PAYMENT SYSTEM OVERSIGHT AND INTEROPERABILITY

ITU-T FOCUS GROUP ON DIGITAL FINANCIAL SERVICES

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

FG-DFS

(11/2016)

ITU-T Focus Group Digital Financial Services

Payment System Oversight and Interoperability

Focus Group Technical Report

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The procedures for establishment of focus groups are defined in Recommendation ITU-T A.7. TSAG set up the ITU-T Focus Group Digital Financial Services (FG DFSs) at its meeting in June 2014. TSAG is the parent group of FG DFS.

Deliverables of focus groups can take the form of technical reports, specifications, etc., and aim to provide material for consideration by the parent group in its standardization activities. Deliverables of focus groups are not ITU-T Recommendations.

About this report

The author of this Technical Report is Biagio Bossone, International Financial Consultant. Contributions were received from the members of the FG DFS Interoperability Working Group, and, in specific, from Daniel Gersten Reiss, Lara Gidvani, Yury Grin, Realeboha Lekhanya, and Thomas Lammer. The Technical Report was reviewed by the ITU Focus Group Digital Financial Services. Thomas Lammer provided the overall guidance for this project.

If you would like to provide any additional information, please contact Vijay Mauree at tsbfgdfs@itu.int

CONTENTS

Page

List of Boxes

Executive Summary

Payment systems have become a vital component of the economic life of contemporary societies. The smooth functioning of payment systems is essential to the overall efficiency and stability of the market systems of which they are core parts. To ensure such smooth functioning, and to facilitate the development of sound payment system infrastructures and services, central banks worldwide have been entrusted with the responsibility to oversee national payment systems. Payment system oversight is essentially about controlling risks in payment systems and promoting payment infrastructure and service development.

As part of their oversight responsibilities, central banks have recently placed increasing emphasis on retail payment systems. Developing efficient and safe retail payment infrastructures has become a key strategic objective of payment system oversight. Critical in this context is the interoperability of payment systems, which allows two or more proprietary payment platforms to interact seamlessly, enabling users to make electronic payment transactions with any other user in a convenient, affordable, fast, and secure way.

Interoperability represents both an important feature of payment system efficiency and, at the same time, an important source of risk. For this reason, pursuing it requires public authorities to adopt suitable oversight provisions, and system operators and payment service providers to implement adequate standards covering legal, organizational, technical, procedural, and business practices.

This report focuses on payment system oversight and the interoperability of payment systems as an increasingly emerging feature of retail payments. The report describes the foundations of payment system oversight and considers how oversight policy should apply to interoperability in retail payment systems. Building on existing international standards for financial market infrastructures, the report elaborates policy principles for public authorities, payment system operators, and payment service providers to ensure that the risks associated with interoperability are managed effectively. Important in this context is the cooperation between relevant authorities, both domestically and internationally, and their effort to cooperate effectively not just in normal circumstances, but, especially, during crisis situations.

The scope of the principles provided in this report extends to several aspects of payment system oversight and interoperability. Besides an opening principle covering the general area of risk identification, monitoring, and management, the other principles are specifically designed to address legal, operational, and financial aspects of interoperability, as well as issues relating to their governance, access, efficiency, and effectiveness. The principles build on international best practices. They assume that the responsibility for managing the risks associated with interoperability lies first and foremost with the operators of and the participants in interoperable systems. The oversight authorities should consider implementing these principles.

This report is not intended to be a regulatory document. Its main aim is to provide policy advice, recommendations, and indications to country authorities, payment system operators and service providers. A companion report on *"Payment System Interoperability and Oversight: The International Dimension"* elaborates complementary principles for the oversight of interoperability between internationally linked or shared payment system infrastructures.

Purpose of this report

1 Payment systems have become a vital component of the economic life of contemporary societies. They consist of increasingly complex and integrated networks of institutions and people involved in the execution of fund transfers across economies (see Box 1). The smooth functioning of payment systems is essential to the overall efficiency and stability of the market systems of which they are core parts. To ensure such smooth functioning, and to facilitate the development of sound payment system infrastructures, central banks worldwide have been entrusted with the responsibility to oversee national payment infrastructures. To this purpose, and considering the growing interconnectedness and mutual interdependence of payment system and other financial market infrastructures, including across national borders, central banks have developed specific oversight policy frameworks and activities.

2 While for many years central banks have mainly focused their attention on large-value fund transfer infrastructures, more recently, they have placed increasing emphasis on retail payment systems. As the evolution of information and communication technology has dramatically changed the means and channels of transferring money across the economy, a strong interest on retail payments has emerged in a growing number of countries, recognizing their importance in facilitating commerce and improving both the efficiency of day-to-day transactions among consumers and businesses, as well as the distribution and collection of payments made by and to government agencies. Research has shown that switching from traditional paper-based to modern (digital) payment instruments can entail yearly savings to a country's economy in the order of one percentage point of GDP or more.[1]

As a result, developing efficient and safe retail payment infrastructures has become a key strategic objective of payment system oversight in many jurisdictions. Retail payments are typically the entry point to broader financial services, and their potential weaknesses regarding security and reliability may impact the financial system and the broader economy in general, in particular by affecting the confidence of users. Innovations in retail payments raise relevant oversight policy issues for central banks. It is paramount that the integrity of the design and operation of retail payment systems is protected, so that users can trust payment service providers (PSPs), the payment mechanisms themselves, and the central bank as the institution responsible for overseeing them.

1 See Humphrey, D., M. Willesson, T. Lindblom, and G. Bergendahl, "What Does it Cost to Make a Payment?", Review of Network Economics 2 (June), 2003: 159–174. In Europe, for example, the same authors show that the gradual move towards the use of electronic payments and substitution of ATMs for traditional banking offices has helped reduce bank operating costs by some US$32 billion, saving 0.38 per cent of 12 nations' GDP over the period 1987–1999. Payment cost studies conducted in the Netherlands estimate the overall social cost of point-of-sales payments at 0.65 per cent of GDP, while the share of the cost of cash is 73 per cent of the total social cost or at 0.48 per cent of GDP. Comparatively, in Belgium, the social cost estimate was at 0.74 per cent of GDP, while the share of cost of cash is 75 per cent of the total social cost, or at 0.58 per cent of GDP. In Finland, estimates of the social cost of payments is at 0.3 per cent of GDP, where the share of the cost of cash is at 0.1 per cent of GDP. These studies further argue that the marginal social cost of cash is much higher than the use of non-cash payment methods, particularly debit cards and electronic purses, so with proper incentives, such cost-savings would lead to the adoption of more efficient payment methods.

Box 1. Payment systems and payment system infrastructures

A payment system is a set of instruments, procedures, and rules for the transfer of funds between or among participants; the system includes the participants and the entity operating the arrangement. Payment systems are typically based on an agreement between or among participants and the operator of the arrangement, and the transfer of funds is effected using an agreed-upon operational infrastructure. Payment systems are generally categorized as either large-value payment systems (LVPSs) or as retail payment systems (RPSs). A LVPS is a funds transfer system that typically handles large-value and high-priority payments. On the other hand, a RPS is a funds transfer system that handles a large volume of relatively low-value payments in such forms as cheques, credit transfers, direct debits, cards, mobile, and Internet. LVPSs and RPSs may be operated either by the private sector or the public sector, using multilateral deferred net settlement or real-time gross settlement (RTGS) mechanisms. Often, LVPSs are operated by central banks. An increasing number of countries are introducing real-time retail payments systems (RT-RPS), which provide irrevocability, support real-time posting and re-use of funds, as well as immediate payment confirmation to both the payer and the payee.

Payment system infrastructures (comprised of institutions, instruments, rules, procedures, standards, and technical means and platforms) enable the execution of the transfer of monetary value between parties discharging mutual obligations. They include payment systems as defined above, payment technologies and schemes, and all arrangements that facilitate the execution, clearing, settlement, and recording of monetary and other financial transactions, such as payments, funds transfers, securities, and derivatives contracts (including for commodities).

