NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Reserve Bank of India (RBI) - Master Direction on Prepaid Payment Instruments (PPI), 2021
Focal Document URL: https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12156
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-ind-rbi-ppi-2021.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
1	Introduction	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
1.1	N/A	In exercise of the powers conferred under Section 18 read with Section 10(2) of the Payment and Settlement Systems Act, 2007 (Act 51 of 2007), the Reserve Bank of India (RBI) being satisfied that it is necessary and expedient in the public interest to do so, hereby, issues these Directions.	Functional	No Relationship	N/A	N/A	N/A	0		
1.2	Short title and commencement	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
1.2.a	N/A	These Directions shall be called the Reserve Bank of India Master Directions on Prepaid Payment Instruments, 2021 (MD-PPIs, 2021); and	Functional	No Relationship	N/A	N/A	N/A	0		
1.2.b	N/A	These Directions shall come into effect from the date they are placed on RBI website. However, in respect of instructions already issued, they shall be effective as per the respective timelines prescribed.	Functional	No Relationship	N/A	N/A	N/A	0		
1.3	N/A	Applicability: The provisions of MD-PPIs shall apply to all Prepaid Payment Instrument (PPI) Issuers and System Participants.	Functional	No Relationship	N/A	N/A	N/A	0		
1.4	Purpose	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
1.4.a	N/A	To provide a framework for authorisation, regulation and supervision of entities issuing and operating PPIs in the country;	Functional	No Relationship	N/A	N/A	N/A	0		
1.4.b	N/A	To foster competition and encourage innovation in this segment in a prudent manner while taking into account safety and security of systems and transactions along with customer protection and convenience; and	Functional	No Relationship	N/A	N/A	N/A	0		
1.4.c	N/A	To provide for harmonisation and interoperability of PPIs.	Functional	No Relationship	N/A	N/A	N/A	0		
1.5	N/A	Banks and non-bank entities issue PPIs in the country after obtaining necessary approval / authorisation from RBI under the Payment and Settlement Systems Act, 2007 (PSS Act). Taking into account the developments in the field and the progress made by PPI issuer, the existing instructions issued on the subject till date have been incorporated and are consolidated in these Master Directions (MD).	Functional	No Relationship	N/A	N/A	N/A	0		
1.6	N/A	The MD lays down the eligibility criteria and the conditions of use for Payment System Operators (PSOs) involved in the issuance and operation of PPIs in the country.	Functional	No Relationship	N/A	N/A	N/A	0		
1.7	N/A	No entity can set up and operate payment systems for PPIs without prior approval / authorisation of RBI.	Functional	No Relationship	N/A	N/A	N/A	0		
2	Definitions	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
2.1	N/A	Closed System PPIs: These PPIs are issued by an entity for facilitating the purchase of goods and services from that entity only and do not permit cash withdrawal. These instruments cannot be used for payment or settlement for third party services. The issuance or operation of such instruments is not classified as a payment system requiring approval / authorisation by RBI and are, therefore, not regulated or supervised by RBI.	Functional	No Relationship	N/A	N/A	N/A	0		
2.2	N/A	Entities / Entity: The term 'entities / entity' refer/s to banks / non-banks who have approval / authorisation from RBI to issue PPIs as well as those who are proposing to issue PPIs.	Functional	No Relationship	N/A	N/A	N/A	0		
2.3	N/A	Holder: Individuals / Organisations who obtain / purchase PPIs from the issuer and use them for purchase of goods and services, financial services, remittance facilities, etc.	Functional	No Relationship	N/A	N/A	N/A	0		
2.4	N/A	Issuer: Entities issuing PPIs to individuals / organisations.	Functional	No Relationship	N/A	N/A	N/A	0		
2.5	N/A	Limits: All limits in the value of instruments stated in this MD, indicate the maximum value of such instruments denominated in INR that shall be issued.	Functional	No Relationship	N/A	N/A	N/A	0		
2.6	N/A	Merchants: Establishments who have a specific contract to accept the PPIs of the PPI issuer (or contract through a payment aggregator / payment gateway) against the sale of goods and services, financial services, etc.	Functional	No Relationship	N/A	N/A	N/A	0		
