enhancements.
- Be represented in governance structures as defined by participation category.
- Appeal decisions that significantly affect participation status or operational rights.
- Receive transparent information on system performance, incidents, and developments.

Commercial Rights:

- Offer instant payment services under their own branding.
- Define and implement pricing strategies for customer-facing services, in line with applicable regulations.
- Develop and provide value-added services based on IPS infrastructure.

.....

ii. Obligations of Participants: Participants shall fulfill the following obligations to ensure the efficiency, security, and integrity of the IPS:

Financial Obligations:

- Maintain sufficient settlement funding to support expected transaction volumes.
- Provide required collateral or guarantees, where applicable.
- Contribute to loss-sharing or guarantee mechanisms if required by the scheme.
- Pay all scheme fees and charges in a timely manner.

Operational Obligations:

- Maintain system connectivity and performance according to agreed service levels.
- Process transactions promptly and in compliance with scheme rules.
- Implement robust security measures and fraud prevention controls.
- Promptly report incidents and participate in collaborative resolution efforts.
- Participate in required testing, certification, and system upgrades.

Compliance Obligations:

- Comply with all applicable scheme rules, technical standards, and procedures.
 - Adhere to legal and regulatory requirements relevant to their role in the IPS.
 - Implement customer protection measures consistent with scheme and regulatory expectations.
 - Cooperate with compliance reviews, audits, and data reporting obligations.
 - Ensure that any sponsored institutions or third-party providers adhere to relevant rules and obligations.
- _____

C

Sponsoring Agent

The relationship between sponsoring direct participants and their sponsored indirect participants is vital to the success of tiered participation models. Clear rules help ensure fair treatment, effective risk management, and service continuity.

i. Contractual Framework: The scheme should set minimum requirements for contracts between sponsors and indirect participants, covering service levels, pricing, termination terms, dispute resolution, and liability. While allowing commercial flexibility, safeguards should prevent unfair terms or sudden disruptions.

ii. Technical and Operational Support: Sponsors must provide essential technical documentation, testing environments, and operational assistance. The scheme should define baseline support standards, with room for sponsors to offer additional services.

iii. Risk Management and Oversight: Sponsors are responsible for settlement and operational risks related to their indirect participants. They must implement appropriate monitoring, collateral arrangements, and oversight. The scheme should guide proportionate risk management that balances system integrity and participant inclusiveness.

D

Technical Service Provider (TSP)

TSPs are essential to the integration, scalability, and operation of instant payment systems. They provide infrastructure, connectivity, and services that help participants, especially smaller or indirect ones, access the system. Clear rules should define their roles, responsibilities, and oversight to ensure resilience and security.

i. Roles and Responsibilities: The scheme should define clear frameworks for how TSPs integrate with the instant payment infrastructure, including:

- **Translation Services:** The scheme should include provisions for services that facilitate translation between different message formats or standards, ensuring interoperability across various systems and platforms.
- **Aggregation Services:** To support smaller participants, the scheme should offer aggregation services that allow groups of smaller entities to pool their resources, thereby enhancing their ability to participate effectively in the instant payment network.
- **Value-Added Services:** The scheme should allow for the provision of value-added services, such as fraud prevention, compliance checking, and data analytics, to enhance security, regulatory compliance, and operational efficiency within the payment ecosystem.

ii. Technical and Operational Requirements: Given their critical connecting role, TSPs should meet enhanced technical and operational standards:

- Higher availability requirements reflecting their position as potential single points of failure.
- Robust security standards for handling transactions across multiple systems.
- Comprehensive monitoring and reporting capabilities across connected networks.
- Clear procedures for managing incidents that affect multiple connected systems.

iii. Governance and Oversight: The scheme should establish appropriate governance mechanisms for TSP participation:

- Certification processes verifying ISP capabilities and compliance with standards.
- Regular assessment of operational performance and risk management.
- Clear allocation of responsibilities between ISPs and the participants they serve.
- Transparency requirements regarding fees, service levels, and connected networks.

Participation Suspension and Termination

Clear suspension and termination conditions define the circumstances and procedures under which a participant's rights within the instant payment scheme may be temporarily restricted or permanently revoked, ensuring transparency, consistency, and fairness in the application of such measures.

A

Suspension Conditions

The scheme should define different types or levels of suspension based on the nature and severity of the underlying issues. This may include partial suspensions affecting only certain transaction types or volumes, monitored operations with enhanced oversight, or full suspensions preventing all transaction processing.

i. Grounds for Suspension:

- **Financial Distress:** Significant deterioration in financial condition creating settlement risk, including breaches of capital requirements, liquidity constraints, or pending insolvency proceedings
- **Operational Failures:** Persistent or severe operational issues compromising the participant's ability to fulfill obligations, including extended outages, critical system failures, or repeated performance standard violations.
- **Security Breaches:** Significant security incidents affecting the participant's systems that create risk for the broader ecosystem, including data breaches, cyber-attacks, or compromised infrastructure.
- **Compliance Violations:** Material or repeated non-compliance with scheme rules, technical standards, or regulatory requirements.
- **Regulatory Actions:** Supervisory measures imposed by regulatory authorities that affect the participant's ability to provide payment services.

ii. Suspension Process: The suspension process should include clearly defined steps:

- Initial identification and assessment of potential suspension conditions.
- Appropriate escalation within the scheme governance structure.
- Communication with the affected participant, including an opportunity to respond where circumstances permit.
- Formal decision through authorized governance bodies.
- Implementation of suspension measures with appropriate technical and operational adjustments.
- Notification to other participants and relevant authorities as required.

iii. Remediation and Restoration Procedures: Structured remediation and restoration procedures provide clear pathways for suspended participants to address underlying issues and return to full participation. The scheme procedures should establish the steps, requirements, and timelines associated with remediation efforts.

- **Remediation Plan Development:** The suspended participant, in collaboration with the scheme operator, must develop a comprehensive remediation plan addressing the specific issues that led to suspension. This plan should include concrete actions, timelines, resource allocations, and success measures.

.....

- **Scheme Approval and Monitoring:** The remediation plan must be formally approved by the scheme through designated governance channels. Once approved, the scheme will establish monitoring mechanisms to track progress against plan milestones.
- **Implementation and Validation:** The participant implements the remediation measures with regular progress reporting to the scheme. The scheme may require independent validation of key improvements, particularly for technical or security-related remediation.
- **Testing and Certification:** Before full restoration, the participant must complete appropriate testing and certification processes to demonstrate that remediated systems and processes meet scheme requirements.
- **Phased Restoration:** Restoration of participation privileges may follow a phased approach, starting with limited transaction types or volumes and gradually expanding to full participation as confidence in the remediation is established.

B

Termination

i. Conditions and Procedures

Termination of participation in the instant payment scheme may be either voluntary or involuntary. Clear and well-defined conditions for both suspension and termination help ensure that a participant's rights can be temporarily restricted or permanently revoked in a fair, transparent, and consistent manner.

ii. Grounds for Involuntary Termination:

- Failure to remediate issues leading to suspension within established timeframes.
- Repeated suspensions demonstrating persistent inability to meet participation requirements.
- Critical financial failure such as insolvency, bankruptcy, or license revocation.
- Severe or deliberate violations of scheme rules that fundamentally undermine trust.
- Prolonged inactivity or failure to maintain minimum participation requirements.

iii. Termination Decision Process: Involuntary termination decisions should follow a structured governance process with appropriate checks and balances:

- Formal recommendation from operational management based on documented evidence.
- Review by relevant governance committees with appropriate participant representation.
- Opportunity for the affected participant to present its case (except in extreme circumstances).
- Final decision by authorized governance body according to established voting procedures.
- Documentation of decision rationale and compliance with termination standards.

iv. Voluntary Withdrawal Process: The scheme should also establish clear procedures for voluntary withdrawal from participation, including:

- Formal notification requirements with minimum notice periods.

- Wind-down planning to manage the transition for customers and counterparties.
- Final settlement and reconciliation processes.
- Return of collateral or guarantee fund contributions according to established timelines.

v. Managing Systemic Impact of Participant Exit: When a participant exits the scheme, whether voluntarily or involuntarily, careful management of the transition is essential to minimize disruption to the broader ecosystem. Comprehensive exit management procedures help protect end-users, maintain system stability, and preserve trust in the payment service.

vi. Transaction Wind-Down Management: The scheme should define clear and comprehensive processes to manage in-flight transactions and ongoing payment relationships during a participant's exit—whether voluntary or involuntary. These processes should include:

- **Completion of Pending Transactions:** Procedures for identifying and appropriately handling transactions that are in progress at the time of exit.
- **Management of Recurring Payment Arrangements:** Protocols for terminating or transferring recurring payments and standing instructions to ensure continuity of service for end-users.
- **Customer Notification Requirements:** Guidelines to ensure timely and effective communication to affected customers regarding service changes, alternative options, or disruptions.
- **Continuity for Sponsored Participants:** For direct participants that sponsor indirect participants, the scheme must ensure a smooth transition by facilitating the reassignment of sponsored entities to new sponsors and minimizing service disruptions.

vii. Customer Protection Measures: Management procedures should incorporate specific customer protection elements, potentially including:

- Standardized customer communication templates explaining the situation and next steps.
- Minimum notice periods for service discontinuation where circumstances permit.
- Facilitated processes for transferring payment relationships to other participants.
- Special handling for vulnerable customers or critical payment services.

viii. Systemic Risk Mitigation: For the exit of significant participants, the scheme should establish coordinated risk management approaches with relevant authorities. **This may include:**

- Enhanced monitoring of other participants for potential contagion effects.
- Temporary liquidity support mechanisms, or adjusted settlement procedures during the transition period.
- Contingency arrangements should be developed for scenarios involving the simultaneous exit of multiple participants during periods of market stress.

Operational Rules

Instant Payment Product

A

The Concept of Instant Payment

Across jurisdictions, a range of terms is used to describe what is commonly referred to as **instant payment**, including **real-time payment**, **immediate payment**, and **faster payment**.

According to the Bank for International Settlements (BIS), faster payments are defined as: “a payment in which the transmission of the payment message and the availability of final funds to the payee occur in real time or near-real time on a 24-hour and seven-day (24/7) basis as possible.”¹⁰

This definition emphasizes the speed of the clearing message and availability of funds to the payee, without necessarily requiring real-time interbank settlement. This Reference Guide adopts the BIS definition to guide the development of the instant payment ecosystem, with a focus on uninterrupted service, immediate funds availability, and user-centric functionality.

B

Key Features of Instant Payment

Instant payments offer a distinctive set of features designed to address modern market needs and provide a competitive edge over traditional instruments:

- **Speed:** Transactions are processed and confirmed within seconds.
- **24/7/365 Availability:** Payments can be initiated and received at any time, including weekends and public holidays.
- **Credit Push Model:** The payer initiates the transaction, offering enhanced control and reducing the risk of fraud.
- **Verification of Payee:** Allows confirmation of the recipient’s identity before execution.
- **Positive Confirmation:** Both payer and payee receive immediate notifications, enhancing trust and transparency.
- **Availability of Funds:** Funds are irrevocably available to the payee once the payment is confirmed.
- **Proxy Services:** Enable payments using simplified identifiers such as mobile numbers, email addresses, or national IDs.
- **Value-Added Services:** Overlay services like **Request to Pay** and **Payment Initiation Requests** enhance flexibility and enable more complex use cases.

Instant payment schemes should ensure these features are embedded in their design to offer a tangible advantage over legacy payment systems.

¹⁰ BIS CPMI: [Fast payments - Enhancing the speed and availability of retail payments](#), November, 2016.

C

Use Cases

Instant payment systems are versatile and support a wide range of transaction types across individuals, businesses, and government entities. Recognizing the distinct roles and requirements of each use case, dedicated operational guidelines should be established for each to ensure efficiency, security, and regulatory compliance.

- **Person-to-Person (P2P):** P2P payments represent one of the most common use cases for instant payment systems, allowing individuals to transfer funds directly to one another. The following aspects should be considered for P2P:
 - **Account Setup and Management:** Effective account setup and management processes are critical to the security, compliance, and user experience of P2P payment services. Payment system operators must establish comprehensive guidelines for financial institutions and payment service providers to follow when onboarding users and managing their accounts throughout the customer lifecycle.
 - **User Identification:** Implement multiple options for recipient identification, including phone numbers, email addresses, and usernames, with appropriate privacy controls. Consider proxy addressing systems (refer to the section on proxy directory service for more details) that mask actual account details while enabling seamless transfers.
 - **Transaction Limits:** Establish daily, weekly, and monthly transaction limits based on user verification level. Consider implementing dynamic limits that adjust based on user behavior patterns and risk scoring to balance security with convenience.
- **Person-to-Business (P2B):** Person-to-Business (P2B) payments represent a critical use case for instant payment systems, enabling consumers to pay merchants or service providers instantly via QR codes, mobile POS, or e-commerce platforms, reducing cash dependence and improving merchant liquidity. P2B payments require special attention to merchant onboarding, verification, and management processes. The following aspects should be considered in the operational guidelines:
 - **Merchant Onboarding:** Operational guidelines must establish comprehensive procedures for the merchant verification process with risk-based due diligence and automated KYB checks, technical integration, and account setup while balancing security, compliance, and user experience considerations.
 - **Merchant Management:** Operational guidelines must establish comprehensive frameworks for ongoing merchant relationship management, performance monitoring, problem resolution, and commercial management throughout the merchant lifecycle.
 - **Payment Acceptance:** Multiple integration options, including QR codes, USSD, mobile application, and POS systems.
 - **Consumer Experience:** Operational guidelines must establish frameworks that ensure consistency, security, and convenience throughout the consumer journey while accommodating the diverse contexts in which P2B payments occur.
 - **Transaction Reporting:** Comprehensive merchant dashboards with real-time sales data and analytics.
 - **Settlement Process:** Flexible settlement options with same-day availability and automated reconciliation.

.....

- **Bill Payments:** Facilitates timely and transparent payment of utilities, school fees, subscriptions, and more, with immediate posting and confirmation. Bill payment functionality requires integration with a wide range of billers, including utilities, government agencies, educational institutions, and service providers. The following aspects should be considered in the operational rules:
 - **Biller Onboarding:** Operational guidelines must establish comprehensive procedures for biller verification, technical integration, and account setup that address the unique characteristics of billers compared to traditional merchants.
 - **Transaction Processing:** Bill payment transaction processing within instant payment systems requires specialized operational procedures that address the unique characteristics of billing transactions. Unlike standard P2P or P2B payments, bill payments often involve additional data elements, validation requirements, and processing models that must be accommodated in the operational framework.
 - **Recurring Payment Management:** Recurring bill payment functionality represents an important capability within instant payment systems, allowing consumers to automate regular payments while giving billers greater certainty about revenue collection. Operational guidelines must establish comprehensive frameworks for managing the unique lifecycle and risk considerations associated with recurring payments.
- **Cash-In and Cash-Out Transactions:** Cash-in and cash-out transactions represent critical bridge functionality between physical currency and digital payment systems, which is particularly important in markets with significant cash usage or limited banking infrastructure.

The instant payment context adds significant value to traditional cash-in/cash-out models by enabling real-time transaction settlement, immediate agent rebalancing, enhanced transaction verification, and improved liquidity management. When combined with Request to Pay functionality, instant payments can optimize the cash-out process by allowing agents to initiate payment requests to consumers, streamlining the interaction and reducing manual steps and potential errors.

The operational guidelines should address the following key aspects for instant payment system operators, financial institutions, payment service providers, and regulatory authorities.

- **Agent Onboarding and Management:** Operational guidelines must establish comprehensive frameworks for agent selection, verification, training, monitoring, and ongoing relationship management that address the unique risks and operational considerations associated with cash handling.
- **Transaction Processing:** Cash transaction processing within instant payment systems requires specialized operational procedures that address the unique characteristics of physical currency handling combined with digital payment processing. Operational guidelines must establish comprehensive frameworks for the end-to-end transaction lifecycle while ensuring security, compliance, and a positive customer experience.
- **Risk Management:** Cash transaction risk management within instant payment systems requires specialized approaches that address the unique risks associated with physical currency handling combined with digital transaction processing. Operational guidelines must establish comprehensive frameworks for identifying, assessing, mitigating, and monitoring these compound risks while maintaining service accessibility and efficiency.

- **Agent Network Management:** Effective agent network management is essential for building a sustainable, accessible, and efficient cash transaction ecosystem within instant payment systems. Operational guidelines must establish comprehensive frameworks for network planning, performance management, incentive structures, and continuous improvement that support both business objectives and financial inclusion goals.
- **Cross-border Payment:** Cross-border instant payments represent a significant evolution in the global financial ecosystem, enabling the rapid transfer of funds across international boundaries. Key operational considerations to implement effective cross-border instant payment systems:
 - **Technical Infrastructure:** The foundation of any cross-border instant payment system is a robust technical infrastructure. It should support the ISO 20022 messaging standard, offer secure and scalable API connectivity, and enable seamless integration with key external systems, including but not limited to foreign exchange platforms, compliance and sanctions screening tools, and real-time fraud detection mechanisms.
 - **Regulatory Compliance and Legal Frameworks:** Cross-border: Instant payments operate within a complex web of international and domestic regulations that vary significantly across jurisdictions. Financial institutions must navigate this regulatory landscape while ensuring compliance with anti-money laundering (AML) and counter-terrorism financing (CTF) requirements in all relevant countries.
 - **Settlement Mechanisms and Liquidity Management:** Effective settlement mechanisms are crucial for cross-border instant payments, as they ensure the finality of transactions and manage the financial risk between participating institutions.
 - **Foreign Exchange and Currency Conversion:** Currency conversion represents one of the most complex operational aspects of cross-border instant payments. Financial institutions must develop strategies to manage FX risk during off-market hours while still providing competitive exchange rates to customers.