3 Critical to the development and diffusion of modern (digital) retail payment services is the interoperability of payment systems. Generally understood as the property of products or systems to work with other products or systems without friction, when referred to retail payments, interoperability enables users to make electronic payment transactions with any other user in a convenient, affordable, fast, seamless, and secure way, possibly via a single transaction account.[2] Thus, interoperable payment systems allow two or more proprietary platforms to interact seamlessly, enabling the exchange of payment transactions between and among PSPs and, consequently, users.[3] By its very nature, interoperability represents both an important feature of payment system efficiency

2 A transaction account is defined as an account (including an e-money account) held with a bank or other authorized and/or regulated PSP, which can be used to make and receive payments and to store value. All deposit accounts held with banks and other authorized deposit-taking financial institutions, referred to as "deposit transaction accounts", that can be used for making and receiving payments qualify as transaction accounts. Prepaid instruments based on e-money, referred to as "e-money accounts", can be offered by banks and other authorized deposit-taking financial institutions, as well as by non-deposit-taking PSPs such as mobile network operators. (See "Payment aspects of financial inclusion", report by the Committee on Payments and Market Infrastructures and the World Bank Group, APRIL 2016.) The desirability of a single account is based on two considerations. First, while interoperability can be achieved even among payment service users who do not possess accounts with banks or other PSPs, such type of interoperability would not be as financially inclusive as one among payment service users who all hold accounts. The difference is between interoperability built around "off-network" transactions (as in the case, for example, of an individual sending money from her mobile account to another individual who doesn't have an account) and "cross-network" transactions: the former requires recipients to cash out the payments received, whereas the latter makes it possible for recipients to store received funds, on-send them, or use them to make payments. The second reason in favor of achieving interoperability via a single transaction account is that this would allow every individual payment service users to make and receive payments from all other payment service users in the economy through only one entry point to the financial system, with maximum efficiency and user convenience.

3 See ITU DFS Focus Group - Ecosystem Working Group Glossary - May 2016.

and, at the same time, a critical source of risks. For this reason, pursuing it requires public authorities to adopt suitable oversight provisions, and system operators and PSPs to implement adequate oversight standards covering legal, organizational, technical, procedural, and business practices.

4 This report focuses on payment system oversight and the interoperability of payment systems as an increasingly emerging feature of retail payments. The report describes the foundations of payment system oversight, and considers how oversight policy should apply to interoperability in retail payment systems (RPSs). This report is not intended to be a regulatory document, as its main aim is to provide policy advice, recommendations and indications to country authorities, payment system operators, and PSPs. The word "should" used in the principles reflects this general intention and should therefore not be misunderstood as imposing rules or requirements.

5 The report is organized as follows: Section II illustrates the role and responsibilities of the oversight of payment systems, and explains the objectives, scope, and instruments of central bank oversight policy. Section III takes on the relevance of payment system interoperability in the context of RPSs development. Based on the premise that establishing interoperability and making sure its associated risks are managed effectively is a key objective of payment system oversight policy, this section proposes a set of oversight recommendations for interoperability in RPSs.

6 A companion report will deal with interoperability and oversight from an international perspective. The report will discuss payment system interoperability and central bank oversight policy in the context of international economic and financial integration.

The Oversight of Payment Systems

A. The critical role of payment systems in contemporary economies

7 To the extent that expanding production and exchange in a market economy requires an increasing interconnection of various, and usually anonymous, decisional units, economic development rests crucially on infrastructures that make those interconnections efficient and reliable. In contexts where many decisions are taken by multitudes of heterogeneous agents, a set of efficient and reliable infrastructures, governed by clear and enforceable rules, is necessary to ensure that transactions are carried out within the terms and conditions agreed to by their originating counterparts. Interconnecting the elements of the infrastructures becomes more essential as modern communication and information technologies make markets independent of specific physical locations. Especially where exchange involves agent commitments to future obligations – as is typically the case with financial contracts – elements of infrastructures, such as the legal system and contract enforcement mechanisms, must be in place to provide trading counterparts with sufficient reassurance that commitments are fulfilled in accordance with their agreed upon terms and conditions.

8 Payment system infrastructures determine the efficiency, safety, and effectiveness with which transaction money is used in the economy, and the risks associated with its use. They contribute fundamentally to the general economic welfare of the society, by underpinning the public's confidence in money, and by allowing its use, production, investment, commerce, and finance. Efficient, safe, and effective payment systems reduce the cost of exchanging goods and services, and are indispensable to the functioning of the interbank, credit, securities, and capital markets, as well as to the implementation of efficient monetary policy. Weak payment systems, on the other hand, may severely affect the stability and developmental capacity of an economy; its failures can result in inefficient use of financial resources, inequitable risk sharing across the agents, ineffective transmission of monetary policy impulses across the economy, actual losses for participants, and loss of confidence in the financial system and of public trust in the very use of money.

9 Payment systems are designed specifically to transfer monetary assets in order to complete transactions originating in all segments of the financial system, as well as in the markets for goods and services. They are highly organized structures, typically involving high degrees of interconnection between different technical infrastructures and among large numbers of entities and individuals.

10 In recent years, many countries have embarked on programs to reform and modernize their payment systems. Policy makers are thus faced with the formidable task of how best to design a country's payment system within fast-changing technological and institutional environments, e.g. the increasing importance of non-banks in the payment system and the emergence of new technologies, like virtual currencies and distributed ledger technology. These tasks become increasingly complex as competition and innovation constantly push to the limit the search for better combinations of efficiency, safety, reliability, operational continuity, and system integrity in the provision of payment services to larger numbers of users and institutions.

B. Payment systems need oversight

What is oversight?

11 Because of the central role of payment systems just discussed, failures to transfer liquidity may affect the performance of every sector of the economy. Moreover, because all segments of the economic and financial system link to the payment system, in order to complete the money transfer leg of all the transactions they originate, major failures in one part of the system to complete the money leg of the effected transactions can feed through the payment system – along connectivity channels, interoperable payment platforms, interrelated institutions, and interlinked financial contracts – and disrupt liquidity transfer within the overall economy.

Box 2. Risk implications of interdependencies

The development of interdependencies has several implications for the safety of payment infrastructures. Interdependencies raise the potential for disruptions to spread widely and quickly across the financial system in at least three ways:

First, they can propagate disruptions sequentially from one system to another. This potential effect arises when the smooth functioning of one or more systems is conditional on that of another system. For example, in the case that a LVPS participant experiences an operational disruption or liquidity shortfall, it may be unable to transfer funds to its counterparties. As a result, other LVPS participants may have lower balances than expected. This shortage of funds could prevent these institutions from receiving incoming securities transfers in a linked central securities depository (CSD), causing securities to fail. In this way, a disruption in the LVPS could pass to the CSD. This type of interdependency creates what might be called a "cross-system" risk between the CSD and the LVPS.

Second, interdependencies can also act to spread disruptions simultaneously to several systems. This potential effect stems from systems depending on other critical systems, large financial institutions, or key PSPs. From an international perspective, many systems are dependent on the Society for Worldwide Interbank Financial Telecommunication SWIFT network. An outage of this network could have direct and immediate implications for many systems. From a domestic perspective, many systems are critically dependent on the primary LVPS, and a disruption affecting a LVPS could impair the functioning of those other systems.

Third, in some circumstances, interdependencies may transmit disruptions beyond systems and their participants to financial markets. The functioning of markets with relatively short settlement cycles, such as the markets for uncollateralized overnight loans and repurchase agreements, might be particularly affected.

The actual impact of a given disruption will depend on many factors, and is difficult to predict. First, systems' and institutions' risk management procedures can help prevent the transmission of disruptions across systems. Second, interdependencies can sometimes be useful in mitigating the impact of a disruption. For example, "liquidity bridges" can allow institutions to move available liquidity resources between systems, possibly helping to manage potential liquidity disruptions, and preventing their further transmission. Third, the reaction of systems and institutions to a particular disruption may significantly influence whether and how a disruption spreads. These reactions may be very difficult for other parties to anticipate. Moreover, market conditions can influence both the initial intensity of a disruption, as well as systems' and institutions' reactions to it.