2.7	N/A	Net-worth: Shall consist of 'paid up equity capital, preference shares which are compulsorily convertible into equity capital, free reserves, balance in share premium account and capital reserves representing surplus arising out of sale proceeds of assets but not reserves created by revaluation of assets' adjusted for 'accumulated loss balance, book value of intangible assets and deferred revenue expenditure, if any'. While compulsorily convertible preference shares reckoned for computation of net-worth can be either non-cumulative or cumulative, these shall be compulsorily convertible into equity shares and the shareholder agreements shall specifically prohibit any withdrawal of this preference share capital at any time.	Functional	No Relationship	N/A	N/A	N/A	0		
2.8	N/A	Prepaid Payment Instruments (PPIs): Instruments that facilitate purchase of goods and services, financial services, remittance facilities, etc., against the value stored therein. PPIs that require RBI approval / authorisation prior to issuance are classified under two types viz. (i) Small PPIs: Issued by banks and non-banks after obtaining minimum details of the PPI holder. They shall be used only for purchase of goods and services. Funds transfer or cash withdrawal from such PPIs shall not be permitted; and (ii) Full-KYC PPIs: Issued by banks and non-banks after completing Know Your Customer (KYC) of the PPI holder. These PPIs shall be used for purchase of goods and services, funds transfer or cash withdrawal.	Functional	No Relationship	N/A	N/A	N/A	0		
3	Eligibility requirements for issuance of PPIs by banks	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
3.1	N/A	Banks that comply with the eligibility criteria, including those stipulated by the respective regulatory department of RBI, shall be permitted to issue PPIs after obtaining approval from RBI. Banks, seeking approval from the RBI under the PSS Act, shall apply to the Department of Payment and Settlement Systems (DPSS), Central Office (CO), RBI, Mumbai along with a 'No Objection Certificate' from their regulatory department, within 30 days of obtaining such clearance.	Functional	No Relationship	N/A	N/A	N/A	0		
4	Capital and other eligibility requirements for issuance of PPIs by non-banks	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
4.1	N/A	Non-banks that comply with the eligibility criteria, including those stipulated by the respective regulatory department of RBI, shall be permitted to issue PPIs after obtaining authorisation from RBI. Non-banks, regulated by any of the financial sector regulators, seeking authorisation from the RBI under the PSS Act shall apply to the DPSS, CO, RBI, Mumbai along with a 'No Objection Certificate' from their respective regulator, within 30 days of obtaining such clearance.	Functional	No Relationship	N/A	N/A	N/A	0		
4.2	N/A	Non-bank entities applying for authorisation shall be a company incorporated in India and registered under the Companies Act, 1956 / 2013.	Functional	No Relationship	N/A	N/A	N/A	0		
4.3	N/A	Non-bank entities having Foreign Direct Investment (FDI) / Foreign Portfolio Investment (FPI) / Foreign Institutional Investment (FII) shall also meet the capital requirements as applicable under the extant Consolidated FDI policy guidelines of Government of India.	Functional	No Relationship	N/A	N/A	N/A	0		
4.4	N/A	The Memorandum of Association (MoA) of the non-bank entity shall cover the proposed activity of PPI issuance.	Functional	No Relationship	N/A	N/A	N/A	0		
4.5	N/A	All non-bank entities seeking authorisation from RBI under the PSS Act shall have a minimum positive net-worth of Rs.5 crore as per the latest audited balance sheet at the time of submitting the application. They shall submit a certificate in the enclosed format (Annex-2) from their Chartered Accountants (CA) to evidence compliance with the applicable net-worth requirement while submitting the application for authorisation. The application shall be processed by RBI based on this net-worth which shall be maintained at all times. Thereafter, by the end of the third financial year from the date of receiving final authorisation, they shall achieve a minimum positive net-worth of Rs.15 crore which shall be maintained at all times.	Functional	No Relationship	N/A	N/A	N/A	0		

