



# **Oversight Framework for Financial Market Infrastructures (FMIs) and Retail Payment Systems (RPSs)**

**Version 2.0**

**Reserve Bank of India**

**Department of Payment & Settlement Systems**

**Central Office**

**June 13, 2020**

## Objective

*This document sets out the policy framework adopted by the Reserve Bank of India for the oversight of Financial Market Infrastructures (FMIs) and Retail Payment Systems (RPSs) operating in India.*

## Table of Contents

<b>Section</b>	<b>Page Number</b>
Section 1: Background	1
Section 2: Introduction	3
Section 3: Legal Framework for Oversight	6
Section 4: Designation of FMIs Regulated by RBI	9
Section 5: Definition and Scope of Oversight	12
Section 6: Oversight Activities	20
Section 7: Cooperation with Other Regulatory Authorities	35
Section 8: Organisation of the Oversight Function	38
Appendix 1: Schedule of Activities	39
Appendix 2: Information Submitted as Part of the Application	44
Appendix 3: Returns, Documents and Other Information to be Submitted by Authorised Payment System Operators / Participants	45
Appendix 4: Data / Information to be Furnished by CCIL	47
Appendix 5: Overview of Principles for Financial Market Infrastructures (PFMIs)	49
Appendix 6: IT Audit, Security, Fraud prevention and Risk Management Framework	62
Appendix 7: System Audit of Authorised Payment System Operators under Payment and Settlement Systems (PSS) Act, 2007 – Review of Scope and Coverage	65
Appendix 8: Format of Data / Returns / Information / Reports	69
Appendix 9: General Applicability of Principles to Specific Type of FMIs	72
Appendix 10: Applicability of PFMIs to Important Retail Payment Systems (IRPS) and Other Retail Payment Systems (ORPS)	74
Appendix 11: Table of Acronyms	75

## **Section 1: Background**

A Financial Market Infrastructure (FMI) is defined as 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. The term FMI generally refers to Systemically Important Payment Systems (SIPS), Central Securities Depositories (CSDs), Securities Settlement Systems (SSSs), Central Counter Parties (CCPs), and Trade Repositories (TRs) that facilitate the clearing, settlement, and recording of financial transactions.

**1.2** FMIs form the backbone of the financial system and contribute to financial stability and economic growth by providing reliable, safe, secure and efficient payment, clearing and settlement services to the users. They perform a unique role in the financial system by connecting a variety of financial institutions and financial markets together by way of their transactions with each other. Market functioning and financial stability rely on ensuring the continuity of the services that these infrastructures provide.

**1.3** Payment and settlement systems enable lending and repayment of money, allow businesses to receive payments for goods and services offered, and facilitate payment of salaries and benefits to the general public. They also enable the transfer of money and financial instruments between economic entities. Payment systems typically handle large volumes and values of transactions, which are necessary for any market economy to function.

**1.4** SSSs enable the purchase and sale of equities and bonds, and also effect their settlement by book entry according to a set of predetermined multilateral rules. A CSD provides securities accounts, central safekeeping services, and asset services, which may include the administration of corporate actions and redemptions and play an important role in ensuring the integrity of securities issues. These are systems that keep records of ownership of individual securities and also facilitate the transfer of ownership of these securities between people or entities. On the other hand, CCPs sit between the buyers and sellers of financial contracts and offer their guarantee and assurance to the participants that their contractual obligations in a range of financial and commodity markets will be honoured even if the original counterparty defaults. A TR is an entity that maintains a centralised electronic record (database) of transaction data.

**1.5** Central Banks are closely involved and have interest in FMIs for the purpose of conduct of its monetary policy and implementation of Government's fiscal policy as well as achieving enhanced financial inclusion, which largely depend on the availability of reliable and effective FMIs. The fundamental purpose of money to function as a means of exchange is fulfilled only by efficient payment and settlement systems. This in-turn affects the Central Banks' objective

of maintaining public confidence in money and in the instruments and systems used to transfer money.

**1.6** While safe and efficient FMIs contribute to maintaining financial stability and promoting economic growth, several incidents in the financial market have also shown that there could be major financial risks embedded in them. If these risks are not managed prudently, they could create a systemic risk situation in which the financial market could stop functioning and be a potential source of financial shocks, such as liquidity dislocations and credit losses.

**1.7** Retail payment systems, especially the electronic ones, which consist of different systems and platforms, payment products and services that allow firms, corporates, individuals, governments, and other economic agents to transfer money on a daily basis without having to use cash, have become increasingly prevalent in the Indian economy. This has been largely due to the dynamism the digital innovation has brought with new mobile and online payment solutions and products. The retail electronic payments eco-system in the country is now characterized by the existence of a wide variety of payment systems, payment instruments and payment channels that can be used by different segments of users (individuals, corporate / businesses, and government) to meet their differing payment needs.

**1.8** Among the new ways adopted by retail payment systems are the use of mobile phones as a device and access channel for making and receiving payments (mobile payments), use of internet on different devices for making purchases (internet payments), use of payment cards in ATM and PoS networks and with contactless technology (card payments and tokenization), electronic billing and use of various systems and platforms for making instant payments. Further, although retail payment systems have traditionally been generated by banks and other financial institutions, the payment space has now been increasingly opened up for non-bank players acting as operators of platforms for payment systems or as payment system providers (PSPs).

**1.9** While efforts continue to be made for promoting universal access to and use of financial services in an attempt to reduce poverty and improve opportunities and living standards for people, retail electronic payment systems is being represented as a highly potential instrument for fostering financial inclusion as individuals and firms interact in the economy via the payments they make to each other. Unlike large value payment systems focused on meeting the needs of financial institutions and large corporations in different financial markets, retail payment systems focus on the needs of each individual for making and receiving payments.

**1.10** Efficiency is thus very relevant for retail payment systems. The speed and ease with which payments can be executed will have the potential to affect economic activity. The speed of processing, the accessibility and convenience of the system, its reliability and accuracy are various aspects of quality that may add value to the users. Central Banks have an operational role in the clearing and settlement services and also perform oversight role on retail payment systems.

**1.11** It is important that FMs as well as retail payment systems are resilient to disruption, including financial and operational shocks, so that they continue to provide critical service to the economy and support wider financial stability and economic development. As such, Central Banks have an important role to play in this area given their responsibility to preserve the smooth functioning of payments systems, and more recently to support efforts for promoting financial inclusion.

## **Section 2: Introduction**

**2.1** The Committee on Payment and Settlement Systems (CPSS, now Committee on Payments and Market Infrastructures – CPMI), in May 2005, published the report on “*Central bank oversight of payment and settlement systems*”<sup>1</sup>. The report highlights the importance of Oversight and states as follows:

*“Oversight of payment and settlement 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.”*

**2.2** This report has listed five general principles to be followed by the central banks for conducting effective oversight of payment and settlement systems, regardless of the differences between central banks in the scope of oversight in terms of the broad public policy objectives of safety and efficiency, which are reproduced below:

- (i) **General oversight principle A: Transparency** – *Central banks should set out publicly their oversight policies, including the policy requirements or standards for systems and the criteria for determining which systems these apply to.*
- (ii) **General oversight principle B: International standards** – *Central banks should adopt, where relevant, internationally recognised standards for payment and settlement systems.*
- (iii) **General oversight principle C: Effective powers and capacity** – *Central banks should have the powers and capacity to carry out their oversight responsibilities effectively.*

---

<sup>1</sup> CPSS – Central Bank oversight of payment and settlement systems – May 2005

- (iv) **General oversight principle D: Consistency** – *Oversight standards should be applied consistently to comparable payment and settlement systems, including systems operated by the central bank.*
- (v) **General oversight principle E: Cooperation with other authorities** – *Central banks, in promoting the safety and efficiency of payment and settlement systems, should cooperate with other relevant central banks and authorities.*

**2.3** The CPSS and International Organisation of Securities Commissions (IOSCO) have established, over the years, international risk-management standards for payment systems that are systemically important, CSDs, SSSs, and CCPs. In February 2010, the CPSS and the Technical Committee of IOSCO launched a comprehensive review of the three existing sets of standards for FMIs<sup>2</sup> – the Core Principles for Systemically Important Payment Systems (CPSIPS), the Recommendations for Securities Settlement Systems (RSSS), and the Recommendations for Central Counterparties (RCCP) – in support of the FSB’s broader efforts to strengthen core financial infrastructures and markets by ensuring that gaps in international standards are identified and addressed. Accordingly, a comprehensive set of 24 principles were issued as part of the report titled “Principles for Financial Market Infrastructures” (PFMI)<sup>3</sup> published in April 2012.

**2.4** The main objectives of these principles for FMIs are to enhance safety and efficiency in payment, clearing, settlement, and recording arrangements, and more broadly, to limit systemic risk and foster transparency and financial stability.

**2.5** The document has, in addition to the Principles, indicated five responsibilities that are expected from the central banks, market regulators and other relevant authorities for FMIs. These are reproduced below:

- (i) **Responsibility A – Regulation, supervision and oversight of FMIs** – FMIs should be subject to appropriate and effective regulation, supervision, and oversight by a central bank, market regulator, or other relevant authority.
- (ii) **Responsibility B – Regulatory, supervisory, and oversight powers and resources** – Central Banks, market regulators, and other relevant authorities should have the powers and resources to carry out effectively their responsibilities in regulating, supervising, and overseeing FMIs.
- (iii) **Responsibility C – Disclosure of policies with respect to FMIs** – Central Banks, market regulators, and other relevant authorities should clearly define and disclose their regulatory, supervisory, and oversight policies with respect to FMIs.

---

<sup>2</sup> CPSS “Core Principles for systemically important payment systems” (January 2001), CPSS-IOSCO “Recommendations for securities settlement systems” (November 2001), and CPSS-IOSCO “Recommendations for central counterparties” (November 2004).

<sup>3</sup> Available at the BIS website (<http://www.bis.org/publ/cpss101a.pdf>).

- (iv) **Responsibility D – Application of the Principles for FMIs** – Central Banks, market regulators, and other relevant authorities should adopt the CPSS-IOSCO PFMI and apply them consistently.
- (v) **Responsibility E – Cooperation with other authorities** – Central Banks, market regulators, and other relevant authorities should cooperate with each other, both domestically and internationally, as appropriate, in promoting the safety and efficiency of FMI.

**2.6** The Reserve Bank of India (RBI) has adopted the above international standards, i.e. “the PFMI” and “Central Bank Oversight of Payment and Settlement Systems” for implementation by the FMI regulated by it, through issuance of Policy document on “*Regulation and Supervision of FMI regulated by RBI*”, in June 2013. This document describes in detail the criteria for designating an FMI<sup>4</sup>, applicability of the PFMI to the FMI, oversight of FMI and other related aspects.

**2.7** From 1998 onwards, RBI has been continuously bringing out a Payment Systems Vision document covering a period of three years, enlisting the road map for implementation. As per Vision 2012-15, the approach was 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. Subsequently, the Vision 2015-18 laid stress on building best of class payment and settlement systems for a ‘less-cash’ India through responsive regulation, robust infrastructure, effective supervision and customer centricity. While building on the constructs and achievements of the Vision statement of 2015-18, the Payment Systems Vision 2019-21 recognises the need for continued emphasis on innovation, cyber security, financial inclusion, customer protection and competition. While the core theme of the current Vision statement is “Empowering Exceptional (e)Payment Experience”, it focusses on empowering every Indian with access to a bouquet of e-payment options that is safe, secure, convenient, quick and affordable. While the pursuit towards a ‘less cash’ society continues, accompanied by the ambition to have a less-card India as well, the endeavour is to also ensure increased efficiency, uninterrupted availability of safe, secure, accessible and affordable payment systems as also to serve segments of the population which are hitherto untouched by the payment systems.

**2.8** The efforts made by RBI have resulted in continuous expansion of payment landscape not only in terms of growth in payment infrastructure but also in terms of volume and value of digital payment transactions. There has been continued decrease in the share of paper-based

---

<sup>4</sup> Real Time Gross Settlement (RTGS), Securities Settlement Systems (SSSs), Clearing Corporation of India Ltd. (CCIL) and Negotiated Dealing System (NDS).

clearing instruments, coupled with consistent growth and launch of new payment systems in individual segments of retail electronic payment systems as well as increase in registered customer base for mobile banking. Especially, the Retail Payment Systems (RPS) have risen to prominence with the new payment systems, such as Unified Payments Interface (UPI) and Aadhaar enabled Payment System (AePS), put in place by National Payments Corporation of India (NPCI) gaining traction, entry of non-bank players in the payment ecosystem bringing in innovation by leveraging technological advancements, and a gradual shift in the customer behaviour from cash to digital payments. With the continuously changing payment system landscape, the oversight objectives and activities have also concomitantly evolved over a period of time. Supervision involves assessing the safety and soundness of payment systems, providing feedback as appropriate, and using powers for timely intervention where necessary. With changing landscape of the payment ecosystem and the need for transparency and clarity among the stakeholders as well as central bank's responsibility to clearly define and disclose their regulatory, supervisory, and oversight policies with respect to FMIs and RPSs, the Reserve Bank of India has revised / updated the existing policy document (published on RBI website in June 2013) as "Oversight Framework for FMIs and Retail Payment Systems".

**2.9** This revised policy document describes the approach of RBI in its oversight of not only FMIs (regulated by RBI) but also the RPSs operating in India. In addition to FMIs, the applicability of PFMIs to some of the important RPSs is also discussed and provided for. Since some of the Principles may not be relevant for certain specific types of FMIs and important RPSs, RBI may impose higher requirements, depending on the gravity of the risks the RPSs expose to the market participants or in the context of wider financial sector stability. The table of acronyms used in the document is given as Appendix 11.

### **Section 3: Legal Framework for Oversight**

**3.1** The Payment and Settlement Systems Act, 2007 (PSS Act) has designated and confers upon the RBI the right to regulate and supervise Payment Systems<sup>5</sup> within the country. The RBI exercises its powers, performs the functions and discharges the duties conferred on it under the PSS Act through the "Board for Regulation and Supervision of Payment and Settlement Systems (BPSS)". Exercising these powers, the RBI has prescribed standards for payment instruments such as cheques, for secure message transmission in the form of SFMS (Structured Financial Messaging System), etc.

---

<sup>5</sup> "Payment system" means a system that enables payment to be effected between a payer and a beneficiary, involving clearing, payment or settlement service or all of them, but does not include a stock exchange. It includes the systems enabling credit card operations, debit card operations, smart card operations, money transfer operations or similar operations. The term "Payment System" shall be construed as reference to a "designated trade repository". "settlement" means settlement of payment instructions and includes the settlement of securities, foreign exchange or derivatives or other transactions which involve payment obligations.



**3.2** Chapter III of the PSS Act lays down that “no person, other than the Reserve Bank, shall commence or operate a payment system except under and in accordance with an authorisation issued by the Reserve Bank under the provisions of this Act”. Thus, it is clear that all payment systems functioning in India, involving payment obligations as a result of clearing or settlement of one or more payment instructions relating to funds, securities or foreign exchange or derivatives or other transactions, have to be authorised by the RBI. The PSS Act also provides powers to RBI to issue authorisation for operating the payment systems, and also to revoke the authorisation given to such system providers in case of contraventions of any provisions of PSS Act, PSS Regulations, 2008, orders or directions issued by the RBI or operation of payment system in contrary to the terms and conditions subject to which the authorisation was issued.

**3.3** After the global financial crisis in 2007-08, several developments took place, driven primarily by the G20, for reforming the Over the Counter (OTC) derivatives markets. The TRs emerged as a new type of FMI particularly in the OTC derivatives market. In line with the G20 commitment and the global developments, the PSS Act was amended to include Trade Repository<sup>6</sup> as another category of payment system. Accordingly, the provisions of PSS Act also apply to the TRs that have been designated as such by the RBI.

**3.4** Chapter IV of the PSS Act and its various Sections / clauses, provide for the Regulation and Supervision of such Payment Systems. The powers to regulate and supervise comprise:

- (i) **Section 10: Power to determine and prescribe standards** – in respect of format, size and shape of payment instructions, timings to be maintained by payment systems, manner of fund transfers, criteria of membership of payment systems and their rights and obligations, and issuance of guidelines for effective management of payment systems.
- (ii) **Section 11: Notice of change in the Payment System** – system providers shall not cause any change effecting the structure and operation of the payment system without prior approval of RBI.
- (iii) **Section 12: Power to call for returns, documents or other information** – empowers RBI to call for returns, documents or other information from any system provider regarding operations of payment systems operated by them.
- (iv) **Section 13: Access to information** – empowers RBI to access any information relating to any payment system with the system provider and the system participants.

---

<sup>6</sup> Trade Repository means a person who is engaged in the business of collecting, collating, storing, maintaining, processing or disseminating electronic records or data relating to such derivatives or financial transactions, as may be specified by the RBI from time to time.

- (v) **Section 14: Power to enter and inspect** – empowers RBI to enter and inspect any premises where a payment system is operated and any equipment including any computer system or other documents.
- (vi) **Section 16: Power to carry out audit and inspection** – empowers RBI to conduct or get conducted audits and inspections of a payment system or system participants.
- (vii) **Section 17: Power to issue specific direction** – empowers RBI to issue directions to a system provider or system participant to cease and desist from any act, omission or course of conduct that would result in systemic risks or affects the payment system, monetary or credit policy of the country.
- (viii) **Section 18: Power of RBI to give directions generally** – empowers RBI to lay down policies relating to the regulation of payment systems, including electronic, non-electronic, domestic and international payment systems affecting domestic transactions, and give directions to system providers or the system participants either generally or to any such agency, pertaining to the conduct of business relating to payment systems.
- (ix) **Section 19: Directions of RBI to be generally complied with** – imposes a duty on every person to whom a direction is issued by the RBI to comply with such direction and submit compliance.

**3.5** Chapter VII of PSS Act and its Sections deal with Offences and Penalties and empowers RBI to impose monetary penalties on persons contravening or committing default of the nature pertaining to wilful omission of any material statement or wilful submission of any false statement, information, returns or other documents, or in case of contravention of any provision of PSS Act or any regulation, order or direction issued thereunder. It also empowers RBI to compound the contraventions of any offence punishable under PSS Act, which are not punishable with imprisonment only, or with imprisonment and also with fine.

**3.6** The PSS Act also provides legal basis for gross or netting procedure and ensures finality and irrevocability of settlement, as soon as the money, securities, foreign exchange or derivatives or other transactions payable as a result of settlement is determined, whether or not such money, securities or foreign exchange or derivatives of other transactions is actually paid. It also mandates the system providers to disclose to the existing or potential system participants, the terms and conditions including the charges and the limitations of liability under the payment system, supply them with copies of the rules and regulations governing the operation of the payment system, netting arrangements and other relevant documents.

**3.7** In exercise of powers conferred by sub-section (1) read with clauses (b) to (f) of sub-section (2) of Section 38 of PSS Act, the RBI notified the Payment and Settlement System Regulations, 2008. The Regulations provide for process and procedures for authorisation of a

Payment System; specification of standards<sup>7</sup>, issued by RBI, to be followed by the authorised system providers; and furnishing of returns, documents and other information including accounts and Balance sheet to the RBI. The PSS Act and the Regulations framed thereunder, provide the legal framework for the conduct of oversight of payment systems, SSSs, CCPs and TRs by RBI.

#### **Section 4: Designation of FMIs Regulated by RBI**

**4.1** The CPSS-IOSCO – PFMI defines an FMI as 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. The Principles are designed to apply to all SIPS, CSDs, SSSs, CCPs and TRs.