Source: *"The Interdependencies of payment and settlement systems." Committee on Payment and Settlement Systems,"* Report of the Committee on Payment and Settlement Systems No. 84. Bank for International Settlements, Basel.

12 As institutions responsible for preserving the trust of the public in the national currencies, central banks exercise a special form of supervision of payment systems called "oversight". The oversight of payment systems is a central bank function whereby the objectives of safety and efficiency are promoted by monitoring existing and planned systems, assessing them against these objectives and, where, necessary, inducing change.[4] Oversight is a public policy activity focused on

4 See "Central bank oversight of payment and settlement systems," Report of the Committee on Payment and Settlement Systems No. 71, Bank for International Settlements, Basel, May 2005.

the efficiency and safety of systems, as opposed to the efficiency and safety of individual participants in such systems.[5] Overseeing payment systems involves putting in place policies to ensure the smooth and efficient provision of payment services to all participants and users in the economy, to control for the risk of systemic transmitting of shocks through the economy, and to promote the development of technical infrastructures and institutional arrangements to meet the economy's growing payment needs.

Oversight scope and powers

13 Oversight is mainly intended to cover payment infrastructures that are systemically important.[6] These include infrastructures whose failure can potentially endanger the operation of the whole economy. The scope of oversight therefore covers large-value payment systems. In an increasing number of jurisdictions, however, the oversight scope has been expanded to also cover those retail payment systems that, while not being systemically important, are nonetheless deemed to be relevant for the purpose of protecting public confidence in the currency and the monetary system of the country. To this purpose, effective oversight, today, increasingly requires central banks to extend their control to payment instruments and schemes and to individual PSPs (including banks, nonbanks, and nonfinancial institutions).

14 Effective oversight requires central banks to have the power and resources to effectively carry out their responsibilities to oversee payment systems.[7] While the primary responsibility for ensuring payment system safety and efficiency lies with system owners and operators, central banks need adequate powers and resources to administer their oversight responsibilities effectively. Today, in the majority of national jurisdictions, the law grants the central bank important powers to carry out oversight, in particular those actions to obtain timely information and to induce change or enforce corrective action, as well as to cooperate with other relevant authorities as necessary. Over recent years, central banks have increased considerably the (financial and human) resources assigned to payment system oversight functions.

Oversight objectives

15 Oversight aims to ensure that payment systems:

i operate smoothly and efficiently for all participants and users,

ii prove to be robust against risks,[8] in particular, the risk of transmitting shocks through the economy,

iii pursue over time the level of technological and institutional development necessary to satisfy the payment needs of a growing, open, and internationally integrated economy, and (increasingly),

iv support financial inclusion.

5 See "Policy issues for central banks in retail payments," Report by the Committee on Payment and Settlement Systems, Bank for International Settlements, Basel, 2003.

6 SEE "PRINCIPLES FOR FINANCIAL MARKET INFRASTRCUTURES," joint report by the Committee on Payment and Settlement Systems and the International Organization of Securities Commissions, Bank for International Settlements, Basel, April 2012.

7 SEE "Responsibilities of central banks, market regulators, and other relevant authorities for financial market infrastructures," under the "PRINCIPLES FOR FINANCIAL MARKET INFRASTRCUTURES," REFERRED TO IN FOOTNOTE 6.

8 Annex I reports a list with a brief description of the risks typically featured by payment systems.

Box 3. Safety and efficiency in payment systems

The concept of **efficiency** generally refers to the resources required by a system to perform its functions. Applied to payment systems, efficiency entails several aspects. One is the overall effect of the payment system on the cost of exchanging goods, services, and assets (including money) in the economy: a more efficient payment system reduces that cost. Relatedly, an efficient payment system provides its users with speedy, affordable, and easy to access use of services. Another aspect of efficiency relates to the resources necessary to operate a system: by introducing specific efficiency solutions, some systems may economize on the use of (costly) liquidity to settle payments, for any given level of settlement risk. Further aspects of payment system efficiency refer to the volume of transactions the system makes possible for any given quantity of money or to the speed of the transmission across the economy of monetary policy impulses.

On the other hand, **safety** is about protecting systems and stakeholders from hazards. Especially as it refers to large value transfer systems, safety means containment of the financial and non-financial risks which typically arise within these systems, or are transmitted by them, and which threaten not only to impair the functioning of the systems, but to jeopardize the financial stability of the overall economy. Safety requires that systems are secure, reliable, and operate without service interruption or recover operation promptly in the event of interruption. As the scope of central bank oversight extends to retail payment systems and instruments, the concept of safety necessarily broadens and involves other aspects, as users' expectations of payment service quality. Here safety, therefore, refers to the protection of user rights, in particular, those concerning safeguards of user own funds, data integrity and privacy, prevention of fraud and cyber-crime, information disclosure and transparency, and claim redress and dispute resolution.

16 Central banks in many jurisdictions have expanded their payment system strategic vision and, with it, the objectives and responsibilities of their oversight function.[9] In particular, as oversight extends to retail payment systems and instruments, efficiency and safety necessarily involve other aspects, since the expectations of payment service users take center stage in the definition of the criteria to assess how well the systems and instruments perform (see Box 3).

9 The case of India is illustrative, and it is interesting to examine how the payment system vision of the Reserve Bank of India (RBI) has progressed over the last decade. In its 2005-08 vision document, the RBI objective was "the establishment of safe, secure, sound and efficient payment and settlement systems for the country." In the subsequent vision document (2009-12), the RBI – much more assertively – indicated that it wanted "to ensure that all the payment and settlement systems operating in the country are safe, secure, sound, efficient, accessible and authorized." Finally, in its latest vision document (2012-2015), the goal has been broadened further "to proactively encourage electronic payment systems for ushering in a less-cash society in India and to ensure payment and settlement systems in the country are safe, efficient, interoperable, authorised, accessible, inclusive and compliant with international standards."

17 A number of other objectives and responsibilities have become integral to the oversight policy framework of central banks. They include:

Inclusiveness

18 Providing easily accessible and affordable payment services to the largest possible number of citizens, especially if unbanked, has become an important goal for many central banks. Since markets alone do not find it commercially convenient to provide payment services to poor communities, especially if located in remote, isolated, or sparsely populated geographical areas, central banks (as well as other financial regulatory agencies) are called upon to create the conditions to extend the availability of at least basic payment and financial services to underserved segments of the population, and to facilitate their progressive inclusion within the financial system.

Fairness

19 The central bank may want to ensure that the country's payment systems are perceived to be fair. Fairness implies that rules are applied consistently and in a non-discriminatory way across all relevant entities, based on objective, proportional, and transparent criteria. It requires that the rights and obligations of all parties to fund transfers in the payment system are allocated in an equitable manner, that participants and users are not subjected to misleading or abusive business-to-consumer commercial practices, and that disputed matters can find appropriate resolutions. Also, fairness means that system rules are designed in ways that reflect the interest of all stakeholders in a balanced manner, and are implemented consistently across the whole jurisdiction under central bank oversight. Fairness relates to avoiding the use of discriminatory practices on access and pricing, and to adopting adequate incentives (including sanctions) to encourage good behavior and penalize wrongdoings.

Transparency

20 Transparency discourages misconduct and abuses of payment systems and allows stakeholders to be more aware of risks and make better-informed decisions. Transparency ensures that the rights and obligations of participants and users, as well as the mechanisms to enforce them, are publicly disclosed. Central banks set regulations requiring payment system operators, participants, and PSPs to disclose rules, key procedures, and market data. Regulations also require PSPs to disclose charges and maximum execution times, to inform users on how to authorize and execute transactions and revoke payment orders, and to indicate the liability in case of unauthorized use of payment instruments and the right to payment refunds.