Messaging Standards

Standardized messaging formats and protocols are fundamental to ensuring interoperability, efficiency, and future-proofing of instant payment schemes. The scheme should adopt internationally recognized message format standards where feasible, while considering local market requirements and existing infrastructure.

The globally recommended standard for financial messaging, offering rich data capabilities, extensibility, and future-proofing. ISO 20022 enables enhanced remittance information, structured addressing, and integration with other payment systems.

While ISO 20022 implementation may present initial complexity, particularly for institutions with legacy systems, its adoption aligns with global trends and supports future interoperability with regional and international payment systems.

A

Message Types:

The scheme should define a comprehensive set of message types covering all aspects of transaction processing and scheme operations, including:

- **Payments Initiation (PAIN):** Messages that support the initiation of a payment from the ordering customer to a financial institution that services a cash account and reports its status.
- **Payments Clearing and Settlement (PACS):** Messages that support the clearing and settlement processes for payment transactions between financial institutions.
- **Cash Management (CAMT):** Messages that support the reporting and advising of the cash side of any financial transactions, including cash movements, transactions, and balances, plus any exceptions and investigations related to cash transactions.
- **Account Management (ACMT):** Messages that support the management of account-related activities, such as the opening and maintenance of an account.
- **Administration (ADMI):** Generic messages, i.e., system event notifications, generic rejections, etc.

The SWIFT Instant Payments Plus (IP+)¹¹ Working Group has developed comprehensive implementation guidelines that serve as a valuable resource for schemes adopting the ISO 20022 messaging standard. These guidelines provide best practices and technical specifications, helping payment schemes to successfully integrate instant payment solutions while ensuring compatibility with the global ISO 20022 framework.

B

Message Security and Validation:

Comprehensive message security standards must be established, including encryption requirements, digital signature standards, and message authentication controls. Detailed message validation rules should be defined, with clear procedures for handling message validation failures.

C

Instant Payment Processing

The processing of instant payments must ensure speed, security, and reliability across all transactions. The following illustrates key considerations that schemes should account for in defining their operational and technical rules. This list is not exhaustive and may evolve as the ecosystem matures:

- **Message Validation:** All messages must conform to ISO 20022 and scheme-defined rules.
- **Payment Controls and Limits:** Transaction caps and daily limits to manage risk and ensure compliance.
- **Transaction Timeouts:** Payments must be completed within set timeframes; otherwise, they are treated as failed.
- **End-User Notification:** Real-time confirmation or failure alerts must be sent to both the payer and the payee.
- **Finality of Payment:** Once confirmed, payments are irrevocable and must be immediately settled.

¹¹ [Domestic market infrastructures create new instant payment guidelines | Swift](#)

- **Strong Authentication and Beneficiary Verification:** Secure login and confirmation of recipient identity before execution.
- **Erroneous and Unauthorized Payments:** Clear protocols must address dispute resolution and error handling.
- **Receiver Response Time:** Receiving institutions must respond promptly to maintain real-time integrity.
- **Immediate Fund Availability:** Funds must be credited and available to the payee instantly.

These considerations form the foundation for robust instant payment operations and support a consistent user experience across participants.

Proxy Directory Service

A Functions

Proxy directory services represent a fundamental advancement in payment systems, enabling users to initiate and receive payments using familiar identifiers such as mobile numbers, email addresses, or national IDs instead of complex account numbers. This capability significantly enhances user experience, reduces payment friction, and drives adoption of digital payment solutions across various demographics.

The core function of a proxy directory is to maintain secure mappings between these user-friendly identifiers (proxies) and actual payment account information.

When a user initiates a payment to a proxy, the system resolves this identifier to the corresponding account details, enabling the transaction to proceed through the payment infrastructure. This resolution process must occur in real-time, with high availability and robust security measures.

B Key Considerations

i. Types of Proxies and Standardization:

The system must support a clearly defined set of proxy identifiers that can be linked to payment accounts.

- These proxies should include common identifiers such as mobile phone numbers, email addresses, national IDs, and business identifiers.
- These identifiers must be familiar to users, widely available, and capable of uniquely identifying individuals or entities within the payment ecosystem.
- Each proxy type must undergo standardization to ensure consistency across the payment ecosystem, including defining format specifications, validation rules, and lifecycle management procedures.
- Furthermore, the scheme should establish clear guidelines for handling special cases such as recycled mobile numbers, expired IDs, or business closures to prevent misdirected payments or unauthorized access.

Key Considerations

i. Types of Proxies and Standardization:

The system must support a clearly defined set of proxy identifiers that can be linked to payment accounts.

- These proxies should include common identifiers such as mobile phone numbers, email addresses, national IDs, and business identifiers.
- These identifiers must be familiar to users, widely available, and capable of uniquely identifying individuals or entities within the payment ecosystem.
- Each proxy type must undergo standardization to ensure consistency across the payment ecosystem, including defining format specifications, validation rules, and lifecycle management procedures.
- Furthermore, the scheme should establish clear guidelines for handling special cases such as recycled mobile numbers, expired IDs, or business closures to prevent misdirected payments or unauthorized access.

ii. Registration and Deregistration Processes:

To maintain the integrity of a proxy directory service, secure, transparent, and auditable processes for managing the full lifecycle of proxy registrations must be established. **This includes:**

Registration:

- Ensuring that only legitimate proxy-account mappings are created and maintained.
- The registration process should capture explicit, informed customer consent before creating any proxy-account mapping, including identity verification and account ownership validation.
- Clear disclosure of how the proxy will be used.
- Registration interfaces must present terms in plain language, with appropriate record-keeping of consent timestamps and channels.
- Before activation, the system must verify both proxy ownership and account access rights through mechanisms such as one-time passwords or account validation checks.

Modification:

- Users should be able to update their proxy-account mappings through secure channels, with appropriate notifications and re-authentication to prevent unauthorized changes.

Deregistration:

- The system must support immediate deregistration upon customer request, suspected fraud, account closure, or regulatory requirement, with confirmation mechanisms, cooling-off periods where necessary, and appropriate notifications.

.....

iii. Proxy Resolution and Payment Generation:

Proxy resolution forms the core technical functionality of the directory service, converting user-friendly proxies into the payment account information needed to initiate transactions. This process must be reliable, fast, and precise to meet the demands of instant payment systems. The resolution process must incorporate error-handling capabilities to manage issues such as inactive proxies, deregistered proxies, or technical failures.

iv. Proxy–Payment Account Relationship Models:

The relationship between proxies and payment accounts is a key design consideration with implications for user experience, system complexity, and risk management. **Two primary models:**

- **One-to-One Relationship:** Each proxy identifier is linked to exactly one payment account. This model simplifies resolution logic, reduces ambiguity, minimizes routing errors, and ensures clear ownership of proxies.
- **Many-to-One Relationship:** Multiple proxy identifiers may be linked to a single payment account, enabling users to register several proxies (e.g., personal and work email addresses) or businesses to create multiple entry points for payments.

v. Proxy Database Architecture: The scheme **must** define whether a centralized or decentralized proxy database is used.

- **A centralized proxy database** consolidates all proxy-account mappings into a single logical database, operated by a scheme authority or designated service provider. This architecture ensures consistency, operational efficiency, and robust governance.
- **A decentralized proxy database** distributes proxy-account mappings across participating institutions, offering benefits such as enhanced data sovereignty, reduced central infrastructure costs, and greater resilience against single-point failures. However, the decentralized model comes with challenges in data synchronization and ensuring consistent data quality across the ecosystem.

vi. Information Exchange and Communication Standards:

All message exchanges within the proxy directory ecosystem must conform to standardized formats and structures, ideally aligned with the ISO 20022 messaging standard.

The message suite should include specialized formats for various functions, including proxy registration, modification, and deregistration requests; resolution queries and responses; error notifications; administrative commands; and reconciliation and audit verification messages.

The scheme should publish message definitions in formal schema repositories, with clear versioning and change management processes.

vii. Consent Management and Data Protection:

Given that the proxy directory service processes personal data, it is crucial to implement rigorous privacy protections and transparent consent management. Key elements of consent management include:

- **Explicit Consent Capture:** Users must provide clear and specific authorization before their proxies are registered.
-

- **Transparency:** The system must provide clear disclosures about data usage, sharing, and retention.
- **User Control:** Participants must have access to self-service tools for managing their consent preferences.
- **Auditability:** The system should maintain complete records of all consent actions and changes to ensure accountability and regulatory compliance.

Settlement and Liquidity Management

A

Settlement Models

The settlement model is a fundamental design choice that significantly impacts the risk profile, liquidity requirements, and operational characteristics of an instant payment scheme. This section outlines settlement model options suitable for instant payment contexts.

- i. **Settlement Model Options:** The scheme must select an appropriate settlement model based on risk appetite, infrastructure availability, and participant capabilities.
 - **Real-Time Gross Settlement (RTGS):** Each transaction is settled individually and immediately on a gross basis, typically through the central bank RTGS system. This model eliminates settlement risk but requires 24/7 availability of the RTGS system, which may not be feasible in all African contexts. Key considerations include:
 - Maximum security with no settlement risk
 - High liquidity requirements for participants
 - Potential need for pre-positioning of funds if RTGS is not 24/7
 - Dependency on RTGS operating hours
 - **Deferred Net Settlement (DNS):** Transactions are accumulated over a defined period, with net positions settled periodically. This model is more liquidity-efficient but introduces settlement risk between settlement cycles. Key considerations include:
 - More efficient liquidity utilization
 - Settlement risk exposure between cycles
 - Need for risk mitigation measures (collateral, limits)
 - Easier implementation with existing infrastructure
 - Flexibility in settlement frequency (e.g., hourly, several times daily)
 - **Hybrid Models:** Some instant payment schemes have implemented hybrid models combining elements of RTGS and DNS approaches:
 - **Pre-funded Settlement Model:** Participants maintain a dedicated settlement pool with prefunded balances. Transactions are settled continuously from this pool, with periodic replenishment.
 - **Liquidity-Saving Mechanisms:** Transactions are queued and settled in optimized batches when liquidity is available, reducing liquidity requirements while minimizing settlement delays.
 - **Tiered Settlement:** Different transaction types or value bands follow different settlement approaches, with high-value or high-risk transactions potentially settled in real-time, while others use deferred settlement.

-
- ii. **Settlement Institution:** The scheme must designate a settlement institution, typically the central bank, which maintains settlement accounts for participants. Settlement through central bank accounts provides settlement finality and eliminates settlement bank risk, making it the preferred approach for instant payment schemes.

_____ The selected settlement model should balance risk management with practical implementation considerations, potentially evolving over time as infrastructure capabilities develop.

B

Settlement Cycles and Timing:

Settlement timing and cycles are essential for managing liquidity and risk within the instant payment ecosystem. The approaches for settlement timing in instant payment schemes are the following:

- i. **Settlement Cycle Definition:** For schemes using deferred net settlement, clearly defined settlement cycles must be established:
- **Frequency:** Settlement cycles should be frequent enough to manage settlement risk while aligning with operational capabilities. Common approaches include hourly settlement during business hours, with less frequent cycles (e.g., every 3-4 hours) during nights and weekends.
 - **Schedule:** Fixed settlement schedules should be established, with precise timing of key settlement events, including position calculation, settlement initiation, and completion confirmation.
 - **Failure Handling:** Clear procedures should be defined for handling settlement cycle failures, including retry attempts, escalation protocols, and contingency arrangements.
- ii. **Settlement Windows:** The scheme should establish defined settlement windows aligned with the operating hours of supporting systems.
- iii. **Calendar Management:** The scheme must maintain a comprehensive settlement calendar accounting for:
- Regular business days and hours in all relevant jurisdictions
 - Official holidays and non-processing days
 - Scheduled maintenance periods for settlement systems
 - Modified settlement schedules for specific calendar events
- This calendar should be published to all participants well in advance, with mechanisms for communicating changes or exceptional circumstances.
- iv. **Position Reporting:** The scheme should provide real-time or near-real-time visibility of current net positions to participants, enabling proactive liquidity management. Position reporting should include:
- Current net position relative to available liquidity
 - Projected positions based on pending transactions
 - Historical settlement patterns and peak positions
 - Notifications when positions approach defined thresholds

_____ Settlement timings should be designed to balance risk management with operational efficiency, recognizing the infrastructure realities in different markets.

C

Prefunding and Collateral

Robust prefunding and collateral arrangements are essential for managing settlement risk in instant payment schemes, particularly those using deferred net settlement models. The recommended approaches for instant payment contexts.

- i. **Prefunding Requirements:** The scheme should establish clear prefunding requirements to mitigate settlement risk.
 - **Prefunding Calculation:** The methodology for determining minimum prefunding requirements should be clearly defined, potentially based on:
 - Historical net debit positions with appropriate multipliers
 - Statistical analysis of peak positions and volatility
 - Participant-specific risk factors and transaction patterns
 - Projected volume growth and seasonal variations
 - **Funding Maintenance:** Participants must maintain required prefunding levels throughout operating hours, with:
 - Real-time monitoring of available funds against requirements
 - Automatic alerts when positions approach thresholds
 - Clear procedures for topping up prefunding when needed
 - Consequences for failing to maintain required levels
 - **Funding Adjustments:** Processes for reviewing and adjusting prefunding requirements should be established.
 - Regularly scheduled reviews (typically monthly or quarterly)
 - Event-triggered reviews following significant volume changes
 - Temporary adjustments for seasonal variations or special events
 - Appeal procedures for participants to request reconsideration
- ii. **Collateral Arrangements:** In addition to or instead of cash prefunding, the scheme may accept eligible collateral to secure settlement obligations:
 - **Eligible Collateral:** Clearly defined criteria for acceptable collateral types, typically focusing on high-quality liquid assets such as government securities or central bank-eligible instruments.
 - **Valuation Methodology:** Transparent approaches for valuing collateral, including application of appropriate haircuts reflecting liquidity and market risk.
 - **Collateral Management:** Procedures for pledging, holding, and releasing collateral, potentially leveraging existing central bank collateral management systems.
 - **Collateral Mobilization:** Clear processes for accessing or liquidating collateral in the event of participant default, including legal frameworks ensuring timely execution.
- iii. **Collateral Arrangements:** In addition to or instead of cash prefunding, the scheme may accept eligible collateral to secure settlement obligations:
 - **Eligible Collateral:** Clearly defined criteria for acceptable collateral types, typically focusing on high-quality liquid assets such as government securities or central bank-eligible instruments.
 - **Valuation Methodology:** Transparent approaches for valuing collateral, including application of appropriate haircuts reflecting liquidity and market risk.

- **Collateral Management:** Procedures for pledging, holding, and releasing collateral, potentially leveraging existing central bank collateral management systems.
- **Collateral Mobilization:** Clear processes for accessing or liquidating collateral in the event of participant default, including legal frameworks ensuring timely execution.

iv. **Settlement Caps:** The scheme should implement a system of settlement caps and transaction limits aligned with prefunding or collateral arrangements:

- Net debit caps limit maximum exposure relative to available prefunding or collateral.
- Transaction value limits for individual payments to manage concentration risk.
- Sender limits controlling total outgoing value within defined timeframes.
- Receiver limits controlling total income from specific counterparties.

Prefunding and collateral requirements should be calibrated to balance risk management with liquidity efficiency, recognizing that excessive requirements may create barriers to participation or increase costs for end-users.

D Liquidity Management Tools

Effective liquidity management is critical for participants in instant payment schemes, enabling them to meet settlement obligations efficiently while optimizing funding costs. This section outlines recommended liquidity management tools and approaches for instant payment contexts.

i. **Liquidity Forecasting:** The scheme should provide tools and information to support participant liquidity forecasting:

- **Historical Analytics:** Detailed data on historical settlement patterns, peak positions, and cyclical variations to support trend analysis and forecasting.
- **Projected Positions:** Near-real-time projections of upcoming settlement positions based on in-flight transactions and historical patterns.
- **Early Warning Indicators:** Alerts and notifications for unusual transaction patterns or emerging liquidity pressures.
- **Stress Testing Tools:** Capabilities for simulating liquidity requirements under various stress scenarios.

ii. **Intraday Liquidity Facilities:** In collaboration with the central bank or settlement institution, the scheme should establish appropriate intraday liquidity facilities.

- **Automated Liquidity Provision:** Automated mechanisms for transferring liquidity between participant accounts, potentially including:
 - Automated sweeps between settlement and operational accounts.
 - Scheduled liquidity transfers aligned with settlement cycles.
 - Threshold-triggered liquidity injections when positions approach defined limits.
- **Emergency Liquidity Support:** Arrangements for addressing unexpected liquidity shortfalls, potentially including
 - Intraday credit facilities from the central bank
 - Collateralized liquidity lines between participants

- Emergency liquidity pools funded by scheme participants
- Procedure for requesting temporary cap increases or extensions

iii. Participant Liquidity Management Interface: The scheme should provide a comprehensive liquidity management interface enabling participants to:

- Monitor current and projected settlement positions in real-time
- View detailed breakdowns of incoming and outgoing payment flows
- Configure automated liquidity management tools and alerts
- Execute manual liquidity transfers when needed

Liquidity management tools should be designed with consideration for the diverse capabilities of African financial institutions, providing both sophisticated options for advanced participants and simpler tools for institutions with more limited resources.

E

Default Handling

Clear procedures for handling participant defaults are essential for maintaining settlement certainty and system stability. This section outlines recommended default management frameworks for instant payment schemes.

i. Default Definition and Declaration: The scheme rules must clearly define what constitutes a participant default, typically including:

- Failure to meet settlement obligations by specified deadlines.
- Regulatory intervention affecting the participant's ability to operate.
- Insolvency or resolution proceedings against the participant.
- Expulsion from the scheme due to rule violations or risk concerns.