**4.2** One of the responsibilities of regulatory authorities is to define and publicly disclose the criteria used to identify FMIs that should be subject to regulation, supervision and oversight. Though the expression ‘FMI’ has not been defined explicitly in the PSS Act, the definition of payment system therein includes all categories of FMIs, including TRs, as well as non-systemically important payment systems.

**4.3 Criteria for declaring a payment system as SIPS** – A payment system, authorised by RBI, would be categorised as an FMI if it has the potential to trigger or transmit systemic disruptions, or as and when it reaches systemic or system wide importance. The parameters considered are: (i) volume and value of transactions handled / processed; (ii) share in the overall payment systems; (iii) markets in which it is operating; (iv) number and types of participants; (v) degree of interconnectedness and interdependencies; (vi) criticality in terms of concentration of payment activities, etc. Based on the above parameters, the RBI shall declare the names of payment systems as SIPS.

**4.4 FMIs operated by RBI** – The RTGS system is the only large value payment system functioning in India and the value of transactions processed as a percentage of total payment transactions is 77% during the month of March 2020. It also settles Multilateral Net Settlement Batch (MNSB) files emanating from other ancillary payment systems including the systems

---

<sup>7</sup> Schedule to PSS Regulations 2008 includes Uniform Regulations and Rules for Bankers’ Clearing Houses, PGs on National Electronic Funds Transfer (NEFT) System, Operational Manual on NEFT System, Real Time Gross Settlement (RTGS) system (Membership) Regulations, 2004, RTGS (Membership) Business Operating Guidelines, 2004, PGs on Cheque Truncation System (CTS) and Bye Laws, Rules and Regulations of Clearing Corporation of India Limited (CCL).

operated by the CCIL<sup>8</sup> and NPCI<sup>9</sup>. Accordingly, it has been designated as a SIPS. Further, the SSS for the government securities<sup>10</sup>, both for outright and repo transactions conducted in the secondary market, operated by the RBI, is designated as an FMI. RBI also acts as the CSD for government securities, and thus designated as an FMI.

**4.5 FMI operated by private sector and regulated by RBI** – The CCIL, functioning as a central counterparty in various segments of the financial markets regulated by the RBI (viz. the government securities segment, tripartite repo, USD-INR and forex forward segments)<sup>11</sup>, is designated as an FMI as per the definition provided in the PFMI Report. RBI has also designated CCIL as a Trade Repository<sup>12</sup> under Section 34 A (2) of PSS Act for OTC interest rate, credit and forex derivative transactions as mandated from time to time, and thus designated as an FMI. NPCI is the umbrella organisation for operating retail payment systems in the country; its share as against the entire payment landscape of India stood at 64.5% by volume and 4.07% by value during the month of March 2020. With the growing retail volumes handled by NPCI and the resultant increase in the extent of concentration of retail payments under NPCI, and given the criticality of its operations in terms of volume of transactions handled, any disruption can have an impact on the payment and settlement of transactions initiated by public at large, especially the lower and middle class population, and the financial inclusion drive of the Government and RBI. Accordingly, NPCI has been designated as a system wide important payment system (SWIPS) and would be assessed against the PFMI.

#### **4.6 Other critical market infrastructures which are designated as FMIs**

**4.6.1** The PFMI in general are not addressed to market infrastructures such as trading exchanges, trade execution facilities, or multilateral trade-compression systems. However, the report states that the relevant authorities may decide to apply some or all of these principles to types of infrastructures not formally covered by the report. Considering the criticality of the

---

<sup>8</sup>CCIL was set up and established in 2001 as RBI's initiative for creating a guaranteed platform for systemically important payment systems. The CCIL is owned and managed by commercial banks. It functions as a CCP for select categories of transactions such as those in the government securities, inter-bank foreign exchange market, call money market, etc. thus effectively managing and mitigating the counterparty risks arising out of possible default by any constituent.

<sup>9</sup> NPCI was established in 2009 for acting as an umbrella organisation with the responsibility to set up and manage country's retail payment ecosystem. Its major objective was to facilitate robust, scalable, secured and affordable payment mechanism to benefit the common man across the country and further the cause of financial inclusion.

<sup>10</sup> The Integrated Banking Department (IBD) of RBI, Mumbai manages and operates the SSS for the government securities, both for outright and repo transactions conducted in the secondary market. Government securities (outright) are settled using DVP model 3 mechanism on a T+1 basis. Repos are settled on T+0 or T+1 basis. In addition, the IBD also acts as depository for dematerialised government securities.

<sup>11</sup> In addition to functions of CCP, CCIL also provides non-guaranteed settlement in the rupee denominated interest rate derivatives like Interest Rate Swaps / Forward Rate Agreement market. It also provides non-guaranteed settlement of cross currency trades to banks in India through Continuous Linked Settlement (CLS) bank by acting as a third-party member of a CLS Bank settlement member.

<sup>12</sup> The provisions of PSS Act shall apply to the designated TR as they apply to, or in relation to, payment systems to the extent applicable.

Negotiated Dealing System-Order Matching (NDS-OM)<sup>13</sup> in the government securities market, it was designated as an FMI in the policy document of June 2013. The CPSS-IOSCO subsequently came out with the 'Assessment methodology for the oversight expectations applicable to critical service providers'. Accordingly, the NDS-OM would be assessed as per this methodology. Accordingly, NDS-OM is not classified as an FMI, but will be overseen and assessed as per the methodology prescribed by CPSS-IOSCO for critical service providers.

**4.6.2** The operations of the FMIs / payment systems are dependent on some critical infrastructure viz. Indian Financial Network (INFINET) – the communication network and SFMS – the messaging infrastructure operated by The Indian Financial Technology and Allied Services (IFTAS). RBI has also given approval to SWIFT India Domestic Services Private Limited (SIDSPL) to provide messaging services for domestic financial transactions in India. The critical infrastructure would thus be assessed against the CPMI-IOSCO "Assessment methodology for the oversight expectations applicable to critical service providers"<sup>14</sup> (to the extent applicable to infrastructure providers). The entities covered would be

- (i) The Negotiated Dealing System-Order Matching (NDS-OM) which is a critical infrastructure for the government securities market;
- (ii) Indian Financial Network (INFINET) /-SFMS; and
- (iii) SIDSPL.

#### **4.7 Applicability of PFMI to FMIs in India**

**4.7.1** As mentioned earlier, RBI has adopted the PFMI through its policy document "Regulation and Supervision of FMIs regulated by RBI". Accordingly, all RBI authorised payment systems declared as SIPS / SWIPS on the basis of above criteria and SSSs, CCPs, CSDs and TRs are expected to comply with the PFMI standards. Thus, RTGS, NPCI, SSS / CSD, and CCIL (as CCP and TR)<sup>15</sup> are mandated by RBI to comply with the PFMI standards. They would also be assessed using the PFMI framework<sup>16</sup>.

**4.7.2** Most principles in PFMI report are applicable to all types of FMIs covered. However, a few principles are only relevant to specific types of FMIs. The applicability of the principles and key considerations to specific types of FMIs in India is shown in **Appendix 9**.

---

<sup>13</sup> NDS-OM is owned by the RBI and is operated by CCIL on behalf of the RBI. NDS-OM, introduced in 2005, is an electronic, screen based, anonymous, order driven trading system for dealing in Government securities. The NDS-OM ensures complete anonymity among the participants and brings transparency in secondary market transactions in Government securities. The NDS-OM facilitates Straight-Through-Processing (STP) as all the trades on the system are automatically sent to CCIL for settlement. With the efficiency and ease of its operations, the NDS-OM today accounts for around 90 per cent of the trading volume in government securities.

<sup>14</sup> The same is available at <https://www.bis.org/cpmi/publ/d123.pdf> and <https://www.bis.org/cpmi/publ/d146.pdf>.

<sup>15</sup> RBI has issued direction to CCIL under Section 10 (2) and 18 of PSS Act that CCIL shall be subjected to regulation and supervision using the PFMI. They have also been directed to adhere with the PFMI requirements for both CCP as well as TR activities.

<sup>16</sup> [https://www.bis.org/cpmi/info\\_pfmi.htm?m=3%7C16%7C598](https://www.bis.org/cpmi/info_pfmi.htm?m=3%7C16%7C598).

**4.7.3** The RPSs, those not designated as SIPS / SWIPS, but regulated by RBI, such as Prepaid Payment Instrument Issuers, card payment networks, ATM networks, Cross-border Money Transfer (in-bound) operators, White Label ATM Operators, Instant Money Transfer Operators, Trade Receivables Discounting System (TReDS) operators, Bharat Bill Payment System (BBPS) Operator, and Bharat Bill Payment Operating Units (BBPOUs), would not be subject to assessment against all PFMI, except for submission of Self-Assessment Template (SAT) dovetailed to their specific requirements on an annual basis. However, some of the PFMI are so fundamental that they should also be observed by even these RPSs. For the purpose, the RBI will be classifying such RPSs as Important Retail Payment Systems (IRPS) and Other Retail Payment Systems (ORPS).

**4.7.4** Although both IRPS and ORPS are required to comply with a select set of PFMI, a differentiation has been made between the two types of retail payment systems according to their share in payment landscape, the potential effects on account of their failure and the potential to undermine public confidence in payment systems. In the light of this, the RBI has identified the PFMI with which IRPS and ORPS should comply with. The same is given in **Appendix 10**. The RBI has decided that 12 and 7 PFMI out of 17 applicable to payment systems, are applicable to IRPS and ORPS, respectively.

## **Section 5: Definition and Scope of Oversight**

### **5.1 Definition of Oversight**

**5.1.1** The definition of “Oversight of payment and settlement system” provided by CPSS in the report on Central Bank Oversight of Payment and Settlement Systems, has been adopted by the RBI.

**5.1.2** By convention, “the term oversight is reserved to designate the specific responsibilities and tools central banks have with regard to payment and settlement systems due to their unique character of being both a public authority and a bank. Oversight is a necessary complement to any other means central banks may use to achieve their public policy objectives for payment and settlement systems (such as operating certain systems themselves or providing settlement services to systems).”<sup>17</sup>

### **5.2 Oversight Responsibilities**

**5.2.1** As indicated earlier, the PSS Act, 2007 and PSS Regulations, 2008 provide for the RBI to conduct oversight of payment and settlement systems, as part of its mandate. The RBI is

---

<sup>17</sup> Central Bank Oversight of Payment and Settlement Systems, May 2005, CPSS, BIS

empowered under the PSS Act to issue guidelines for the proper and efficient management of the payment systems generally or with reference to any particular payment system.

### **5.3 Oversight Objectives**

**5.3.1** The main objective of PFMI is to enhance safety and efficiency in payment, clearing, settlement and recording arrangements, and more broadly, to limit systemic risk and foster transparency and financial stability. Poorly designed and operated FMIs can contribute to and exacerbate systemic crises if the risks of these systems are not adequately managed, and as a result, financial shocks could be transmitted from one participant or FMI to others. The effects of such disruption could extend beyond and thus threaten the stability of broader economy.

**5.3.2** RBI issues bank notes and provides banking facilities in the form of current accounts to all banks and financial institutions functioning in the country. RBI promotes settlement of all payment transactions in central bank money and plays a role in ensuring safety and efficiency in FMIs so as to prevent systemic risk.

**5.3.3 Prevention of systemic risk** – RBI oversees FMIs and all authorised payment systems, including RPSs, so as to contain the systemic risk implications that have the potential to affect nation's financial system and consequently its monetary and financial stability. Any malfunctioning of an FMI is likely not only to have a negative effect on the FMI's participants but it could also give rise to broader risk externalities, if participants are no longer able to complete their payment or securities transactions on time. The situation could worsen due to the interconnectedness feature of payment systems. As a result, the liquidity strains of the participants might spread more widely through the financial system, putting pressure on asset prices and reducing market confidence and thus potentially endangering the stability of financial system. Furthermore, if FMIs including payment and settlement systems, which facilitate the exchange of money for goods, services and financial assets, were inefficient or failed altogether, money would not fulfill its function of acting as means of exchange effectively and one of the key tasks of central banks, namely to maintain public confidence in money and in the instruments and systems used to transfer money, would not be achieved.

**5.3.4** Payment and Settlement Systems typically exhibit economies of scale, i.e. they have high fixed costs and marginal costs that are very low with increase in number of processed transactions. In such a scenario, concentration among a few large-scale providers, or even a natural monopoly, may be the most efficient market structure. Significant market concentration, however, may lead to a high dependency on a few key payment and settlement systems, without readily available alternatives. Moreover, market concentration may be significant enough to give payment and settlement providers market power that leads them to

provide lower levels of services at higher prices, lower investment in risk reduction and perhaps a lower level of innovation than is socially optimal.

**5.3.5** Considering the above issues, the RBI has, apart from safety, security and efficiency of FMI and payment systems, adopted customer confidence, wider accessibility and customer convenience, and customer protection as its oversight objectives, and transformed them into its various regulations, standards, directions, and guidelines applicable to them. These objectives are also enshrined in RBI's Payment Systems Vision Document.

**5.3.6** With a view to promoting safety, security and efficiency of FMI and RPSs, the RBI aims for following outcomes:

**5.3.6.1 Governance arrangements** – They should document clear and transparent governance arrangements<sup>18</sup> with clear lines of roles and responsibilities as well as accountability of its Board, its board level sub-committees and management. They should have objectives in line with those with RBI, and also support the stability of the broader financial system. Their Board and Management should be composed of suitable members with an appropriate mix of skills, experience, and knowledge of the FMI and / or RPSs.

**5.3.6.2 Comprehensive management of risks** – They should have a board approved sound risk management framework, including policies, processes, procedures and systems, for identification and assessment, measurement, monitoring and management of range of risks (such as legal, credit, liquidity, operational, business and other risks) arising in or out of the business as well as it poses to other entities as a result of interdependencies. Their Board should regularly monitor their risk profile to ensure that it is consistent with their business strategy and risk-tolerance policy.

**5.3.6.3 Credit risk management**<sup>19</sup> – They may face credit risk from their participants, its payment and settlement processes, or both. The default of a participant (and its affiliates) could have the potential to cause severe disruptions to an FMI / RPS, its other participants, and more broadly to the financial markets. Therefore, FMI and RPSs should establish a robust framework to manage their credit exposures to their participants and the credit risk arising from their payment, clearing, and settlement processes.

**5.3.6.4 Liquidity risk management** – They should have a robust framework to manage their liquidity risk arising from their participants, settlement banks, nostro agents, custodian banks,

---

<sup>18</sup> RBI has, in October 2018, issued policy directions, under Section 18 of Payment and Settlement Systems (PSS) Act, 2007, relating to capital requirements and governance framework for CCPs as also providing a framework for recognition of foreign CCPs.

<sup>19</sup> The PFMI Principles relating to credit and liquidity risks are not applicable to CSDs and TRs as they do not face credit and liquidity risks.



liquidity providers and other entities. They should also maintain sufficient liquid resources, with thorough rigorous stress testing by considering wide range of stress scenarios, in all relevant currencies to effect same day settlement or intraday or multiday settlement, of payment obligations with high degree of confidence.

**5.3.6.5 Collateral** – In order to manage the risk from a participant default, they should consider the impact of participant defaults by collateralising their current and potential future credit exposures. The collateral should be with low credit, liquidity and market risks after enforcing appropriately conservative haircuts and concentration limits in order to ensure that the liquidation value of the collateral is greater than or equal to the obligation that the collateral secures in extreme but plausible market conditions.

**5.3.6.6 Default management** – They should have clearly defined rules and procedures that enable them to meet their obligations to non-defaulting participants in the event of a participant default as well as for replenishment of resources.

**5.3.6.7 Operational risk management** – Operational risk is the risk that arises from deficiencies in information systems, internal processes, and personnel or disruptions from external events, that result in the reduction, deterioration, or breakdown of services provided by the FMIs. Thus, the FMIs and RPSs should establish a robust framework to manage their operational risks with appropriate systems, policies, procedures and controls. They should also ensure that the systems have scalable capacity so as to handle increasing volumes. As a part of the framework, they should also have a business continuity plan that addresses events posing a significant risk of disrupting operations, for timely recovery of operations and fulfilment of FMI's obligations, including in the event of a wide-scale or major disruption.

**5.3.6.8 Recovery and Resolution Plans** – The FMIs should ensure that they can continue to provide critical services in all circumstances. However, it is possible that in certain extreme circumstances, an FMI may become non-viable as a going concern or insolvent. Such a situation would lead to systemic disruptions to the institutions and markets supported by the FMI and financial system more broadly. The FMIs should, therefore, identify scenarios that may potentially prevent them from providing their critical operations and services as a going concern, and prepare a host of viable range of options for their recovery to normalcy or their ultimate resolution and orderly wind-down, for instance transferring their critical operations and services to an alternate entity. The range of options for recovery should be documented in the form of Recovery and Resolution Plan (RRP), which should contain, inter-alia, identification of FMI's critical operations and services, summary of key recovery or resolution strategies, and description of measures to be taken to implement the key strategies. The RRP shall be approved by the RBI on an annual basis.

**5.3.6.9 Disclosure of rules and procedures** – In order to help the current and prospective participants, authorities and public to understand risks, fees and other material costs, the FMIs and RPSs should have clear and comprehensive rules and procedures, which should be publicly disclosed. The rules shall, inter-alia, include the system’s design and operations, rights and obligations of FMI / RPS and its participants, risk-based objective criteria for participation by direct and indirect (tiered) participants and other FMIs / RPS, as well as procedures for facilitating the suspension and orderly exit of a participant that breaches or no longer meets the participation requirements.

**5.3.6.10 Settlement finality** – They should provide clear and certain final settlement. The same should be clearly defined in their rules and procedures.

**5.3.6.11 Settlement in central bank money** – They should preferably conduct their money settlements in central bank money, where practical and available, to avoid credit and liquidity risks.

**5.3.6.12** The FMIs and RPSs should be efficient and effective in meeting the requirements of their participants and the markets they serve.

## **5.4 Scope of Oversight**

**5.4.1** The term “scope of oversight” refers to those FMIs and RPSs that central banks oversee by applying some form of standards or policies. The PSS Act, designates the RBI as the authority to regulate and supervise payment systems in India and for matters related therewith or incidental thereto. Accordingly, the scope of oversight is enshrined in the PSS Act. The scope of oversight thus covers all authorised payment systems and aspects / matters related to payment systems. It includes all types of payment systems, SSSs, CSDs, CCPs and TRs.

**5.4.2** The PSS Act, also provides that no person can operate a payment system without authorisation from the RBI. It is necessary to ensure that all payment systems operate in a safe and efficient manner as also as per the provisions of the statute, Regulations framed thereunder and the instructions / guidelines / circulars / directives issued by the RBI from time to time. In addition, as indicated earlier, the RBI also lays out its strategies and focus as part of its Payment System Vision document. Thus, all designated FMIs and RPSs<sup>20</sup> fall within the scope of oversight by RBI.

---

<sup>20</sup> The list of 'Payment System Operators' authorised by RBI to set up and operate in India under the PSS Act, 2007 is given at <https://www.rbi.org.in/Scripts/PublicationsView.aspx?id=12043>.

**5.4.3** Availability of robust infrastructure to support electronic payments is a critical factor influencing the adoption of electronic payments. The service providers of the following critical infrastructure also fall within the scope. Oversight of these service providers would be undertaken by following the CPMI-IOSCO “Assessment methodology for the oversight expectations applicable to critical service providers”<sup>21</sup> (to the extent applicable to infrastructure providers).