Market competition and integrity

21 Another oversight responsibility is to make sure that the market for the provision of payment services is protected against anti-competitive and abusive behaviors. This does not necessarily imply that the central bank should conduct antitrust policy in their market for payment services. However, the central bank is in a privileged position to monitor market developments and to intervene, or collaborate, with the competent authorities, in the event of anti-competitive practices. Also, the central bank may want to be satisfied that payment system operators, participants, and PSPs do not act in ways that breach public confidence in the payment system. In this regard, in cooperation with other relevant authorities, it guards against various forms of criminal abuse of payment systems, such as fraud, breaching of data integrity, cybercrime, money laundering, and the financing of criminal and terrorist activities.

Consumer protection

22 In several jurisdictions, the central bank is given the responsibility to protect payment system users from possible malpractices and abuses. To this end, the central bank ensures that PSPs put in place facilities through which customers can lodge complaints about unsatisfactory or below-standard services, abusive or unfair commercial or financial practices, and cases of non-compliance with legal and financial obligations. The central bank also strengthens its own internal consumer protection facilities, and makes sure that effective dispute resolution mechanisms are established so that users may resort to affordable and time-efficient means to settle payment-related claims. Moreover, the central bank keeps pressure on the payments industry to deploy adequate technological and organizational resources to minimize breaches of information security and privacy.

Interoperability

23 A robust environment of interoperability in the payment system benefits all payment system stakeholders. As discussed in the second part of this report, through interoperability among payment system infrastructures, payment system users (including consumers, merchants, governments, and other types of enterprises) find it easier to make and accept payments. Payment system interoperability can also improve efficiency by reducing cost and increasing safety by enabling better risk management. The role of the central bank as a catalyst can be crucial, especially where interoperability of multi-party systems does not happen on its own, where independent efforts may end up in processes or technologies that are not compatible, or where market competitors oppose interoperability and support proprietary solutions instead.

Oversight instruments

24 Payment system oversight is essentially about controlling risks in payment systems and promoting payment infrastructure and service development. Oversight instruments, therefore, should enable the overseer to be satisfied that critical payment system infrastructures have robust processes in place for identifying, prioritizing, sourcing, monitoring, and managing risks, and that these processes are improved continuously in a fast-changing business environment. Also, the use of oversight instruments should be proportionate to the nature, scale, and complexity of the risks inherent in the business of payment service provision, and the intensity and consequences of their use should be commensurate with the objectives of oversight. Finally, the oversight authorities need instruments to promote the modernization of payment system infrastructures and to foster the development of the market for the provision of payment services.

25 The oversight policy framework typically includes the following instruments:

Licensing & identification

26 The central bank should have the power to license any entity that intends to operate a payment system or to provide payment services after submission of appropriate documents and information, as prescribed by regulation. Licensing should be granted based on the fulfillment by the applicants of the regulatory requirements. The objective of licensing is to bring payment system operators and PSPs within the regulatory jurisdiction of the central bank. Prior to issuing a license, the central bank should be satisfied that the operator or PSP is capable of managing effectively the risks associated to their activity. The central bank should require information and documentation, which allows it to decide whether that system may be operated or the service provided in such a manner as not to pose excessive risks.

Box 4. Licensing and overseeing PSPs

The issue of licensing PSPs is becoming especially important as the number of non-financial entities offering payment or payment-related services is growing rapidly in an increasing number of jurisdictions, as in the case of business for the provision of mobile and Internet payment services. Identifying the "right" criteria for licensing and overseeing these entities requires a careful balancing act in that the oversight authority should want to ensure the payment system against the risks these entities bring into the systems while being able to avoid subjecting them to disproportionate regulatory requirements that might jeopardize their innovation capacity or put them at a competitive disadvantage vis-à-vis the financial PSPs.

Licensing requirements may include, inter alia, the following information to be provided by the applicant entity to the satisfaction of the oversight authority:

- A program of operations, setting out the type of payment services to be provided.
- A business plan, which should include an initial budget showing the resources available to the applicant, how it would employ them, and indications of business sustainability.
- Evidence of adequate capital: adequacy may vary in relation to the type of payment services to be provided, with higher capital required for services implying the operation of payment accounts or the issuance/acquiring of payment instruments, and smaller capital required for the provision of remittances or transactions that do not imply operation of payment accounts.
- Evidence of adequate own funds (in addition to capital): adequacy may be defined, alternatively, as a share of fixed overhead costs, as an increasing share of the payments volume, or as an increasing share of net income, adjusted for a factor that changes in relation to the type of services provided.
- Measures to safeguard payment service users' funds.
- A description of the applicant's governance arrangements and internal control mechanisms (including administrative, risk management, and accounting procedures).
- A description of the applicant's organizational structure, including, where applicable, a description of the intended use of agents and branches and a description of outsourcing arrangements, and of participation in a national or international payment system.
- A description of the applicant's technology solutions underpinning its operation and supply of services, and the arrangements adopted to ensure operational continuity under critical events.
- A description of the applicant's audit arrangements and measures to protect the interests of users and to ensure continuity and reliability in the performance of payment services.
- The identity of persons holding qualifying holdings in the applicant, the size of their holdings, and evidence of their suitability against the PSS oversight objectives.
- The identity of directors and managers, and indications of their suitability for the job.
- The applicant's legal status of association, and head office address.

27 Through identification, the central bank recognizes the systems that will be subjected to its oversight. The central bank should identify systems that it deems to be systemically important and those it considers to be critical for public confidence. The level of criticality of a payment system

should be determined based on a set of objective and transparent criteria. Identified systems should be assessed against selected oversight standards.

Monitoring, analysis & compliance

28 The central bank monitors payment system functioning on a continuous basis. It controls system operation through access to real-time systems and through regular information and data collection. The central bank analyzes payment system incidents and risks, and identifies weaknesses and needs for improvement or change. The central bank assesses the performance of payment systems, and, in particular, their robustness against risks. The central bank assesses the compliance of systems and providers with given rules and standards.

Rules & standards

29 The central bank issues regulations and adopts standards to induce payment system operators and PSPs to operate safely and efficiently. Regulations should be based on functions rather than institutions, and should be proportional to the risk profile of the regulated entities. Regulations should set rules, inter alia, for licensing PSPs, the operation of systems and the provision of services, the issuance of payment instruments, the use agents, the outsourcing of services, and the protection of user rights. In cases of non-compliance with existing laws and regulations, the central bank should administer appropriate sanctions. Regulations should support competition and a level playing field for participants. To induce payment system operators and PSPs to have robust procedures in place to handle risks effectively, the central bank should promote the adoption of best practices in line with internationally accepted principles and oversight standards.

Policy, research & development (R&D)

30 The central bank should promote R&D activities on payment system issues. These activities might range across several areas, from operational to legal, institutional, technological, and developmental areas. R&D should study payment system and payment services developments, providing essential inputs to payment system modernization strategy making, as well as methodological inputs to payment system stress testing and risk analysis.

Policy dialogue

31 The central bank should promote an active policy dialogue with all payment system stakeholders, including users. The dialogue should secure a fair representation of all relevant public and private interests involved in payment activities, and should offer a channel for the central bank to communicate its policy orientation and collect stakeholder views. The central bank should undertake consultations with payment system stakeholders on policy issues and options to mobilize knowledge, raise awareness, and build consensus around policy decisions. Thus, where practicable, the central bank and payment system stakeholders should agree on solutions to be adopted.

Inducing change

32 However, oversight should be conducted in the shadow of the powers granted by the law. Therefore, oversight powers should be used where necessary to effect change. In cases where stakeholders fail to act in ways that are consistent with the interests of the payment systems and the collectivity in general, the central bank, in full respect of its legal powers, should exercise the authority to impose the actions it deems necessary.

Payment System Interoperability

A. Relevance of interoperability

33 Interoperability of payment systems is important because of its effect on consumers, businesses, and the economy in general. In advanced markets and where scale has been achieved, interoperability helps businesses to manage costs, increase efficiency through shared infrastructures, and expand transaction volumes. Customers benefit from network effects and lower transaction costs. Governments believe that interoperability may greatly facilitate financial inclusion and reduce the costs associated with traditional cash and paper-based payment instruments.