Formal procedures for default declaration must be established, specifying authority for making default determinations, required evidence, notification protocols, and appeal mechanisms where appropriate.

ii. Immediate Response Measures: Upon default declaration, the scheme should implement immediate response measures:

- **Transaction Suspension:** Immediate suspension of the defaulting participant's ability to submit new transactions to the system.
- **Position Calculation:** Prompt calculation of the defaulter's final net position, including all accepted but unsettled transactions.
- **Resource Assessment:** Evaluation of available resources to cover the defaulter's obligations, including prefunding, collateral, and guarantee arrangements.
- **Stakeholder Notification:** Communication to other participants, regulatory authorities, and critical service providers regarding the default event.

iii. Settlement Completion: The scheme must establish clear procedures for completing settlement despite the default:

- **Prefunding Utilization:** Application of the defaulter's prefunded balance toward outstanding obligations.
- **Collateral Liquidation:** Execution of procedures to liquidate or apply available collateral if prefunding is insufficient.

- **Guarantee Fund Access:** Utilization of any collective guarantee fund, if established as part of the scheme design.
- **Loss Allocation:** Implementation of defined loss allocation mechanisms if prefunding, collateral, and guarantees are insufficient.

iv. **Operational Continuity:** The scheme must establish arrangements for maintaining critical payment services for customers of the defaulting participant, potentially including:

- Transfer of customer payment services to alternative providers.
- Special operating procedures for processing payments during the transition period.
- Customer communication templates and channels for providing guidance.

Default management procedures should be tested regularly through simulation exercises involving all relevant stakeholders, ensuring operational readiness for actual default scenarios.

Consumer Protection and Dispute Resolution

A

Core Principles

Robust consumer protection is fundamental to building trust in instant payment systems and driving adoption. This section outlines core consumer protection principles for instant payment schemes.

i. **Foundational Consumer Protection Principles:** The scheme should establish comprehensive consumer protection principles including:

- **Transparency:** Consumers must receive clear, accessible information about instant payment services, including fees, processing times, and potential risks. Information should be provided in simple language appropriate for varying literacy levels, potentially in multiple languages for diverse markets.
- **Redress:** Effective mechanisms must be available for resolving disputes and addressing errors. Procedures should be accessible to all consumers regardless of location or socioeconomic status.
- **Security:** Robust security measures must protect consumers from unauthorized transactions and fraud. Security controls should be proportionate to risks while remaining usable for consumers with varying technical capabilities.
- **Privacy:** Personal and financial data must be protected with clear limitations on collection, use, and sharing. Consumers should maintain appropriate control over their information while enabling necessary processing for service delivery.

ii. **Consumer Protection Policy Framework:** The scheme should establish a comprehensive consumer protection policy framework:

- **Minimum Standards:** Clearly defined baseline protection requirements that all participants must implement, covering security controls, disclosure practices, complaint handling, and fraud management.
- **Participant Obligations:** Specific responsibilities for protecting consumers at different stages of the payment journey, with clear allocation of accountability between originating and receiving institutions.

- **Scheme Monitoring:** Mechanisms for assessing participant compliance with consumer protection requirements, potentially including customer experience metrics, complaint analysis, and targeted reviews.
- **Evolution Process:** Structured approach for enhancing consumer protection measures based on emerging risks, incident patterns, customer feedback, and regulatory developments.

B

Transaction Transparency

Clear and accessible transaction information is essential for enabling consumers to make informed decisions and monitor their payment activities. This section outlines transaction transparency requirements for instant payment schemes.

- Pre-Transaction Disclosure:** The scheme should establish minimum standards for information that must be provided to customers before they authorize a transaction:
 - **Transaction Details:** Clear presentation of essential transaction elements, including recipient identity, amount, and purpose.
 - **Fees and Charges:** Transparent disclosure of all applicable fees, presented in absolute amounts rather than percentages where possible.
 - **Execution Timeframe:** Clear indication of when the funds will be available to the recipient.
 - **Transaction Finality:** Explicit notification about the irrevocable nature of instant payments once authorized.
 - **Security Information:** Contextual security guidance relevant to the specific transaction type or amount.
- Transaction Confirmation:** Comprehensive confirmation information should be provided immediately upon transaction completion:

Element	Requirement
Transaction Reference	Unique identifier for the transaction that can be used for future inquiries or disputes
Transaction Status	Clear indication of whether the transaction was completed successfully
Amount Details	Confirmation of the transaction amount, any fees deducted, and total amount debited
Recipient Information	Confirmation of the recipient's identity in a recognizable format
Timestamp	Date and time when the transaction was processed
Available Balance	Remaining account balance after the transaction (where applicable)

.....

iii. Transaction History: Customers should have access to comprehensive transaction history information:

- Complete record of all instant payment transactions, accessible for at least a minimum period to be defined by the scheme.
 - Multiple access channels, including mobile applications, online platforms, and statements.
 - Search and filtering capabilities to help locate specific transactions.
- _____

C

Authentication Standards

Robust yet usable authentication standards are essential for ensuring that instant payments are authorized by legitimate users while maintaining accessibility.

i. Authentication Principles: The scheme should establish fundamental principles guiding authentication requirements.

- **Risk-Based Approach:** Authentication strength should be proportionate to transaction risk, considering factors such as amount, recipient, channel, and historical patterns.
- **Security-Usability Balance:** Authentication mechanisms should provide meaningful security while remaining usable across different customer segments and device types.
- **Multi-Factor Authentication:** High-risk transactions should require multiple authentication factors from different categories (knowledge, possession, and inherence).
- **Inclusive Design:** Authentication options should accommodate varying levels of technical capability, literacy, and device access.

ii. Authentication Requirements: The scheme should establish minimum authentication standards:

- **Base Authentication:** Minimum requirements for standard transactions:
 - Unique identifier (username, phone number)
 - Secret knowledge factor (PIN, password)
 - Account lockout after failed attempts
 - Session management controls
 - Enhanced Authentication
 - **Enhanced Authentication:** Additional requirements for higher-risk transactions
 - Secondary verification (OTP, push notification)
 - Transaction verification details
 - Biometric verification where available
 - Device binding/recognition
- _____

D

Complaint Handling

Effective complaint handling procedures are essential for maintaining customer trust and resolving issues efficiently.

- i. **Complaint Handling Principles:** The scheme should establish fundamental principles guiding complaint management:
 - **Timeliness:** Complaints should be acknowledged and resolved within clearly defined timeframes appropriate to their nature and complexity.
 - **Transparency:** Customers should receive clear information about complaint procedures, progress updates, and the rationale for decisions.
 - **Accessibility:** Complaint channels should be accessible to all customers regardless of location, technical capability, or literacy level.
 - **Fairness:** Complaint assessment should be objective and consistent, with equitable outcomes based on established principles.
- ii. **Participant Requirements:** The scheme should establish minimum standards for participant complaint management:
 - **Multiple Access Channels:** Provision of various complaint submission methods, including in-person, phone, digital, and potentially USSD for feature phone users.
 - **First Response Timelines:** Maximum timeframes for initial acknowledgment (typically 24-48 hours) and provisional assessment of complaints.
 - **Investigation Standards:** Structured approach to complaint investigation, including evidence collection, transaction tracing, and root cause analysis.
 - **Resolution Timeframes:** Maximum periods for completing investigations and providing final responses (typically 5-15 days for standard complaints).
 - **Documentation Requirements:** Standards for recording complaint details, investigation steps, and resolution outcomes.
- iii. **Dispute Management and Escalation Framework:** In addition to participant-level complaint handling mechanisms, the scheme should establish a structured framework for escalating unresolved disputes. This ensures the timely and fair resolution of issues that may arise between participants, between a participant and a customer, or between a participant and the scheme manager.

The escalation process should follow a progressive, tiered approach designed to resolve issues at the lowest appropriate level while ensuring fairness and transparency for more complex cases.

The table below presents an illustrative escalation pathway that scheme managers and participants may adapt based on institutional arrangements, regulatory requirements, and the specific nature of the dispute.

Escalation Level	Responsible Party	Example Use Cases	Illustrative Timeframe	Typical Resolution Mechanism
Level 1 – Participant Resolution	Customer support or operations team of the initiating or receiving participant	End-user complaints, transaction errors, and failed payment reversals	Within 2 business days	Resolved through the institution’s standard complaint process
Level 2 – Bilateral Coordination	Designated focal points of the involved participants	Disputes between participants (e.g., misrouted payments, unmatched transactions)	Within 5 business days	Joint investigation and resolution using scheme-aligned procedures
Level 3 – Scheme-Level Facilitation	Scheme manager or designated dispute unit	Escalated disputes, repeated failures, or non-compliance with agreed procedures	Within 7–10 business days	Mediation or guided facilitation by the scheme manager, with documented decisions
Level 4 – Independent Determination	Appointed expert or neutral panel	Complex, high-value, or sensitive disputes not resolved at the scheme level	Within 20 business days	Independent review and binding recommendation based on scheme rules and documentation
Level 5 – Regulatory Referral (if applicable)	Relevant financial regulator or consumer protection authority	Regulatory breaches, systemic non-compliance, or unresolved customer protection issues	Per regulatory guidelines	Escalated to the competent authority under national legal or supervisory frameworks

E

Fraud Protection and Liability

Clear frameworks for fraud protection and liability allocation are essential, given the immediate and irrevocable nature of instant payments.

i. Customer Fraud Protection Measures: The scheme should establish minimum fraud protection measures for customers:

- **Preventive Controls:** Measures to prevent fraudulent transactions:
 - Risk-based transaction screening
 - Payee confirmation requirements
 - New beneficiary cooling-off periods
 - Transaction value limits
 - Unusual activity detection
- **Customer Empowerment:** Tools enabling customers to control their security:
 - Customizable transaction limits
 - Real-time transaction notifications
 - Temporary service freezes
- **Customer Education:** The scheme should establish requirements for customer education on fraud risks:
 - Clear information about common fraud scenarios and warning signs.
 - Contextual security messages at key transaction points.
 - Regular fraud awareness updates through appropriate channels.
 - Targeted education for vulnerable customer segments.
 - Practical guidance on security measures customers can implement.

ii. Liability Framework: The scheme should establish clear principles for allocating liability in fraud scenarios:

Table 6: Liability scenarios

Scenario	Typical Liability Approach
Unauthorized Transactions (Account Compromise)	Participant liability unless customer negligence can be demonstrated (burden of proof on participant).
Authorized Push Payment Fraud (Social Engineering)	More complex determination based on whether the participant provided adequate warnings and whether the customer followed security guidance.
Technical Error or System Vulnerability	Liability typically rests with the participant or scheme responsible for the compromised system.
Merchant Fraud (Non-Delivery of Goods/Services)	Typically, outside the liability framework of the payment system, though consumer guidance should be provided.

.....

iii. **Fraud Recovery Processes:** Despite the immediate finality of instant payments, the scheme should establish procedures for attempting recovery in fraud cases:

- Rapid response protocols when fraud is reported, including immediate recipient bank notification.
- Processes for freezing funds in recipient accounts when legally permissible.
- Standardized information sharing protocols for fraud investigations.
- Coordination mechanisms with law enforcement agencies.

Fraud protection and liability frameworks should balance consumer protection with practical implementation considerations in African markets, recognizing variations in regulatory requirements, technical capabilities, and customer awareness levels.

F

Data Protection:

Strong data protection frameworks are essential for maintaining customer trust and complying with evolving privacy regulations.

i. **Data Protection Principles:** The scheme should establish fundamental principles for handling customer data:

- **Purpose Limitation:** Personal data should only be collected and processed for specified, explicit, and legitimate purposes related to payment processing and associated services. Secondary uses should require specific consent or another legal basis.
- **Data Minimization:** Only data necessary for the specific purpose should be collected and retained. Payment systems should avoid collecting excessive information not required for transaction processing or risk management.
- **Transparency:** Customers should receive clear information about how their data is collected, used, shared, and protected, with appropriate consent mechanisms for discretionary processing activities.
- **Security:** Appropriate technical and organizational measures must protect personal and financial data against unauthorized access, loss, or alteration throughout the data lifecycle.

ii. **Data Protection Requirements:** The scheme should establish specific requirements for participants:

- **Privacy Notices:** Clear, accessible information about data processing activities, presented in understandable language appropriate for varied literacy levels.
 - **Consent Management:** Mechanisms for obtaining and recording valid consent for discretionary processing, with appropriate options for consent withdrawal.
 - **Data Security:** Comprehensive controls protecting data during transmission, processing, and storage, including encryption, access controls, and monitoring systems.
 - **Data Retention:** Clear policies defining retention periods for different data types, with secure deletion or anonymization at the end of necessary retention.
 - **Data Subject Rights:** Procedures for handling access requests, correction requirements, and other data subject rights under applicable regulations.
-

.....

iii. **Data Sharing Governance:** The scheme should establish frameworks governing data sharing within the ecosystem:

- **Inter-Participant Sharing:** Clear rules for data sharing between participants for transaction processing, risk management, and dispute resolution.
- **Third-Party Processing:** Requirements for participant agreements with service providers who process customer data, ensuring equivalent protection levels.
- **Regulatory Disclosure:** Protocols for sharing data with regulatory authorities for compliance, oversight, and financial intelligence purposes.
- **Cross-Border Transfers:** Safeguards for transferring data across national borders, particularly relevant for regional payment systems.

iv. **Data Breach Management:** The scheme must establish comprehensive data breach response protocols:

- Clear definition of what constitutes a reportable data breach.
- Notification requirements and timelines for participants to report breaches to the scheme.
- Procedures for notifying affected customers and relevant authorities.
- Requirements for breach investigation and remediation.

_____ Data protection frameworks should align with relevant data protection regulations while recognizing practical implementation challenges in diverse markets.

Technical Infrastructure and Security

A

System Architecture

A robust, secure, and scalable technical architecture is the foundation of any successful instant payment scheme.

i. **Architectural Principles:** The scheme's technical architecture should be guided by fundamental principles:

- **Performance:** Architecture designed to deliver consistent low-latency transaction processing under varying load conditions.
- **Security:** A security-by-design approach with defense-in-depth and the principle of least privilege embedded at all levels.
- **Scalability:** Capacity to scale horizontally and vertically to accommodate growing transaction volumes and participant numbers.
- **Resilience:** Ability to maintain operations despite component failures, with no single points of failure in critical paths.

ii. **Core System Components:** The technical architecture typically includes several fundamental components:

- **Switching Infrastructure:** The central processing hub responsible for routing transactions between participants, applying scheme rules, and coordinating the end-to-end transaction lifecycle should include redundant processing capabilities with load balancing and automatic failover.
-

- **Settlement Engine:** The system component managing the settlement process, including calculation of positions, management of settlement windows, and interaction with the settlement institution, must maintain absolute data integrity with comprehensive reconciliation capabilities.
- **Participant Interfaces:** Communication gateways enabling participant connectivity to the central infrastructure, supporting defined message formats and security protocols, should accommodate varying participant technical capabilities.
- **Support Systems:** Auxiliary components providing essential functions such as participant management, fraud monitoring, reporting, billing, and administrative interfaces must integrate seamlessly with core processing components.

iii. **Deployment Models:** The scheme should consider appropriate deployment approaches based on local conditions:

- **On-Premises Deployment:** A traditional approach with dedicated physical infrastructure in controlled data centers, offering maximum control but requiring significant capital investment and specialized operational expertise.
- **Private Cloud:** Virtualized infrastructure deployed on dedicated resources, providing greater flexibility and resource optimization while maintaining strong control over the environment.
- **Hybrid Models:** A combination of on-premises critical components with cloud-based supporting systems, potentially offering an optimal balance for many African contexts.
- **Public Cloud:** Leveraging third-party cloud infrastructure for rapid deployment and cost-efficiency, though requiring careful security assessment and potential regulatory approval.

The chosen architecture should balance international best practices with practical considerations relevant to African markets, including infrastructure reliability, skills availability, and regulatory requirements.

B

Connectivity and Integration

Reliable, secure connectivity between participants and the central system is critical for instant payment scheme operation.

- i. **Connectivity Models:** The scheme should establish flexible connectivity options reflecting diverse participant capabilities.
- **Primary Connectivity:** Main connectivity channel for transaction processing:
 - Dedicated private network connections offering maximum security and reliability.
 - MPLS (Multiprotocol Label Switching) or similar managed network services with guaranteed quality of service.
 - Secure VPN tunnels over public internet where dedicated connections are not feasible.
 - End-to-end encryption regardless of underlying network infrastructure.

Connectivity and Integration

Reliable, secure connectivity between participants and the central system is critical for instant payment scheme operation.

i. **Connectivity Models:** The scheme should establish flexible connectivity options reflecting diverse participant capabilities.

- **Primary Connectivity:** Main connectivity channel for transaction processing:
 - Dedicated private network connections offering maximum security and reliability.
 - MPLS (Multiprotocol Label Switching) or similar managed network services with guaranteed quality of service.
 - Secure VPN tunnels over public internet where dedicated connections are not feasible.
 - End-to-end encryption regardless of underlying network infrastructure.

ii. **Backup Connectivity:** Redundant channels for business continuity:

- Independent secondary connections using different technologies and providers.
- Automatic failover mechanisms with minimal switching time.
- Regular testing of backup channels to ensure readiness.
- Alternative routing arrangements for critical transaction types.
- Dedicated private network connections offering maximum security and reliability.

iii. **Network Architecture:** The network infrastructure should incorporate multiple security layers:

- **Network Segmentation:** Logical separation of different functional domains with controlled interfaces between segments.
- **Defense in Depth:** Multiple security controls at different network layers, including firewalls, intrusion detection/prevention systems, and traffic filtering.
- **Secure Access Management:** Strictly controlled network entry points with comprehensive authentication, authorization, and audit mechanisms.
- **Traffic Monitoring:** Real-time monitoring of network traffic patterns with anomaly detection and alerting capabilities.

iv. **Integration Approaches:** The scheme should support multiple integration options for participants:

- **Direct API Integration:** API-based integration using standardized interfaces, enabling flexible, efficient system-to-system communication with comprehensive security controls.
- **Middleware Solutions:** Integration adapters or middleware components that translate between the scheme's messaging standards and participants' internal systems, simplifying integration for institutions with legacy systems.
- **Web Portal Access:** Web-based interfaces for smaller participants or those with limited technical capabilities, offering essential functionality through secure browser-based access.