- (i) NDS-OM;
- (ii) INFINET / SFMS; and
- (iii) SIDSPL.

**5.4.4** Presently, the card payment networks, except NPCI, and Cross-border Money Transfer (in-bound service) operators are regulated and overseen by way of off-site surveillance only as they are incorporated in foreign jurisdictions. These entities are required to submit System Audit Report of their entire systems, including the domestic infrastructure, on an annual basis. Continuous engagements are made with these entities to understand any gaps in their risk assessments and customer grievance redressal mechanism and also mandate them to make further improvements, if considered necessary. Going forward, steps shall be taken to further intensify the oversight process for such entities by way of on-site inspections, if required.

**5.4.5** Some designated FMIs, such as SSS and CSD are owned and operated by RBI. Though RBI is exempted from the authorisation requirements as an operator of payment systems under the PSS Act, RBI oversees as well as assesses these FMIs against the international standards<sup>22</sup> with the same rigour as in case of other FMIs and, where necessary, takes action to remedy deficiencies, if any.

**5.4.6** CCIL has been designated as TR for OTC interest rate and forex derivative transactions. TRs have emerged as a new type of FMI and have recently grown in importance, particularly in the OTC derivatives market, especially as a channel for reporting transaction data to relevant authorities and the public, for the purpose of enhancing the transparency of the OTC derivatives market. In addition to the principals to a trade, their agents, CCPs, and other service providers offering complementary services, the data stored in a TR may be used by a wider range of entities and stakeholders. Considering that the continuous availability, reliability, and accuracy of such data is critical, RBI also oversees TRs.

---

<sup>21</sup> The same is available at <https://www.bis.org/cpmi/publ/d123.pdf> and <https://www.bis.org/cpmi/publ/d146.pdf>

<sup>22</sup> The PFMI says that “In general, the principles are applicable to FMIs operated by central banks, as well as those operated by the private sector. Central Banks should apply the same standards to their FMIs as those that are applicable to similar private sector FMIs. However, there are exceptional cases where the principles are applied differently to FMIs operated by central banks due to requirements in relevant law, regulation, or policy. (Para 1.23 of PFMI).

## **5.4.7 Regulation of Payment Gateway Service Providers and Payment Aggregators and outsourced technology service providers**

**5.4.7.1** Annex F of the PFMI outlines five oversight expectations for critical service providers in order to support a financial market infrastructure's (FMI) overall safety and efficiency. The operational reliability of an FMI may be dependent on the continuous and adequate functioning of third party service providers that are critical to an FMI's operations, such as information technology and messaging providers.

**5.4.7.2** With the enhanced facilitation by banks and PPI Issuers, the use of electronic / online payment modes for payments to merchants for goods and services like bill payments, online shopping, etc., has gained large scale momentum over the years, which has led to increasing role of Technology Service Providers (TSPs), Third Party Application Service Providers, intermediaries such as Payment Gateways (PGs)<sup>23</sup> and Payment Aggregators (PAs)<sup>24</sup>, etc. Further, Electronic Commerce and Mobile Commerce (e-commerce and m-commerce) service providers act as intermediaries by providing platforms for facilitating such payments. These outsourced TSPs and intermediaries act as the bridge between the merchants and customers, and also play a role in processing and completion of payment transactions. Being part of the payment process chain these entities also handle sensitive customer data. Managing customer data, data privacy, Know Your Customer (KYC) requirements of merchants are also important from the point of view of security and customer confidence in the ecosystem. In addition, currently most of acquiring of merchants is done by third party aggregators and technology providers. Entities may also provide cross border settlement services and are governed by guidelines issued by Foreign Exchange Department (FED, RBI) on Online Payment Gateway Service Providers (OPGSPs).

**5.4.7.3** The customer, ordinarily has very limited / no access to these service providers and intermediaries and thus has to rely on merchants or banks who only can seek redress from the service providers and intermediaries. Lack of proper redress mechanism and uniformity in practice across the entities is also a matter of concern. The technology set-up of the service providers and intermediaries varies amongst the entities and the architecture changes over time keeping in view their predominant business objective including the need to provide efficient processing, seamless customer experience, etc. They may resort to multiple integration to provide redundancy.

---

<sup>23</sup> PGs are entities that provide technology infrastructure to route and facilitate processing of an online payment transaction without any involvement in handling of funds.

<sup>24</sup> PAs are entities that facilitate e-commerce sites and merchants to accept various payment instruments from the customers for completion of their payment obligations without the need for merchants to create a separate payment integration system of their own. PAs facilitate merchants to connect with acquirers. In the process, they receive payments from customers, pool and transfer them on to the merchants after a time period.

**5.4.7.4** RBI had earlier issued guidelines on managing risks in respect of outsourcing of financial services by banks. Further, with a view to safeguard the interests of the customers and users and to ensure that the payments made by the intermediaries (PGs and / or PAs) using electronic / digital / online payment modes were duly accounted for by the intermediaries receiving such payments and transmitted to the accounts of the merchants or to similar other entities, certain guidelines were issued to banks and payment system operators for addressing a few aspects of the functioning of intermediaries. As such, these entities were not subjected to direct regulation nor regulations for outsourcing arrangements were made applicable to them.

**5.4.7.5** Since these service providers and intermediaries also have exposure to the payment system landscape and are, therefore, exposed to the associated cyber threats, and thus could be potential source of risk in such a technology and customer experience intensive business, RBI had announced measures in its Monetary Policy Statements for 2018-19 for mandating certain regulatory controls on these entities. Based on the feedback received on discussion paper and taking into account the important functions of the intermediaries in the online payments space as also keeping in view their role vis-à-vis handling funds, it was decided to (a) regulate in entirety the activities of PAs, and (b) provide baseline technology-related recommendations to PGs. Accordingly, the RBI shall regulate and supervise non-bank PAs and the existing non-bank PAs are also required to submit application seeking for authorisation on or before June 30, 2021. On the other hand, the PGs shall be considered as 'technology providers' or 'outsourcing partners' of banks or non-banks, as the case may be and have been prescribed to put in place certain baseline technology related cyber security controls.

**5.4.7.6** Recognizing the cyber threat that critical service providers pose to the payment system landscape, certain base lines requirements have been mandated for such service providers of the banking sector through the RBI regulated entities. To start with, instructions were issued mandating baseline Cyber Security Controls for the third-party ATM Application Switch Service Providers. The RBI regulated entities have also been advised and are required to ensure that the contract agreement signed between them and the third party ATM Application Switch Service Providers as well as those providing any other type of payment system related services to them (limited to the IT ecosystem, such as physical infrastructure, hardware, software, reconciliation system, network interfaces, security solutions, hardware security module, middleware, associated people, processes, systems, data, information, etc.) necessarily mandate such service providers to comply with the specified cyber security controls on an ongoing basis and to provide access to the RBI for on-site / off-site supervision.

## Section 6: Oversight Activities

**6.1** The three key ways in which oversight activity is carried out are through (i) monitoring existing and planned systems; (ii) assessment of the FMI and RPS against the oversight objectives; and (iii) inducing change for improvements, where necessary. The activities and the tools used for the same are briefly indicated below<sup>25</sup>:

### **6.2 Monitoring existing and planned systems**

**6.2.1** Monitoring a system implies that the overseer (regulator) has a good understanding of the system. To obtain such an understanding, the overseer has to have information on the design, risk management, operations and other aspects of the payment system. To this end, information on the system is obtained from various sources, which are as under:

#### ***(i) Sources of information***

- Official system documentation such as system rules, member documentation, business continuity plans, system operational processes and procedures;
- Reports on system activity, including volume and value of transactions, and operating performance;
- Information on financial position of the entity, including balance sheet and profit and loss information;
- Internal reports of board and other board level sub-committee meetings;
- Reports from auditors (internal and external);
- Bilateral and multilateral meetings with system provider and system participants;
- Meetings with industries or participation in committees;
- On-site inspections;
- Expert legal opinions;
- Customer feedback;
- Information from other regulators;
- Market Intelligence; and
- Any other source.

***(ii) Powers to obtain information:*** Powers to obtain information and perform on-site inspections are closely related to regulatory authorities' powers to induce change. RBI has adequate powers under its statute, i.e. PSS Act and PSS Regulations to call for returns, documents or other information from any authorised payment system operator in regard to the operation of particular payment systems in such form and in such manner as it may prescribe from time to time. RBI also has powers to enter any premises where a payment system is being operated and may inspect any equipment,

---

<sup>25</sup> Central Bank Oversight of Payment and Settlement Systems, May 2005, CPSS, BIS

including any computer system or other documents situated at such premises and call upon any employee of such system provider or participant thereof, to furnish any information or documents required.

**(iii) Information on system participants:** The central banks typically use some information about the individual participants in systems in order to carry out oversight. This is required because participants' behaviour can affect the safety, security and efficiency of the FMI or payment system. Thus, it becomes necessary to judge whether the design or process and procedure of FMI or payment system needs to be changed. Such aspects are expected to be controlled at the time of initial on-boarding of the participants in the FMI or payment system and continuous inspection and audit to be conducted of the system participants, as per the documented operation rules of FMI or payment systems. The rules, inter-alia, include risk-based objective criteria for participation by direct and indirect (tiered) participants and other FMIs, as well as procedures for facilitating the suspension and orderly exit of a participant that breaches or no longer meets the participation requirements.

## **6.2.2 Monitoring of Planned systems**

**6.2.2.1 Authorisation process<sup>26</sup>:** The authorisation is a pre-emptive process set up by the RBI to monitor new and planned payment systems. The details regarding the design, operation of the system, access criteria (business rules), process flow of transaction, technology to be used, security features, interoperability, financials, fit-and-proper criteria of the promoters, etc. are examined and vetted by RBI, before authorisation is granted. As such, authorisation process set up by RBI in respect of new and planned systems ensures weeding out payment systems with weak system design, risk and financial parameters. The details of information sought from various payment systems at the time of authorisation are given in **Appendix 2**.

**6.2.2.2 Other data / information sources:** Apart from the information furnished by the entity seeking authorisation, the RBI may request for additional information based on the system proposed to be operated, e.g. for entities desirous of operating cross-border payment systems, the license issued by the overseas regulators is sought for. Also for entities incorporated in India, information / no objection from the respective regulators is obtained.

**6.2.2.3 Approval by the BPSS / Empowered Committee:** The information submitted by an applicant of new payment system is examined before proposing to the BPSS / Empowered Committee for final approval for authorisation. The powers for authorisation shall be handled in accordance with the powers delegated by the appropriate authority (BPSS / Empowered

---

<sup>26</sup> Section 4 of PSS Act, 2007 implies that any person before commencing or operating a payment system shall obtain authorisation from the RBI and for the purpose it shall apply in a prescribed format to RBI as defined in PSS Regulations, 2008.

Committee). The entities are issued in-principle approval for the proposed payment system and the final Certificate of Authorisation (CoA) is issued only after submission of a satisfactory system audit report of the systems proposed to be operated as payment system.

### **6.2.3 Monitoring of existing systems**

**6.2.3.1** RBI has adopted a risk-based approach for conducting oversight of existing payment and settlement systems. More focus of its oversight activities is directed to the largest risks to the financial system. The oversight of FMIs is typically accompanied by an assessment of the importance of particular FMI to financial stability and to the functioning of the economy as a whole.

**6.2.3.2 Oversight Process and Tools** – The oversight of FMIs and RPSs is primarily a combination of offsite supervision / surveillance and onsite inspection.

**6.2.3.2.1 Off-site surveillance** – The off-site surveillance and monitoring of FMIs and authorised RPSs are conducted by way of various tools, such as (a) submission of prescribed data / information by the regulated entities, (b) fraud monitoring / system of alerts, (c) regular meetings with authorised payment system operators, (d) market intelligence, and (e) oversight reports and surveys.

(i) Data / Information collection and compilation

(a) The PSS Regulations details the types of returns, documents and other information that are to be submitted by FMIs and authorised RPSs to RBI. The returns / information that have been mandated for submission at prescribed frequencies are given in **Appendix 1, Appendix 3, Appendix 4 and Appendix 8**.

(b) RBI is also empowered to call for / access any information relating to the operation of the FMIs / payment systems as well as their participants which helps to measure and monitor the performance of the FMIs / payment systems against the oversight objectives. In addition, RBI collects periodic and ad-hoc information and data. The formats for submission of data by the authorised entities / participants in payment systems are given in **Appendix 8**. Some returns (presently nine) have been migrated to eXtensible Business Reporting language (XBRL).

(c) The data / information collected would be confidential unless required to be shared as per section 15 (2) of the PSS Act. The RBI may disclose the information on aggregate basis in the public domain. The disclosure on disaggregated basis would be after internal analysis within the RBI and in the interest of the public. This is applicable for RBI operated systems as well.



(ii) Fraud Monitoring / System of Alerts

- (a) With the digital payment ecosystem making substantial progress in terms of growth of payment infrastructure as well as volume and value of digital payment transactions, fraud risk monitoring and management by the stakeholders has assumed importance.
- (b) Fraud monitoring is undertaken by ensuring that FMI and RPSs have a system of alerts, to be reported within and to RBI on occurrence of any abnormal event. The timely alert to RBI enables it to take necessary corrective action and ensure efficient functioning of the payment system. The entities are required to put in place adequate information and data security infrastructure and systems for prevention and detection of frauds.
- (c) The FMI and RPSs are required to put in place a mechanism for proactively reporting on a priority basis any abnormal events/ developments, aberrations, delays, incidents, etc., to the RBI at the earliest possible time. The system of alerts is to track the various risk events in a timely manner so as to prevent any disruptions in the functioning of the FMI and RPSs.
- (d) In view of increasing instances of fraudulent transactions reported on account of using cards, the card networks are required to put in place an Incident Reporting Mechanism, covering incidents of cyber-attacks / system downtime / fraudulent transactions / settlement delays, etc., whereby the incidents need to be reported to RBI immediately, but not later than 24 hours of the incident.
- (e) Simultaneously, a mechanism has been put in place on pilot basis for reporting of payment related fraud transactions by some banks / non-bank Prepaid Payment Instrument (PPI) Issuers / Payment System Operators (PSOs), as reported by their customers, in a Central Payment Fraud Information Registry created by RBI. (CPFIR). This will enable RBI to analyse trends, release periodic reports and ensure robust fraud risk monitoring and management by the stakeholders. It is envisaged that over time a comprehensive database would be available with details of suspect account numbers, mobile numbers, email ids, website, PAN, Aadhaar Number, etc., used for undertaking fraudulent transactions, which would be shared with banks / PPI issuers / PSOs on a near real-time basis to help them take preventive action at their end to identify the suspect beneficiaries and contain the instances of frauds. The aggregated fraud data will be published to formulate appropriate and forward-looking policies and educate customers on emerging risks. A web-based system for online reporting of payment frauds through a reporting module, is also being put in place.

(iii) Regular meetings with authorised payment system operators – RBI conducts meetings with senior executives of FMI and RPSs, and their major system participants to discuss their strategic plans and risk management practices. Quarterly review meetings are conducted with

the senior management of CCIL and NPCI, as well as quarterly / half-yearly meetings with other authorised retail payment system operators. RBI also engages with a broad range of stakeholders, such as Payments Council of India, Internet and Mobile Association of India, Confederation of ATM Industry, Indian Banks Association, etc., on periodic basis.

(iv) Market Intelligence – Market Intelligence is a key feature of any oversight process. Market intelligence is gathered from a variety of sources such as : periodical informal meetings / discussions with system operators and participants; participation in industry level meetings / conferences / symposia; media reports; web browsing on a regular basis for keeping track of payment system developments; participant complaints on frequent disruptions in promised service functionality / faulty service; customer complaints; surveys; interactions with other departments within the RBI, etc.

(v) Oversight report / surveys – An important factor which contributes to refinement of oversight strategy and regulatory framework is, in addition to feedback received through market intelligence, customer feedback, complaints, etc., the ability to gauge first-hand, the issues / difficulties faced by customers with respect to usage of payment systems. In order to ascertain these issues, RBI engages with various stakeholders / professionals to conduct periodic user / customer surveys on specific aspects of payments systems. The findings from these engagements / surveys not only provide insights into the ease of usage of existing payment products and processes by customers for meeting their various payment needs but also generate ideas for reviewing policies and empowering the users through structured awareness intervention. Periodic / Need based surveys are undertaken / feedback obtained from customer. Based on analysis of the data collected, the survey findings are summarised and published.

#### **6.2.3.2.2 Point of Arrival and Performance Metrics**

RBI has created the Point of Arrival (PoA) and Performance Metrics (PM) to assess and monitor the payment systems and participant entities respectively, on a regular basis. The purpose of creation of a PoA and PM is to augment the monitoring system through a periodic assessment with broadened scope and to facilitate the applicants and participants for conscious efforts to strive towards improvement. It will ensure that all system operators, participants and prospective entrants in a payment system category are aware of regulatory and supervisory expectations. It will also help in not only promoting efficiency of payment systems but also providing a robust environment that enables innovation towards making them safe, secure and fast.

PoA comprises of specifying goal-posts for a payment system like KYC of system participants, business proliferation, financial position, customer grievance handling, regulatory comfort on

value to the segment, etc. based on which its continuance or otherwise in the ecosystem can be decided. PM involves defining a set of targets for identified parameters like meeting business projections, business and technical declines, uptime / settlement delays, governance issues, etc., to be fulfilled by the participants at the point of gaining access along with certain time-based targets for monitoring the efficiency and effectiveness of the payment system participants. While the former addresses the system-related aspects of performance, the latter takes care of the participant-related aspects.

### **6.3 Assessment**

**6.3.1** Assessment is carried out to ensure that the entities' systems meet the relevant policy guidelines, standards and oversight objectives. For systemically important / system-wide important payment systems and FMIs that could potentially impact the country's economy and financial stability, the RBI uses international standards, i.e. the PFMI as the benchmark for oversight, evaluates whether the entities meet the requirements set out in the international standards, and make its own assessment.

**6.3.2** Assessment could be carried out in the form of Self-Assessment by the entities itself, which help emphasise that the entity has undertaken the responsibility of meeting the required standards and an external assessment in the form of on-site inspections by the central bank, which enables the central bank to form its own assessment based on all the information available to it.

#### **6.3.2.1 Off-site self-assessment**

- (i) The FMIs and SIPS are required to undertake periodic self-assessment against the CPSS-IOSCO's PFMI. The frequency of such self-assessment for FMIs / SIPS is annual or as advised by RBI from time to time. Payment systems viz., CCIL and NPCI are required to submit the assessment as per the format applicable to FMIs.
- (ii) The RPS operators are also required to undertake / conduct self-assessment as per the Assessment Template for Retail (SAT for retail) prescribed by RBI, on an annual basis or as per frequency advised from time to time. The SAT consists of questionnaire based on relevant principles of CP-SIPS.
- (iii) The template provides inputs to take a risk-based approach for undertaking on-site inspection. On review of the filled-in self-assessment templates, further supervisory actions, if considered necessary, are initiated by RBI.
- (iv) RBI has advised the authorised payment system operators to undertake external and / or internal independent audit of its operations, IT system, information security and BCP / DR arrangements. The scope of such audits is to verify the existence of risk control measures, the suitability of such measures, effectiveness of the risk controls and adherence to the risk control measures on an ongoing basis. The payment system

operators are required to submit the operational, technology and other audit reports as prescribed by the RBI along with the compliance measures to the RBI on a periodic basis. The minimum aspects to be covered as part of audit is given at **Appendix 6**.