34 Interoperability can help to achieve a number of strategic payment system objectives. It can enable cost-efficient payments to and from the unbanked population. Distributing physical cash to the unbanked (e.g., through salary payments or government welfare programs) remains expensive and insecure. Governments, businesses, and other large bulk payers should be able to use electronic payments (e.g. e-money, including mobile money) as a cost-efficient and reliable payment channel to reach this population. Industry collaboration, including interoperability, can facilitate these large bulk payments more efficiently. Interoperability also facilitates the use of these electronically received funds from customers without easy access to a physical bank branch. Second, interoperability may facilitate the replacement of cash with electronic means of payment in day-to-day transactions. The current use of e-money is still dominated by a money transfer followed by cash-out. By providing tailored solutions for retailers, and establishing interoperability with existing and future retail payment infrastructures, operators can expand the use of e-money. This would reduce cash conversions, provide convenience for customers, lower costs for operators, and increase the relevance of e-money. However, introducing interoperability alone (be it on a voluntary basis or by regulation), does not ensure that a market can reap all potential benefits – the timing and certain other environmental factors (e.g. the market share of individual providers) seem to be important factors when it comes to the success of interoperability – some of these aspects are discussed in other deliverables of the working group. The CPMI-WBG Payment Aspects of Financial Inclusion Report addresses the basic foundations and catalytic pillars for the universal access to and usage of transaction accounts comprehensively, to which interoperability can contribute.

Box 5. Terminology

In the context of electronic payments, the taxonomy of interoperability is extensive and several different types of interoperability have been defined in the existing literature.

- **Platform-level interoperability:** Permits customers of one PSP to send money to customers of another PSP.
- **Agent-level interoperability:** Permits agents of one service to serve customers of another service.
- **Customer-level interoperability:** Permits customers to access their account through any subscriber identity module (SIM) card.

These forms of interoperability entail e-money services in one market interworking with each other. It is also possible for e-money operators to interwork with other platforms outside their country and industry. Such forms of interoperability include:

- **E-money interconnection**: two PSPs, each offering two commercially and technically independent e-money services, interconnect their respective technical platforms to enable a customer affiliated with one service to send money from his or her e-money wallet to the e-money wallet of a customer affiliated with another service.
- **Interconnection with financial institutions**: one PSP, operating its own commercially and technically independent e-money service, interconnects its technical platform with the technical platform of a traditional financial PSP to enable interaction between the two platforms (i.e., a customer sending money from a mobile account to a bank account).
- **Interconnection with other payment networks**: one PSP, operating its own commercially and technically independent e-money service, interconnects with a separate payment system (i.e., connecting with the Visa or MasterCard payment networks).

Other definitions of interoperability include the following:

- **Scheme interoperability**: a feature of payment schemes, which consumers and businesses access through their relationships with their banks or other PSPs. Payment schemes are sets of rules and technical standards for the execution of payment transactions that must be followed by adhering PSPs. Banks or other PSPs join a scheme and agree to be bound by the rules set by the scheme. Payments flow from an end user that is the customer of one bank to an end user that is a customer of another bank; both banks are "in the scheme." Cheques, Electronic Funds Transfer schemes, as well as open-loop debit and credit card schemes are examples of this type of interoperability.
- **Network interoperability**: when one payment scheme negotiates an exchange agreement with another scheme. This is typically the case of cross-border or cross-regional payments acceptance arrangements, which allow the holder of a domestic credit card to use that card in another country. Network interoperability is rarely used when bank network members compete for business within a single market, since network interoperability would facilitate out-of-network banks competing for business with local banks.
- **Parallel system interoperability** allows the merchant or agent accepting payment from a consumer to participate in multiple schemes. A commercial PSP acts as an intermediary between the various schemes and the merchant. Although the merchant is technically separately accepting payments in the various schemes, doing so achieves some of the effects of interoperability. In many markets around the world, for example, merchants accept multiple card brands (Visa, MasterCard, American Express, etc.). These brands do not interoperate, but the experience for the merchant is essentially the same.

Source**:** *Davidson N. and P. Leishman, "The case for interoperability: Assessing the value that the interconnection of mobile money services would create for customers and operators," GSMA, Annual Report 2012, pp.13-24; "Interoperability in Electronic Payments: Lessons and Opportunities," CGAP, 2012.*

B. Interoperability and oversight policy

35 An interoperable payment system and the effective management of risks associated with interoperability should be a key objective of payment system oversight. It is important to have a clear understanding of how and to what extent current international oversight standards provide for effective means to promote safe and efficient interoperability. It will then be possible to consider ways to strengthen the oversight policy framework, including identifying expectations specifically tailored for interoperability, against which payment system operators and PSPs should be held accountable.

Interoperability and international standards

36 Interoperability is addressed by the *Principles of financial market infrastructures* (PFMIs).[10] As one of the different forms of interdependencies among financial market infrastructures (FMIs), interoperability is addressed in the PFMIs report under various principles. Principle 20 explicitly addresses FMIs links and their risk management by requiring that a FMI that establishes a link with one or more FMIs should identify, monitor, and manage link-related risks. In addition, interdependencies are covered in: (a) Principle 2 on governance, which states that FMIs should consider the interests of the broader markets; (b) Principle 3 on the framework for the comprehensive management of risks, which states that FMIs should consider the relevant risks that they bear from and pose to other entities; (c) Principle 17 on operational risk, which states that a FMI should identify, monitor, and manage the risks that other FMIs pose to its operations and the risks its operations pose to other FMIs; (d) Principle 18 on access and participation requirements, which states that FMIs should provide fair and open access, including to other FMIs; (e) Principle 21 on efficiency and effectiveness, which states that FMIs should be designed to meet the needs of their participants; and (f) Principle 22 on communication procedures and standards, which states that FMIs should use, or at a minimum accommodate, relevant internationally accepted communication procedures and standards. The combination of these principles should achieve a strong and balanced approach to interoperability.

Establishing RPS-specific principles for interoperability

37 While the PFMIs address interoperability in several contexts, it should be recognized that they have not been designed specifically to cover the risks associated with interoperability in RPS. In Europe, policy guidelines have been produced for interoperability between EU central counterparties,[11] while the European Central Bank (ECB) has formulated oversight expectations for overseeing links that connect retail payment systems – an area that only broadly relates with interoperability.[12] In fact, no institution or jurisdiction has so far considered setting up oversight criteria especially conceived for interoperability in RPSs.

38 It is therefore advisable to define a consistent set of oversight principles for managing the risks that may arise in connection with interoperability in RPS. The principles elaborated below cover risks associated with the legal, financial, and operational aspects of interoperability, as well as issues relating to their governance, access, efficiency, and effectiveness. The principles build on

10 See REFERENCE IN FOOTNOTE 6.

11 See the "Guidelines and Recommendations for establishing consistent, efficient and effective assessments of interoperability arrangements: final report," 10 June, 2013, issued by the European Securities and Markets Authority (ESMA), under Article 54(4) of the European Market Infrastructures Regulation.

12 See the "Oversight expectations for links between retail payment systems," European Central Bank, Frankfurt, November 2012.

international best practices.[13] They are based on the principle that the responsibility for managing the risks associated with interoperability lies first and foremost with the RPSs and each retail payment entity (RPE) operating and/or participating in interoperable systems. The oversight authorities should be responsible for making sure that such recommendations are fulfilled.

39 Importantly, any sound oversight framework for managing risks relating to interoperability in RPSs will require strong cooperation between relevant authorities. As interoperability of RPS involves several related dimensions (including legal, financial, operational, technical, procedural, and business aspects), different institutions bearing oversight, supervisory, and regulatory responsibilities – not just in the financial area – may need to be involved (on a regular or an ad hoc basis) to make sure that interoperability is established and sustained in a way that is consistent with overall payment system efficiency and safety.[14] Authorities should cooperate with each other, both domestically and internationally, as needed, with a view to fostering efficient and effective communication and consultation in order to support each other in fulfilling their respective mandates. Cooperation needs to be effective in normal circumstances and should be adequately flexible to facilitate communication, consultation, or coordination, as appropriate, especially during crisis situations. Issues of cooperation between different country authorities will be discussed in the companion report on payment system interoperability and central bank oversight policy in an international context.