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Reserve Bank of India (RBI) - Master Direction on Prepaid Payment Instruments (PPI), 2021**
Focal Document URL: https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12156
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-ind-rbi-ppi-2021.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
4.6	N/A	Non-bank PPI issuer (authorised till October 11, 2017) shall comply with the minimum positive net-worth requirement of Rs.15 crore for the financial position as on September 30, 2021 (provisional balance sheet). This shall be reported to RBI, along with CA certificate in the enclosed format (Annex-2) and provisional balance sheet, by October 31, 2021 failing which they may not be permitted to carry out this business. Thereafter, the minimum positive net-worth of Rs.15 crore shall be maintained at all times. Till September 30, 2021, the existing PPI issuer shall continue to maintain the capital requirements applicable to it at the time of its authorisation.	Functional	No Relationship	N/A	N/A	N/A	0		
4.7	N/A	Authorised non-bank PPI issuer shall submit a net-worth certificate every year in the enclosed format (Annex-2) to evidence compliance with the applicable net-worth requirement as per the audited balance sheet of the financial year within six months of completion of that financial year.	Functional	No Relationship	N/A	N/A	N/A	0		
4.8	N/A	Newly incorporated non-bank entities that may not have an audited statement of financial accounts shall submit a certificate in the enclosed format (Annex-2) from their CA regarding the current net-worth along with provisional balance sheet.	Functional	No Relationship	N/A	N/A	N/A	0		
4.9	N/A	Non-bank PPI issuer shall also be guided by DPSS circular CO.DPSS.AUTH.No.S190/02.27.005/2021-22 dated June 14, 2021 (as amended from time to time) on Investment in entities from FATF non-compliant jurisdictions.	Functional	No Relationship	N/A	N/A	N/A	0		
5	Authorisation process for non-banks	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
5.1	N/A	A non-bank entity desirous of issuing PPIs shall apply for authorisation in Form A (available on RBI website www.rbi.org.in) as prescribed under Regulation 3(2) of the Payment and Settlement Systems Regulations, 2008 (PSS Regulations) along with the requisite application fees.	Functional	No Relationship	N/A	N/A	N/A	0		
5.2	N/A	The application shall initially be screened by RBI to ensure prima facie eligibility of the applicant. The directors of the applicant entity shall submit a declaration in the enclosed format (Annex-3). RBI shall also check 'fit and proper' status of the applicant. Application of entities not meeting the eligibility criteria, or those that are incomplete / not in the prescribed form with all details, shall be returned without refund of the application fees.	Functional	No Relationship	N/A	N/A	N/A	0		
5.3	N/A	In addition to the compliance with the applicable guidelines, RBI shall also apply checks, inter-alia, on certain essential aspects like customer service and efficiency, technical and other related requirements, safety and security aspects, etc., before granting in-principle approval to the applicants.	Functional	No Relationship	N/A	N/A	N/A	0		
5.4	N/A	Subject to meeting the eligibility criteria and other conditions, the RBI shall issue an 'in-principle' approval, which shall be valid for a period of six months. The entity shall submit a satisfactory System Audit Report (SAR) to RBI within these six months, failing which the in-principle approval shall lapse automatically. SAR shall be accompanied by a certificate from the CA regarding compliance with the minimum positive net-worth. An entity can seek one-time extension for a maximum period of six months for submission of SAR by making a request in writing, to DPSS, CO, RBI, Mumbai, in advance with valid reasons. The RBI reserves the right to decline such a request for extension.	Functional	Intersects With	Independent Assessors	CPL-08	Mechanisms exist to utilize independent assessors to evaluate security, compliance and resilience at planned intervals or when the Technology Asset, Application and/or Service (TAAS) undergoes significant changes.	3		CPL-03.1