- (v) In order to enhance the resilience of the payment systems by improving the current defenses in addressing new and advanced risks and also to bring in standardisation and ensure that relevant areas of information system processes and applications are covered, a revised scope and coverage of system audit has been formulated and conveyed to authorised non-bank payment system operators. The revised scope is given in **Appendix 7**.

#### **6.3.2.2 Onsite Inspection**

- (i) Onsite inspection / audit complements the offsite monitoring and surveillance mechanism put in place for the FMIs / retail payment systems.
- (ii) Onsite inspection activity is based on the risk profile of the entity derived from the annual self-assessment carried out by the entity and the information furnished by the entity and market intelligence, if any. FMIs and RPSs are subjected to periodic onsite inspection as determined by RBI from time to time.
- (iii) Prior approval of changes – Section 11 of PSS Act enjoins upon the FMIs and payment systems not to cause any change in the system which would affect the structure or the operation of payment system, without prior approval from RBI. Thus, the offsite monitoring as well as on-site inspection would also include assessment of any changes / amendments to the FMI's system rules, regulations, bye-laws, notifications, risk management framework, in order to ensure that such changes are within the accepted risk management and efficiency standards.
- (iv) The on-site inspection of CCIL is conducted on an annual basis, whereas in case of SWIPS (NPCI), it is done once in two years with a compliance audit to be carried out before undertaking the on-site inspection. TR is also covered as part of CCIL. The on-site inspection of RTGS, CSD and SSS is proposed to be carried out periodically. Further, the assessment of FMIs and SIPS / SWIPS against the PFMI are also carried out as part of the on-site inspection by RBI. The assessment of the FMIs operated by RBI are also to be carried out as per the PFMI.
- (v) Since clear and comprehensive disclosures enhance safety and efficiency in payment, clearing, settlement and recording arrangements, all FMIs and SIPS / SWIPS are also expected to provide clear and sufficient information to their participants and prospective participants, authorities and public to enable them to identify clearly and understand fully the risks and responsibilities of participating in the system. As a measure of enhanced transparency, CCIL discloses its self-assessment in compliance with the PFMI on an annual basis, as per the CPSS-IOSCO 'Disclosure Framework

and Assessment Methodology'<sup>27</sup>, prescribed in the PFMLs. CCIL also publishes its quantitative disclosures on a quarterly basis as per the public disclosure standards for CCPs<sup>28</sup>.

(vi) In case of PPI Issuers, the frequency of on-site inspection has been linked to the categorisation of the entities based on certain criteria / parameters, i.e. number of PPIs issued, amount outstanding and value of PPI transactions. The entities have been categorised into three types, i.e. small, medium and large, as provided hereunder:

- No. of outstanding PPIs as on 31<sup>st</sup> March of immediate preceding year  $\geq$  200 lakh; OR amount outstanding as on 31<sup>st</sup> March of immediate preceding year  $\geq$  Rs. 50 crore; OR total value of PPI transactions processed during the immediate preceding financial year  $\geq$  Rs. 5000 crore – Large PPI Issuer;
- No. of outstanding PPIs as on 31<sup>st</sup> March of immediate preceding year is between 10 lakh and 200 lakh; OR amount outstanding as on 31<sup>st</sup> March of immediate preceding year is between Rs.10 lakh and Rs.50 crore; OR total value of PPI transactions processed during the immediate preceding financial year is between Rs.1000 crore and Rs.5000 crore – Medium PPI Issuer;
- No. of outstanding PPIs as on 31<sup>st</sup> March of immediate preceding year  $\leq$  10 lakh; OR amount outstanding as on 31<sup>st</sup> March of immediate preceding year  $\leq$  Rs.10 lakh; OR total value of PPI transactions processed during the immediate preceding financial year  $\leq$  Rs.1000 crore – Small PPI Issuer.

Accordingly, the on-site inspection periodicity of large PPI Issuers is annual, biennial for medium and triennial for small PPI Issuers. For new PPI Issuers, on-site inspection shall be done within six months of commencement of PPI operations. Needless to add, the periodicity can be flexible and increased / modified depending on market intelligence, developments and / or other cases of need.

(vii) In case of NEFT system<sup>29</sup>, keeping in view the volume and value of transactions processed as part of the total retail payment transactions at 8% and 59% respectively during the financial year 2019-20, the on-site inspection as well as assessment against the relevant PFMLs shall be conducted bi-annually by RBI.

(viii) The card networks and cross-border money transfer (in-bound service) operators are presently assessed through submission of off-site returns and are not within the scope of on-site inspection by RBI. However, in order to ensure that the technology deployed to operate the authorised payment system/s is / are being

---

<sup>27</sup> The document CPSS-IOSCO – PFMLs – Disclosure Framework and Assessment Methodology – December 2012 is available at <https://www.bis.org/cpmi/publ/d106.pdf>.

<sup>28</sup> The document CPSS-IOSCO – Public quantitative disclosure standards for CCPs – February 2015 is available at <https://www.bis.org/cpmi/publ/d125.pdf>

<sup>29</sup> NEFT system is a retail payment system, owned and operated by RBI.

operated in a safe, secure, sound and efficient manner and as per the process flow submitted by them at the time of authorisation, they have been mandated to get a System Audit done on an annual basis by a Certified Information System Auditor (CISA) qualified auditor and registered with the ISACA or by a holder of a Diploma in Information System Audit (DISA) qualification of the Institute of Chartered Accountants of India (ICAI). Steps will be taken to conduct on-site inspection of such entities and to start with, the need for an onsite visit will be examined by RBI for the purpose of interaction with the executives of the entities as well as the overseas regulators.

(ix) The schedule of activities that would be conducted on an ongoing basis in respect of various FMIs and RPSs is given in **Appendix 1**.

## **6.4 Inducing change**

**6.4.1** On the basis of information collected and received as part of monitoring and assessment, in some cases RBI may conclude that the FMIs as well as retail payment systems' design, risk management practices, and business operations specific to authorised systems, has a sufficient degree of safety and efficiency and that no further action is required. If any deficiencies are observed in systems of FMIs / RPSs and it is concluded that some issues require improvements and it is necessary to induce change, RBI takes action and induces change using a range of tools at its disposal<sup>30</sup>.

**6.4.2** Considering that the discussions with the system operator and participants play an important part in achieving oversight objectives, RBI believes to have regular dialogues / discussions with the authorised payment system operators and participants with respect to issues for improvement and inducing change by way of possible solutions that have a bearing on their system's design and operational structure. Such dialogues help both RBI as well as the system operators to come to a common understanding and solution for improvement which are in line with the oversight objectives of safety, security and efficiency of payment systems.

**6.4.3** In cases where the issues are identified in majority of the payment systems, RBI issues advisory in the form of public statements so that the market self-discipline's itself. Another important tool used by the RBI is issuance of Displeasure or Cautionary letter and / or taking penal action in terms of the powers conferred on it under the provisions contained in PSS Act. The penal action could include revocation of the CoA issued to the entity. In cases where RBI imposes monetary penalty on authorised payment system operators on account of contraventions, such entities are mandatorily required to disclose the details of monetary penalty paid in their Notes to Accounts that are part of Annual Financial Statements for the

---

<sup>30</sup> The tools available to central banks to induce change vary significantly, ranging from moral suasion to statutory powers to enforce oversight decisions. The tools include: Moral suasion, public statements, Voluntary agreements and contracts, Participation in systems, cooperation with other authorities, statutory power to require change, and enforcement and sanctions.

financial year in which the penalty was levied. Further, RBI also discloses the information about penalty levied on its website.

**6.4.4** The RBI has powers under PSS Act to issue specific directions to a payment system or a system participant if its act, omission or course of conduct will result / is likely to result in systemic risk or affect the payment system, monetary policy or credit policy of the country.

**6.4.5** If there are major supervisory concerns against an entity, RBI may also choose not to renew its Certificate of Authorisation (CoA) at the end of its validity.

#### **6.4.6 Customer protection**

**6.4.6.1** RBI has put in place following mechanisms for effective redressal of grievances:

- (i) **Reserve Bank – Integrated Ombudsman Scheme, 2021** – The RB-IOS provides a single reference point for customers to file complaints, submit documents, track status and provide feedback against RBI regulated entities specified therein. A toll-free number is also available for customers to seek assistance in filing complaints and information on grievance redress, with multi-lingual support.
- (ii) **Internal Ombudsman Scheme for non-bank System Participants, 2019** – The Internal Ombudsman (IO) scheme for the large non-bank system participants, with more than one crore PPIs outstanding, was institutionalised in 2019. The scheme facilitates a swift, efficient and effective complaint redressal mechanism within the entity to ensure that customer complaints are adequately addressed at the level of non-bank System Participant itself by an independent authority placed at the apex level in the entity's grievance redress mechanism.
- (iii) **Limiting Liability of Customers in Unauthorised Electronic Banking Transactions** – With the increased thrust on financial inclusion and customer protection from the loss due to unauthorized transactions, the Reserve Bank has, in July 6, 2017, formulated the criteria for determining the customer liability in these circumstances to be implemented by commercial banks. Accordingly, zero liability of customer exists where the unauthorized transactions has occurred due to contributory fraud/negligence/ deficiency on the part of bank (irrespective of whether the transactions is reported by the customer or not) and in case of third party breach where the deficiency lies neither with the bank nor with the customer but lies elsewhere in the system, and the customer notifies the bank within three working days of transactions. The above circular is also applicable to bank PPI Issuers.

Banks are also required to provide customers with 24x7 access through multiple channels (at a minimum, via website, phone banking, SMS, e-mail, IVR, a dedicated toll-free helpline, reporting to home branch, etc.) for reporting unauthorised

transactions that have taken place and / or loss or theft of payment instrument such as card, etc. The loss / fraud reporting system shall also ensure that immediate response (including auto response) is sent to the customers acknowledging the complaint along with the registered complaint number.

- (iv) **Limiting Liability of Customers in Unauthorised Electronic Payment Transactions in Prepaid Payment Instruments (PPIs) issued by Authorised Non-banks** – Similar criteria, like those for banks above, have also been formulated for determining the customers' liability in unauthorised electronic payment transactions resulting in debit to their PPIs issued by non-bank PPI Issuers. Accordingly, zero liability of customer exists where the unauthorized transactions has occurred due to contributory fraud/negligence/ deficiency on the part of PPI Issuer (irrespective of whether the transactions is reported by the customer or not) and in case of third party breach where the deficiency lies neither with the PPI Issuer nor with the customer but lies elsewhere in the system, and the customer notifies the PPI Issuer within three working days of transactions.
- (v) **Harmonising Turn Around Time (TAT) for resolution of customer complaints and compensation for failed payment transactions** - A large number of customer complaints emanate on account of unsuccessful or 'failed' transactions. Failure could be on account of various factors not directly attributable to the customer such as disruption of communication links, non-availability of cash in ATMs, time-out of sessions, non-credit to beneficiary's account due to various causes, etc. Rectification / Compensation paid to the customer for these 'failed' transactions is not uniform.

In order to bring uniformity and discipline in reversal of such failed transactions, RBI has put in place a framework harmonising the Turn Around Time for resolution of customer complaints and customer compensation for failed transactions in some payment systems, i.e. ATMs, Unified Payments Interface (UPI), Immediate Payment Service (IMPS), PPIs and card payments. The framework has come into effect from October 15, 2019. The framework prescribes the TAT for failed transactions as also a compensation framework providing *suo moto* compensation to customers for delay in execution or reversal of such transactions beyond the prescribed TAT. Wherever financial compensation is involved, the same shall be effected to the customer's account *suo moto*, without waiting for a complaint or claim from the customer. The principle behind the TAT is based on the following:

- (a) If the transaction is a 'credit-push' funds transfer and the beneficiary account is not credited while the debit to originator has been effected, then credit is to be effected within the prescribed time period failing which the penalty has to be paid to the beneficiary;



- (b) If there is delay in initiation of a transaction at the originator bank's end beyond the TAT, then penalty has to be paid to the originator.

#### **6.4.7 Resilience of infrastructure**

**6.4.7.1** Resilience is ensured by continuously monitoring the technical, operational, and financial viability of the entities to ensure continuous system viability. Measures are laid out to ensure that the entities monitor payment and settlement flows, have enough early warning devices guarding against abnormalities across the payment circuits, and have well-tested emergency procedures in place. This enables the entities to operate smoothly at all points of their process, and to be resilient to disturbances.

#### **6.4.8 Guidance on cyber resilience for FMIs**

**6.4.8.1** The level of cyber resilience, which contributes to an FMI's operational resilience, is a decisive factor in the overall resilience of the financial system and the broader economy. "Cyber resilience" is an FMI's ability to anticipate, withstand, contain, and rapidly recover from a cyber-attack. CPMI and IOSCO have published guidance on cyber resilience for FMIs.

**6.4.8.2** An FMI should have a framework that clearly articulates how it determines its cyber resilience objectives and cyber risk tolerance, as well as how it effectively identifies, mitigates, and manages its cyber risks to support its objectives. The FMI's Board should endorse this framework, ensuring it is aligned with the FMI's formulated cyber resilience strategy. The FMI's cyber resilience framework should support financial stability objectives while ensuring the ongoing efficiency, effectiveness and economic viability of its services to its users. To be effective in keeping pace with the rapid evolution of cyber threats, FMIs are directed to implement an adaptive cyber resilience framework that evolves with the dynamic nature of cyber risks and allows the FMI to identify, assess and manage security threats and vulnerabilities for the purpose of implementing appropriate safeguards into its systems.

**6.4.8.3** FMIs regulated by RBI are required to have the cyber resilience framework put in place as per the standards stipulated by RBI from time to time and guided in the CPMI document<sup>31</sup>.

#### **6.4.8.4 Measures to Strengthen Cyber Security in Banks / system participants –**

- (i) In view of the rapid growth in use of Information Technology by banks and their constituents, RBI had provided guidelines on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds in April 2011, advising banks to proactively create/fine-tune/modify their policies, procedures and technologies based on new developments and emerging concerns.

---

<sup>31</sup> <https://www.bis.org/cpmi/publ/d146.htm> - Guidance on cyber resilience for financial market infrastructure – June 2016.

- (ii) With continuous increase in number, frequency and impact of cyber incidents / attacks in the recent past, and the urgent need to enhance the resilience of the banking system by improving the current defences in addressing cyber risks, the RBI issued detailed guidelines in June 2016 advising banks to put in place an adaptive Incident Response, Management and Recovery framework to deal with adverse incidents / disruptions, if and when they occur. Banks were also advised to adhere to following:
- (a) Board approved Cyber-security Policy – A Board approved cyber-security policy elucidating the strategy containing an appropriate approach to combat cyber threats given the level of complexity of business and acceptable levels of risk.
  - (b) Distinct Cyber Security Policy – The Cyber Security Policy should be distinct and separate from the broader IT policy / IS Security policy so that it can highlight the risks from cyber threats and the measures to address / mitigate these risks.
  - (c) Continuous Surveillance – In order to ensure continuous surveillance, banks have been advised to set up and operationalise a Security Operations Centre (SOC) to monitor and manage cyber risks in real time.
  - (d) Secured IT architecture – The IT architecture should be designed in such a manner that it takes care of facilitating the security measures to be in place at all times.
  - (e) An indicative, but not exhaustive, minimum baseline cyber security and resilience framework has been provided for implementation by the banks.
  - (f) Network and database security – Banks have been mandated to ensure that unauthorized access to networks and databases is not allowed and wherever permitted, these are through well-defined processes which are invariably followed.
  - (g) Protection of customer information – Banks, as owners of such data, should take appropriate steps in preserving the confidentiality, integrity and availability of the same, irrespective of whether the data is stored/in transit within themselves or with customers or with the third party vendors.
  - (h) Cyber crisis Management Plan – A Cyber Crisis Management Plan (CCMP) should be formulated as part of the overall Board approved strategy. The traditional BCP/DR arrangements may be reviewed to ensure coverage of cyber risks. CCMP should address the following four aspects: (i) Detection (ii) Response (iii) Recovery and (iv) Containment. Banks have also been advised to take necessary preventive and corrective measures in addressing various types of cyber threats including, but not limited to, denial of service, distributed denial of services (DDoS), ransom-ware / crypto ware, destructive malware, business email frauds including spam, email phishing, spear phishing, whaling, vishing frauds, drive-by downloads, browser gateway fraud, ghost administrator exploits, identity frauds, memory update frauds, password related frauds, etc.

- (i) Cyber Security preparedness indicators – Banks should develop indicators for assessing the level of cyber risk / preparedness as well as for assessing its adequacy and adherence to cyber resilience framework.
- (j) Sharing of information on cyber security incidents with RBI - Banks are required to report all unusual cyber-security incidents (whether they were successful or were attempts which did not fructify) to the Reserve Bank.
- (k) Organisational arrangements – Banks should review the organisational arrangements so that the security concerns are appreciated, receive adequate attention and get escalated to appropriate levels in the hierarchy to enable quick action.
- (l) Cyber security awareness among stakeholders / Top Management / Board – Top Management and Board should also have a fair degree of awareness of the fine nuances of the threats and appropriate familiarisation may be organized. Banks should also proactively promote, among their customers, vendors, service providers and other relevant stakeholders an understanding of the bank's cyber resilience objectives, and require and ensure appropriate action to support their synchronised implementation and testing.
- (iii) Standing Committee on Cyber Security – The Reserve Bank of India has set up an Inter-disciplinary Standing Committee on Cyber Security (with members drawn from academia / various disciplines) to, inter alia, review the threats inherent in the existing/emerging technology; study adoption of various security standards/protocols; interface with stakeholders; and suggest appropriate policy interventions to strengthen cyber security and resilience.
- (iv) A Crisis Management Group (CMG) has been set up within the RBI to deliberate on the response measures to be taken by the stakeholders in the wake of critical/potential cyber-attacks.
- (v) Under the guidance of the Standing Committee, four sub-groups have been constituted to examine in detail, specific areas of concerns, i.e. Card based Payments and Security, Mobile Banking and Security, Vendor Risk Management, and Cloud computing services and security.
- (vi) A web-based application portal is being developed to further enhance the efficiency and consistency of offsite monitoring over all the supervised entities.

#### **6.4.9 Storage of Payment System Data**

In recent times, there has been considerable growth in the payment ecosystem in the country, particularly in the realm of digital transactions. Such systems are also highly technology dependent, which necessitate adoption of safety and security measures, which are best in class, on a continuous basis. Ensuring safety and security of the payment systems has always

been the cornerstone of the RBI's approach towards payment system regulation and development. Multiple players with niche roles are part of each digital transaction and many of such players have global presence. To ensure better monitoring and to have unfettered supervisory access to data stored with the system providers as also with their service providers / intermediaries / third party vendors and other entities in the payment ecosystem, all system providers are required to ensure that the entire data relating to payment systems operated by them is stored in a system only in India. This data should include the full end-to-end transaction details / information collected / carried / processed as part of the message / payment instruction. For the foreign leg of the transaction, if any, the data can also be stored in the foreign country, if required.

#### **6.4.10 Publishing of Payment System Indicators**

The Reserve Bank publishes data on aggregates of various payment and settlement system indicators on the RBI website for the information of the stakeholders and general public. The scope of dissemination of such data has since been enhanced to include more granular information on payment data covering the payment systems authorised by the Reserve Bank.