.....

v. Integration Standards: The scheme should establish comprehensive integration standards:

- Detailed API specifications with complete documentation, reference implementations, and test environments.
- Consistent error handling and status reporting conventions across all interfaces.
- Version management procedures for managing API evolution while maintaining backward compatibility.
- Performance requirements, including response times, throughput capabilities, and availability expectations.

Connectivity and integration approaches should recognize the varying technical maturity of African financial institutions, providing accessible options for less sophisticated participants while enabling efficient integration for advanced institutions.

————

C Processing Capacity and Performance

Adequate processing capacity and consistent performance are essential for reliable instant payment services.

i. Capacity Planning: The scheme should implement structured capacity planning processes.

- **Baseline Capacity:** Initial capacity should accommodate projected transaction volumes with substantial headroom (e.g., 200-300% of expected peak volumes) to address unexpected growth and usage spikes.
- **Growth Projections:** Capacity planning should incorporate detailed growth projections considering factors such as participant onboarding, new use cases, seasonal variations, and market development initiatives.
- **Stress Testing:** Regular stress testing should validate system performance under extreme conditions, including sustained high volumes and sudden traffic spikes.
- **Scalability Planning:** Clear roadmaps for horizontal and vertical scaling should be established, with defined triggers for capacity expansions based on utilization thresholds and growth rates.

ii. Performance Requirements: The scheme should establish comprehensive performance standards. Annex 3 provides examples of performance metrics.

iii. Performance Optimization: The scheme should implement performance optimization strategies:

- **Efficient Architecture:** System design optimized for high-throughput transaction processing, with efficient data flows and minimal processing overhead.
 - **Resource Allocation:** Appropriate allocation and tuning of computing resources across different system components based on operational patterns.
 - **Caching Strategies:** Intelligent use of caching for frequently accessed data to reduce database load and improve response times.
 - **Database Optimization:** Database design and tuning focused on transaction processing efficiency, with appropriate indexing, partitioning, and query optimization.
-

.....

iv. Performance Monitoring: Comprehensive performance monitoring should be implemented:

- Real-time monitoring of key performance indicators across all system components.
 - Historical performance analysis to identify trends and patterns.
 - Automated alerting when performance metrics approach defined thresholds.
 - End-to-end transaction tracing to identify performance bottlenecks.
 - Regular performance reporting with detailed metrics and improvement recommendations.
- _____

D

Data Management

Effective data management is critical for maintaining transaction integrity, supporting operational needs, and meeting regulatory requirements.

i. Data Architecture: The scheme should implement a comprehensive data architecture:

- **Data Models:** Clearly defined data models for all critical information domains, with standardized structures, relationships, and validation rules.
- **Data Classification:** Structured classification of data based on sensitivity, criticality, and regulatory requirements, with appropriate handling requirements for each category.
- **Data Lifecycle:** Defined policies for data creation, storage, retention, archiving, and destruction aligned with business needs and regulatory requirements.
- **Data Integration:** Coherent approach to data sharing and synchronization between different system components and external interfaces.

ii. Database Management: Robust database systems are fundamental to instant payment operations:

- **Database Technology:** Selection of appropriate database technologies optimized for transaction processing, considering requirements for throughput, consistency, and availability.
- **High Availability:** Database architecture ensuring continuous operation despite component failures, potentially including clustering, replication, and automated failover.
- **Data Integrity:** Comprehensive mechanisms for maintaining data accuracy and consistency, including constraint enforcement, transaction management, and verification procedures.

iii. Data Security: Comprehensive data security controls must be implemented:

- **Access Controls: Granular data access management:**
 - Role-based access control
 - Principle of least privilege
 - Segregation of duties
 - Privileged access management
 - Regular access reviews
-

.....

- **Data Protection: Protective measures for data:**

- Encryption for data at rest
- Encryption for data in transit
- Secure key management
- Data masking for sensitive fields
- Secure disposal procedures

- **Data Retention and Archiving:** Clear policies for data lifecycle management:

- Retention periods defined for different data types based on operational needs and regulatory requirements.
- Structured archiving processes for data that must be retained but not frequently accessed.
- Secure, verifiable data destruction when retention periods expire.
- Data retrieval capabilities for archived information when needed for investigations or compliance.

Data management approaches should balance international best practices with practical considerations relevant to African markets, including infrastructure limitations, skills availability, and specific regional regulatory requirements.

E Security Requirements

Comprehensive security controls are essential for protecting the instant payment systems against evolving threats. This section outlines security requirements for the instant payment scheme.

i. Security Governance: The scheme should establish robust security governance structures.

- **Security Policy Framework:** Comprehensive policies covering all aspects of information security, aligned with international standards (e.g., ISO 27001) and adapted to payment system requirements.
- **Security Organization:** Clearly defined security roles and responsibilities, with appropriate segregation of duties and independent security oversight.
- **Risk Assessment:** Structured security risk assessment processes, including threat modeling, vulnerability assessment, and risk treatment planning.
- **Security Metrics:** Defined security performance indicators (see annex 3) with regular measurement and reporting to governance bodies.

ii. Technical Security Controls: The scheme must implement comprehensive technical security measures:

- **Perimeter Security:** Network boundaries protected by multiple defense layers.
 - **Network Security:** Secure network design with segmentation and traffic control.
 - **System Security:** Hardened infrastructure with minimal attack surface.
 - **Application Security:** Secure development practices and runtime protection.
 - **Data Security:** Protection for sensitive information at all stages.
-

.....

iii. **Cryptographic Requirements:** Strong cryptographic controls are fundamental to payment system security:

- **Encryption Standards:** Use of industry-standard encryption algorithms and appropriate key lengths for different security contexts.
- **Key Management:** Secure processes for cryptographic key generation, distribution, storage, rotation, and revocation.
- **Digital Signatures:** Implementation of non-repudiation mechanisms for critical transactions using digital signature technologies.
- **Secure Storage:** Protection of cryptographic materials using hardware security modules or equivalent controls.

iv. **Security Monitoring and Incident Response:** Comprehensive capabilities for detecting and responding to security events:

- **Security Monitoring:** Real-time monitoring of security events across network, system, and application layers, with correlation and analytics to identify potential threats.
 - **Threat Intelligence:** Integration of threat intelligence to enhance detection capabilities for emerging attack patterns.
 - **Incident Management:** Structured processes for security incident handling, including detection, classification, containment, eradication, recovery, and post-incident analysis.
- _____

F

Disaster Recovery

Robust disaster recovery capabilities are essential for ensuring business continuity in the face of significant disruptions. This section outlines disaster recovery frameworks for instant payment schemes:

i. **Disaster Recovery Strategy:** The scheme should establish a comprehensive disaster recovery strategy:

- **Risk Assessment:** Structured assessment of potential disaster scenarios that could impact system operations, including natural disasters, infrastructure failures, cyberattacks, and other major disruptions. The assessment should consider the specific risk landscape in relevant African regions.
 - **Recovery Strategy:** Overall approach to recovery, determining whether to implement hot, warm, or cold recovery sites, considering factors such as cost, complexity, and recovery time requirements. Given the critical nature of payment systems, hot or warm standby approaches are typically required.
 - **Network Redundancy:** Diverse network paths connecting to the recovery site, potentially using different carriers and technologies.
 - **Infrastructure Equivalence:** A recovery environment with processing capabilities equivalent to the primary environment or, at a minimum, sufficient to handle critical functions.
-

- **Recovery Objectives:** Clearly defined recovery targets, including Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for different system components. Critical payment functions typically require RTOs of less than 30 minutes and RPOs approaching zero data loss.
- **Recovery Priorities:** Defined sequence for system recovery, identifying the most critical functions that must be restored first, typically focusing on core transaction processing and settlement functions before administrative capabilities.

ii. **Disaster Recovery Infrastructure:** The scheme should implement appropriate recovery infrastructure.

- **Recovery Sites:** Geographically distributed alternative processing locations with sufficient separation to mitigate regional disasters yet close enough to manage effectively.

iii. **Data Replication:** Mechanisms for maintaining synchronized data between primary and recovery environments, with appropriate replication frequency based on RPO requirements.

Recovery Procedures: Detailed recovery procedures must be established:

- **Disaster Declaration:** Criteria and authority for formally declaring a disaster and invoking recovery procedures, with clear decision-making protocols.
- **Failover Execution:** Step-by-step procedures for activating the recovery environment, including technical operations and communication activities.
- **Operational Transfer:** Processes for transferring operations to the recovery site, including staff relocation or remote access arrangements.
- **Verification:** Procedures for confirming successful recovery, including system integrity checks and functional testing.

G

AI-Driven Fraud Management for Instant Payment Systems

i. Background

As instant payment systems (IPS) become increasingly embedded in daily financial activity, the need for advanced, real-time fraud detection is more critical than ever. The irrevocable nature and speed of instant payments heighten the risk exposure, making early detection and rapid response essential.

Traditionally, fraud detection relied on static rules, manual reviews, and post-transaction analysis. While effective in certain contexts, these legacy systems struggle to detect complex fraud patterns or adapt to evolving tactics such as social engineering and authorized push payment (APP) fraud.

The emergence of artificial intelligence (AI) and machine learning (ML) has revolutionized the fight against financial fraud. AI-powered systems can process large volumes of transaction data in real time, detect anomalies, learn from new fraud patterns, and enable predictive threat identification, all at the speed IPS demands.

While this Reference Guide remains technologically neutral, allowing implementers the flexibility to choose solutions suited to their context, the recommendation of AI-driven fraud management solutions is motivated by the unique challenges of instant payments, particularly their speed, irrevocability, and exposure to sophisticated fraud schemes.

As IPS expands to serve a broader, more inclusive user base, including previously underserved populations, fraud vectors such as social engineering, synthetic identity fraud, and coordinated network abuse are on the rise. These challenges necessitate more adaptive and intelligent approaches to fraud detection, beyond what traditional systems can offer.

ii. Use Cases of AI in Fraud Detection for IPS

AI can be applied across the entire transaction lifecycle in IPS to detect and prevent various types of fraud. Key use cases include:

- **Real-time Transaction Scoring:** Assigning risk scores to each transaction based on behavioral, contextual, and historical data.
- **Anomaly Detection:** Identifying out-of-pattern transactions that deviate from a user's typical behavior.
- **APP (Authorized Push Payment) Fraud Prevention:** Detecting indicators of manipulation, coercion, or unusual behavioral changes that may precede APP fraud.
- **Account Takeover Detection:** Monitoring access and authentication patterns to flag suspicious logins or device changes.
- **Synthetic Identity and Impersonation Fraud:** Using AI to detect fake accounts and bot-driven attacks.
- **Merchant and Agent Fraud:** Monitoring for unusual behavior such as abnormal settlement frequency, split transactions, or excessive refunds.
- **Network-level Fraud Detection:** Correlating fraud signals across participants to detect coordinated attacks or mule account networks.

iii. Why AI is Better Suited for Instant Payment Fraud Detection:

• Limitations of the Traditional Rule-Based Fraud Detection

Traditional fraud detection systems in payment ecosystems have primarily relied on rule-based mechanisms, predefined sets of conditions that trigger alerts or block transactions (e.g., transaction amount exceeding a threshold, activity from blacklisted IP addresses, or unusually high frequency within a short timeframe). While these systems have played an essential role in early fraud management, they present significant limitations in the context of real-time and increasingly sophisticated fraud typologies targeting IPS.

• Key Limitations of Traditional Rule-Based Approaches:

- **Static and Reactive:** Rule-based systems rely on known fraud patterns and predefined thresholds. They are inherently reactive and struggle to detect novel or evolving fraud tactics such as synthetic identity fraud or socially engineered APPs.
- **High False Positives:** Because rules are often broad to ensure caution, many legitimate transactions get flagged unnecessarily. This leads to user frustration, operational inefficiencies, and reputational risk for providers.
- **Maintenance Burden:** Updating and fine-tuning rule sets requires constant human intervention and expert input. This leads to increased operational costs and slow adaptation to emerging threats.
- **Lack of Contextual Understanding:** Rule engines typically evaluate transactions in isolation. They are unable to consider complex patterns over time, behavioral profiles, or relationships across entities.
- **Scalability Challenges:** As transaction volumes grow, rule systems become harder to manage without introducing inefficiencies, redundancy, or system latency.

• **Capability of the AI-driven Fraud Management Platform**

AI-driven solutions offer a proactive, dynamic, and scalable alternative that aligns with the real-time, high-volume, and trust-dependent nature of IPS. The key advantages include:

- **Behavioral Risk Modeling:** AI evaluates transactions in the context of a user's historical behavior, enabling personalized risk assessment that rules cannot deliver.
- **Adaptive Learning:** AI models continuously learn from new data and feedback (fraud labels, customer disputes, transaction outcomes), enabling quicker adaptation to emerging fraud tactics.
- **Multidimensional Analysis:** AI can simultaneously assess hundreds of features such as device metadata, transaction velocity, geolocation patterns, and peer-to-peer relationships within milliseconds.
- **Lower False Positives, Higher Detection Rates:** By identifying subtle, nonlinear patterns, AI significantly reduces false positives while improving true fraud detection accuracy.
- **Real-Time Scalability:** AI platforms are built to operate at massive scale without degrading performance, making them suitable for national IPS platforms with high throughput demands.

It is important to note that AI does not necessarily replace rules-based systems. In practice, hybrid models are often adopted, where AI models score transactions, and business rules guide final decisions, especially for regulatory compliance, alert prioritization, or specific risk policies.

iv. **Solution Architecture Overview**

An AI-driven fraud detection platform for IPS typically includes the following components:

- **Data Ingestion Layer:** Aggregates transaction data, device metadata, behavioral signals, and third-party risk indicators in real-time.
- **Feature Engineering Engine:** Transforms raw data into meaningful attributes for modeling, such as transaction velocity, geolocation anomalies, and device fingerprinting.
- **Model Scoring Engine:** Applies trained AI/ML models to assess transaction risk in milliseconds.
- **Decision Engine:** Uses model outputs and business rules to determine actions, e.g., approve, hold, or decline transactions.
- **Alert & Investigation Module:** Generates alerts for flagged transactions and provides explainability for analysts.
- **Feedback & Learning Loop:** Continuously updates models with outcomes to improve detection accuracy.

The platform may be hosted centrally by the IPS operator (e.g., scheme-level AI fraud service) or deployed within participants' environments with data-sharing arrangements under a federated model.

v. **Success Factors for Implementing AI-Driven Fraud Solutions**

The successful deployment of AI-driven fraud detection in instant payment systems depends not only on technical capabilities but also on ecosystem readiness, governance maturity, and data stewardship. The following prerequisites and success factors should be considered by scheme managers, system operators, and participants before or during implementation:

Success Factor	Description
Data Quality & Availability	AI models require large volumes of accurate, timely, and well-structured data for effective training, scoring, and learning.
Data Sharing and Interoperability Frameworks	Effective fraud detection often requires real-time data sharing among participants. Secure APIs, shared intelligence layers, and data anonymization techniques support this.
Skilled Human Capital	Specialized skills are needed in data science, fraud analytics, compliance, and AI model management. Institutions should invest in continuous capacity-building and cross-functional collaboration.
Model Governance and Regulatory Compliance	Institutions must adopt model risk management frameworks covering validation, explainability, fairness, and compliance with data protection laws.
Real-Time Integration and System Readiness	AI fraud systems must be seamlessly integrated with the IPS transaction flow, supporting real-time decisioning without degrading user experience or performance.
Risk Appetite and Threshold Calibration	Participants must define acceptable risk levels and set transaction blocking, alerting, or escalation thresholds accordingly.
Ongoing Learning and Feedback Loops	Effective fraud detection depends on continuous learning from confirmed fraud cases, false positives, and user feedback to improve model accuracy.

vi. Scheme Rule Considerations

To ensure the effective and coordinated implementation of AI-based fraud detection solutions across all participants, the instant payment scheme rules should incorporate clear provisions addressing governance, obligations, data sharing, accountability, and technical standards. These provisions help drive consistent fraud responses, ecosystem-wide learning, and alignment with regulatory and ethical expectations.

Key Considerations Include:

- **Minimum Fraud Management Standards:** Define baseline capabilities expected of participants, such as real-time screening, use of adaptive fraud detection tools, and periodic updates of detection models based on emerging threats.
- **Roles and Responsibilities:** Clarify the responsibilities of the scheme manager, system operator, and participants in fraud detection, investigation, model updates, and response coordination.

- **Real-Time Screening Requirements:** Mandate or recommend that participants implement real-time fraud screening mechanisms, enabling timely flagging and blocking of suspicious transactions.
- **Data Sharing and Privacy:** Specify categories of permissible data (e.g., behavioral, transactional, device-based) for fraud analytics and outline secure data-sharing protocols across participants. Provisions must align with applicable privacy and data protection laws, enabling cross-institutional intelligence without compromising user rights.
- **Model Governance:** Require documentation of model architecture, logic, thresholds, validation procedures, and periodic performance reviews. Models must be explainable and auditable to ensure fairness, prevent discriminatory outcomes, and support regulatory oversight.
- **Fraud Reporting and Escalation:** Mandate standardized reporting of fraud incidents, including timeliness, format, and content. Define escalation procedures for high-impact or systemic fraud cases requiring centralized coordination.
- **SLAs for Fraud Flagging and Blocking:** Establish minimum performance benchmarks for fraud detection and mitigation actions, such as latency limits for scoring and blocking suspicious transactions within milliseconds to preserve the real-time nature of the system.
- **Liability Framework:** Define how liability is allocated in cases of fraud-related losses, especially distinguishing between centralized fraud management models (operated by the scheme or central system) and participant-level models. This includes clarity on false positives, detection gaps, and user redress processes.
- **Incentives and Sanctions:** Provide mechanisms for rewarding institutions that demonstrate strong fraud control performance (e.g., fewer incidents, effective model management) and penalizing those failing to meet minimum standards or compliance obligations.
- **Hybrid Decisioning Approaches:** Recognize that AI models may be best used in combination with rule-based systems, particularly for regulatory compliance, exception handling, or policy enforcement. Scheme rules may recommend this hybrid architecture as a best practice.
- **Capacity Building and Certification:** Promote regular training and professional development for fraud analysts, AI model developers, and risk teams. Where applicable, require certification or qualification standards for operating AI-based fraud detection systems.
- **Collaboration and Feedback Loops:** Encourage mechanisms for participant collaboration, including joint intelligence platforms, fraud typology sharing, and structured feedback loops to retrain AI models and improve system-wide fraud resilience.