5.4	N/A	Subject to meeting the eligibility criteria and other conditions, the RBI shall issue an 'in-principle' approval, which shall be valid for a period of six months. The entity shall submit a satisfactory System Audit Report (SAR) to RBI within these six months, failing which the in-principle approval shall lapse automatically. SAR shall be accompanied by a certificate from the CA regarding compliance with the minimum positive net-worth. An entity can seek one-time extension for a maximum period of six months for submission of SAR by making a request in writing, to DPSS, CO, RBI, Mumbai, in advance with valid reasons. The RBI reserves the right to decline such a request for extension.	Functional	Intersects With	Security Assessment Report (SAR)	IAO-13	Mechanisms exist to produce a Security Assessment Report (SAR) at the conclusion of a security assessment to certify the results of the assessment and assist with any remediation actions.	5		IAO-02.4
5.5	N/A	Subsequent to the issue of the in-principle approval, if any adverse features regarding the entity / promoters / group or business practices, etc., come to notice, RBI may impose additional conditions and if warranted, the in-principle approval may be withdrawn.	Functional	No Relationship	N/A	N/A	N/A	0		
5.6	N/A	Pursuant to receipt of satisfactory SAR, net-worth certificate and due diligence, RBI shall grant final Certificate of Authorisation (CoA). Entities granted final authorisation shall commence business within six months from the grant of CoA failing which the authorisation shall lapse automatically. An entity can seek one-time extension for a maximum period of six months by making a request in writing, to DPSS, CO, RBI, Mumbai, in advance with valid reasons. RBI reserves the right to decline such a request for extension.	Functional	No Relationship	N/A	N/A	N/A	0		
5.7	N/A	CoA shall be granted to all PSOs on a perpetual basis subject to the conditions stated in DPSS circular DPSS.CO.AD.No.724/02.27.005/2020-21 dated December 4, 2020 (as amended from time to time).	Functional	No Relationship	N/A	N/A	N/A	0		
5.8	N/A	Entities seeking renewal of authorisation shall apply in writing to DPSS, CO, RBI, Mumbai at least three months before the expiry of validity of CoA, failing which RBI reserves the right to decline the request for renewal.	Functional	No Relationship	N/A	N/A	N/A	0		
5.9	N/A	Any proposed major change, such as changes in product features / process, structure or operation of the payment system, etc., shall be communicated with complete details to the Chief General Manager (CGM), DPSS, CO, RBI, Mumbai. RBI shall endeavour to reply within 15 working days after receipt of above communication at DPSS, CO, RBI, Mumbai.	Functional	Intersects With	Stakeholder Notification of Changes	CHG-08	Mechanisms exist to ensure stakeholders are made aware of and understand the impact of proposed changes.	5		CHG-05
5.1	N/A	Any takeover or acquisition of control or change in management of a non-bank entity shall be communicated to the CGM, DPSS, CO, RBI, Mumbai within 15 days with complete details, including 'Declaration and Undertaking' (Annex-3) by each of the new directors, if any. RBI shall examine the 'fit and proper' status of the management and, if required, may place suitable restrictions on such changes.	Functional	Intersects With	Mergers, Acquisitions & Divestitures (MA&D)	GOV-19	Mechanisms exist to define standardized practices to conduct Mergers, Acquisitions and Divestiture (MA&D) activities.	3		GOV-20
5.11	Cooling Period	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
5.11.a	N/A	PPI issuer whose CoA is revoked or not-renewed for any reason; or	Functional	No Relationship	N/A	N/A	N/A	0		
5.11.b	N/A	CoA is voluntarily surrendered for any reason; or	Functional	No Relationship	N/A	N/A	N/A	0		
5.11.c	N/A	Application for authorisation has been rejected by RBI; or	Functional	No Relationship	N/A	N/A	N/A	0		
5.11.d	N/A	New entities that are set-up by promoters involved in any of the above categories; definition of promoters for the purpose, shall be as defined in the Companies Act, 2013. In respect of entities whose application for authorisation is returned for any reason by RBI, condition of Cooling Period shall be invoked after giving the entity an additional opportunity to submit the application. During the Cooling Period, entities shall be prohibited from submission of applications for operating any payment system under the PSS Act.	Functional	No Relationship	N/A	N/A	N/A	0		