#### **6.4.11 Annual Report to BPSS**

The activities undertaken by the department during the year, covering the policy initiatives, authorisation granted to entities and oversight activities pertaining to all the regulated entities are informed to the BPSS in the form of an Annual Report. The report is also intended to track the achievement of the Payment System Vision and monitor progress of the activities undertaken by the department. In addition, ad-hoc reports are placed before the Board on functioning of various payment and settlement systems.

### **Section 7: Co-operation with Other Regulatory Authorities**

**7.1** While performing oversight, it is important to have a clear understanding about the interconnectedness and interdependencies of a particular FMI and its participants with other entities not falling within the regulatory domain of RBI. There could be cross-sectoral risks arising from such interdependencies between the member participants of a payment system and their technology service providers. Further, in cases where systems deal with multiple public authorities, co-operation between the authorities is expected to be beneficial. Effective co-operation between authorities is thus essential and necessary to help to avoid the possibility of gaps, inefficiency, duplication and inconsistencies in the oversight function.

**7.2** In addition, due to globalisation, the cross-border FMs and payment systems have significantly increased over time. Interdependencies between FMs operating in different jurisdictions have become more obvious with indirect connections between global banks as participants across FMs.

**7.3 Inter-Regulatory and Intra-Regulatory Committees** – In order to have a coordinated approach towards regulation and supervision of FMs and retail payment systems, the RBI has set up an Inter-regulatory Committee comprising of sectoral regulatory authorities – SEBI, IRDA, TRAI, etc., to remove frictions in regulation and ease system operator / customer comfort. The endeavour is also to have a coordinated approach to regulation and supervision within RBI across different related departments – Department of Regulation, Department of Supervision, Financial Markets Regulation Department, Financial Markets Operations Department, Foreign Exchange Department, Customer Education and Protection Department, Department of Information Technology, Department of Economic and Policy Research, Department of Statistics and Information Management, Department of Government and Bank Accounts, etc. Similar engagements are already in place with the subsidiaries of Reserve Bank – Institute for Development and Research in Banking Technology (IDRBT), Reserve Bank Information Technology Pvt. Ltd. (ReBIT), etc. Accordingly, an Intra-regulatory Committee has been set up to encourage regulatory cooperation and sort out issues in guidelines and instructions. The Committees shall meet at periodic intervals and help enable coordinated supervision over the regulated entities in the payments space as also facilitate augmenting growth of digital transactions in the country.

**7.4** At present, there are no RBI authorised payment system operators providing payment services outside India. However, with the availability of low cost innovative digital payment products in India, many countries have expressed interest in partnering in this growth and replicating our products based on their country specific requirements. Cross-country co-operation with Bhutan is already in place with our CTS, NACH and NEFT operational there as well. NEFT is available for one-way transfers from India to Nepal. Specific interests / requests are being received for implementing CTS, NEFT, UPI, messaging solutions, etc., by certain jurisdictions. Thus, there is scope for enhancing global outreach of our payment systems, including remittance services, through active participation and co-operation in international and regional fora by collaborating and contributing to standard setting. Considering that efforts are being taken to increase and widen the scope, coverage and usage of RuPay card scheme and UPI to enhance their brand value internationally, the risks of such systems would also be high. The participants in a domestic system might become dependent on the funds they are to receive in an offshore system to fund their domestic debt position, leading to possible liquidity risk issues. This could also be on account of different time zones and also due to lacking nature of suitable depth in the currency markets of such economies, and more so in

the event of financial distress. In such cases, there would be a requirement for constant cooperation with the concerned central banks and other regulatory authorities.

**7.5** The Reserve Bank has been facilitating the increased participation of non-bank players in the payments ecosystem in India. These entities are playing a significant role in provision of payment services by bringing in innovation and convenience to customers and leveraging on technological developments. Since such entities are not mandated to be necessarily a RBI regulated one but could also perform other forms of unregulated business, with a view to ensuring that such entities do not pose a risk to their subsidiaries which also conduct financial business that are regulated by any one of the financial regulators, a system is put in place for seeking information from the concerned financial regulator for ensuring fit and proper criteria of the promoters and management is ensured while granting any authorization / licence to do relevant financial business.

#### **7.6 Participation in Domestic and International Fora and Committees**

RBI is represented in various international and domestic fora pertaining to payment and settlement systems and financial market infrastructures. These, inter-alia, include the Committee on Payments and Market Infrastructures (CPMI), Regulatory Oversight of LEI, Task Force on Payment Aspects of Financial Inclusion (constituted by CPMI), SAARC Payments Council, SWIFT Oversight Forum.

#### **7.7 Benchmarking Exercise**

**7.7.1** RBI has undertaken an exercise of benchmarking India's Payment Systems vis-à-vis payment systems in a mix of 21 countries, representing advanced economies, Asian economies and the BRICS nations. The analysis was attempted under 41 indicators covering 21 broad areas including regulation, oversight, payment systems, payment instruments, payment infrastructure, utility payments, Government payments, customer protection and grievance redressal, securities settlement and clearing systems and cross border personal remittances. The study found that India has a strong regulatory system and robust large value and retail payment systems which have contributed to the rapid growth in the volume of transactions in these payment systems. There has been substantial growth in e-payments by Government and also in digital infrastructure in terms of mobile networks.

**7.7.2** Such exercises provide a perspective on the performance of India compared to other countries, in the payment systems space. It highlights strengths and weaknesses relative to comparable payments and usage trends in other countries. The exercise, therefore, attempted to (a) arrive at an understanding of preferences Indians have for making and receiving payments and how these preferences compare with other countries, and (b) measure the efficiency of our payment systems. Such exhaustive domestic and international assessments

of our payment systems augment their efficiency and provide insights into areas of further focus.

## **7.8 Study to assess the progress of digitisation from cash to electronic**

**7.8.1** With cash being the well-established and widely used payment instrument, and at the same time rapid increase in non-cash payments, especially those using electronic or digital modes, prompted RBI to conduct a study to assess the level of digitisation in payments. The study analysed the measures of cash (proxy for cash payments), the enablers for payment systems and the measures of electronic payments over a timeframe of the last 5 financial years to ascertain the shift in India, if any, from cash to digital payments. Further, a comparison with the 26 member countries of the Committee on Payments and Market Infrastructures (CPMI) over the same five year period has also been attempted to evaluate India's performance vis-à-vis other countries.

**7.8.2** The parameters considered as indicative of cash payments are Currency in Circulation (CIC), Share of High Value denominated currency and Low Value denominated currency, and Cash Withdrawals from ATMs, whereas parameters used for assessing the level of digitisation were Growth of digital payments, Digital Payments to GDP, and infrastructure.

**7.8.3** The study revealed that while CIC across the country increased at a CAGR of 10.2% over the past 5 years, the CIC to GDP reduced from 11.6% in 2014-15 to 11.2% in 2018-19. The cash withdrawals from ATMs increased during the same period, however, the percentage of cash withdrawals to GDP was constant at around 17%. Further, while the digital payments in the country have witnessed CAGR of 61% and 19% in terms of volume and value, respectively, the value of digital payments to GDP has also increased from 660% in 2014-15 to 862% in 2018-19. In addition, the deployment of ATMs has grown at a low pace (CAGR – 4%) and the PoS terminals contrastingly grown at high pace (CAGR – 35%).

**7.8.4** The study findings indicate that cash, as a payment mode, is still important but it is increasingly seen as a way to store value, more than to make payments. India's growing use of retail digital payments, along with the radical reconstruction of its cash economy, indicates a shift in the relationship with cash. This is evidenced by the steep growth observed in the retail digital payments.

## **Section 8: Organisation of the Oversight Function**

**8.1** In order to conduct effective oversight, the central banks need to have the ability to carry out oversight effectively by having sufficient resources, including suitably qualified personnel and an organisational structure that allows those resources to be used effectively.

It is important that those involved in carrying out oversight are able to draw on the skills and expertise of other central bank functions (for example, legal, markets, credit, audit and IT).

**8.2** A dedicated Oversight Division in the Department of Payment and Settlement Systems (DPSS) at Central Office of RBI has been institutionalised and is tasked with the responsibility to conduct oversight of all payment systems. The Central Office Oversight Division is supported by DPSS cells set-up at four Regional Offices at Mumbai, Delhi, Chennai and Kolkata. Skilled resources are drawn from other departments while undertaking the assessment / onsite inspection of FMIs / RPSs. While the DPSS Cells at four Regional Offices conduct on-site inspection of various retail payment systems and Cheque Clearing Houses, the Central Office Oversight Division carries out on-site inspection of FMIs and SWIPS (NPCI).



**Schedule of Activities****A. FMIs**

The FMIs would be overseen as per the “Oversight Framework for Financial Market Infrastructures and Retail Payment Systems”. The entities covered as part of this framework and the activities to be undertaken are as follows:

(i) **Real Time Gross Settlement System (RTGS):** RTGS system is owned and operated by the RBI. Assessment would be against the PFMI -

- Alerts / Incident reporting: (i) SOD / EOD, (ii) delay in any of the activity, (iii) reporting of incidents, if any.
- Self-Assessment undertaken annually by the operator i.e. Division of Bank Accounts, Mumbai Regional Office.
- On-site inspection and assessment at periodic intervals.

(ii) **Central Securities Depository (CSD) - Securities Settlement Systems (SSS):** The CSD-SSS for the Government Securities system is operated by PDO / Mumbai office. Assessment would be against the PFMI.

- Self-Assessment undertaken annually by the operator i.e. Integrated Banking Department of Mumbai Regional Office of RBI.
- On-site inspection and assessment at periodic intervals.

(iii) **Clearing Corporation of India Ltd (CCIL)**

- Disclose self-assessment on compliance with PFMI on an annual basis as per the Disclosure Framework prescribed in PFMI.
- Quantitative Disclosure as per the disclosure Framework prescribed by the CPMI-IOSCO on a Quarterly basis.
- Onsite inspection and assessment of CCIL to be undertaken annually by DPSS or get conducted by external agency.
- Before initiation of Onsite inspection, an Onsite Compliance Audit to be undertaken to verify compliance against the Inspection observations. The minimum coverage should be as per the framework prescribed.
- To ensure resilience of the system, CCIL to conduct Operations Review on a monthly basis and also undertake an IT System Review by external auditors and to also submit a System Audit Report on an annual basis.
- CCIL will undertake a System Audit and submit the report to the RBI on an annual basis. The minimum coverage of the system audit should be as per the revised scope prescribed vide letter DPSS.CO.OD.No. 1325/06.11.001/2019-20 dated January 10, 2020.
- CCIL to undertake an annual validation and review of its Risk Management framework by external auditors to ensure that its systems are resilient.

- CCIL to seek the RBI's approval before initiating changes in any systems or processes and before introducing any new product.
- CCIL is also expected to intimate the RBI in case of any abnormal developments.
- CCIL to furnish on a monthly / quarterly / semi-annual basis the reports / data / information as prescribed in the Appendices 4 and 8, to the RBI.

**(iv) National Electronic Funds Transfer (NEFT):** NEFT system is owned and operated by the RBI. Though it is a retail payment system, keeping in view the volume of transactions processed by it, it will be assessed on an on-going basis against the PFMI –

- Self-Assessment to be undertaken annually by National Clearing Cell of Mumbai Regional Office of RBI.
- On-site inspection and assessment to be conducted periodically.

**(v) National Payments Corporation of India (NPCI):**

The RBI oversees the NPCI, an umbrella organisation for all retail payments systems in India.

- NPCI, as per the Disclosure Framework prescribed in PFMI to disclose its self-assessment on its compliance with PFMI on an annual basis and also submit a copy to the RBI.
- On-site inspection and assessment to be conducted bi-annually by the DPSS or get conducted by external agency.
- Before initiation of Onsite inspection, an On-Site Compliance Audit will be undertaken to verify NPCI compliance against the Inspection observations.
- To ensure resilience of the payment systems, NPCI will undertake a System Audit and submit the report to the RBI on an annual basis. The minimum coverage of the system audit should be as per the revised scope prescribed vide letter DPSS.CO.OD.No. 1325/06.11.001/2019-20 dated January 10, 2020.
- NPCI will also submit its audited financial statements to the RBI on an annual basis.
- NPCI to furnish monthly reports / data / information to the RBI as prescribed in Appendix 8 for each of the payment system operated by it.

## **B. Retail Payment Systems**

The Retail Payment Systems regulated by the RBI are:

**(i) Cards Payment Networks**

- Self-Assessment to be submitted annually as per template prescribed.
- Submit System Audit Report and segmented financial statements for India specific operations to the RBI on an annual basis. The minimum coverage of the system audit should be as per the revised scope prescribed vide letter DPSS.CO.OD.No. 1325/06.11.001/2019-20 dated January 10, 2020.
- Submit a monthly return on card statistics for Cards affiliated under its scheme in the format prescribed by RBI.

- *The segmented financial statements for India specific operations to be submitted to the RBI for each quarter and for the entire year.*
  - *On-site inspection would be restricted to visit if needed / interaction with the executives of the card networks and with the primary regulator.*
- (ii) **Cross-border Money Transfer – in-bound only – Operators**
- *Self-Assessment to be submitted to the Department of Payment and Settlement Systems, Kolkata Regional Office, RBI on an annual basis as per the prescribed Template.*
  - *Submit System Audit Report to the RBI on an annual basis. The minimum coverage of the system audit should be as per the revised scope prescribed vide letter DPSS.CO.OD.No. 1325/06.11.001/2019-20 dated January 10, 2020.*
  - *The segmented financial statements for India specific operations to be submitted to the RBI for each quarter and also for the entire year.*
  - *On-site inspection would be restricted to visit, if needed / interaction with the executives of the authorised entity (located overseas) and with the primary regulator.*
  - *Returns as indicated in Appendix 8 to be submitted in the format, form and manner prescribed by the RBI.*
- (iii) **ATM Networks**
- *Self-Assessment to be submitted against the prescribed Template on an annual basis.*
  - *ATM Network operators (non-bank operator) to submit the System Audit Report to the RBI on an annual basis. The minimum coverage of the system audit should be as per the revised scope prescribed vide letter DPSS.CO.OD.No. 1325/06.11.001/2019-20 dated January 10, 2020.*
  - *ATM Network operators to submit Financial Statements to the RBI on an annual basis.*
  - *ATM Network operators to submit a monthly return on ATM Statistics in the format prescribed.*
  - *ATM Network operators to submit a quarterly return on Deployment of ATM's containing State-wise ATMs deployed during the quarter and summary of ATMs deployed in Metro, Urban, Semi-urban and Rural areas. The returns to be submitted in the format, form and manner prescribed by the RBI.*
  - *Returns to be submitted in the format, form and manner prescribed by the RBI.*
  - *On-site inspection to be conducted bi-annually by the DPSS or get conducted by external agency.*
- (iv) **Pre-paid Payment Instruments (PPIs)**
- *Self-Assessment to be submitted against the prescribed Template on an annual basis to the DPSS Regional Offices of RBI depending upon the location of the Registered Offices of the authorised entities.*

- *PPI issuers need to submit their System Audit Report and Financial statements to the RBI on an annual basis. The minimum coverage of the system audit should be as per the revised scope prescribed vide letter DPSS.CO.OD.No. 1325/06.11.001/2019-20 dated January 10, 2020.*
- *PPI issuers need to submit financial statements to the RBI on an annual basis.*
- *PPI issuers need to submit data/information on expired PPIs, Customer Grievances and a Certificate from the auditor on balance in Escrow Account to the RBI on quarterly basis in formats indicated in Appendix 8.*
- *PPI issuers need to submit the PPI Statistics to RBI monthly. The returns to be submitted in the format, form and manner prescribed by the RBI as indicated in Appendix 8.*
- *Fraud monitoring report to be submitted monthly in format indicated in Appendix 8.*
- *Payment fraud report to be submitted on daily basis to RBI in Electronic Data Submission Portal (EDSP) as per format indicated in Appendix 8 (going forward, this shall be replaced with the web-based payment fraud reporting mechanism).*
- *Returns as indicated in Appendix 8 to be submitted in the format, form and manner prescribed by the RBI.*
- *On Site Inspection of PPI providers to be undertaken at least once every three years by the respective DPSS Regional Office of RBI based on the location of the Registered Offices of PPI issuer. The frequency of on-site inspection will depend on its classification as large, medium or small PPI Issuer. The Inspection report will be submitted by the Regional Offices of DPSS to DPSS, Central Office.*

(v) **Bharat Bill Payment System (BBPS)**

BBPS is an integrated bill payment system which will offer interoperable bill payment service to customers online as well as through a network of agents. NPCI has been granted approval to function as the Bharat Bill Payment Central Unit (BBPCU) which is a single authorised entity operating the BBPS. The BBPCU has formulated necessary operational, technical and business standards for the entire system and its participants, after approval of the RBI. Banks and non-bank entities function as Bharat Bill Payment Operating Units (BBPOU)

- *The BBPCU (NPCI) would be covered as part of the NPCI assessment till the activity is hived off to another entity.*
- *Oversight of the BBPOUs will be undertaken by the RBI and NPCI (restricted to the BBPOUs as participant in BBPS).*
- *BBPOUs to submit System Audit Reports to the RBI annually. The minimum coverage of the system audit should be as per the revised scope prescribed vide letter DPSS.CO.OD.No. 1325/06.11.001/2019-20 dated January 10, 2020.*
- *BBPOUs to submit Financial Statements to the RBI annually.*
- *The Statistical operational information will be sent by the BBPOUs to NPCI. The BBPOUs will also be required to send all the data/ information reports to NPCI as*

deemed necessary by NPCI. Any delay in submission of data to NPCI would attract the same penal action for delay / non-submission to RBI. NPCI to report the data to RBI in the format prescribed.

(vi) **Trade Receivables Discounting System (TReDS)**

- Self-Assessment to be submitted against the prescribed Template on an annual basis.
- TReDS operators to undertake and submit a System Audit report to the RBI on an annual basis. The minimum coverage of the system audit should be as per the revised scope prescribed vide letter DPSS.CO.OD.No. 1325/06.11.001/2019-20 dated January 10, 2020.
- TReDS operators to submit audited financial statements to the RBI on an annual basis.
- TReDS operators to furnish monthly reports/ data/ information to the RBI as prescribed. The returns to be submitted in the format, form and manner prescribed by the RBI as indicated in Appendix 8.

(vii) **White Label ATM Operators (WLAOs)**

- Self-Assessment to be submitted against the prescribed Template on an annual basis to the DPSS Regional Offices of RBI depending upon the location of the Registered Offices of the authorised entities.
- WLA Operators need to submit their System Audit Report and Financial statements to the RBI on an annual basis. The minimum coverage of the system audit should be as per the revised scope prescribed vide letter DPSS.CO.OD.No. 1325/06.11.001/2019-20 dated January 10, 2020.
- Submit returns in the format, form and manner indicated in Appendix 8.

(viii) **Other retail payment systems**

- Self-Assessment to be submitted against the prescribed Template on an annual basis to the DPSS Regional Offices depending on the location of Registered Office of authorised entities.
- System Audit Report and Financial statements to the RBI on an annual basis. The minimum coverage of the system audit should be as per the revised scope prescribed vide letter DPSS.CO.OD.No. 1325/06.11.001/2019-20 dated January 10, 2020.
- Business, Customer Grievances on the periodicity prescribed. The operator should submit the Statistics to the RBI accordingly. The returns to be submitted in the format, form and manner prescribed by the RBI.
- On Site Inspection of providers will be undertaken at least once every three years by the respective DPSS RO based on the location of the operator.
- Submit returns in the format, form and manner indicated in Appendix 8.
- Any other requirement would be prescribed based on the design / process of operations.