User Experience Guideline

The scheme should issue a user experience (UX) guideline that provides foundational standards for participants developing user-facing applications and services within the instant payment ecosystem. Adhering to these principles and obligations will ensure a consistent, secure, and user-friendly experience, thereby fostering user trust and accelerating adoption across the ecosystem.

Foundational Principles

User-facing applications and services within the instant payment scheme should be built upon the following core principles:

- **User-Centricity:** Design decisions must prioritize understanding and solving real user needs and pain points related to instant payments. User research and feedback should inform all stages of development.
- **Accessibility:** Payment services must be designed to be usable by individuals with diverse abilities and in various contexts (e.g., varying levels of digital literacy, different device capabilities, and environmental conditions).
- **Usability:** Interfaces must be intuitive, easy to navigate, and require minimal learning. Clear information architecture, consistent design patterns, and user-friendly workflows are essential.
- **Usefulness:** Features and functionalities offered must meet genuine user needs and provide tangible value in the context of instant payments. Avoid implementing features that are technically complex but offer limited practical benefit.
- **Credibility and Desirability:** User interfaces and communication must build trust through reliable information, transparent processes, and an appealing design that aligns with the scheme's brand and values.
- **Consistency:** A coherent and predictable user experience must be maintained across all touchpoints, including different devices, channels, and applications offered by participants. Consistent design language, terminology, and workflows are crucial.

Guidance to Participants

Participants developing user-facing applications and services for the instant payment scheme should adhere to the following obligations:

A

Application Design and Navigation:

A well-designed application interface is essential for delivering a seamless and inclusive user experience. Participants must ensure that their digital channels are intuitive, coherent, and accessible across all user devices. **The following principles should be applied:**

- **Intuitive Navigation:** Applications must provide clear and consistent navigation pathways, allowing users to easily locate and access core functionalities such as initiating payments, viewing transaction history, and managing account details.

Application Design and Navigation:

A well-designed application interface is essential for delivering a seamless and inclusive user experience. Participants must ensure that their digital channels are intuitive, coherent, and accessible across all user devices. **The following principles should be applied:**

- **Intuitive Navigation:** Applications must provide clear and consistent navigation pathways, allowing users to easily locate and access core functionalities such as initiating payments, viewing transaction history, and managing account details.
- **Clarity and Simplicity:** Information must be presented using simple language and a concise format. Technical jargon should be avoided or clearly explained to promote understanding across a broad user base, including those with limited financial or digital literacy.
- **Responsive Design:** User interfaces must adapt seamlessly to a range of devices and screen sizes (e.g., smartphones, tablets, desktops), ensuring consistency and usability across platforms.
- **Visual Coherence and Branding:** The application's visual design should be clean and uncluttered. Participants should align with the scheme's branding and accessibility guidelines to promote familiarity and trust.
- **Guided User Flow and Feedback:** Clear visual cues (e.g., progress indicators, confirmation messages, error highlights) must guide users through the payment journey, from initiation to completion. Feedback mechanisms should be immediate and informative, helping users understand system responses or required actions.
- **Inclusivity Considerations:** Participants must ensure that application design, communication channels, and service delivery approaches are inclusive of underserved populations, particularly women and users in rural or remote areas. To this end:
 - Usability testing should incorporate gender and rural representation to ensure solutions are practical for all demographics.
 - Interfaces and communications should support local languages and reflect cultural contexts.

B

Agent networks or assisted digital channels should leverage multiple methods for initiating instant payments to cater to diverse user preferences and scenarios, including:

- **Account Number Input:** Allowing users to manually enter the recipient's account number. Clear guidance on the required format should be provided.
- **Proxy Lookup and Selection:** Seamless integration with the scheme's proxy directory service, enabling users to search and select recipients using their registered aliases (mobile number, email, national ID, etc.). Clear display of the recipient's verified name (where available) is required.
- **QR Code Scanning:** Functionality to scan QR codes generated by recipients for payment initiation. Clear visual cues and instructions for scanning should be provided.

C

User Communication Standards:

All user-facing communication related to instant payments **must** adhere to the following standards:

- **Success, Error, and Guidance Messages:**
 - Provide clear and concise messages confirming successful transactions.
 - Display informative and actionable error messages that help users understand and resolve issues. Avoid technical error codes.
 - Offer contextual guidance and tips to assist users throughout the payment process.
 - To increase physical reach.
 - Digital skills training or simplified user modes should be considered to support users with limited digital proficiency.

D

Payment Initiation Methods:

Participants' applications **must** offer users:

- **Mandatory Nomenclature:** Participants must use the standard terminology defined by the instant payment scheme for key actions, statuses, and features to ensure consistency across the ecosystem.
- **Notification of Suspicious Transactions:** Implement clear and timely mechanisms to notify users of potentially suspicious transactions and guide them on necessary actions (e.g., verification, reporting).
- **Credit Usage Notifications (if applicable):** If a participant supports credit-based instant payments, clear and timely notifications regarding credit usage, limits, and repayment terms must be provided.

E

Transaction Notifications:

To ensure transparency and keep users informed, participants must implement robust notification mechanisms for all instant payment activities:

- Users **must** receive timely notifications for all initiated and received instant payment transactions.
- Notifications should include essential details such as the counterparty (name/proxy), amount, date and time, and transaction status.
- Participants should offer users customizable notification preferences (e.g., push notifications, SMS, email).
- Notifications should be clear, concise, and easily understandable.

F

Proxy-Based Payments

To improve user convenience and minimize the need for account numbers, Participants should be required to fully integrate with the scheme's proxy directory service, enabling comprehensive proxy functionality:

- Seamless integration for user registration, management, and utilization of preferred proxies for sending and receiving payments.
- An intuitive proxy registration process that mandates explicit user consent.
- Clear communication to users regarding the advantages and security features of proxy usage.
- User-friendly tools for viewing, modifying, and deregistering their linked proxies.

G

Recipient Verification

To minimize misdirected payments and build user trust, participants must implement effective recipient verification mechanisms during the payment process:

- **Verified Name Display:** Show the verified name associated with a proxy (where available) during proxy-based transactions to confirm recipient identity.
- **Confirmation Screens:** Provide users with a clear summary of recipient details (e.g., name, proxy/account number) before authorizing a payment.
- **Risk Warnings:** Clearly alert users about the risks of sending payments to unverified recipients, especially in cases where proxy validation is unavailable.

H

QR Code Payments

QR code functionality enables seamless face-to-face or remote transactions. Applications must ensure a smooth and secure QR experience by adhering to the following:

- Provide a reliable and intuitive interface for scanning QR codes to initiate payments.
- Include clear, step-by-step instructions on how to scan and complete QR-initiated transactions.
- Before confirming the transaction, display critical details such as the recipient name and amount (if pre-encoded in the QR).
- Allow users to generate their own QR codes for receiving payments, with options to encode fixed or editable amounts and descriptions.

I

Transaction Receipts and History

Comprehensive payment records are essential for transparency and issue resolution. Participants must:

- Provide a searchable, easy-to-navigate transaction history, accessible within the application.
- Include key transaction details: date, time, amount, recipient (name/proxy/account), status, and a unique reference number.
- Offer options for users to generate and share transaction receipts (e.g., PDF download, email sharing).
- Ensure long-term access to historical data within reasonable retention limits.

J

Customer Support and Issue Resolution

Responsive customer support is critical for maintaining user trust. Participants are required to:

- Ensure support is easily accessible within the app via FAQs, help sections, chat, contact forms, or phone support.
- Clearly display support response time expectations and escalation processes.
- Establish transparent dispute resolution mechanisms for failed or incorrect transactions, and communicate these to users.
- Provide multilingual support where applicable to accommodate local user bases.

K

Security and Authentication:

Security is a cornerstone of user confidence. Participants must implement strong, proportional safeguards:

- Proportional Security Measures: Tailor security levels to transaction risk (e.g., higher-value transactions may require stronger authentication).
- Fraud Detection and Prevention: Utilize real-time monitoring and AI-driven analytics to detect and prevent fraudulent behavior.
- Transaction Cancellation During Review: Allow users to cancel payments that are flagged and placed under review, where supported by scheme rules.
- Authentication Methods: Implement secure yet user-friendly authentication options (e.g., PIN, biometric, password, OTP, or MFA).
- Transaction Limits: Communicate applicable transaction limits clearly and allow users to manage limits where allowed.

L

Multi-Channel Consistency:

For participants offering services across different platforms (mobile, web, USSD, etc.), the user experience must remain consistent:

- Use unified design language, terminology, and workflows across all channels to reduce user confusion.
- Where differences are unavoidable (e.g., limited features on USSD), these must be clearly explained to users.
- Ensure feature parity across channels to the extent possible and appropriate.

5.6 Branding Guidelines

To build a trusted, recognizable, and inclusive brand identity for an instant payment system, each scheme should adopt a unified branding approach grounded in clear principles. The following are high-level branding guidelines that every IPS should integrate into its governance, operations, and participant communications.

A

Brand Value and Identity: The scheme should mandate that the IPS brand embodies four core values: **Instant, Available, Affordable, and Easy**. These values must be clearly communicated through all visual, verbal, and experiential touchpoints of the system. They reflect the essence of instant payments and are critical to fostering public trust and widespread adoption. The scheme should ensure that this brand personality resonates with all users, individuals, businesses, and public institutions, and promote the system as a secure, modern, and inclusive financial service.

B

Brand Mark: The scheme should provide a complete and standardized **brand mark**, composed of a distinctive symbol representing technology and financial transactions, a custom logotype designed exclusively for the system, and a message identifying the authority backing the scheme (e.g., a central bank or national regulator).

It should mandate three permissible formats for applying the brand: (1) the full version with symbol, logotype, and message, (2) a digital-friendly version combining the symbol and logotype, and (3) a compact version featuring the symbol only, reserved for mobile icons and constrained interfaces. Use of the logotype alone should be prohibited to preserve the brand's recognisability and integrity.

C Proportions: To maintain consistent visual presentation across media and platforms, the scheme should provide exact specifications for proportions, layout, minimum sizes, and clear space requirements. These rules ensure that the brand remains legible and professional in both print and digital formats. The scheme should mandate the use of official brand files only and prohibit participants from redrawing, modifying, or distorting the brand elements in any way.

D Color Palette: The scheme should also establish a primary color palette that visually communicates trust, innovation, and accessibility. This palette must include a main brand color, a complementary tone, and a neutral base, all culturally appropriate and distinctive within the African context.

E Brand Coexistence and Partner Usage: When the IPS brand is presented alongside other payment methods in signage or promotional materials, the scheme should mandate equal prominence and visual alignment. The IPS brand must be displayed at the same size and frequency as other payment options, following strict alignment rules, both horizontal and vertical, to avoid visual crowding or misrepresentation. This ensures that the IPS is always recognized as a legitimate and universal payment option.

F Derivative Branding: For systems offering derivative services such as QR-based payments or agent cash-out, the scheme should establish clear branding rules. All derivative brands must maintain visual coherence with the primary brand while using distinct colors and labels for each function. Typography and proportions must follow a consistent design system. The scheme should centralize the creation and approval of derivative brands, explicitly prohibiting participants from developing their own sub-brands.

G Brand Name Usage and Messaging: The IPS brand name must be used correctly in all written and spoken contexts. The scheme should provide a set of approved public-facing key messages (e.g., "Make a payment" and "Pay anytime, any day, in seconds") to support consistent communications across all stakeholders.

H Communication and Education Standards: To preserve brand integrity, the scheme should prohibit any form of advertising or messaging that confuses the public or implies that the IPS is exclusive to a single institution. All participants must clearly convey that the payment system is a shared, public-good infrastructure. The scheme should also provide recommended terminology tailored for different audiences: simple, user-friendly terms for the public; operational terms for merchants; and more technical language for specialist audiences.

I Brand Governance and Licensing: The scheme should establish the IPS brand as the exclusive property of the scheme manager, granting participants a limited, revocable license for use. It must mandate brand presence in all physical and digital media related to the payment system and require that branding be installed in high-visibility locations. Any deteriorated physical assets (e.g., signage) must be replaced promptly. These measures help safeguard the brand's reputation and reinforce its role as a symbol of safe, accessible, and reliable digital finance for all.

Compliance Monitoring Framework

An effective compliance monitoring framework ensures that participants maintain adherence to scheme rules and requirements throughout their participation lifecycle. This framework helps identify and address compliance issues before they create significant risks to the system or other participants.

A

Monitoring Approaches:

- **Self-Certification:** Regular attestations from participants regarding their continued compliance with key requirements (see annex).
- **Data Analysis:** Review of operational metrics, transaction patterns, and performance data to identify potential compliance issues.
- **Targeted Reviews:** Focused assessments of specific compliance areas based on risk indicators or scheduled review cycles.
- **Comprehensive Audits:** Periodic in-depth evaluations of overall compliance status, potentially involving on-site visits or third-party assessors.

B

Monitoring Dimensions

The monitoring framework should address all key aspects of participant obligations, including:

- Financial requirements and settlement performance
- Operational reliability and service level adherence
- Technical standards compliance and security controls
- Risk management effectiveness
- Regulatory compliance and customer protection

The intensity and frequency of monitoring activities should follow a risk-based approach, with greater scrutiny applied to higher-risk participants or those with previous compliance issues. The framework should include clear escalation procedures for addressing identified concerns, ranging from informal guidance for minor issues to formal remediation plans for significant deficiencies.

The scheme should maintain transparent documentation of monitoring approaches, evaluation criteria, and potential consequences of non-compliance. Regular reporting on aggregate compliance trends and anonymized case studies can help all participants better understand expectations and improve their own compliance practices.



Executive
Summary

1

Introduction

2

Guiding Approach
to Scheme Rules
Development

3

The Legal
Framework of
Instant Payment
Schemes

4

Core Components
of Participation
Agreements

5

Core Components
of the Scheme
Rules



6

PRICING POLICY

7

Education
and Awareness
Framework

8

Conclusion and
Path Forward

9

Annexes



6.1

Core Principles for Inclusive Pricing

A truly inclusive instant payment pricing policy must be built upon fundamental principles that ensure the system serves all segments of society while remaining financially viable. **These core principles should guide all pricing decisions and policy development:**

- **Affordability:** Pricing must be set at levels that do not exclude low-income or vulnerable populations. The cost to end-users should be proportionate to their financial capacity, with special considerations for those at risk of financial exclusion.
- **Transparency:** All fees and charges must be clearly disclosed to all participants in simple, understandable terms. Hidden costs and complex fee structures may undermine trust and adoption.
- **Sustainability:** The pricing model must ensure the long-term financial viability of the system, covering operational costs, ongoing maintenance, and future investments in technology and security.
- **Incentivizing Adoption:** Pricing should encourage participation from all stakeholders, including financial institutions, merchants, and consumers, potentially using promotional pricing during initial rollout phases.

These principles should not be viewed in isolation but rather as interconnected elements of a cohesive pricing strategy. The tension between affordability and sustainability, for instance, requires careful balancing to ensure that the system remains inclusive without compromising its long-term viability.

6.2

Pricing Models for Instant Payments

Several pricing models can be implemented for instant payment systems, each with distinct implications for financial inclusion, market adoption, and system sustainability. The selection of an appropriate model should be guided by market conditions, policy objectives, and the maturity of the payment ecosystem. **Below is an overview of the primary pricing models applicable to instant payment systems.**

A

Processing Fee Models

Processing fees are charges imposed by the payment system operator on participating financial institutions and payment service providers for executing, clearing, and/or settling instant payment transactions. While these fees are not directly visible to end users, they significantly influence the cost structure of the system and can affect end-user pricing.

Several processing fee models are commonly used, each aligned with different policy goals and institutional contexts:

- **Cost-Recovery Model:** Fees set to recover the operational costs of the central infrastructure without generating profit. This approach focuses on system sustainability rather than commercial returns, often employed in public infrastructure models. It requires transparent cost accounting and regular review to ensure continued alignment with actual operational expenses.

- **Utility Pricing Model:** Treats the payment system as a public utility with regulated pricing. Fees are determined through regulatory processes that balance system sustainability with public interest objectives. This model typically involves significant oversight and may include cross-subsidization between different services or user segments.
- **Volume-Based Pricing:** Offers discounted per-transaction fees for higher volumes, incentivizing greater usage. This approach can drive adoption while reflecting the economies of scale in payment processing. It must be carefully structured to avoid disadvantaging smaller institutions that may have lower transaction volumes.
- **Subscription/Membership Model:** Charges fixed periodic fees for participation in the system, potentially with additional per-transaction fees. This model provides predictable revenue for system operators and can reduce per-transaction costs for high-volume participants. It may include different tiers based on institution size or expected usage.

The selection of processing fee models should consider market structure, policy objectives, and the institutional framework of the payment system. In many successful instant payment implementations, processing fees evolve over time, often starting with subsidized or minimal fees to encourage adoption before transitioning to more sustainable models as transaction volumes increase.

B

Interchange Fee Models

Interchange fees are payments made between financial institutions, typically from the receiving (acquiring) institution to the sending (issuing) institution to compensate for the costs of processing and risk management in a transaction. While interchange is most commonly associated with card-based systems, some instant payment systems may incorporate similar fee mechanisms to balance commercial incentives between participants.