6	Safeguards against money laundering provisions	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
6.1	N/A	The Know Your Customer (KYC) / Anti-Money Laundering (AML) / Combating Financing of Terrorism (CFT) guidelines issued by the Department of Regulation (DoR), RBI, in 'Master Direction - Know Your Customer Direction, 2016', as updated from time to time, shall apply mutatis mutandis to all the entities issuing PPIs.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-02	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	3		CPL-01
6.1	N/A	The Know Your Customer (KYC) / Anti-Money Laundering (AML) / Combating Financing of Terrorism (CFT) guidelines issued by the Department of Regulation (DoR), RBI, in 'Master Direction - Know Your Customer Direction, 2016', as updated from time to time, shall apply mutatis mutandis to all the entities issuing PPIs.	Functional	Intersects With	Identity Proofing (Identity Verification)	IAC-05	Mechanisms exist to verify the identity of a user before issuing authenticators or modifying access permissions.	5		IAC-28
6.2	N/A	Provisions of Prevention of Money Laundering Act, 2002 (PMLA) and Rules framed thereunder, as amended from time to time, shall be applicable to PPI issuer.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-02	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	3		CPL-01
6.3	N/A	PPI issuer shall maintain a log of all the transactions undertaken using the PPIs for at least ten years. This data shall be made available for scrutiny to RBI or any other agency / agencies as may be advised by RBI. The PPI issuer shall also file Suspicious Transaction Reports (STRs) to Financial Intelligence Unit-India (FIU-IND).	Functional	Intersects With	Media & Data Retention	DCH-27	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	5		DCH-18

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Reserve Bank of India (RBI) - Master Direction on Prepaid Payment Instruments (PPI), 2021**
Focal Document URL: https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12156
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-ind-rbi-ppi-2021.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
6.3	N/A	PPI issuer shall maintain a log of all the transactions undertaken using the PPIs for at least ten years. This data shall be made available for scrutiny to RBI or any other agency / agencies as may be advised by RBI. The PPI issuer shall also file Suspicious Transaction Reports (STRs) to Financial Intelligence Unit-India (FIU-IND).	Functional	Intersects With	Event Log & Security-Relevant Telemetry Retention	MON-13	Mechanisms exist to retain event logs and security-relevant telemetry for a time period consistent with records retention requirements to provide support for after-the-fact investigations of security incidents and to meet statutory, regulatory and contractual retention requirements.	5		MON-10
7	Issuance, loading and reloading of PPIs	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
7.1	N/A	All entities approved / authorised to issue PPIs by RBI are permitted to issue reloadable or non-reloadable PPIs depending upon the permissible type / category of PPIs as laid down in paragraph 9 and 10 of these Directions.	Functional	No Relationship	N/A	N/A	N/A	0		
7.2	N/A	PPI issuer shall have a clear laid down policy, duly approved by its Board, for issuance of various types / categories of PPIs and all activities related thereto.	Functional	No Relationship	N/A	N/A	N/A	0		
7.3	N/A	PPI issuer shall ensure that the name of the company which has received approval / authorisation for issuance and operating of PPIs, is prominently displayed along with the PPI brand name in all instances. PPI issuer shall also keep RBI informed regarding the brand names employed / to be employed for its products.	Functional	No Relationship	N/A	N/A	N/A	0		
7.4	N/A	PPI issuer shall not pay any interest on PPI balances.	Functional	No Relationship	N/A	N/A	N/A	0		
7.5	N/A	PPIs shall be permitted to be loaded / reloaded by cash, debit to a bank account, credit and debit cards, PPIs (as permitted from time to time) and other payment instruments issued by regulated entities in India and shall be in INR only.	Functional	No Relationship	N/A	N/A	N/A	0		
7.6	N/A	Cash loading to PPIs shall be limited to Rs.50,000/- per month subject to overall limit of the PPI.	Functional	No Relationship	N/A	N/A	N/A	0		