**Information submitted as part of the application**

PART – A: Covering the details of the applicant, constitution of applicant, address of Registered Office and Principal Offices (if applicant is a company), principal place of business, main business of the applicant company / firm / other entity, management information, etc.

PART – B: Covering particulars of Payment System sought to be set up (full details to be furnished) including process flow, technology to be used, security features, inter-operability, etc., expected benefits to the financial system / country from the operationalisation of the payment system sought to be set up, previous experience of applicant and associated companies / firms / entities in the payment systems area, type of payment system proposed to be set up, method of settlement of payment claims, namely .whether gross, net or a hybrid method combining both gross and net methods, whether the applicant or settlement agent will act as a central counterparty to provide guaranteed / secured settlement, customer grievances redressal machinery proposed for the payment system sought to be set up, the time proposed to be taken to dispose customer complaints, etc.

PART – C: covering amount of finance required for executing payment system project, sources of finances for executing the payment system project, rate of return on investment expected from the payment system sought to be set up, how does the applicant proposes to recover investment and earn income, etc.

PART – D: Any other information the applicant wishes to furnish.

**Returns, documents and other information to be submitted by Authorised Payment Systems**

1. Every Authorised Payment System provider shall submit the returns as prescribed and at the frequency indicated by the RBI.
2. Details of the defaults in fulfilling the payment obligations by the system participants to be reported on the date of occurrence.
3. Monthly return containing the details of the defaults in fulfilling the payment obligations by the system participants. This to be submitted within seven working days from the end of the month. (The return and format for submission is as Appended).
4. Quarterly certificate from the bankers about functioning of system provider's escrow account with them.
5. Quarterly statement regarding any disputes between participants or between participants and the system provider. This to be submitted within seven working days from the end of the quarter.
6. Annual return relating to the staff strength, income and expenditure.
7. Annual return from the system provider showing changes in its Board of Directors or partners, as the case may be, changes in shareholding pattern whereby the aggregate shareholding of an individual or a group becomes equivalent to 5% or more of the paid-up capital of the system provider and changes in Memorandum or Articles of Association of the system provider.
8. Furnishing of accounts and balance sheets:
  - (1) Every system provider shall furnish to the Bank within three months from the date on which its annual accounts are closed and balanced, a copy of its audited balance sheet as on the last date of the relevant year together with a copy of the profit and loss account for the year and a copy of the Auditor's report.

Provided that the Bank may, on an application made by the system provider, extend the said period of three months for furnishing of returns by a further period not exceeding three months.
  - (2) The system provider shall also publish, a copy of its balance sheet, profit and loss account and Auditor's report submitted to the Bank under sub-regulation (1), in any two leading newspapers, one in English and the other in Hindi, or place a copy of the same on its website within a period of one month from the date of submission of the same to the Bank.

The documents / information shall be submitted by the system provider from its registered office to the RBI (Department of Payment and Settlement Systems, Central Office) situated in

Mumbai. The RBI may at any time, direct that certain returns / data and documents stated above to be submitted to any of its other office as may be specified.



**Data / Information to be furnished by CCIL**

- *Authorised CCP shall inform RBI about the appointment / reappointment of the Directors and shall send to RBI within 15 calendar days from the date of appointment by the Board, the Directors' profile, declaration on "fit and proper" criteria submitted by Directors as prescribed and their consent to act as Directors.*
- *Authorised CCP shall inform about transfer or divestment within 15 calendar days of approval of transfer or divestment of equity shares by its Board.*
- *Monthly and Fortnightly report on Forex Participation and Settlement Statistics.*
- *Monthly report for trades settled in all segments.*
- *Details of shortage/ default in any segment to be submitted to the RBI on the same day. Also submit a monthly report for each segment with the details of shortage/ defaults during the month.*
- *Monthly certificate from auditors confirming segment-wise segregation of collaterals.*
- *Annual return on staff strength, income and expenditure.*
- *Annual return on changes in Board of directors, changes in shareholding and changes in Memorandum of Association or Articles of Association.*
- *Submit Audited Balance Sheet, Profit & Loss Account & Auditors Report on an annual basis.*
- *Submit Operations audit report, concurrent audit report and implementation status review of the operations audit report for every month.*
- *Submit the IT process operation review report quarterly.*
- *Submit the Systems Audit report from CISA qualified auditor annually.*
- *Submission of ISO Audit Report annually.*
- *Comprehensive Risk Management Framework annually.*
- *Submit the report of Monthly Summary of Stress Test Result.*
- *Submit the investment policy for the year to the RBI annually.*
- *Submission of report of risk assessment by external experts annually.*
- *Deviations in membership eligibility criteria for participants in any segment submitted annually and periodically in case of interim review.*
- *Imposition of restrictions on members, as and when any restriction is imposed.*
- *Report on FX-CLEAR API trading activity.*
- *Submission of Business Continuity Plan on an annual basis.*
- *Submission of the Information Security Policy and Cyber Security Policy on an annual basis.*
- *Periodic intimation of Business Continuity Drills and submission of report thereof.*
- *Calendar of review items placed before the board on an annual basis.*

- *Information regarding any notification/circular issued to members, as and when the notification/circular is issued.*
- *Information regarding any changes in Bye-laws, rules and regulations, as and when the same is revised.*
- *Intimation and report of Table Top Exercise, as and when conducted.*
- *Intimation and report of Portfolio Compression Exercise in Derivatives segment, as and when conducted.*
- *Intimation of any disruption or delayed payment, as and when such incident occurs.*
- *Submission of Quantitative Disclosures on quarterly basis.*
- *Submission of Qualitative Disclosures on annual basis.*
- *Submission of Self-Assessment on Annual basis.*
- *Submission of daily data for disclosure on RBI website.*
- *Every authorised CCP shall submit an audited net-worth certificate as at close of financial year from the statutory auditor within six months of the closure of the financial year.*
- *Submission of Default History Report of Securities/Triparty Repo segment on half-yearly basis.*
- *Submission of report on important issues identified by Independent Directors which may involve conflict of Interest that may have significant impact on the functioning of authorised CCP or may not be in the interest of its market segments.*

**Overview of the Principles for Financial Market Infrastructures**

**General organisation**

**Principle 1: Legal basis**

An FMI should have a well-founded, clear, transparent, and enforceable legal basis for each material aspect of its activities in all relevant jurisdictions.

**Key considerations**

1. *The legal basis should provide a high degree of certainty for each material aspect of an FMI's activities in all relevant jurisdictions.*
2. *An FMI should have rules, procedures, and contracts that are clear, understandable, and consistent with relevant laws and regulations.*
3. *An FMI should be able to articulate the legal basis for its activities to relevant authorities, participants, and, where relevant, participants' customers, in a clear and understandable way.*
4. *An FMI should have rules, procedures, and contracts that are enforceable in all relevant jurisdictions. There should be a high degree of certainty that actions taken by the FMI under such rules and procedures will not be voided, reversed, or subject to stays.*
5. *An FMI conducting business in multiple jurisdictions should identify and mitigate the risks arising from any potential conflict of laws across jurisdictions.*

**Principle 2: Governance**

An FMI should have governance arrangements that are clear and transparent, promote the safety and efficiency of the FMI, and support the stability of the broader financial system, other relevant public interest considerations, and the objectives of relevant stakeholders.

**Key considerations**

1. *An FMI should have objectives that place a high priority on the safety and efficiency of the FMI and explicitly support financial stability and other relevant public interest considerations.*
2. *An FMI should have documented governance arrangements that provide clear and direct lines of responsibility and accountability. These arrangements should be disclosed to owners, relevant authorities, participants, and, at a more general level, the public.*
3. *The roles and responsibilities of an FMI's board of directors (or equivalent) should be clearly specified, and there should be documented procedures for its functioning, including procedures to identify, address, and manage member conflicts of interest. The board should review both its overall performance and the performance of its individual board members regularly.*
4. *The board should contain suitable members with the appropriate skills and incentives to fulfil its multiple roles. This typically requires the inclusion of non-executive board member(s).*
5. *The roles and responsibilities of management should be clearly specified. An FMI's management should have the appropriate experience, a mix of skills, and the integrity necessary to discharge their responsibilities for the operation and risk management of the FMI.*
6. *The board should establish a clear, documented risk-management framework that includes the FMI's risk-tolerance policy, assigns responsibilities and accountability for risk decisions, and addresses decision making in crises and emergencies. Governance arrangements should ensure that the risk-management and internal*

*control functions have sufficient authority, independence, resources, and access to the board.*

- 7. The board should ensure that the FMI's design, rules, overall strategy, and major decisions reflect appropriately the legitimate interests of its direct and indirect participants and other relevant stakeholders. Major decisions should be clearly disclosed to relevant stakeholders and, where there is a broad market impact, the public.*

### **Principle 3: Framework for the comprehensive management of risks**

An FMI should have a sound risk-management framework for comprehensively managing legal, credit, liquidity, operational, and other risks.

#### **Key considerations**

- 1. An FMI should have risk-management policies, procedures, and systems that enable it to identify, measure, monitor, and manage the range of risks that arise in or are borne by the FMI. Risk-management frameworks should be subject to periodic review.*
- 2. An FMI should provide incentives to participants and, where relevant, their customers to manage and contain the risks they pose to the FMI.*
- 3. An FMI should regularly review the material risks it bears from and poses to other entities (such as other FMIs, settlement banks, liquidity providers, and service providers) as a result of interdependencies and develop appropriate risk-management tools to address these risks.*
- 4. An FMI should identify scenarios that may potentially prevent it from being able to provide its critical operations and services as a going concern and assess the effectiveness of a full range of options for recovery or orderly wind-down. An FMI should prepare appropriate plans for its recovery or orderly wind-down based on the results of that assessment. Where applicable, an FMI should also provide relevant authorities with the information needed for purposes of resolution planning.*

### **Credit and liquidity risk management**

#### **Principle 4: Credit risk**

An FMI should effectively measure, monitor, and manage its credit exposures to participants and those arising from its payment, clearing, and settlement processes. An FMI should maintain sufficient financial resources to cover its credit exposure to each participant fully with a high degree of confidence. In addition, a CCP that is involved in activities with a more-complex risk profile or that is systemically important in multiple jurisdictions should maintain additional financial resources sufficient to cover a wide range of potential stress scenarios that should include, but not be limited to, the default of the two participants and their affiliates that would potentially cause the largest aggregate credit exposure to the CCP in extreme but plausible market conditions. All other CCPs should maintain additional financial resources sufficient to cover a wide range of potential stress scenarios that should include, but not be limited to, the default of the participant and its affiliates that would potentially cause the largest aggregate credit exposure to the CCP in extreme but plausible market conditions.

#### **Key considerations**

- 1. An FMI should establish a robust framework to manage its credit exposures to its participants and the credit risks arising from its payment, clearing, and settlement processes. Credit exposure may arise from current exposures, potential future exposures, or both.*

2. *An FMI should identify sources of credit risk, routinely measure and monitor credit exposures, and use appropriate risk-management tools to control these risks. \*
3. *A payment system or SSS should cover its current and, where they exist, potential future exposures to each participant fully with a high degree of confidence using collateral and other equivalent financial resources (see Principle 5 on collateral). In the case of a DNS payment system or DNS SSS in which there is no settlement guarantee but where its participants face credit exposures arising from its payment, clearing, and settlement processes, such an FMI should maintain, at a minimum, sufficient resources to cover the exposures of the two participants and their affiliates that would create the largest aggregate credit exposure in the system.*
4. *A CCP should cover its current and potential future exposures to each participant fully with a high degree of confidence using margin and other prefunded financial resources (see Principle 5 on collateral and Principle 6 on margin). In addition, a CCP that is involved in activities with a more-complex risk profile or that is systemically important in multiple jurisdictions should maintain additional financial resources to cover a wide range of potential stress scenarios that should include, but not be limited to, the default of the two participants and their affiliates that would potentially cause the largest aggregate credit exposure for the CCP in extreme but plausible market conditions. All other CCPs should maintain additional financial resources sufficient to cover a wide range of potential stress scenarios that should include, but not be limited to, the default of the participant and its affiliates that would potentially cause the largest aggregate credit exposure for the CCP in extreme but plausible market conditions. In all cases, a CCP should document its supporting rationale for, and should have appropriate governance arrangements relating to, the amount of total financial resources it maintains.*
5. *A CCP should determine the amount and regularly test the sufficiency of its total financial resources available in the event of a default or multiple defaults in extreme but plausible market conditions through rigorous stress testing. A CCP should have clear procedures to report the results of its stress tests to appropriate decision makers at the CCP and to use these results to evaluate the adequacy of and adjust its total financial resources. Stress tests should be performed daily using standard and predetermined parameters and assumptions. On at least a monthly basis, a CCP should perform a comprehensive and thorough analysis of stress testing scenarios, models, and underlying parameters and assumptions used to ensure they are appropriate for determining the CCP's required level of default protection in light of current and evolving market conditions. A CCP should perform this analysis of stress testing more frequently when the products cleared or markets served display high volatility, become less liquid, or when the size or concentration of positions held by a CCP's participants increases significantly. A full validation of a CCP's risk-management model should be performed at least annually.*
6. *In conducting stress testing, a CCP should consider the effect of a wide range of relevant stress scenarios in terms of both defaulters' positions and possible price changes in liquidation periods. Scenarios should include relevant peak historic price volatilities, shifts in other market factors such as price determinants and yield curves, multiple defaults over various time horizons, simultaneous pressures in funding and asset markets, and a spectrum of forward-looking stress scenarios in a variety of extreme but plausible market conditions.*
7. *An FMI should establish explicit rules and procedures that address fully any credit losses it may face as a result of any individual or combined default among its participants with respect to any of their obligations to the FMI. These rules and procedures should address how potentially uncovered credit losses would be allocated, including the repayment of any funds an FMI may borrow from liquidity providers. These rules and procedures should also indicate the FMI's process to replenish any financial resources that the FMI may employ during a stress event, so that the FMI can continue to operate in a safe and sound manner.*

### **Principle 5: Collateral**

An FMI that requires collateral to manage its or its participants' credit exposure should accept collateral with low credit, liquidity, and market risks. An FMI should also set and enforce

#### **Key considerations**

1. *An FMI should generally limit the assets it (routinely) accepts as collateral to those with low credit, liquidity, and market risks.*
2. *An FMI should establish prudent valuation practices and develop haircuts that are regularly tested and take into account stressed market conditions.*
3. *In order to reduce the need for procyclical adjustments, an FMI should establish stable and conservative haircuts that are calibrated to include periods of stressed market conditions, to the extent practicable and prudent.*
4. *An FMI should avoid concentrated holdings of certain assets where this would significantly impair the ability to liquidate such assets quickly without significant adverse price effects.*
5. *An FMI that accepts cross-border collateral should mitigate the risks associated with its use and ensure that the collateral can be used in a timely manner.*
6. *An FMI should use a collateral management system that is well-designed and operationally flexible. appropriately conservative haircuts and concentration limits.*

### **Principle 6: Margin**

A CCP should cover its credit exposures to its participants for all products through an effective margin system that is risk-based and regularly reviewed.

#### **Key considerations**

1. *A CCP should have a margin system that establishes margin levels commensurate with the risks and particular attributes of each product, portfolio, and market it serves.*
2. *A CCP should have a reliable source of timely price data for its margin system. A CCP should also have procedures and sound valuation models for addressing circumstances in which pricing data are not readily available or reliable.*
3. *A CCP should adopt initial margin models and parameters that are risk-based and generate margin requirements sufficient to cover its potential future exposure to participants in the interval between the last margin collection and the close out of positions following a participant default. Initial margin should meet an established single-tailed confidence level of at least 99 percent with respect to the estimated distribution of future exposure. For a CCP that calculates margin at the portfolio level, this requirement applies to each portfolio's distribution of future exposure. For a CCP that calculates margin at more-granular levels, such as at the subportfolio level or by product, the requirement must be met for the corresponding distributions of future exposure. The model should (a) use a conservative estimate of the time horizons for the effective hedging or close out of the particular types of products cleared by the CCP (including in stressed market conditions), (b) have an appropriate method for measuring credit exposure that accounts for relevant product risk factors and portfolio effects across products, and (c) to the extent practicable and prudent, limit the need for destabilising, procyclical changes.*
4. *A CCP should mark participant positions to market and collect variation margin at least daily to limit the build-up of current exposures. A CCP should have the authority and operational capacity to make intraday margin calls and payments, both scheduled and unscheduled, to participants.*
5. *In calculating margin requirements, a CCP may allow offsets or reductions in required margin across products that it clears or between products that it and another CCP clear, if the risk of one product is significantly and reliably correlated with the risk of the*

- other product. Where two or more CCPs are authorised to offer cross-margining, they must have appropriate safeguards and harmonised overall risk-management systems.*
- 6. A CCP should analyse and monitor its model performance and overall margin coverage by conducting rigorous daily backtesting and at least monthly, and more-frequent where appropriate, sensitivity analysis. A CCP should regularly conduct an assessment of the theoretical and empirical properties of its margin model for all products it clears. In conducting sensitivity analysis of the model's coverage, a CCP should take into account a wide range of parameters and assumptions that reflect possible market conditions, including the most-volatile periods that have been experienced by the markets it serves and extreme changes in the correlations between prices.*
  - 7. A CCP should regularly review and validate its margin system.*

### **Principle 7: Liquidity risk**

An FMI should effectively measure, monitor, and manage its liquidity risk. An FMI should maintain sufficient liquid resources in all relevant currencies to effect same-day and, where appropriate, intraday and multiday settlement of payment obligations with a high degree of confidence under a wide range of potential stress scenarios that should include, but not be limited to, the default of the participant and its affiliates that would generate the largest aggregate liquidity obligation for the FMI in extreme but plausible market conditions.