C. Oversight principles for interoperability in RPS

40 The principles discussed in this section are intended for a broad audience. They are meant to provide policy indications on interoperability to payment system oversight authorities and to supervisory and regulatory institutions that cooperate with the oversight authorities. They are also addressed to operators of interoperable systems, payments scheme administrators, and retail payment entities as defined below. It must be noted that while it would be the responsibility of the oversight authorities to adopt the principles and include them as part of the internationally recognized standards for interoperable payment infrastructures, it would be the responsibility of system operators and payment scheme administrators to design rules that are consistent with the principles, administer the rules, and ensure, rules compliance from participants. The oversight authorities would assess the infrastructures against the principles and hold system operators and scheme administrators accountable for the implementation of the principles. The active involvement of system operators and scheme administrators in the implementation of the principles may help central banks to better accomplish the oversight objectives while reducing their handling of system administration. The companion report on *"Payment System Interoperability and Oversight: The International Dimension"* elaborates complementary principles for the oversight of interoperability between internationally linked or shared payment system infrastructures.

Definitions

41 In this section, the following definitions are used:

- **Retail payment entity (RPE):** a payment service provider (PSP) offering payment services to users or a payment infrastructure provider (PIP) supplying infrastructure services to PSPs. PSPs include deposit-taking institutions, credit institutions, and other authorized service

13 In particular, the proposed principles build on the ECB's oversight expectations for links between retail payment systems (see previous footnote) and on the EACHA Instant Payments Interoperability Guidelines V1.1, European Automated Clearing House Association, 19 November 2015.

14 In light of the technical nature of interoperability and, more broadly, in consideration of the increasing role that information and telecommunication technology providers play in RPSs, cooperation between the central bank as payment system overseer and the telecommunication regulatory authorities is required and practiced in several jurisdictions worldwide.

providers like postal offices, money transfer organizations or e-money institutions. PIPs include providers of automated clearing houses, automated cheque processing, payment switches, and settlement systems.

- **Interoperability agreement**: an arrangement among retail payment systems (RPSs) and retail payment entities (RPEs) to facilitate the delivery of interoperable payment services to users, consisting of a combination of: i) technical, legal, commercial and contractual agreements among participating institutions, ii) shared telecommunication links and common standards for the exchange of transaction data between access and acceptance devices of RPEs, and iii) a central coordinating structure to manage the clearing and settlement of transactions as well as related business aspects such as rules, procedures, fees, sanctions, etc.
- **Interoperable systems:** retail payment systems (RPSs) that are linked by an interoperability agreement.

GENERAL

Principle 1: RPEs that establish an interoperability agreement should identify, monitor, and manage its related risks.

Key issues:

1.1 RPEs should identify and assess all potential sources of risk arising from an agreement before entering into it and continue to assess on an ongoing basis once the agreement is established.

1.2 RPEs participating in an interoperability agreement should be able to meet all of their related obligations to the other participating RPEs in a timely manner.

1.3 RPEs that participate in an interoperability agreement should ensure that the risks generated in one system do not spill over and affect other systems.

1.4 Interoperability should not affect the ability of each RPE to continue to observe all applicable oversight principles to which it is subjected.

42 Prior to entering into an interoperability agreement, RPEs should conduct an initial assessment to evaluate the sources of risks potentially arising from the agreement. The type and degree of risk varies according to the design and complexity of the agreement and depends on whether one or more jurisdictions are involved in the agreement. Interoperability should be designed in such a way that risks are adequately mitigated.

43 RPEs participating in an interoperable agreement should assess their risk management procedures to ensure that they can effectively manage the risks that may arise from the agreement. In particular, RPEs should have robust risk management procedures to manage the legal, financial, and operational risks they are exposed to through other entities, as well as those they pose to other entities. These procedures should include business continuity plans allowing for a rapid recovery and resumption of critical activities, or alternative channels for processing cross-system payments.

44 An RPE participating in an interoperability agreement should be able to meet in a timely manner all of its related obligations to the other participating RPEs. Furthermore, an RPE's participation in an interoperability agreement should not compromise its ability to meet in a timely manner its obligations toward its own customers.

45 Furthermore, RPEs that participate in an interoperability agreement should ensure that the risks generated in one system do not spill over and affect the soundness of the other systems. Mitigation of such spillover effects may require the use of strong risk management controls. Particular attention should be placed on the links connecting the systems by virtue of the agreement and the risks that could be transmitted through such links.

Principle 2: A RPS that uses a RPE to achieve interoperability should measure, monitor and manage the additional risks arising from the use of the RPE.

2.1 Before establishing an interoperability agreement, the RPS should analyse all the risks related to the RPE selected to achieve interoperability.

2.2 The RPS should measure, monitor, and manage the additional risks (including legal, financial, and operational) arising from the use of the RPE.

2.3 The RPS should ensure that the RPE does not unduly restrict usage of the link by any participant.

46 An RPS could use an RPE to achieve interoperability. This could be, for example, a switch platform or a PSP such as a financial intermediary or a network operator. The RPS should measure, monitor, and manage the risks related to the RPE on an ongoing basis and provide evidence to the oversight authority that adequate measures have been implemented to limit and monitor these risks.

47 The management of risks should be commensurate to the number of parties involved in the interoperability agreement. In particular, if the RPE is a provider of clearing and/or settlement services and intervenes in the processing of the transactions, the number of entities through which the payment is routed increases and raises the risks involved. As a result, the risks should be assessed, monitored, and mitigated taking into consideration the higher number of entities involved in the agreement. The RPS should provide participants with the information necessary to conduct an assessment of the risks associated with the RPE.

48 The RPE should not unduly restrict any participant's usage of interoperability. Therefore, the RPS should examine the rules and procedures set by the RPE, and undertake any necessary action in the event of any restriction or discrimination.

LEGAL RISK

Principle 3: Interoperability agreements should have a well-founded, clear, and transparent legal basis that is enforceable in all relevant jurisdictions and provide adequate protection to the participating RPEs.

Key issues:

3.1 The legal framework (laws, regulations, rules and procedures) underpinning an interoperability agreement should provide a high degree of certainty for every aspect relating to interoperability.

3.2 The rules, procedures, and contracts governing the agreement should be clear, understandable, and consistent with relevant laws and regulations. They should be readily available as appropriate for all parties with a legitimate interest.

3.3 The rules, procedures, and contracts governing the agreement should be complete, valid, and enforceable in all relevant jurisdictions. There should be a high degree of certainty that actions taken under such rules and procedures will not be stayed, voided, or reversed.

3.4 The agreement should be consistent with the applicable regulatory frameworks.

3.5 In cross-border interoperable systems, risks arising from any potential conflicts of laws across jurisdictions should be identified and mitigated.

49 Payments processed via interoperable systems may be subject to higher legal risks, compared with those processed in a single system. Conflicts may arise if it is not clear which are the specific laws, regulations, rules, or procedures applicable to payments processed via interoperable systems. In exceptional circumstances (e.g., the default of a participant in one of the systems),

uncertainties or conflicts could arise if the rules governing interoperability do not clearly specify the procedures to be followed.

50 Conflicts may also arise when the legal basis, in particular the contracts, do not clearly define the rights and obligations of the RPEs participating in an interoperability agreement. Conflicts can stem from differences in laws and regulations defining rights and obligations, finality, and irrevocability, and settlement finality. In order to safeguard the protection of customers' assets, RPEs should determine appropriate liability regimes to minimize the potential loss for their customers. Legal risks should also be mitigated in case interoperability involves a settlement agent that temporarily holds the funds transferred between one RPE and another in a transitional account.

OPERATIONAL RISK

Principle 4: RPEs participating in an interoperability agreement should carefully assess the operational risks related to the interoperability.

Key issues:

4.1 The scope of information security policy of RPEs that participate in interoperable systems should cover all aspects relating to interoperability.