- i. **Zero Interchange:** No interchange fees between participating institutions.
 - Simplifies the fee structure and reduces settlement complexity
 - Creates a balanced ecosystem where all participants bear their own costs
 - May not adequately compensate sending institutions for their investments and risks
- ii. **Fixed Interchange:** Set fee per transaction paid between institutions, regardless of transaction value.
 - Provides predictable compensation for sending institutions
 - Simple to implement and understand
 - May not reflect the varying costs associated with different transaction types
- iii. **Variable Interchange:** Fees that vary based on transaction type, amount, or other parameters.
 - Can be tailored to reflect different cost structures and risk profiles
 - Allows for more nuanced incentive structures
 - Increases complexity and may create market distortions

When considering interchange for instant payments, it's important to recognize fundamental differences from card systems. Instant payments typically have lower fraud rates, different risk profiles, and distinct value propositions compared to cards. Therefore, interchange models should be specifically designed for instant payment characteristics rather than simply adopting card-based approaches.

.....

In many instant payment systems, particularly those focused on financial inclusion, zero or minimal interchange is preferred to reduce overall system costs and simplify implementation. However, some form of interchange may be necessary to incentivize participation and investment, especially in markets with significant imbalances between sending and receiving institutions.

————

C End-User Fee Models

End-user fees are the charges directly paid by consumers and businesses when using instant payment services. These fees are a critical component of the overall pricing strategy, as they directly influence user behavior, adoption rates, and long-term engagement. Designing end-user fees with clarity, fairness, and inclusivity in mind is essential to achieving widespread usage—particularly in low-income and underserved segments. The following are the main fee models commonly applied in instant payment systems:

i. **Fixed Fee Structure:** A single, flat fee is charged per transaction, regardless of the amount being transferred.

- **Advantages:**

- **Simplicity:** Easy for users to understand, every transaction costs the same, which helps build trust and reduces confusion.
- **Predictability:** Users know in advance what they will be charged, allowing for easier budgeting.
- **Ease of Implementation:** Operationally straightforward for providers to manage, track, and audit.

- **Disadvantages:**

- **Regressive Impact:** The same fee on both high- and low-value transactions means small-value payments incur a proportionally higher cost.
- **Usage Deterrence:** May discourage users from conducting frequent or everyday micro-transactions, especially among lower-income groups.

- **Application Context:**

- Most effective in markets where most transactions fall within a narrow value range or where instant payments are used mainly for medium- to high-value transfers.

ii. **Percentage-Based Structure:** The transaction fee is calculated as a fixed percentage of the transaction amount.

- **Advantages:**

- **Equity in Pricing:** The fee adjusts according to transaction size, making it more affordable for low-value users.
- **Encourages Inclusion:** By keeping costs lower for small transactions, it supports usage among lower-income or financially vulnerable users.
- **Revenue Alignment:** Provider revenue scales naturally with transaction size, aligning with usage value.

- **Disadvantages:**

- **High-Value Disincentive:** As transaction amounts grow, so does the fee, potentially deterring larger transfers.
-

- **Lack of Transparency:** Users may not know the final cost until after the transaction value is entered, which may reduce confidence and trust.
- **Application Context:**
 - Suitable for diverse economies with wide transaction value ranges. It can be attractive for promoting usage in early stages.
- **Disadvantages:**
 - **High-Value Disincentive:** As transaction amounts grow, so does the fee, potentially deterring larger transfers.
 - **Lack of Transparency:** Users may not know the final cost until after the transaction value is entered, which may reduce confidence and trust.

iii. Tiered Fee Structure: Transaction fees are assigned based on defined value ranges, with each tier applying a different flat or percentage rate.

- **Advantages:**
 - **Balanced Approach:** Provides a middle ground between the predictability of fixed fees and the fairness of percentage-based models.
 - **Market Customization:** Fee levels can be tailored to accommodate different segments (e.g., individuals, small businesses, government-to-person payments).
 - **Supports Both Affordability and Cost Recovery:** Encourages small-value use while ensuring that high-value transactions contribute adequately to system sustainability.
- **Disadvantages:**
 - **Communication Complexity:** More difficult to explain to users, especially those with low financial or digital literacy.
 - **Behavioral Thresholds:** Users may intentionally limit transaction values to remain within lower tiers, which can distort natural transaction flows.
- **Application Context:**
 - Well-suited for mature or transitioning markets with diverse users and payment use cases. It allows for flexible adaptation to shifting payment volumes and user preferences.

iv. Key Considerations in End-User Fee Design

When implementing any end-user fee structure, it is essential to determine **who bears the cost**—the sender, the receiver, or both. Many inclusive payment systems follow a **“sender-pays” model**, ensuring that receiving funds is always free to encourage widespread adoption among individuals and small merchants. Additionally, targeted measures such as **fee waivers, subsidies, or tier-specific discounts** can be employed to support vulnerable groups or promote usage during early adoption phases. These strategies not only enhance financial inclusion but also help build transaction volume and trust, paving the way toward long-term system sustainability.

6.3

Key Elements to Consider in the Scheme Rules

This section outlines the essential components for creating a robust framework for pricing within instant payment systems. It covers how fees are set, disclosed, calculated, and enforced, ensuring fairness and transparency for all participants and end-users.

A

Pricing Governance

Scheme rules should establish clear processes and responsibilities for setting, reviewing, and adjusting fees.

- **Pricing Governance Structure:** The scheme rules should define the governance bodies responsible for pricing decisions, including their composition, authority, and decision-making processes. This typically includes a dedicated pricing committee with representation from diverse stakeholders, including smaller institutions serving underserved communities.
- **Fee Review Mechanisms:** Rules should establish regular review cycles for all fee components, with clear criteria for evaluation. These reviews should consider system costs, market conditions, participant feedback, usage patterns, and financial inclusion impacts. The process should include consultation with stakeholders and transparent communication of findings.
- **Fee Change Procedures:** The rules should outline the process for implementing fee changes, including notice periods, communication requirements, and implementation timelines. This provides predictability for participants and allows them to adjust their business models and customer offerings accordingly.
- **Dispute Resolution for Pricing Issues:** Mechanisms should be established for addressing disputes or concerns related to fee application or calculation. This includes clear procedures for raising issues, timeframes for resolution, and escalation paths if needed.

B

Fee Disclosure Requirements

The scheme rules should establish comprehensive disclosure requirements that ensure all participants understand their obligations and rights regarding fees.

- **Participant Disclosure Requirements:** Rules should specify what fee information participating institutions must disclose to the scheme operator, including their end-user fee structures, any surcharges, and special arrangements. This enables monitoring of compliance with scheme principles and assessment of the overall fee landscape.
- **Consumer Disclosure Standards:** The scheme should establish minimum standards for how fees are disclosed to end-users, including timing, format, and content requirements. These standards should ensure that consumers receive clear, understandable information about fees before initiating transactions.
- **Fee Comparison Requirements:** Rules may require standardized formats for fee disclosure that facilitate comparison across providers. This promotes competition and helps users identify the most cost-effective options for their needs.
- **Fee Change Notification Standards:** The scheme should establish minimum notice periods and communication requirements for fee changes. This includes both notifications from the scheme to participants and from participants to end-users.

C Fee Calculation and Collection

Scheme rules should establish standardized approaches that minimize administrative burden while ensuring accurate and timely fee processing.

- **Fee Calculation Methodologies:** Rules should define precise methodologies for calculating each type of fee, including the data points used, calculation formulas, rounding conventions, and handling of special cases. These methodologies should be documented in detail to ensure consistent application.
- **Billing Cycles and Processes:** The scheme should establish standard billing periods, invoice formats, and payment terms for all fee types. This includes specifying whether fees are collected in real-time, daily, weekly, or monthly, and through what mechanisms (e.g., direct debit, separate settlement process).
- **Reconciliation Procedures:** Rules should outline processes for participants to verify fee calculations, raise discrepancies, and resolve billing issues. This includes access to transaction data and fee calculation details to support reconciliation.
- **Fee Distribution Mechanisms:** For interchange and shared fees, the scheme must establish clear procedures for distributing collected fees among participants. This includes timing, notification requirements, and handling of exceptions.

D Compliance and Enforcement:

Scheme rules should establish robust compliance mechanisms and appropriate enforcement measures for pricing-related requirements.

- **Fee Monitoring Framework:** Rules should establish systematic monitoring of participant fee practices, including regular reporting requirements, spot checks, and analysis of transaction data. This monitoring should verify compliance with scheme rules and identify potential issues such as excessive fees or discriminatory practices.
- **Violation Categories and Penalties:** The scheme should define different categories of pricing violations based on their severity, frequency, and impact on users or system integrity. Corresponding penalties should be established for each category, ranging from warnings to financial penalties or, in extreme cases, suspension from the system.
- **Investigation Procedures:** Clear processes should be defined for investigating suspected pricing violations, including information gathering, participant rights, timeframes, and decision-making authority. These procedures should ensure fairness while allowing for the timely resolution of issues.
- **Appeal and Remediation Processes:** Participants should have defined pathways to appeal compliance decisions and implement remediation plans for addressing violations. This includes clear criteria for successful remediation and processes for monitoring ongoing compliance.



Executive
Summary

1

Introduction

2

Guiding Approach
to Scheme Rules
Development

3

The Legal
Framework of
Instant Payment
Schemes

4

Core Components
of Participation
Agreements

5

Core Components
of the Scheme
Rules

6

Pricing Policy

7

EDUCATION AND AWARENESS FRAMEWORK

8

Conclusion and
Path Forward

9

Annexes



7.1

Purpose

Education and awareness are critical enablers for the successful implementation, adoption, and sustained use of an IPS. This section sets out the guidelines for developing and delivering education and training programs to ensure that all stakeholders, ranging from agents, merchants, and biller networks to end users (consumers, small businesses, and public-sector payees), have the knowledge and capacity to interact confidently and responsibly with the IPS.

The objective of this framework is to:

- Promote informed and inclusive participation in the IPS ecosystem.
- Support stakeholder readiness and operational excellence.
- Build public trust in instant payments through improved digital literacy and fraud awareness.
- Advance financial inclusion, particularly among underserved and vulnerable populations.

7.2

Key Learning Areas

Educational initiatives should be tailored to the audience, but generally cover the following themes:

Themes	Key Activities
IPS Fundamentals	• Definition and core features of instant payments (24/7/365, real-time, irrevocable). • Common use cases (e.g., P2P, P2B, G2P, B2B, bill payments, cash-in/out). • Benefits for users, businesses, and the broader economy.
Roles and Responsibilities	• Institutional responsibilities of the scheme manager, operator, and participants. • Regulatory and compliance obligations. • Overview of transaction flow, settlement, and scheme governance.
Customer Onboarding and Proxy Use	• KYC/KYB procedures and inclusive onboarding practices. • Use of proxy identifiers and their limitations (e.g., no personal/sensitive data embedded). • Data privacy and consent management expectations.

Themes	Key Activities
Transaction Journey	- Initiating, receiving, and confirming payments. - Handling errors or failed transactions. - Understanding transaction costs, limits, and timelines.
Fraud Risk and Cybersecurity	- Common fraud typologies (e.g., phishing, SIM swap, social engineering). - Safe authentication and verification practices. - Procedures for reporting fraud or suspicious activity.
Consumer Protection and Complaint Resolution	- End-user rights and responsibilities. - How to submit complaints or request transaction reversals. - Resolution timelines and escalation paths.
Financial Literacy and Empowerment	- Budgeting with instant payments. - Transitioning from cash to digital. - Supporting digital confidence in low-literacy and underserved groups.

7.3 Delivery Channels and Methods

Educational content should be delivered through diverse and inclusive channels to accommodate varied literacy levels and technology access:



Digital Platforms

Mobile apps, websites, e-learning modules, and social media.



Mass Media Campaigns

Radio, television, and SMS-based messaging.



In-Person Training

Capacity-building workshops for PSPs, agents, and merchants.



Printed Materials

Flyers, posters, and brochures in local languages.



Train-the-Trainer Models

To cascade education through PSP staff, agent networks, and civil society partners.

7.4

Institutional Responsibilities

Stakeholder	Responsibility
Scheme Manager	Develop national IPS education strategy, core messages, and baseline materials.
Regulators	Promote public education on user rights and fraud prevention; ensure participant compliance.
Participants (PSPs)	Train staff, agents, and customers; adapt materials to local needs.
System Operator	Provide technical training, integration guidance, and onboarding toolkits.
Civil Society and NGOs	Support community-level outreach and inclusion of vulnerable groups.

CONCLUSION AND PATH FORWARD

This *Reference Guide* provides a comprehensive framework for developing robust, inclusive, and efficient payment systems that meet the unique needs of African markets. By addressing all key domains from legal foundations to operational procedures, risk management, and user experience, the Reference Guide offers a holistic approach to instant payment implementation while allowing for necessary adaptations to specific country contexts.

The successful implementation of instant payment systems across Africa has the potential to dramatically transform financial services on the continent, advancing financial inclusion, reducing cash dependency, enabling new business models, and supporting regional economic integration. While each country's journey will be unique, reflecting local priorities and constraints, the principles and standards outlined in this Reference Guide provide a common foundation for developing systems that are robust, interoperable, and aligned with international best practices.

To ensure continued relevance and responsiveness to evolving market dynamics and technological innovation, this Reference Guide shall be reviewed and updated on an annual basis. The periodic review process will incorporate feedback from stakeholders, lessons from implementation, and developments in global payment standards and technologies, thereby ensuring the Reference Guide remains a living tool that supports the long-term evolution of instant payment ecosystems in Africa.



**Executive
Summary**

1

Introduction

2

**Guiding Approach
to Scheme Rules
Development**

3

**The Legal
Framework of
Instant Payment
Schemes**

4

**Core Components
of Participation
Agreements**

5

**Core Components
of the Scheme
Rules**

6

Pricing Policy

7

**Education
and Awareness
Framework**

8

**Conclusion and
Path Forward**



9

Annexes

ANNEX 1: GLOSSARY

Terms	Definition
Access	The ability to use an instant payment system's services, including the direct use of the IPS's services by participants, other market infrastructures, and, where relevant, service providers. Access is fundamental to ensuring that payment systems are inclusive while maintaining operational integrity.
Access Criteria	Specific requirements and conditions that must be met by financial institutions and other entities seeking to participate in an instant payment system. These criteria typically include technical capabilities, financial soundness, regulatory compliance, and operational resilience. The criteria are designed to balance the need for broad participation with the need to maintain the security and stability of the payment system.
Alias	An alternative identifier associated with a payment account (such as an IBAN), registered in the alias auxiliary application of the instant payment system. Aliases are designed to simplify the payment initiation process by allowing users to identify payment recipients using familiar information rather than complex account numbers. Common examples of aliases include mobile phone numbers, email addresses, or custom usernames.
Alias/Proxy Directory	A database that maps user-friendly identifiers (aliases) such as mobile phone numbers, email addresses, or custom usernames to the underlying bank account details required for payment routing. The alias directory serves as a lookup service within the IPS ecosystem.
Application Programming Interface (API)	A set of protocols, routines, and tools that define how different software components should interact. APIs serve as the technical foundation for connecting participants to the central infrastructure, integrating value-added services, and enabling third-party innovations within the IPS ecosystem. In modern IPS implementations, APIs typically follow REST (Representational State Transfer) or SOAP (Simple Object Access Protocol) architectural styles, with standardized data formats such as JSON or XML.
Availability	The percentage of time that the system is operational and capable of processing transactions as designed. Given the 24/7/365 nature of instant payments and their increasing importance in economic activities, IPS typically targets extremely high availability levels, often expressed as "five nines" (99.999%) or higher, which translates to just minutes of downtime per year.

Terms	Definition
Beneficiary	An individual, business, or entity that receives funds through an instant payment transaction. The beneficiary is the ultimate recipient of the payment and typically holds an account with a financial institution that participates in the IPS, either directly or indirectly through a sponsoring participant.
Caps	Quantitative limits on the funds transfer activity of individual participants in a system may be set by each individual participant or may be imposed by the body managing the system; limits can be placed on the net debit position or net credit position of participants in the system.
Clearing	The process of transmitting, reconciling, and, in some cases, confirming payment orders prior to settlement. This process includes the netting of instructions and the establishment of final positions for settlement.
Central Bank Money	Monetary liabilities issued by a central bank that serve as the ultimate settlement asset within a country's payment system. It exists in two primary forms: physical cash (banknotes and coins) and reserves or settlement accounts that commercial banks maintain at the central bank. Central bank money offers various advantages in terms of settlement finality and credit risk elimination, unlike commercial bank money.
Collateral	An asset or third-party commitment that is used by a collateral provider to secure an obligation vis-à-vis a collateral taker.
Collateral Arrangements	A specific agreement between a collateral provider and a collateral taker to use collateral to secure an obligation. These arrangements may include detailed criteria for the eligibility of assets that can be used as collateral, as well as haircuts (reductions in the value of the collateral to account for potential market fluctuations). Collateral arrangements can take different legal forms, such as title transfer or pledge arrangements.
Commercial Bank Money	A liability of a commercial bank, in the form of deposits held at the commercial bank, which can be used for settlement purposes. Commercial bank money is often used as the settlement asset for transactions between participants, particularly in systems where the central bank is not directly involved in the settlement process.
Consumer	A natural person acting for purposes other than trade, business, or profession in payment service contracts. This distinction is important for regulatory and consumer protection purposes, as consumers often receive additional protections compared to business users of payment services.