#### **Key considerations**

- 1. An FMI should have a robust framework to manage its liquidity risks from its participants, settlement banks, nostro agents, custodian banks, liquidity providers, and other entities.*
- 2. An FMI should have effective operational and analytical tools to identify, measure, and monitor its settlement and funding flows on an ongoing and timely basis, including its use of intraday liquidity.*
- 3. A payment system or SSS, including one employing a DNS mechanism, should maintain sufficient liquid resources in all relevant currencies to effect same-day settlement, and where appropriate intraday or multiday settlement, of payment obligations with a high degree of confidence under a wide range of potential stress scenarios that should include, but not be limited to, the default of the participant and its affiliates that would generate the largest aggregate payment obligation in extreme but plausible market conditions.*
- 4. A CCP should maintain sufficient liquid resources in all relevant currencies to settle securities-related payments, make required variation margin payments, and meet other payment obligations on time with a high degree of confidence under a wide range of potential stress scenarios that should include, but not be limited to, the default of the participant and its affiliates that would generate the largest aggregate payment obligation to the CCP in extreme but plausible market conditions. In addition, a CCP that is involved in activities with a more-complex risk profile or that is systemically important in multiple jurisdictions should consider maintaining additional liquidity resources sufficient to cover a wider range of potential stress scenarios that should include, but not be limited to, the default of the two participants and their affiliates that would generate the largest aggregate payment obligation to the CCP in extreme but plausible market conditions.*
- 5. For the purpose of meeting its minimum liquid resource requirement, an FMI's qualifying liquid resources in each currency include cash at the central bank of issue and at creditworthy commercial banks, committed lines of credit, committed foreign exchange swaps, and committed repos, as well as highly marketable collateral held in custody and investments that are readily available and convertible into cash with prearranged and highly reliable funding arrangements, even in extreme but plausible market conditions. If an FMI has access to routine credit at the central bank of issue,*

*the FMI may count such access as part of the minimum requirement to the extent it has collateral that is eligible for pledging to (or for conducting other appropriate forms of transactions with) the relevant central bank. All such resources should be available when needed.*

- 6. An FMI may supplement its qualifying liquid resources with other forms of liquid resources. If the FMI does so, then these liquid resources should be in the form of assets that are likely to be saleable or acceptable as collateral for lines of credit, swaps, or repos on an ad hoc basis following a default, even if this cannot be reliably prearranged or guaranteed in extreme market conditions. Even if an FMI does not have access to routine central bank credit, it should still take account of what collateral is typically accepted by the relevant central bank, as such assets may be more likely to be liquid in stressed circumstances. An FMI should not assume the availability of emergency central bank credit as a part of its liquidity plan.*
- 7. An FMI should obtain a high degree of confidence, through rigorous due diligence, that each provider of its minimum required qualifying liquid resources, whether a participant of the FMI or an external party, has sufficient information to understand and to manage its associated liquidity risks, and that it has the capacity to perform as required under its commitment. Where relevant to assessing a liquidity provider's performance reliability with respect to a particular currency, a liquidity provider's potential access to credit from the central bank of issue may be taken into account. An FMI should regularly test its procedures for accessing its liquid resources at a liquidity provider.*
- 8. An FMI with access to central bank accounts, payment services, or securities services should use these services, where practical, to enhance its management of liquidity risk.*
- 9. An FMI should determine the amount and regularly test the sufficiency of its liquid resources through rigorous stress testing. An FMI should have clear procedures to report the results of its stress tests to appropriate decision makers at the FMI and to use these results to evaluate the adequacy of and adjust its liquidity risk-management framework. In conducting stress testing, an FMI should consider a wide range of relevant scenarios. Scenarios should include relevant peak historic price volatilities, shifts in other market factors such as price determinants and yield curves, multiple defaults over various time horizons, simultaneous pressures in funding and asset markets, and a spectrum of forward-looking stress scenarios in a variety of extreme but plausible market conditions. Scenarios should also take into account the design and operation of the FMI, include all entities that might pose material liquidity risks to the FMI (such as settlement banks, nostro agents, custodian banks, liquidity providers, and linked FMIs), and where appropriate, cover a multiday period. In all cases, an FMI should document its supporting rationale for, and should have appropriate governance arrangements relating to, the amount and form of total liquid resources it maintains.*
- 10. An FMI should establish explicit rules and procedures that enable the FMI to effect same-day and, where appropriate, intraday and multiday settlement of payment obligations on time following any individual or combined default among its participants. These rules and procedures should address unforeseen and potentially uncovered liquidity shortfalls and should aim to avoid unwinding, revoking, or delaying the same-day settlement of payment obligations. These rules and procedures should also indicate the FMI's process to replenish any liquidity resources it may employ during a stress event, so that it can continue to operate in a safe and sound manner.*

## **Settlement**

### **Principle 8: Settlement finality**

An FMI should provide clear and certain final settlement, at a minimum by the end of the value date. Where necessary or preferable, an FMI should provide final settlement intraday or in real time.



### **Key considerations**

1. *An FMI's rules and procedures should clearly define the point at which settlement is final.*
2. *An FMI should complete final settlement no later than the end of the value date, and preferably intraday or in real time, to reduce settlement risk. An LVPS or SSS should consider adopting RTGS or multiple-batch processing during the settlement day.*
3. *An FMI should clearly define the point after which unsettled payments, transfer instructions, or other obligations may not be revoked by a participant.*

### **Principle 9: Money settlements**

An FMI should conduct its money settlements in central bank money where practical and available. If central bank money is not used, an FMI should minimise and strictly control the credit and liquidity risk arising from the use of commercial bank money.

### **Key considerations**

1. *An FMI should conduct its money settlements in central bank money, where practical and available, to avoid credit and liquidity risks.*
2. *If central bank money is not used, an FMI should conduct its money settlements using a settlement asset with little or no credit or liquidity risk.*
3. *If an FMI settles in commercial bank money, it should monitor, manage, and limit its credit and liquidity risks arising from the commercial settlement banks. In particular, an FMI should establish and monitor adherence to strict criteria for its settlement banks that take account of, among other things, their regulation and supervision, creditworthiness, capitalisation, access to liquidity, and operational reliability. An FMI should also monitor and manage the concentration of credit and liquidity exposures to its commercial settlement banks.*
4. *If an FMI conducts money settlements on its own books, it should minimise and strictly control its credit and liquidity risks.*
5. *An FMI's legal agreements with any settlement banks should state clearly when transfers on the books of individual settlement banks are expected to occur, that transfers are to be final when effected, and that funds received should be transferable as soon as possible, at a minimum by the end of the day and ideally intraday, in order to enable the FMI and its participants to manage credit and liquidity risks.*

### **Principle 10: Physical deliveries**

An FMI should clearly state its obligations with respect to the delivery of physical instruments or commodities and should identify, monitor, and manage the risks associated with such physical deliveries.

### **Key considerations**

1. *An FMI's rules should clearly state its obligations with respect to the delivery of physical instruments or commodities.*
2. *An FMI should identify, monitor, and manage the risks and costs associated with the storage and delivery of physical instruments or commodities.*

### **Central securities depositories and exchange-of-value settlement systems**

#### **Principle 11: Central securities depositories**

A CSD should have appropriate rules and procedures to help ensure the integrity of securities issues and minimise and manage the risks associated with the safekeeping and transfer of

securities. A CSD should maintain securities in an immobilised or dematerialised form for their transfer by book entry.

### **Key considerations**

1. *A CSD should have appropriate rules, procedures, and controls, including robust accounting practices, to safeguard the rights of securities issuers and holders, prevent the unauthorised creation or deletion of securities, and conduct periodic and at least daily reconciliation of securities issues it maintains.*
2. *A CSD should prohibit overdrafts and debit balances in securities accounts.*
3. *A CSD should maintain securities in an immobilised or dematerialised form for their transfer by book entry. Where appropriate, a CSD should provide incentives to immobilise or dematerialise securities.*
4. *A CSD should protect assets against custody risk through appropriate rules and procedures consistent with its legal framework.*
5. *A CSD should employ a robust system that ensures segregation between the CSD's own assets and the securities of its participants and segregation among the securities of participants. Where supported by the legal framework, the CSD should also support operationally the segregation of securities belonging to a participant's customers on the participant's books and facilitate the transfer of customer holdings.*
6. *A CSD should identify, measure, monitor, and manage its risks from other activities that it may perform; additional tools may be necessary in order to address these risks.*

### **Principle 12: Exchange-of-value settlement systems**

If an FMI settles transactions that involve the settlement of two linked obligations (for example, securities or foreign exchange transactions), it should eliminate principal risk by conditioning the final settlement of one obligation upon the final settlement of the other.

### **Key consideration**

1. *An FMI that is an exchange-of-value settlement system should eliminate principal risk by ensuring that the final settlement of one obligation occurs if and only if the final settlement of the linked obligation also occurs, regardless of whether the FMI settles on a gross or net basis and when finality occurs.*

### **Default management**

### **Principle 13: Participant-default rules and procedures**

An FMI should have effective and clearly defined rules and procedures to manage a participant default. These rules and procedures should be designed to ensure that the FMI can take timely action to contain losses and liquidity pressures and continue to meet its obligations.

### **Key considerations**

1. *An FMI should have default rules and procedures that enable the FMI to continue to meet its obligations in the event of a participant default and that address the replenishment of resources following a default.*
2. *An FMI should be well prepared to implement its default rules and procedures, including any appropriate discretionary procedures provided for in its rules.*
3. *An FMI should publicly disclose key aspects of its default rules and procedures.*
4. *An FMI should involve its participants and other stakeholders in the testing and review of the FMI's default procedures, including any close-out procedures. Such testing and review should be conducted at least annually or following material changes to the rules and procedures to ensure that they are practical and effective.*

#### **Principle 14: Segregation and portability**

A CCP should have rules and procedures that enable the segregation and portability of positions of a participant's customers and the collateral provided to the CCP with respect to those positions.

##### **Key considerations**

1. *A CCP should, at a minimum, have segregation and portability arrangements that effectively protect a participant's customers' positions and related collateral from the default or insolvency of that participant. If the CCP additionally offers protection of such customer positions and collateral against the concurrent default of the participant and a fellow customer, the CCP should take steps to ensure that such protection is effective.*
2. *A CCP should employ an account structure that enables it readily to identify positions of a participant's customers and to segregate related collateral. A CCP should maintain customer positions and collateral in individual customer accounts or in omnibus customer accounts.*
3. *A CCP should structure its portability arrangements in a way that makes it highly likely that the positions and collateral of a defaulting participant's customers will be transferred to one or more other participants.*
4. *A CCP should disclose its rules, policies, and procedures relating to the segregation and portability of a participant's customers' positions and related collateral. In particular, the CCP should disclose whether customer collateral is protected on an individual or omnibus basis. In addition, a CCP should disclose any constraints, such as legal or operational constraints, that may impair its ability to segregate or port a participant's customers' positions and related collateral.*

#### **General business and operational risk management**

##### **Principle 15: General business risk**

An FMI should identify, monitor, and manage its general business risk and hold sufficient liquid net assets funded by equity to cover potential general business losses so that it can continue operations and services as a going concern if those losses materialise. Further, liquid net assets should at all times be sufficient to ensure a recovery or orderly wind-down of critical operations and services.

##### **Key considerations**

1. *An FMI should have robust management and control systems to identify, monitor, and manage general business risks, including losses from poor execution of business strategy, negative cash flows, or unexpected and excessively large operating expenses.*
2. *An FMI should hold liquid net assets funded by equity (such as common stock, disclosed reserves, or other retained earnings) so that it can continue operations and services as a going concern if it incurs general business losses. The amount of liquid net assets funded by equity an FMI should hold should be determined by its general business risk profile and the length of time required to achieve a recovery or orderly wind-down, as appropriate, of its critical operations and services if such action is taken.*
3. *An FMI should maintain a viable recovery or orderly wind-down plan and should hold sufficient liquid net assets funded by equity to implement this plan. At a minimum, an FMI should hold liquid net assets funded by equity equal to at least six months of current operating expenses. These assets are in addition to resources held to cover participant defaults or other risks covered under the financial resources principles. However, equity held under international risk-based capital standards can be included where relevant and appropriate to avoid duplicate capital requirements.*

4. *Assets held to cover general business risk should be of high quality and sufficiently liquid in order to allow the FMI to meet its current and projected operating expenses under a range of scenarios, including in adverse market conditions.*
5. *An FMI should maintain a viable plan for raising additional equity should its equity fall close to or below the amount needed. This plan should be approved by the board of directors and updated regularly.*

### **Principle 16: Custody and investment risks**

An FMI should safeguard its own and its participants' assets and minimise the risk of loss on and delay in access to these assets. An FMI's investments should be in instruments with minimal credit, market, and liquidity risks.

#### **Key considerations**

1. *An FMI should hold its own and its participants' assets at supervised and regulated entities that have robust accounting practices, safekeeping procedures, and internal controls that fully protect these assets.*
2. *An FMI should have prompt access to its assets and the assets provided by participants, when required.*
3. *An FMI should evaluate and understand its exposures to its custodian banks, taking into account the full scope of its relationships with each.*
4. *An FMI's investment strategy should be consistent with its overall risk-management strategy and fully disclosed to its participants, and investments should be secured by, or be claims on, high-quality obligors. These investments should allow for quick liquidation with little, if any, adverse price effect.*

### **Principle 17: Operational risk**

An FMI should identify the plausible sources of operational risk, both internal and external, and mitigate their impact through the use of appropriate systems, policies, procedures, and controls. Systems should be designed to ensure a high degree of security and operational reliability and should have adequate, scalable capacity. Business continuity management should aim for timely recovery of operations and fulfilment of the FMI's obligations, including in the event of a wide-scale or major disruption.

#### **Key considerations**

1. *An FMI should establish a robust operational risk-management framework with appropriate systems, policies, procedures, and controls to identify, monitor, and manage operational risks.*
2. *An FMI's board of directors should clearly define the roles and responsibilities for addressing operational risk and should endorse the FMI's operational risk-management framework. Systems, operational policies, procedures, and controls should be reviewed, audited, and tested periodically and after significant changes.*
3. *An FMI should have clearly defined operational reliability objectives and should have policies in place that are designed to achieve those objectives.*
4. *An FMI should ensure that it has scalable capacity adequate to handle increasing stress volumes and to achieve its service-level objectives.*
5. *An FMI should have comprehensive physical and information security policies that address all potential vulnerabilities and threats.*
6. *An FMI should have a business continuity plan that addresses events posing a significant risk of disrupting operations, including events that could cause a wide-scale or major disruption. The plan should incorporate the use of a secondary site and should be designed to ensure that critical information technology (IT) systems can resume operations within two hours following disruptive events. The plan should be designed*

to enable the FMI to complete settlement by the end of the day of the disruption, even in case of extreme circumstances. The FMI should regularly test these arrangements.

7. An FMI should identify, monitor, and manage the risks that key participants, other FMIs, and service and utility providers might pose to its operations. In addition, an FMI should identify, monitor, and manage the risks its operations might pose to other FMIs.

## **Access**

### **Principle 18: Access and participation requirements**

An FMI should have objective, risk-based, and publicly disclosed criteria for participation, which permit fair and open access.

#### **Key considerations**

1. An FMI should allow for fair and open access to its services, including by direct and, where relevant, indirect participants and other FMIs, based on reasonable risk-related participation requirements.
2. An FMI's participation requirements should be justified in terms of the safety and efficiency of the FMI and the markets it serves, be tailored to and commensurate with the FMI's specific risks, and be publicly disclosed. Subject to maintaining acceptable risk control standards, an FMI should endeavour to set requirements that have the least-restrictive impact on access that circumstances permit.
3. An FMI should monitor compliance with its participation requirements on an ongoing basis and have clearly defined and publicly disclosed procedures for facilitating the suspension and orderly exit of a participant that breaches, or no longer meets, the participation requirements.

### **Principle 19: Tiered participation arrangements**

An FMI should identify, monitor, and manage the material risks to the FMI arising from tiered participation arrangements.

#### **Key considerations**

1. An FMI should ensure that its rules, procedures, and agreements allow it to gather basic information about indirect participation in order to identify, monitor, and manage any material risks to the FMI arising from such tiered participation arrangements.
2. An FMI should identify material dependencies between direct and indirect participants that might affect the FMI.
3. An FMI should identify indirect participants responsible for a significant proportion of transactions processed by the FMI and indirect participants whose transaction volumes or values are large relative to the capacity of the direct participants through which they access the FMI in order to manage the risks arising from these transactions.
4. An FMI should regularly review risks arising from tiered participation arrangements and should take mitigating action when appropriate.

### **Principle 20: FMI links**

An FMI that establishes a link with one or more FMIs should identify, monitor, and manage link-related risks.

#### **Key considerations**

1. Before entering into a link arrangement and on an ongoing basis once the link is established, an FMI should identify, monitor, and manage all potential sources of risk arising from the link arrangement. Link arrangements should be designed such that each FMI is able to observe the other principles in this report.

2. *A link should have a well-founded legal basis, in all relevant jurisdictions, that supports its design and provides adequate protection to the FMIs involved in the link.*
3. *Linked CSDs should measure, monitor, and manage the credit and liquidity risks arising from each other. Any credit extensions between CSDs should be covered fully with high-quality collateral and be subject to limits.*
4. *Provisional transfers of securities between linked CSDs should be prohibited or, at a minimum, the retransfer of provisionally transferred securities should be prohibited prior to the transfer becoming final.*
5. *An investor CSD should only establish a link with an issuer CSD if the arrangement provides a high level of protection for the rights of the investor CSD's participants.*
6. *An investor CSD that uses an intermediary to operate a link with an issuer CSD should measure, monitor, and manage the additional risks (including custody, credit, legal, and operational risks) arising from the use of the intermediary.*
7. *Before entering into a link with another CCP, a CCP should identify and manage the potential spill-over effects from the default of the linked CCP. If a link has three or more CCPs, each CCP should identify, assess, and manage the risks of the collective link arrangement.*
8. *Each CCP in a CCP link arrangement should be able to cover, at least on a daily basis, its current and potential future exposures to the linked CCP and its participants, if any, fully with a high degree of confidence without reducing the CCP's ability to fulfil its obligations to its own participants at any time.*
9. *A TR should carefully assess the additional operational risks related to its links to ensure the scalability and reliability of IT and related resources.*

## **Efficiency**

### **Principle 21: Efficiency and effectiveness**

An FMI should be efficient and effective in meeting the requirements of its participants and the markets it serves.

#### **Key considerations**

1. *An FMI should be designed to meet the needs of its participants and the markets it serves, in particular, with regard to choice of a clearing and settlement arrangement; operating structure; scope of products cleared, settled, or recorded; and use of technology and procedures.*
2. *An FMI should have clearly defined goals and objectives that are measurable and achievable, such as in the areas of minimum service levels, risk-management expectations, and business priorities.*
3. *An FMI should have established mechanisms for the regular review of its efficiency and effectiveness.*

### **Principle 22: Communication procedures and standards**

An FMI should use, or at a minimum accommodate, relevant internationally accepted communication procedures and standards in order to facilitate efficient payment, clearing, settlement, and recording.

#### **Key consideration**

1. *An FMI should use, or at a minimum accommodate, internationally accepted communication procedures and standards.*

## **Transparency**

### **Principle 23: Disclosure of rules, key procedures, and market data**

An FMI should have clear and comprehensive rules and procedures and should provide sufficient information to enable participants to have an accurate understanding of the risks, fees, and other material costs they incur by participating in the FMI. All relevant rules and key procedures should be publicly disclosed.

#### **Key considerations**

- 1. An FMI should adopt clear and comprehensive rules and procedures that are fully disclosed to participants. Relevant rules and key procedures should also be publicly disclosed.*
- 2. An FMI should disclose clear descriptions of the system's design and operations, as well as the FMI's and participants' rights and obligations, so that participants can assess the risks they would incur by participating in the FMI.*
- 3. An FMI should provide all necessary and appropriate documentation and training to facilitate participants' understanding of the FMI's rules and procedures and the risks they face from participating in the FMI.*
- 4. An FMI should publicly disclose its fees at the level of individual services it offers as well as its policies on any available discounts. The FMI should provide clear descriptions of priced services for comparability purposes.*
- 5. An FMI should complete regularly and disclose publicly responses to the CPSS-IOSCO Disclosure framework for financial market infrastructures. An FMI also should, at a minimum, disclose basic data on transaction volumes and values.*

### **Principle 24: Disclosure of market data by trade repositories**

A TR should provide timely and accurate data to relevant authorities and the public in line with their respective needs.

#### **Key considerations**

- 1. A TR should provide data in line with regulatory and industry expectations to relevant authorities and the public, respectively, that is comprehensive and at a level of detail sufficient to enhance market transparency and support other public policy objectives.*
- 2. A TR should have effective processes and procedures to provide data to relevant authorities in a timely and appropriate manner to enable them to meet their respective regulatory mandates and legal responsibilities.*
- 3. A TR should have robust information systems that provide accurate current and historical data. Data should be provided in a timely manner and in a format that permits it to be easily analysed.*

**IT Audit, Security, Fraud prevention and Risk Management Framework**

A strong risk management system is necessary for the entities to meet the challenges of fraud and ensure customer protection. Entities are expected to put in place adequate information and data security infrastructure and systems for prevention and detection of frauds.