4.2 Operational arrangements for interoperability should be agreed to by the RPEs and communicated to all relevant parties.

4.3 RPEs should ensure that their risk management capacity is sufficiently scalable and reliable in order for them to comply with the operational requirements of interoperability both at the current and projected peak volumes of activity and to achieve the agreed service level objectives.

4.4 Interoperability should be appropriately tested and monitored, and incidents should be logged and followed up. RPEs participating in interoperable systems and all parties involved should agree on business continuity plans that preserve interoperability under even extreme adverse circumstances.

51 RPEs participating in an interoperability agreement should assess the operational risks arising from interoperability. They should identify the possible effects of interoperability on their own ability to process payments in the normal course of business, and to manage risks that stem from other participating RPEs experiencing an external operational failure. RPEs should be committed to providing reliable services, not only for the benefit of their customers, but for all entities that would be affected by their inability to effect payments.

52 Participating RPEs should agree on specific service levels. These levels should be defined in a service level agreement and include operational reliability requirements for interoperability. RPE availability should be specified as part of the agreement rules, including the strategies for dealing with RPE non-availability in a way that still provides satisfaction to customers.

53 An interoperability agreement should impose on participating RPEs, general obligations to follow and comply with. The agreements should include an obligation for RPEs to have a compliance program to ensure service continuity. The impact on customers when a RPE is non-compliant is different in batch systems and real time payment systems. In a batch system, there may be time for a remitting RPE to correct and resubmit rejected payments without customers being aware, whereas in a real-time system payment rejections impact the customer immediately. Therefore, real time systems normally require higher levels of testing to ensure continuity of service both during implementation and also when RPEs and central processors make changes post live. Participating RPEs should agree bilaterally what testing regimes they need to apply to ensure that all actors remain compliant with all agreed technical rules and standards.

54 Connectivity and security policies of RPEs should be covered by an interoperability agreement. One solution could be for full alignment between systems and security provisions and for preferred technology solutions to be agreed and specified under the agreements. As an alternative, networks and security protocols could be agreed upon bilaterally by participating RPEs. In practice, there may be a general rule whereby the sending RPE uses the connectivity solutions and complies with the security of the receiving RPE.

55 RPEs participating in an interoperability agreement need to share information. RPEs should provide an appropriate level of information to share with each other in order for each of them to perform a robust and periodic assessment of the operational risks associated with interoperability and take measures to contain these risks. Systems and communication arrangements should be reliable and secure so that interoperability does not pose a significant operational risk to the participating RPEs. Any reliance on a critical service provider by a RPE should be disclosed as appropriate to the other RPEs. In addition, in the case of a cross-border interoperability arrangement, participating RPEs should consider operational risks resulting from complexities or inefficiencies associated with differences in time zones, particularly as these differences can affect staff availability.

56 Operational malfunctioning should require cooperation. In case of operational malfunctioning, an incident is likely to be resolved more efficiently if the measures are undertaken by the participating RPEs in cooperation with each other and in accordance with pre-established, clear, and immediately available procedures, stating the division of responsibilities and contact information. It must be considered that an incident in interoperable systems could impact the processing of payments not involving interoperability, and vice versa. Thus, rules and procedures related to business continuity should be coordinated and regularly tested; contact lists should be kept updated for both normal and abnormal circumstances.

FINANCIAL RISK

Principle 5: RPEs participating in an interoperability agreement should closely monitor and effectively measure and manage the financial risks arising from the agreement.

Key issues:

5.1 RPEs should have a clear understanding of the impact interoperability has on each of the financial risks they incur.

5.2 The assets used for settling payments via interoperable systems should carry little or no credit or liquidity risk.

5.3 Payments exchanged via interoperable systems should be settled promptly, preferably on an intraday basis.

5.4 The terms and conditions of an interoperability agreement should ensure adequate arrangements for managing and containing the risks associated with the inability of one of the participating retail payment entities to promptly fulfil its obligations.

57 RPEs participating in an interoperability agreement might be exposed to additional credit and liquidity risks. Interoperability causes an exposure of one RPE and its customers to another RPE and its customers. A risk can materialize if a participating RPE defaults, causing liquidity pressures on other RPEs. This risk may increase when a netting process takes place. Also, interoperability causes an additional exposure if a participating RPE temporarily holds the funds transferred between one retail payment entity and the other in a transitional account. Moreover, interoperability may create significant credit and liquidity interdependencies between systems. Problems may arise if, for example:

- One of the systems permits provisional transfers of funds that may be subject to an unwinding procedure.
- There are differences regarding the moment of finality.
- One of the systems experiences an operational problem that could expose participants in the arrangement to losses.

58 Interoperability agreements should specify rules on payment finality. Participating RPEs should state in their rulebooks that payments are final once they are confirmed as successful to the remitting RPE. In other words, when the remitting PSP receives a positive confirmation from the beneficiary RPE via the interbank system, payment finality has been achieved and the payment may not be recalled by the payer without the consent of the beneficiary. In addition, settlement should be guaranteed to ensure there is no settlement risk and that settlement is assured in the event of the insolvency and exclusion of a RPE, particularly where settlement is based on a deferred model. The system of guarantees used will require agreement with the relevant national central bank(s).

59 Where interoperability involves more than one RPS, interoperability agreements should include rules for settlement finality. Guaranteed finality should apply to each step in the chain, i.e., where a payment flows from one RPS to another, the payment will be guaranteed in the first system before being passed to the second system.

60 There are a variety of strategies for guaranteeing settlement in interoperable systems. All such strategies require the remitting RPE in some way guaranteeing payment to the beneficiary RPE in a way that would not be affected by insolvency or RPE failure. Some of the options are as follows:

- cash prefunding (either periodic deferred net settlement or settlement in real time),
- pledging non-cash collateral to the central bank,
- bilateral guarantees between banks,
- loss-sharing agreements,
- trust lines.

61 RPEs participating in an interoperable agreement should have access to all the information necessary to conduct an assessment of credit and liquidity risks associated with interoperability.

ACCESS CRITERIA

Principle 6: Criteria for access to interoperable systems should be clear, objective, non-discriminatory, and publicly disclosed.

Key issues:

6.1 Access criteria should be justified in terms of the safety and efficiency of the system, as well as the broader financial markets.

6.2 Price setting in interoperable systems should be non-discriminatory and transparent.

6.3 Exit rules and procedures from interoperability agreements should be clearly defined and disclosed.

62 Access criteria to interoperable systems should ensure a level playing field among RPEs. Access criteria should be justified in terms of the safety and efficiency of the system, as well as the broader financial markets. From a risk mitigation perspective, the access criteria should aim to minimize legal, financial, and operational risks. A RPS should assess whether participating RPEs have the requisite operational capacity, financial resources, legal foundation, and risk-management expertise so that risks are adequately mitigated and managed. From an efficiency viewpoint, the

access criteria may be based on the business case. The access criteria should have the least restrictive impact on access that circumstances permit.

63 Access criteria should be commensurate with the risks generated by interoperability and those to which participating RPEs may be exposed.

64 If access to interoperable systems is refused by system owners or operators to an applicant RPE, the reasons should be explained to the applicant in writing on the basis of the access criteria adopted.

654 When access criteria constitute terms and conditions for maintaining an interoperability agreement, they should be continuously applied. RPEs should monitor compliance with participation requirements on an ongoing basis through the receipt of timely and accurate information. If conditions for maintaining interoperability are no longer met, rules and procedures should be legally set either for the termination of the non-complaint RPEs or for dismantling an interoperability agreement, depending on the extent of the problem.

66 The pricing policies adopted by interoperable systems should be transparent and non-discriminatory.

EFFICIENCY AND EFFECTIVENESS

Principle 7: Interoperability should meet the requirements of participating RPEs and the markets they serve.

Key issues:

7.1 A RPS should have clearly defined, achievable, and (where feasible) measurable goals concerning interoperability, e.g., in the areas of minimum service levels, risk management expectations, and business priorities. An RPS should have established mechanisms for the regular review of the efficiency and effectiveness of interoperability.