Terms	Definition
Credit Risk	The risk that a counterparty, whether a participant or other entity, will be unable to fully meet its financial obligations when due, or at any time in the future. This risk is particularly significant in payment systems due to the time-critical nature of settlement obligations and the potential for systemic impacts if a major participant defaults.
Credit Transfer Instruction	A payment instruction in electronic format, processed in the IPS, where the payer initiates the payment and the associated exception handling instructions. This is the fundamental transaction type in most instant payment systems, enabling the immediate transfer of funds from the payer's account to the payee's account.
Cross-Border Payment	A payment in which the financial institutions of the payer and the payee are located in different jurisdictions. Cross-border instant payments represent an evolution from traditional international transfers, which often took days to complete and involved multiple intermediaries.
Customer Due Diligence (CDD)	A process financial institutions use to verify the identity of their clients and assess the potential risks associated with their financial activities. This critical compliance function helps prevent money laundering, terrorist financing, and other financial crimes that could exploit the speed and convenience of real-time payment networks.
Data Protection	Policies, procedures, and technical safeguards that are implemented to secure sensitive financial and personal information throughout the payment process. As real-time payment networks process vast amounts of data across multiple participants, robust protection mechanisms are essential to maintain user trust and comply with regulatory requirements.
Debit Transfer	A transaction model where the payment is initiated by the recipient (payee) rather than the sender (payer). In this arrangement, the payee "pulls" funds from the payer's account based on a pre-established authorization or mandate, contrasting with the more common credit push model, where the payer actively initiates the transfer.
Defaulter Pays Approach	A risk management arrangement in payment systems whereby each participant is required to cover exposures it has vis-à-vis other participants in the arrangement. As a result, losses from a party's default are borne by the defaulting party through the non-defaulter's liquidation/enforcement of the collateral posted by the defaulting party.
Deferred Net Settlement (DNS)	A mechanism that settles on a net basis at the end of a predefined settlement cycle. The DNS represents an alternative to real-time gross settlement for managing the transfer of funds between participating financial institutions. In a DNS arrangement, the IPS accumulates payment instructions over a specified period (the clearing cycle), calculates the net position of each participant at the end of the cycle, and then initiates a single settlement transaction for each participant to cover its net obligations.

Terms	Definition
Direct Participant	An entity that has direct access to the FMI's services and is directly bound by the rules of the FMI. Direct participants typically maintain an account with the FMI or its settlement agent and can submit instructions directly to the system without intermediaries.
Direct Non-Settling Participant	A participant that does not have a settlement account in the settlement system and that has an agreement with a settling participant to act on the participant's behalf with respect to its settlement obligations under the IPS scheme rules and operating procedures. This arrangement is a form of tiered participation, where some participants access the system indirectly through others.
Direct Settling Participant	A participant that has a settlement account in the settlement system and whose net position is settled on its own settlement account opened in the settlement system. As a DSP, the participant takes on the responsibility for managing its own settlement obligations within the IPS.
Directives Relatives	Specific directives related to the reject, return, recall, and request for recall by the sender processes within an instant payment system.
Disaster Recovery	Strategies, processes, and technologies implemented to restore system functionality following a disruptive event such as a natural disaster, major technical failure, or cyberattack. Given the critical nature of payment infrastructure and the expectation of 24/7/365 availability for instant payments, robust disaster recovery capabilities are essential components of IPS design and operation.
End User	Those who use, or are likely to use, services provided by payment systems (e.g., consumers, businesses, and government).
Exception Handling Instructions	These instructions are an essential component of the IPS scheme, as they define how participants should handle various exceptional situations that may arise during the processing of instant payments.
Financial Market Infrastructure (FMI)	A multilateral system among participating institutions, including the operator of the system, used for the purposes of clearing, settling, or recording payments, securities, derivatives, or other financial transactions. Instant payment systems are a specific type of FMI focused on enabling real-time or near-real-time transfers of funds between accounts at different financial institutions.
Fraud Monitoring	Technologies, processes, and organizational structures implemented to detect, prevent, and respond to fraudulent activities. The real-time and irrevocable nature of instant payments creates unique fraud risk challenges, as transactions cannot be easily recalled once settled, making effective monitoring particularly critical.

Terms	Definition
Governance	Set of relationships between the payment system's owners, board of directors (or equivalent), management, and other relevant parties, including participants, authorities, and other stakeholders (such as participants' customers, other interdependent FMIs, and the broader market). It encompasses the processes, structures, and information used for directing and overseeing the management of the system.
Indirect Participant (in an FMI)	An entity that does not have direct access to the FMI's services and is typically not directly bound by the FMI's rules, but whose transactions are cleared, settled, or recorded by the FMI through a direct participant. An indirect participant has a bilateral agreement with a direct participant to access the services of the FMI. In the context of an IPS, indirect participants are often smaller financial institutions or non-bank payment service providers that do not meet the criteria for direct participation or choose not to become direct participants due to cost, technical, or operational considerations.
Instant Credit Transfer	A credit transfer that is executed immediately (at once, without delay) 24 hours a day and on any calendar day.
Instant Payment Systems	Electronic payment solutions that enable the immediate or near-immediate transfer of funds between accounts, typically 24/7/365.
Interoperability	The ability for payments to be processed (exchanged, cleared, and settled) across multiple systems or jurisdictions (e.g., cross-border) without manual assistance; generally facilitated by the adoption of common standards and/or technical compatibility.
ISO 20022 Standard	An ISO standard for electronic data interchange between financial institutions. It describes a metadata repository containing descriptions of messages and business processes, and a maintenance process for the repository content. It encompasses the physical representation of payment transactions in XML syntax, in accordance with business rules and implementation guidelines of the payment schemes. This standard has become increasingly important in the context of instant payment systems, as it provides a common language for communication between participants.
Know Your Customer (KYC)	A mandatory process that financial institutions use to verify the identity of their clients and assess their suitability before allowing them to access real-time payment services. This critical regulatory requirement helps prevent financial crimes such as money laundering, terrorist financing, and fraud by ensuring that payment system participants know who they're doing business with.
Legal Risk	The risk of the unexpected application of a law or regulation, usually resulting in a loss. Legal risk can also arise if the application of relevant laws and regulations is uncertain.

Terms	Definition
Liquidity Management	Strategies, tools, and processes that financial institutions employ to ensure they have sufficient funds available to meet their settlement obligations continuously throughout the day. The 24/7/365 nature of instant payments, combined with the requirement for immediate funds availability to recipients, creates unique liquidity challenges compared to traditional payment systems with predictable settlement cycles.
Liquidity Risk	The risk that a counterparty, whether a participant or other entity, will have insufficient funds to meet its financial obligations as and when expected, although it may be able to do so in the future. This risk is particularly significant in instant payment environments due to the immediate nature of transactions and the continuous availability of the service.
Loss-Sharing Arrangement	An agreement among participants in a clearing or settlement system regarding the allocation of any losses arising from the default of a participant in the system or of the system itself.
Message Flow	A set of actions that describe the messages and processes a transaction undergoes in order to transfer payment and non-payment-related messages from one participant to another in the IPS. Understanding the message flow is essential for participants to implement their systems correctly and for the overall efficiency and reliability of the payment process.
Message Format	Structured arrangement and syntax of data exchanged between participants during the processing of real-time transactions. These formats define how payment information is organized, encoded, and transmitted across the network, ensuring that all parties can accurately interpret and process the data they receive.
Multilateral Netting	The offsetting of obligations between or among multiple participants to result in a single net position per participant. This process is a key component of net settlement systems.
Net (Credit or Debit) Position	A net credit or net debit position in a netting system is the sum of the value of all the transfers it has received up to a particular point in time, less the value of all transfers it has sent. If the difference is positive, the participant is in a net credit position; if the difference is negative, the participant is in a net debit position. Depending on the model, these net positions may be calculated on a bilateral or multilateral basis.
Net Settlement System	A settlement system in which final settlement of transfer instructions occurs on a net basis at one or more discrete, pre-specified times during the processing day. In the context of instant payment systems, net settlement represents an alternative to real-time gross settlement for managing the transfer of funds between participating financial institutions.

Terms	Definition
Netting	The conversion into one net claim or one net obligation of claims and obligations resulting from transfer orders that a participant or participants either issue to, or receive from, one or more other participants, with the result that only a net claim can be demanded or a net obligation be owed. This process is a fundamental concept in many payment systems, particularly those that use deferred settlement mechanisms.
Non-Payment Message	A message other than a payment message or payment message response, in the format specified in the IPS technical specifications, that is transmitted between the IPS and a participant or between participants. Non-payment messages include payment-related messages and payment-related message responses.
Open Banking	Regulatory frameworks and technical standards that enable secure sharing of financial data and payment initiation capabilities between banks and authorized third-party providers through standardized application programming interfaces (APIs). This approach creates an ecosystem where consumers can use non-bank applications and services to initiate instant payments directly from their bank accounts, fostering innovation and competition in the payment landscape.
Operational Resilience	The ability of the payment infrastructure and its participants to deliver critical services without disruption, even in the face of adverse events such as technical failures, cyberattacks, natural disasters, or other operational challenges. As instant payment systems become increasingly essential to economic activity, their continuous availability and reliability have become matters of national importance in many jurisdictions.
Operational Risk	Risk that deficiencies in information systems or internal processes, human errors, management failures, or disruptions from external events will result in the reduction, deterioration, or breakdown of services provided by an IPS. Given the real-time nature and continuous availability of instant payments, operational risk management is particularly critical for these systems.
Overlay Services	Value-added functionalities built on top of the core payment infrastructure to enhance user experience, expand use cases, or provide additional features beyond basic payment processing. These services leverage the speed and reliability of the underlying IPS while adding layers of convenience, information, or specialized capabilities. Examples: Request to pay, alias directory, bill payment service (e-invoice).
Participant	A payment service provider that has entered into a participation agreement with the scheme manager. Participants are the core entities that make up the IPS ecosystem, connecting their customers to the instant payment infrastructure and enabling the exchange of funds between different financial institutions.

Terms	Definition
Participant Onboarding	A structured process through which financial institutions or payment service providers join the system and establish the technical, operational, and legal foundations for their participation. This process is critical for maintaining the integrity and performance of the IPS while expanding its reach and utility through new participants.
Payer	Individual or entity responsible for initiating and funding a payment. They are typically the source of the funds and bear the financial obligation for the payment. The payer's role is central to the instant payment process, as their authorization is what triggers the movement of funds.
Payment Aggregator	A payment aggregator is a specialized payment service provider that enables e-commerce merchants to process their payment transactions through a single integration point.
Payment Initiation Channel	Any method, device, or procedure through which payers can place payment orders with their payment service provider (PSP) for a credit transfer, including online banking, a mobile banking application, or in any other way on the premises of the PSP. These channels serve as the interface between end-users and the instant payment infrastructure.
Payment Initiation Service Providers (PISP)	PSPs that provide a service to initiate a payment instruction at the request of the customer with respect to a payment account held at another PSP. PISPs represent a new category of payment service providers that emerged with the development of open banking frameworks, particularly in regions like the European Union under the revised Payment Services Directive (PSD2).
Payment Order	An order or instruction sent by a payer or, in some systems, a payee ordering the execution of a payment transaction. This message is the fundamental unit of communication that initiates the movement of funds within the payment system.
Payment-related Message	A message, other than a payment message or a payment response message, in the format specified by the IPS technical specifications that is transmitted between participants. A payment-related message may be a request to pay, a payment initiation request, a request for information, a payment acknowledgment, a payment status request, or a request for return of funds.
Payment Service Providers (PSPs)	Entities that offer payment services to end-users, enabling them to send and receive instant payments. PSPs serve as the interface between end-users and the payment infrastructure, playing a crucial role in the adoption and usage of instant payments.

Terms	Definition
Payment 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. This broad definition encompasses various types of payment systems, including instant payment systems, which are specifically designed to enable real-time or near-real-time transfers of funds.
Positive Confirmation	A message sent to the sender of the funds regarding completion of the instant payment, thus giving an assurance to the sender that the funds have been successfully credited to the beneficiary account. This confirmation is a key feature of instant payments, providing immediate certainty about the status of the transaction.
Prefunded Balance Account	Special deposit account established by the settling participant on its behalf or on behalf of sponsored non-settling participants for the purpose of supporting the operations of the IPS. This account holds funds that are dedicated to covering the settlement obligations arising from instant payment transactions.
Proxy	Data required in order to retrieve a payment account identifier (e.g., mobile phone number, e-mail address, etc.). This is sometimes referred to as an “alias.” A proxy could be used to replace a payment account identifier, simplifying the process of initiating payments by allowing users to identify recipients using familiar information rather than complex account numbers.
QR Code Payment	A method of initiating real-time transactions by scanning a two-dimensional barcode with a mobile device. This technology creates a bridge between physical and digital payment environments, enabling instant payments without requiring specialized merchant hardware beyond the ability to display or generate QR codes.
Real-Time Gross Settlement (RTGS)	The real-time settlement of payments, transfer instructions, or other obligations individually on a transaction-by-transaction basis. This approach contrasts with deferred net settlement systems, where payments are accumulated over a period and then settled based on the net amounts.
Receiving Participant	The participant that holds the receiver’s account and that receives a payment message. This entity plays a crucial role in the instant payment process, as it is responsible for making the funds available to the payee immediately upon successful processing of the payment.
Reconciliation	A procedure to verify that two sets of records issued by two different entities match. This process is essential for ensuring the accuracy and integrity of payment processing, as it helps identify and resolve any discrepancies that may arise during the transmission and settlement of payments.

Terms	Definition
Request to Pay (RtP)	A message that a participant, acting on behalf of themselves or their end customer (the payee), sends to another participant or their end customer (the payer) via the IPS to request a payment. This functionality represents an evolution beyond basic credit transfers, enabling more interactive and payee-initiated payment scenarios.
Risk Management	A comprehensive framework of policies, procedures, controls, and technologies designed to identify, assess, mitigate, and monitor the various risks associated with real-time payment processing. The immediate and irrevocable nature of instant payments creates distinct risk challenges compared to traditional payment methods, requiring specialized approaches to maintain system security and stability.
Scheme Rule	A set of procedures, rules, and technical standards that govern how transactions are executed (CPMI 2016a). Scheme rules define the terms for maintaining an effective payment system, including rules for how participants will work together, how economic incentives will be balanced, and how disputes will be managed.
Scheme Manager	Entity responsible for the overall governance, strategic direction, and operational oversight of the IPS. This role is critical for ensuring that the system functions effectively, evolves to meet changing needs, and maintains the trust of all stakeholders.
Sender	A customer of a sending participant who sends a payment instruction to the sending participant. The sender is the individual or entity that initiates the payment process by providing instructions to their financial institution to transfer funds to a recipient.
Sending Participant	A participant who holds the sender's account and initiates an instant payment. A sending participant is similar to a payer or originator participant. This entity plays a crucial role in the instant payment process, as it is responsible for validating the payment instruction, ensuring sufficient funds are available, and initiating the transaction in the IPS.
Set Off	A method of canceling or offsetting reciprocal obligations and claims (or the discharge of reciprocal obligations up to the amount of the smaller obligations). Set off can operate by force of law or pursuant to a contract.
Settlement	Process by which financial obligations between participating institutions are discharged, representing the actual transfer of funds that backs the payments made by end users. While customers experience instant payments as immediate transfers, the underlying settlement between financial institutions may follow various models depending on the system design, each with different implications for timing, risk, and liquidity management.

Terms	Definition
Settlement Finality	The irrevocable and unconditional transfer of an asset or financial instrument, or the discharge of an obligation by the FMI or its participants in accordance with the terms of the underlying contract. Final settlement is a legally defined moment. This concept is fundamental to IPS, as it provides certainty to payment recipients that they can immediately use or disburse received funds without risk of reversal.
Settlement Risk	Risk that the settlement in a payment system will not take place as expected. This risk is particularly significant in IPS due to the immediate and irrevocable nature of payments, which creates potential exposures if a participant fails to meet its settlement obligations while other participants have already credited their customers' accounts based on expected receipts.
Scheme Rules	A comprehensive set of standards, procedures, and obligations that govern the operation of the system and the relationships between participants. These rules form the contractual foundation of the IPS, establishing clear expectations for all parties and providing mechanisms for addressing operational issues, disputes, and exceptional situations.
Standards	Messaging and communication standards, technical infrastructure standards, and contingency standards that participants must adhere to in order to become and remain members of the IPS. These standards provide a common framework that ensures interoperability, security, and reliability across the payment ecosystem.
Straight-Through Processing (STP)	Complete automation of the payment process from initiation to final settlement, without requiring manual intervention under normal circumstances. This end-to-end automation is essential for achieving the speed, efficiency, and reliability expected in real-time payment environments, where transactions must be completed within seconds regardless of transaction volume or time of day.
Strong Customer Authentication	Authentication based on the use of two or more elements categorized as knowledge (something only the user knows), possession (something only the user possesses), and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data.
Survivors Pay	An approach to loss-sharing arrangements in payment systems, where losses arising from a defaulting participant are borne by non-defaulting participants according to pre-agreed rules.
System Operator	Entity responsible for the technical operation, development, and maintenance of the infrastructure of an instant payment system (IPS). This critical role encompasses ensuring the continuous availability and performance of the system, implementing technical updates and enhancements, managing system configurations, and coordinating with participants to maintain operational integrity.

Terms	Definition
Systemic Risk	The risk that the failure of one participant in a payment system to meet its required obligations will cause other participants or financial institutions to be unable to meet their obligations when due. Such a failure may cause significant liquidity or credit problems and, as a result, might threaten the stability of the entire financial system.
Technical Specification	A comprehensive document that defines the technical requirements and standards for participating in an instant payment system. It provides detailed information about the system's architecture, interfaces, message formats, security protocols, and operational procedures, enabling participants to develop and implement the necessary technical capabilities to connect to and interact with the system.
Third-Party Provider (TPP)	An entity that offers payment-related services by accessing customer accounts held at other financial institutions through secure interfaces.
Transaction Limits	Maximum value thresholds applied to individual payments or cumulative transactions over a defined period. These limits serve multiple purposes within the IPS ecosystem, balancing the desire for broad payment functionality with risk management considerations and operational constraints.
Use Case	Specific payment functions and services designed for and made available to participants and their customers to meet a particular participant and/or customer need. These use cases represent the practical applications and value propositions of the IPS infrastructure, translating technical capabilities into tangible financial services that address real-world requirements. Common IPS use cases include P2P, P2M, P2B, CICO, B2P, P2G,
User Experience (UX)	Overall perception and response a person has when using real-time payment services, encompassing all aspects of the interaction, including usability, accessibility, performance, design, and emotional response. As instant payment adoption grows globally, UX has become a critical differentiator among service providers and a key factor in driving user acceptance and transaction volumes.