2. In order to ensure that the technology deployed to operate the payment system/s authorised is/are being operated in a safe, secure, sound and efficient manner, the authorised entities were advised in December 2009 to furnish their respective System Audit Report (SAR) conducted by a Certified Information Systems Auditor (CISA) registered with Information Systems Audit and Control Association (ISACA) or by a holder of a Diploma in Information System Audit (DISA) qualification of the Institute of Chartered Accountants of India (ICAI), on an annual basis within two months of close of their respective financial year. For entities which follow an April-March financial year, the system audit report should be submitted by 1<sup>st</sup> June of that year. Entities, which follow a calendar year annual closing, are advised to submit their system audit reports by 1<sup>st</sup> March of the following year. The scope of the System Audit should include evaluation of the hardware structure, operating systems and critical applications, security and controls in place, including access controls on key applications, disaster recovery plans, training of personnel managing systems and applications, documentation, etc. The audit should also comment on the deviations, if any, in the processes followed from the process flow submitted to the Reserve Bank while seeking authorisation.

3. The authorised payment system operators were advised in November 2010 to observe the following minimum practices:

- (i) A Strong password policy should be implemented with a history of password usage being maintained. Periodical change of passwords has to be strictly enforced with the system barring the user from reusing the three previous passwords.
- (ii) Regular review of the logs of the application system, database and the operating system should be done.
- (iii) A well-documented and tested Business Continuity and Disaster Recovery Plan should be put in place with proper logs.
- (iv) Network scanning / monitoring should be done on regular basis for the Denial of Service (DOS) attack as well as other intrusion and spy ware.

4. In addition, the Prepaid Payment Instrument Issuers were advised to put in place a strong risk management system and adequate information and data security infrastructure and systems to meet the challenges of fraud and ensure customer protection. They were also advised to adopt following best practices:



- i. All PPI Issuers shall put in place Board approved Information Security policy for the safety and security of the payment systems operated by them and implement security measures in accordance with this policy to mitigate identified risks. Entities shall review the security measures (a) on on-going basis but at least once a year, (b) after any security incident or breach, and (c) before / after a major change to their infrastructure or procedures.
- ii. Entities shall ensure that a framework is put in place to address the safety and security concerns, and for risk mitigation and fraud prevention. Entities shall put in place suitable mechanism to prevent, detect and restrict occurrence of fraudulent transactions. Also, a suitable internal and external escalation mechanisms in case of suspicious operations, besides alerting the customer in case of such transactions to be put in place. Entities may also put in place mechanism for velocity check on the number of transactions effected in an instrument.
- iii. Entities may put in place centralised database / management information system (MIS) to keep a track of the issuance/ usage of the payment instrument.
- iv. Where direct interface is provided to their authorised / designated agents, entities shall ensure that the compliance to regulatory requirements is strictly adhered to by these systems also.
- v. Authorised non-bank PPI Issuers have also been advised to submit the System Audit Report, including cyber security audit conducted by CERT-IN empanelled auditors, within two months of the close of their financial year to the CO / respective Regional Office of DPSS, RBI. The scope of the Audit shall include the following:
  - a. Security controls shall be tested both for effectiveness of control design (Test of Design – ToD) and control operating effectiveness (Test of Operating Effectiveness – ToE).
  - b. Technology deployed to ensure that the authorised payment system is being operated in a safe, secure, sound and efficient manner.
  - c. Evaluation of the hardware structure, operating systems and critical applications, security and controls in place, including access controls on key applications, disaster recovery plans, training of personnel managing systems and applications, documentation, etc.
  - d. Evaluating adequacy of Information Security Governance and processes of those which support payment systems.
  - e. Compliance as per security best practices, specifically the application security lifecycle and patch / vulnerability and change management aspects for the authorised system and adherence to the process flow approved by RBI.
  - f. Comment on the deviations, if any, in the processes followed from the process flow submitted to RBI while seeking authorisation.

- vi. All entities shall, at the minimum, put in place following framework:
  - a. Application Life Cycle Security: The source code audits shall be conducted by professionally competent personnel / service providers or have assurance from application providers / OEMs that the application is free from embedded malicious / fraudulent code.
  - b. Security Operations Centre (SOC): Integration of system level (server), application level logs of applications with SOC for centralised and co-ordinated monitoring and management of security related incidents.
  - c. Anti-Phishing: Entities shall subscribe to anti-phishing / anti-rouge app services from external service providers for identifying and taking down phishing websites / rouge applications in the wake of increase of rogue apps / phishing attacks.
  - d. Risk-based Transaction Monitoring: Risk-based transaction monitoring or surveillance process shall be implemented as part of fraud risk management system.
  - e. Vendor Risk Management: (i) Entities shall enter into an agreement with the service provider that amongst others provides for right of audit / inspection by the regulators of the country; (ii) RBI shall have access to all information resources (online / in person) that are consumed by entity, to be made accessible to RBI officials when sought, though the infrastructure / enabling resources may not physically be located in the premises of entity; (iii) Entities shall adhere to the relevant legal and regulatory requirements relating to geographical location of infrastructure and movement of data out of borders; (iv) Entities shall review the security processes and controls being followed by service providers regularly; (v) Service agreements of authorised entities with provider shall include a security clause on disclosing the security breaches if any happening specific to issuer's ICT infrastructure or process including not limited to software, application and data as part of Security incident Management standards, etc.
  - f. Disaster Recovery: Authorised entities shall consider having DR facility to achieve the Recovery Time Objective (RTO) / Recovery Point Objective (RPO) for the system to recover rapidly from cyber-attacks / other incidents and safely resume critical operations aligned with RTO while ensuring security of processes and data is protected.

5. Entities shall establish a mechanism for monitoring, handling and follow-up of cyber security incidents and cyber security breaches. The same shall be reported immediately to DPSS, RBI, Central Office, Mumbai. It shall also be reported to CERT-IN as per the details notified by CERT-IN.

**System Audit of Authorised Payment System Operators under Payment and Settlement Systems (PSS) Act, 2007 – Review of Scope and Coverage<sup>32</sup>**

1. Authorised entities shall furnish their respective System Audit Report (SAR) conducted by CERT-IN empanelled auditors or a Certified Information Systems Auditor (CISA) registered with Information Systems Audit and Control Association (ISACA) or by a holder of a Diploma in Information System Audit (DISA) qualification of the Institute of Chartered Accountants of India (ICAI), on an annual basis within two months of close of their respective financial year. For entities which follow an April-March financial year, the system audit report should be submitted by 1<sup>st</sup> June of that year. Entities, which follow a calendar year annual closing, are advised to submit their system audit reports by 1<sup>st</sup> March of the following year.
2. There should not be any conflict of interest for auditor, i.e. the firm conducting system audit or any of its sister concerns should not have been engaged in providing any type of service/s to the audited entity during the last two financial years.
3. The scope of system audit must include the items indicated below. Auditors need to comment on each item, indicating any observation (or the lack of it). Controls need to be tested for both Design (Test of Design – ToD) and Operating Effectiveness (Test of Operating Effectiveness – ToE).
  - (i) Information Security Governance – Assessment of the top management’s role in overseeing the development, implementation and maintenance of the organization’s information security management. It should include the following amongst others:
    - (a) Policies related to information security;
    - (b) Defined roles and responsibilities of various governance structure;
    - (c) Identification and assessment of threats and vulnerabilities;
    - (d) Management reviews of information security practices;
    - (e) Additional checks based on the risk perception or threats as they emerge;
    - (f) Key Risk Indicators (KRIs) by the entity as part of self-assessment.
  - (ii) Access Control – Assessment of the access control mechanism in place to restrict and filter access to the IT assets of the organisation. It should include the following amongst others:
    - (a) Granting access on a “need-to-have” and “need-to-know” basis;
    - (b) Periodic user access reviews & revocation of access;
    - (c) Privileged User Access Management;
    - (d) Controlled access to vendors and service providers;

---











<sup>32</sup> Implemented vide letter DPSS.CO.OD.No. 1325/06.11.001/2019-20 dated January 10, 2020.







- (e) Maintaining audit trail for system activities.
- (iii) Hardware Management – Assessment of controls with regard to hardware asset management from acquisition through disposal. Validation of effectiveness of controls on secure use of removable media.
- (iv) Network Security – Assessment of the countermeasures in place to protect the network from malicious attacks and minimise or eliminate the possibility of any losses being incurred by the entity as a result of the network being compromised.
- (v) Data Security - Assessment of the security measures implemented across the information life cycle starting from collection/ creation of data to storage, access, transmission and its eventual archival and/or deletion.
- (vi) Physical and Environmental Security – Assessment of the physical and environmental security controls in place to protect assets from internal and external threats.
- (vii) Human Resource Security – Assessment of the controls pertaining to human factors to prevent threats such as data leakage, data theft and misuse of data. It should include the following amongst others:
  - (a) Recruitment (background checks, roles and responsibilities);
  - (b) Information security training and user awareness;
  - (c) Termination (removal of access to data and systems).
- (viii) Business Continuity Management – Assessment of the disaster recovery capabilities of the audited entity and regular BCP drills. Controls should be designed so as to enable the entity to recover rapidly from any disrupting event and safely resume critical operations aligned with recovery time and recovery point objectives while ensuring security of processes and data is protected.
- (ix) System Scalability – Assessment of controls relating to scalability of systems from a growth perspective and Turn Around Time (TAT) of transaction processing.
- (x) IT Project Management – Assessment of controls in place for developing or acquiring new systems focusing on project risk. Examine whether systems are based on sound design principles which have built in security functionality such as Secure Software Development Life Cycle (S-SDLC) and are able to withstand malicious attacks by design and ensure that no security weaknesses have been introduced during the build process.
- (xi) Vendor / Third Party Risk Management – Assessment of controls in place to ensure that outsourcing related risks are managed through adequate oversight measures that should include the following amongst others:
  - (a) Service level agreement (it should mandatorily include right of audit / inspection by the home country regulators);
  - (b) Assessment of the security controls during on-boarding or off-boarding

- (c) Implementation of baseline cyber security controls by the service provider;
  - (d) Responsibility of service providers to get their systems audited to ensure error-free operation;
  - (e) Mandatory disclosure of any security incident specific to the entity's systems or processes.
- (xii) Incident Management – Assessment of the entity's response mechanism in the event of a security incident. Examine the organisation's capability to identify the incident, contain the damage, investigate the incident, effectively respond and restore normal operations as quickly as possible with the least possible impact. Also, verify the effectiveness of controls around determination and elimination of the root cause to prevent the occurrence of repeated incidents.
  - (xiii) Change Management – Assessment of controls in place for ensuring that changes are applied appropriately and do not compromise the information security of the organisation.
  - (xiv) Patch Management – Assessment of the mechanism in place to consistently monitor and configure systems and applications against known vulnerabilities in operating systems and other software.
  - (xv) Log Management – Assessment of the security controls around generation, transmission, access, analysis, storage, archiving and ultimate disposal of log data.
  - (xvi) Secure Mail and Messaging systems – Assessment of controls in place to ensure that the entity's inbound and outbound traffic in the form of mail, messages or any other media are secure.
  - (xvii) Mobile and/or other Input / Output Device Management Policy – Assessment of security controls with regard to portable devices (e.g. smartphones, laptops etc.) having access to sensitive data.
  - (xviii) Security Testing and Source Code Review – Assessment of the adequacy of system performance under stress-load scenarios, security controls including vulnerability assessment, penetration testing, configuration review and source code review.
  - (xix) Online Systems Security – Assessment of controls in place to ensure security of payment information processing systems and Application Programming Interfaces (APIs) provided to internal/ external applications.
  - (xx) Mobile Online Services (applicable for entities offering services through mobile applications) – Assessment of the controls in place to protect mobile applications and provided by the entity to its customers from malicious attacks.
4. The auditors need to check open observations and compliance noted in the previous system audit so as to ensure sustained compliance.








5. Deviations, if any, in the processes followed by the entity from the process flow submitted to RBI while seeking authorisation should be mentioned by the auditor.
6. The SAR and compliance status must be placed before the Board of the entity. For each open observation, specific time-bound (maximum 3 months) corrective action must be taken and reported to RBI. It is imperative that timelines of compliance should be given adequate importance. SAR observations shall be closed only after receiving closure acceptance from the auditor.

**Format of Data / Returns / Information / Reports**

<b>Entity</b>	<b>Reports</b>	<b>Template</b>
ALL	Data / Information as prescribed in policy / letter / direction / circular or my any means	
ALL	System Audit Report	
ALL	Financial Statements Report	
All	Annual Return on changes in Board of directors, shareholding, Memorandum or Articles of Association (MOA / AOA)	 Annual Return Changes in BoD sha
All	Annual Statement on income and expenditure	 Annual Statement Income and Exp (3).c
All	Annual Statement on staff strength	 Annual Statement Staff Strength.docx
Banks (having ATMs and issued Cards)	ATM and Card Statistics	 Card Statistics - ORFS Format.xlsx   Card Statistics - Interim data Format.   Card Statistics - XBRL Format.XLSX
Banks and WLAOs (having ATMs)	Deployment of ATMs	 Deployment of ATMs- Format.xlsx   Sectorial Deployment of ATM.XLSX
Banks (having ATMs)	Quarterly data on ATM failed customer complaints	 DPSS01_ATM Failed Complaints.xlsx   ATM Failed customer complaints_XBRL.XLSX

Entity	Reports	Template
Banks (having ATMs)	Quarterly data on ATM Transactions approved, Transactions declined due to Business reasons/ Technical decline	 DPSS09_ATM_Transaction_Decline.xlsx
CCIL	Operations Review Report	
CCIL	IT System Review Report	
CCIL	Segment-wise Defaults	
CCIL	<i>Return on staff strength, income and expenditure</i>	
CCIL	Return on change in Board of Directors, 5% holding, MOA / AOA	
CCIL	Report on Forex Participation & Settlement Statistics	
CCIL	Certificate on segregation of collateral	
CCIL	Investment Policy	
FMI	PFMI Disclosure Template – Self Assessment	
Cross-border Money Transfer (in-bound only) Operators	Monthly Data on State-wise & Region-wise Remittance Destinations	 DPSS04_MTSS_Business.xlsx
Cross-border Money Transfer (in-bound only) Operators	Quarterly Certificate from the bankers with regard to the dealings of the firm in respect of the facilities availed	 Quarterly certificate from the bankers.doc
Cross-border Money Transfer (in-bound only) Operators	Quarterly Statement regarding disputes between participants or between participants and the system provider	Y
NPCI	<i>NFS - Summary sheet and Bank-wise approved transaction break-up</i>	Y
NPCI	<i>IMPS - Summary and Bank-wise transaction details</i>	Y
NPCI	<i>CTS - Summary and implementation in all grids</i>	Y
NPCI	<i>Summary and bank-wise transaction details of all payment systems – NACH (Credit / debit / APBS), AePS, UPI (including USSD), BHIM Aadhaar Pay, NETC, BBPS, etc.</i>	Y
NPCI	<i>Implementation Status Update on payment system initiatives</i>	Y
PPI Issuers	Statistics on expired PPIs	 Expired PPI-Format.xlsx
PPI Issuers	Quarterly data on Customer Grievances	 DPSS05_PPI_grievances.xlsx
PPI Issuers	Certificate from the auditor on balance in Escrow Account	 Auditor Certificate on maintaining escrow ac



Entity	Reports	Template
PPI Issuers	Monthly data on PPI Statistics	 DPSS06 - PPI Statistics.xlsx   Interim PPI return format.xlsx
PPI Issuers	Fraud Monitoring	 Fraud Format.xlsx
WLAOs	Monthly data on WLA Statistics	 WLA STATISTICS FORMAT.xlsx
TReDS Operators	Statistics on transactions	 TReDS Returns format.xlsx
Retail	Self-Assessment Template	Y
Banks and non-bank PPI Issuers	Payment Fraud Reporting (daily basis)	 FUNCTIONAL TEMPLATE - FINAL.doc   TECHNICAL RECORD FORMAT.doc

## General applicability of principles to specific type of FMIs

Principle	PSs	CSDs	SSSs	CCPs	TRs
1. Legal basis	•	•	•	•	•
2. Governance	•	•	•	•	•
3. Framework for the comprehensive management of risks	•	•	•	•	•
4. Credit risk	•		•	•	
5. Collateral	•		•	•	
6. Margin				•	
7. Liquidity risk	•		•	•	
8. Settlement finality	•		•	•	
9. Money settlements	•		•	•	
10. Physical deliveries		•	•	•	
11. Central Securities Depositories		•			
12. Exchange-of-value settlement systems	•		•	•	
13. Participant Default Rules and Procedures	•	•	•	•	
14. Segregation and Portability				•	
15. General business risk	•	•	•	•	•
16. Custody and Investment Risks	•	•	•	•	
17. Operational risk	•	•	•	•	•
18. Access and participation requirements	•	•	•	•	•
19. Tiered participation arrangements	•	•	•	•	•
20. FMI Links		•	•	•	•
21. Efficiency and effectiveness	•	•	•	•	•
22. Communication procedures and standards	•	•	•	•	•

23. Disclosure of rules, key procedures, and market data	•	•	•	•	•
24. Disclosure of market data by Trade Repositories					•

**Applicability of PFMI to Important Retail Payment Systems (IRPS) and Other Retail Payment Systems (ORPS)**

<b>S. No.</b>	<b>Principles for FMIs</b>	<b>IRPS</b>	<b>ORPS</b>
1.	Principle 1: Legal basis	X	X
2.	Principle 2: Governance	X	X
3.	Principle 3: Framework for comprehensive management of risks	X	X
4.	Principle 4: Credit Risk		
5.	Principle 5: Collateral		
6.	Principle 7: Liquidity Risk		
7.	Principle 8: Settlement Finality	X	X
8.	Principle 9: Money settlements	X	
9.	Principle 13: Participant default rules and procedures	X	
10.	Principle 15: General Business Risk	X	
11.	Principle 16: Custody and investment risks		
12.	Principle 17: Operational risk	X	X
13.	Principle 18: Access and participation requirements	X	
14.	Principle 21: Efficiency and effectiveness	X	X
15.	Principle 22: Communication procedures and standards	X	
16.	Principle 23: Disclosure of rules, key procedures, and market data	X	X

## Table of Acronyms

AePS	Aadhaar enabled payment system
APBS	Aadhaar Payment Bridge System
DPSS	Department of Payment and Settlement Systems
BBPCU	Bharat Bill Payment Central Unit
BBPOU	Bharat Bill Payment Operating Unit
BBPS	Bharat Bill Payment System
CCIL	Clearing Corporation of India Limited
CO	Central Office
CPMI	Committee on Payments and Market Infrastructures
CPSS	Committee on Payment and Settlement Systems
CTS	Cheque Truncation System
FMI	Financial Market Infrastructure
IMPS	Immediate Payment Service
IOSCO	International Organisation of Securities Commissions
MTSS	Money Transfer Service Scheme
NCC	National Clearing Cell
NDS-OM	Negotiated Dealing System - Order Matching
NEFT	National Electronic Fund Transfer
NFS	National Financial Switch
NPCI	National Payments Corporation of India
PFMI	Principles for Financial Market Infrastructures
PPI	Pre-Paid Instruments
PSS	Payment and Settlement Systems
RO	Regional Office
RTGS	Real Time Gross Settlement
SFMS	Structured Financial Messaging System
SSS	Securities Settlement System
SWIPS	System Wide Important Payment System
TReDS	Trade Receivables Discounting System