7.2 Interoperability should be designed to meet the current and future needs of its participants and the markets it serves.

7.3 The establishment of interoperability should not put the balance of RPEs at risk in terms of risk management and efficiency.

67 Interoperability should be consistent with the objective to improve payment system efficiency and effectiveness. Interoperability should facilitate the clearing of payments by ensuring a single gateway to multiple systems and jurisdictions (in case of cross-border arrangements). Furthermore, the establishment of interoperability agreements should support the relevant public policies, e.g., by facilitating the exchange of payments domestically or internationally and improving the reachability of the RPS participants and their customers. The ultimate objective of interoperability should be to improve efficiency when settling payments initiated by any customer in terms of shortening the settlement time and reducing the fees for processing payments.

68 To ensure efficiency for its users, an interoperability agreement should be designed with the users' current and future needs in mind. These may include the size of their activity (number of payments), the efficiency of the channels currently used for clearing payments, and the jurisdictions within which they exchange payments. The decision on whether to establish interoperability should be based on a cost-benefit analysis.

69 Interoperability is effective when it allows for exchanging payments reliably and in a timely manner, and when it allows to achieve the public policy goals of safety and efficiency for participants and the markets it serves. In the context of oversight, interoperability effectiveness requires meeting service and security requirements. To facilitate assessments of effectiveness, an RPS

should have clearly defined goals and objectives. For example, it should set minimum service level targets (such as the time it takes to exchange a payment).

70 The efficiency and effectiveness of interoperability should be measurable. A RPS should have established mechanisms for the regular review of interoperability efficiency and effectiveness, such as periodic measurement of its progress against its goals and objectives.

71 Interoperable systems should provide users with practical services. Rules and solutions to establish interoperability should consider market practices and technology and/or accommodate internationally accepted communication procedures and standards adhered to by participating RPEs.

GOVERNANCE

Principle 8: The governance of interoperable systems should be clear and transparent, promote the safety and efficiency of interoperability, and support the objectives of relevant stakeholders and relevant public interest considerations.

Key issues:

8.1 The governing bodies of RPSs should formulate a clear strategy on the establishment of an interoperability agreement, which should be disclosed to owners, relevant authorities, RPEs, other RPSs, and users.

8.2 The governing bodies of RPEs participating in an interoperability agreement should be responsible for ensuring the efficient and safe provision of interoperable services.

8.3 A RPS should have objectives that place a high priority on the safety and efficiency of interoperability and explicitly support the public interest.

8.4 Governance should ensure whether a decision to establish interoperability appropriately reflects the objectives and interests of the relevant stakeholders and, if so, how.

8.5 A RPS involved in an arrangement should set rules for the exchange of data, sharing relevant information with relevant stakeholders, and consulting them when needed.

72 Interoperability may represent a significant strategic objective of RPS development, as it increases reachability and allows RPSs to expand their service provision. The governing bodies (board of directors, management, and staff) of interoperable systems should define a clear strategy regarding the establishment of interoperability arrangements, which should be disclosed to owners, relevant authorities, RPEs, users, and other RPSs, and should be ultimately responsible for ensuring safe and efficient interoperable services. The governing bodies of the RPS should put in place a well-defined policy framework to govern interoperability.

73 Any decision pertaining to the establishment or dismantling of an interoperability agreement should be taken in the context of an open, transparent, and inclusive decision-making process. It should be ensured that the relevant stakeholders are consulted and that their interests are addressed as much as possible. This implies that the governance of the interoperability should, at the very least, include the relevant stakeholders. The relevant stakeholders should be consulted prior to the establishment of an interoperability agreement. Also, the relevant stakeholders should be notified of any change affecting it once the agreement is established.

74 Interoperability entails relationships between several parties. The division and sharing of responsibilities for the operation of interoperability must be determined. Some decisions regarding interoperability might need to be taken collectively. Therefore, all the parties involved should preferably implement formalized mechanisms for taking decisions on, for example: (i) the alignment of business strategies; (ii) problems encountered in ensuring interoperability; (iii) user needs and claims; and (iv) changes to business and operational procedures. The sharing and division

of responsibilities should be strongly supported by an efficient exchange of information. The exchange of data should be rules-based. All entities involved should agree on a regular exchange of information and periodic meetings allowing for issues of common interest to be discussed.

75 Interoperability requires managing diverse stakeholder interests and opinions. As opinions and interests among parties involved in interoperability may differ, there should be clear processes for identifying and appropriately managing the diversity of stakeholder views and any conflicts of interest between stakeholders. Without prejudice to local requirements of confidentiality and disclosure, there should be processes to clearly and promptly inform stakeholders and the wider public of the outcome of major decisions concerning interoperability.

Annex I

Payment system risk glossary

Credit risk	The risk that a counterparty will not settle an obligation for full value, either when due, or at any time thereafter. In exchange-for-value systems, the risk is generally defined to include replacement cost risk and principal risk.
Finality risk	The risk that a provisional transfer of funds or securities will be rescinded.
Financial risk	Term covering a range of risks incurred in financial transactions – both liquidity and credit risks.
Foreign exchange settlement risk	The risk that one party to a foreign exchange transaction will pay the currency it sold but not receive the currency it bought.
Fraud	Risk of financial loss for one of the parties involved in a payment transaction arising from wrongful or criminal deception. The risk that a transaction cannot be properly completed because the payee does not have a legitimate claim on the payer.
Gridlock	A situation that can arise in a funds or securities transfer system in which the failure of some transfer instructions to be executed (because the necessary funds or securities balances are unavailable) prevents a substantial number of other instructions from other participants from being executed.
General business risk	Any potential impairment of the FMI's financial position (as a business concern) because of a decline in its revenues or an increase in its expenses, such that expenses exceed revenues and result in a loss that must be charged against capital.
Legal risk	The risk of loss due to the unexpected application of a law or regulation, because a contract cannot be enforced, or because laws or regulations do not support the rules of the securities settlement system, the performance of related settlement arrangements, or the property rights and other interests held through the settlement system. Legal risk also arises if the application of laws and regulations is unclear.
Liquidity risk	The risk that a counterparty (or participant in a settlement system) will not settle an obligation for full value when due. Liquidity risk does not imply that a counterparty or participant is insolvent since it may be able to settle the required debit obligations at some unspecified time thereafter.
Market risk	The risk of losses in on- and off-balance sheet positions arising from movements in market prices.
Operational risk	The risk that deficiencies in information systems or internal controls could result in unexpected losses. These deficiencies could be caused by

	human error or a breakdown of some component of the hardware, software, or communications systems that are crucial to settlement.
Pre-settlement risk (or replacement cost risk)	The risk that a counterparty to an outstanding transaction for completion at a future date will fail to perform on the contract or agreement during the life of the transaction. The resulting exposure is the cost of replacing the original transaction at current market prices and is also known as replacement cost risk.
Principal risk	The risk that the seller of a security delivers a security but does not receive payment or that the buyer of a security makes payment but does not receive delivery. In this event, the full principal value of the securities or funds transferred is at risk. In the settlement process, this term is typically associated with exchange-for-value transactions when there is a lag between the final settlement of the various legs of a transaction (i.e., the absence of delivery versus payment).
Reputational risk	The risk of loss of confidence in the payment system due to lack of management control, capacity, security, business continuity plans, and/or contingency measures.
Settlement risk	General term used to designate the risk that settlement in a transfer system will not take place as expected. If a party defaults on one or more settlement obligations to its counterparties or to a settlement agent, this can generate both credit and liquidity risk.
Systemic disruption	Events whose impact has the potential to threaten the stability of the financial system, by transmission from one financial institution to another, including through the payment system.
Systemic risk	The risk that the failure of one participant in a transfer system, or in financial markets generally, to meet its required obligations will cause other participants or financial institutions to be unable to meet their obligations (including settlement obligations in a transfer system) when due. Such a failure may cause significant liquidity or credit problems and, as a result, might threaten the stability of financial markets.