ANNEX 2: GLOBAL BENCHMARKING

Instant Payment	Country	Launch Date	Scheme Manager	System Operator	Message Standards	Proxy Directory	Settlement Model
UK FSP	United Kingdom	2008	Pay.UK (formerly Faster Payments Scheme Limited)	Vocalink (a Mastercard company)	ISO 8583 (legacy format), moving toward ISO 20022	Centralized (payment service for mobile number proxy)	Deferred Net Settlement
SEPA Instant Credit Transfer (SCT Inst)	Pan-European (SEPA zone)		European Payment Council	Multiple clearing mechanisms (EBA CLEARING's RT1, ECB's TIPS, ...)	ISO 20022 XML	Decentralized (varies by country/provider)	Varies by clearing mechanism (TIPS offers real-time settlement in central bank money)
Real-Time Payments (RTP)	United States	2017	The Clearing House	The Clearing House	ISO 20022 XML	Doesn't support the use of aliases or proxies for payments. Though the network allows third parties to enable payment. E.g., PayPal and Venmo	Real-time settlement through the Federal Reserve

Instant Payment	Country	Launch Date	Scheme Manager	System Operator	Message Standards	Proxy Directory	Settlement Model
PIX	Brazil	2020	Banco Central do Brasil	Banco Central do Brasil	ISO 20022 XML	Centralized	Real-time settlement in central bank money
FedNow Service	United States	2023	Federal Reserve	Federal Reserve	ISO 20022 XML	Decentralized (managed by participating institutions)	Real-time settlement in central bank money
Unified Payments Interface (UPI)	India	2016	National Payments Corporation of India (NPCI)	National Payments Corporation of India (NPCI)	Proprietary message XML	Centralized (NPCI manages virtual payment addresses)	Deferred Net Settlement multiple times daily
Fast And Secure Transfers (FAST)	Singapore	2014	Singapore Clearing House Association (SCHA)	Banking Computer Services Pte Ltd (BCS)	ISO 20022 XML	Centralized (PayNow service for proxy identifiers)	Deferred Net Settlement with collateralization
New Payments Platform (NPP)	Australia	2017	NPPA	Australia Payment Plus	ISO 20022 XML	Centralized (PayID service)	Real-time settlement in central bank money

Instant Payment	Country	Launch Date	Scheme Manager	System Operator	Message Standards	Proxy Directory	Settlement Model
Interbank Electronic Payment System (SPEI)	Mexico	2015	Bank of Mexico (Banco de México)	Bank of Mexico (Banco de México)	Recently moved to ISO 20022	Decentralized (CLABE system for standardized account numbers)	Hybrid model with frequent settlement cycles
Fawri+	Bahrain	2019	Central Bank of Bahrain	The Benefit Company	ISO 20022	Centralized	Deferred Net Settlement
RPP	Malaysia	December 2018	PayNet	PayNet	ISO 20022	Centralized	Real-time Gross Settlement
PesaLink	Kenya	2017	Integrated Payment Services Ltd	Integrated Payment Services Ltd	ISO 8583/ISO 20022	Centralized	Real-time Gross Settlement
PayShap	South Africa	2023	Payment Association of South Africa	Bankserv Africa	ISO 20022	Centralized (ShapID)	Deferred Net Settlement
NIBSS (NIP)	Nigeria	2011	NIBSS	NIBSS	Proprietary message XML	Centralized	Deferred Net Settlement
GhIPSS (GIP)	Ghana	2015	GhIPSS	GhIPSS	ISO 8583	Centralized	Deferred Net Settlement
eKash	Rwanda	2022	National Bank of Rwanda	Rwanda Information Society Authority	ISO 20022	Centralized (eKash ID)	Deferred Net Settlement
FastPay	Ethiopia	2023	National Bank of Ethiopia	EthSwitch S.C.	ISO 8583/ISO 20022	Centralized	Deferred Net Settlement

ANNEX 3: KEY PERFORMANCE METRICS FOR INSTANT PAYMENT

Metric	Description	Target Value (examples)	Measurement Method
Transaction Processing Performance Metrics			
End-to-End Processing Time	Total elapsed time from payment initiation to funds availability	< 10 seconds (95th percentile)	System timestamps at transaction initiation and completion
Transaction Throughput	Number of transactions processed per second	Minimum 1,000 TPS with the ability to scale to 5,000+ TPS during peak periods	Continuous monitoring of system throughput
Transaction Success Rate	Percentage of transactions completed successfully	> 99.9%	Ratio of successful transactions to total transactions
Transaction Rejection Rate	Percentage of transactions rejected due to validation errors	< 0.5%	Count of rejected transactions divided by total transaction attempts
Settlement Time	Time between transaction authorization and final settlement	<5 seconds for instant settlement model	Timestamps at authorization and settlement completion
System Availability and Reliability Metrics			
System Uptime	Percentage of time the system is fully operational	99.999% (five nines)	Continuous monitoring with automated alerting
Mean Time Between Failures	Average time between system failures	> 3,000 hours	Time tracking between documented failure incidents
Mean Time to Recovery	Average time to restore service after failure	< 5 minutes	Time tracking from failure detection to resolution
Recovery Time Objective	Time to restore service after a major disaster	< 30 minutes	Disaster recovery testing and actual incident data

Metric	Description	Target Value (examples)	Measurement Method
Recovery Point Objective	Maximum acceptable data loss during recovery	Zero data loss (synchronous replication)	Analysis of recovered data after incidents or tests
Component Availability	Availability of individual system components	>99.99% per component	Component-level monitoring
Planned Maintenance Impact	Transaction success rate during maintenance	>99.9% (minimal impact)	Comparison of success rates during maintenance vs. normal operation
Performance Scalability Metrics			
Maximum Throughput Capacity	The upper limit of transactions the system can process per second	> 5,000 TPS with ability to scale to 10,000+ TPS	Controlled load testing at increasing volumes
Horizontal Scaling Efficiency	Performance improvement when adding processing nodes	> 85% linear scaling efficiency	Performance comparison with a varying number of nodes
Vertical Scaling Limits	Performance constraints when adding resources to existing nodes	Documented limits with clear upgrade paths	Benchmark testing with increasing resources
Network Bandwidth Utilization	Percentage of available network capacity used during peak loads	< 70% of available bandwidth	Network traffic monitoring across all interfaces
Security and Fraud Prevention Metrics			
Fraud Rate	Value of fraudulent transactions as a percentage of total value	< 0.005% (5 basis points)	Analysis of confirmed fraud cases
False Positive Rate	Legitimate transactions incorrectly flagged as fraudulent	< 0.5% of all transactions	Tracking of fraud alerts and subsequent validations
False Negative Rate	Fraudulent transactions not detected by security systems	< 0.001% of all transactions	Post-transaction fraud analysis
Authentication Failure Rate	Failed authentication attempts by legitimate users	< 5% on first attempt	Authentication log analysis

Metric	Description	Target Value (examples)	Measurement Method
Security Vulnerability Remediation Time	Time to patch identified security vulnerabilities	Critical: < 24 hours High: < 7 days Medium: < 30 days	Tracking from vulnerability discovery to patch deployment
Data Encryption Coverage	Percentage of sensitive data encrypted at rest and in transit	100% of sensitive data	Security configuration audits
Penetration Testing Frequency	Regularity of security testing by independent parties	Quarterly comprehensive tests	Documentation of completed penetration tests
API Performance and Integration Metrics			
API Response Time	Time from request receipt to response delivery	< 200ms (95th percentile)	API gateway response time tracking
API Throughput	Number of API requests processed per second	> 2,000 requests per second	API gateway throughput monitoring
API Error Rate	Percentage of API calls resulting in server errors	< 0.1% server error rate	HTTP status code monitoring
API Version Adoption	Percentage of traffic on each API version	> 95% on current version	API traffic analysis by version
SDK Integration Success Rate	Percentage of SDK integrations completed successfully	> 95% success rate	SDK integration analytics and developer feedback

ANNEX 4: FINANCIAL INCLUSION METRICS

Metric	Description	Measurement Method
Access and Adoption Metrics		
Registration Rate	Percentage of the eligible population registered for instant payment services	Survey data, provider statistics
Active User Rate	Percentage of registered users who actively use the system (e.g., at least once per month)	Transaction data from payment providers
Demographic Penetration	Adoption rates across different demographic groups (age, gender, income, education, rural/urban)	Surveys, provider data with demographic information
Geographic Coverage	Percentage of regions/districts with access to instant payment infrastructure	Provider coverage maps, infrastructure data
Digital Divide Reduction	Narrowing the gap in digital financial service usage between privileged and underprivileged groups	Comparative analysis
Usage and Transaction Metrics		
Transaction Volume	Number of transactions per user per time period	Payment system data
Transaction Value	Average and median value of transactions	Payment system data
Transaction Types	Distribution of transaction purposes (e.g., P2P, bill payments, merchant payments)	Categorized transaction data
Frequency of Use	How often users engage with the system	Transaction timestamp analysis
Time of Use	Distribution of transactions across different times of day/week	Transaction timestamp analysis
Substitution Effect	Reduction in cash usage or other payment methods	Surveys, comparative payment method data
Cost and Affordability Metrics		
Transaction Fees	Direct cost per transaction to the user	Provider fee schedules
Fee as a Percentage of Transaction	Transaction fee relative to the amount transferred	Calculated from fee schedules
Fee as a Percentage of Income	Transaction costs relative to user income levels	Fee data combined with income surveys

Metric	Description	Measurement Method
Total Cost of Ownership	All costs associated with using the system (device, data, fees)	Comprehensive cost analysis
Cost Comparison	Cost relative to alternative payment methods	Comparative analysis of payment options
User Experience and Trust Metrics		
System Reliability	Percentage of successful transactions	System performance data
Transaction Speed	Average time to complete a transaction	System performance data
User Satisfaction	Overall satisfaction with the payment system	User surveys
Ease of Use	Perceived simplicity of completing transactions	Usability surveys
Trust Level	Users' confidence in system security and reliability	Trust assessment surveys

ANNEX 5: KEY COMPONENTS OF THE SCHEME RULES

Scheme Rule Element	Description
Business Purpose	Defines the objectives of the scheme, focusing on inclusion, efficiency, and wide accessibility.
Governance Model	Outlines the roles, responsibilities, and structure (e.g., integrated vs. separated governance).
Participation Rules	Sets eligibility criteria, onboarding requirements, and types of participants (direct/indirect).
Use Cases and Transaction Types	Specifies supported use cases (P2P, P2B, bill payment, cash in/cash out, payment return, etc.) and the associated operational rules.
Transaction Processing	Defines the end-to-end flow, validation steps, authorization, and timing for processing payments.
Settlement Model	Describes how and when funds are settled (e.g., real-time, netting, prefunding, deferred).
Liquidity and Risk Management	Provides mechanisms for managing credit, liquidity, and operational risks.
Dispute Resolution	Establishes the process for handling complaints, errors, and unauthorized transactions.
Consumer Protection	Includes safeguards such as transparency, consent, and redress mechanisms for end-users.
Pricing Governance	Defines the process for setting, reviewing, and disclosing participant and end-user fees.
Service Level Standards (SLS)	Sets expectations on system availability, transaction speed, and responsiveness.
Compliance and Audit	Establishes monitoring mechanisms, reporting requirements, and sanctions for non-compliance.
Proxy Directory Services	Enables alias-based payments using phone numbers, emails, etc., while ensuring privacy and control.
Scheme Branding and Communications	Sets rules for the use of scheme brand assets and participant marketing practices.

Scheme Rule Element	Description
Education and Awareness	Provides guidance for stakeholder training and end-user education to promote adoption and trust.
Monitoring and Evaluation	Outlines performance indicators and feedback mechanisms to guide continuous improvement.
Technology and Interoperability	Provides guidance on technical standards, APIs, and compatibility with international norms.
Change Management	Establishes processes for updating scheme rules and introducing new features.

ANNEX 6: ILLUSTRATIVE TEMPLATE – PARTICIPANT COMPLIANCE REPORTING

This template provides a reference structure for participants in an instant payment scheme to regularly report on their compliance with scheme rules. It supports self-certification and can also be used by the scheme manager to consolidate monitoring results across all participants. It is adaptable to risk-based monitoring cycles (e.g., quarterly, biannually, annually).

Section 1: Participant Information

Field	Description
Institution Name	Reporting the participant’s official name
Period Covered	Reporting period (e.g., Q1 2025)
Submission Date	Date of report submission
Compliance Focal Person	Name and contact details of the responsible officer

Section 2: Compliance Summary by Domain

Participants should self-assess and report their compliance status across the following dimensions, aligned with scheme obligations. Supporting documentation should be available upon request.

Compliance Area	Relevant Rule Reference	Compliance Status (Yes / No / Partial)	Remarks / Key Evidence	Remediation Timeline (if needed)
Adherence to Technical Specifications (ISO 20022, APIs)	I.3 / Technical Annex			
Participation Agreement Compliance	I.1			
Scheme Rules Adherence	I.1			

Compliance Area	Relevant Rule Reference	Compliance Status (Yes / No / Partial)	Remarks / Key Evidence	Remediation Timeline (if needed)
Settlement Performance & Funding Obligations	III.1 / III.2		Include any settlement delays or breaches	
SLA and Operational Reliability	II.3		Uptime percentage, support tickets, and downtime explanations	
Fraud Management and Risk Controls	V.1		System alerts, fraud response logs	
Customer Protection Measures	IV.2		Dispute logs, user education	
Regulatory Reporting and Data Privacy Compliance	IV.3 / IV.5		Internal audit, data handling policies	

Section 3: Significant Events or Incidents

Participants should disclose any significant compliance incidents, breaches, or unresolved operational risks during the reporting period.

Event Type	Date	Description	Resolution Status	Actions Taken / Planned
Example: SLA Breach	2025-02-10	Downtime exceeded 30 mins	Resolved	System patch and process update implemented
Example: Fraud Case	2025-03-04	APP scam incident	Under investigation	Customer notified; reversal request initiated

Signature:

Date:

Section 4: Declaration

“We confirm that this compliance report accurately reflects our institution’s adherence to the scheme rules and that any identified deficiencies will be addressed in line with the scheme’s remediation expectations.”

Authorized Signatory:

Name:

Position:

ANNEX 7: EXAMPLES OF EXISTING INSTANT PAYMENT SCHEMES

Country/Region	Scheme Name	Managing Entity	Documentation Availability
Brazil	Pix	Central Bank of Brazil	Publicly available on the Central Bank's official website.
United States	RTP Network	The Clearing House	Publicly available on The Clearing House website.
United States	FedNow	Federal Reserve	Publicly available on the Federal Reserve's website.
Mexico	SPEI	Banco de México	Not publicly available.
Canada	Real-Time Rail (RTR)	Payments Canada	Not publicly available; select documents shared with participants.
Chile	TEF	Banco Central de Chile	Not publicly available.
European Union	SEPA Instant Credit Transfer (SCT Inst)	European Payments Council (EPC)	Publicly available on the EPC website.
United Kingdom	Faster Payments Scheme (FPS)	Pay.UK	Not publicly available; access requires registration.
Sweden	Swish	Getswish AB	Not publicly available; limited high-level information published.
Denmark	Straksclearing	Finance Denmark	Not publicly available; restricted to financial institutions.
Hungary	GIRO Instant Payment System	GIRO Zrt.	Not publicly available; accessible only to scheme participants.
Poland	Express Elixir	KIR	Not publicly available; documentation available upon formal request.
India	Unified Payments Interface (UPI)	NPCI	Publicly available on the NPCI website.

Country/Region	Scheme Name	Managing Entity	Documentation Availability
Singapore	FAST	ABS	Not publicly available; limited information on ABS and MAS sites.
Thailand	PromptPay	Bank of Thailand	Not publicly available; only partial rules published.
Australia	New Payments Platform (NPP)	NPP Australia / Reserve Bank of Australia	Available on Australian Payment Plus.
Hong Kong	Faster Payment System (FPS)	Hong Kong Monetary Authority	Not publicly available; technical documents accessible to participants.
Malaysia	DuitNow	PayNet	Not publicly available; registration required to access rules.
Philippines	InstaPay	Philippine Payments Management Inc.	Not publicly available; rulebook shared only with licensed institutions.
Ghana	GhIPSS Instant Pay (GIP)	Ghana Interbank Payment & Settlement Systems	Not publicly available; rulebook available upon request.
Nigeria	NIBSS Instant Payment (NIP)	Nigeria Inter-Bank Settlement System (NIBSS)	Publicly available (“Regulation on Instant Payment.pdf”).
Kenya	PesaLink	Integrated Payment Services Limited (IPSL)	Not publicly available; limited documentation disclosed.
South Africa	Rapid Payments Programme (RPP)-PayShap	BankservAfrica and PASA	Not publicly available; documents accessible only to participants.
UAE	Immediate Payment Instruction (IPI)	Central Bank of the UAE	Not publicly available; restricted to licensed institutions.
Saudi Arabia	SARIE (Saudi Arabian Riyal Interbank Express)	Saudi Central Bank	Not publicly available; technical details shared with participants only.



AfricaNenda Foundation

C1-402, 4th Floor, Block C, Grand Baie La Croisette, Grand Baie, Mauritius

website www.africanenda.org | email info@africanenda.org



October 2026

© 2026 - All Rights Reserved
AfricaNenda Foundation