7.7	N/A	PPIs may be issued as cards, wallets, and in any such form / instrument which can be used to access the PPI and to use the amount therein. No PPI shall be issued in the form of paper vouchers.	Functional	No Relationship	N/A	N/A	N/A	0		
7.8	N/A	Banks shall be permitted to load / reload PPIs through BCs subject to compliance with BC guidelines issued by RBI.	Functional	No Relationship	N/A	N/A	N/A	0		
7.9	PPIs loaded / reloaded through authorised outlets or designated agents	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
7.9.a	N/A	Having a Board approved policy clearly laying down the framework for engaging agents;	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-04	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	3		GOV-02
7.9.a	N/A	Having a Board approved policy clearly laying down the framework for engaging agents;	Functional	Intersects With	Third-Party Management	TPM-02	Mechanisms exist to facilitate the implementation of third-party management controls.	5		TPM-01
7.9.b	N/A	Carrying out proper due diligence of the persons appointed as authorised / designated agents;	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	5		TPM-04.1
7.9.c	N/A	Being responsible as the principal for all acts of omission or commission of their authorised / designated agents, including safety and security aspects;	Functional	Intersects With	Third-Party Services	TPM-12	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-04
7.9.d	N/A	Preserving records and confidentiality of customer information in their possession as well as in the possession of their authorised / designated agents;	Functional	Intersects With	Sensitive / Regulated Data Protection	DCH-07	Mechanisms exist to protect sensitive and/or regulated data wherever it is processed and/or stored.	5		DCH-01.2
7.9.d	N/A	Preserving records and confidentiality of customer information in their possession as well as in the possession of their authorised / designated agents;	Functional	Intersects With	Data Privacy Requirements for Contractors & Service Providers	PRI-14	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5		PRI-07.1
7.9.e	N/A	Monitoring regularly the activities of their authorised / designated agents and carrying out review of the performance of various agents engaged by them at least once in a year; and	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	8		TPM-08
7.9.f	N/A	Ensuring adherence to applicable laws of the land, including KYC / AML / CFT norms as indicated in paragraph 6.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-02	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	3		CPL-01
7.9.f	N/A	Ensuring adherence to applicable laws of the land, including KYC / AML / CFT norms as indicated in paragraph 6.	Functional	Intersects With	Contract Flow-Down Requirements	TPM-14.1	Mechanisms exist to ensure applicable security, compliance and resilience requirements are included in contracts that flow-down to applicable subcontractors and suppliers.	5		TPM-05.2
7.1	N/A	PPI issuer shall ensure that there is no co-mingling of funds originating from any other activity that they may be undertaking such as BC of bank/s, intermediary for payment aggregation, payment gateway, etc.	Functional	No Relationship	N/A	N/A	N/A	0		
7.11	PPIs under co-branding arrangements	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
7.11.a	N/A	The co-branding arrangement shall be as per the Board approved policy of the PPI issuer. The policy shall specifically address issues pertaining to the various risks associated with such an arrangement including reputation risk and the PPI issuer shall put in place suitable risk mitigation measures. The policy shall also clearly lay down the roles, responsibilities and obligations of each co-branding partner.	Functional	Intersects With	Third-Party Management	TPM-02	Mechanisms exist to facilitate the implementation of third-party management controls.	5		TPM-01
7.11.a	N/A	The co-branding arrangement shall be as per the Board approved policy of the PPI issuer. The policy shall specifically address issues pertaining to the various risks associated with such an arrangement including reputation risk and the PPI issuer shall put in place suitable risk mitigation measures. The policy shall also clearly lay down the roles, responsibilities and obligations of each co-branding partner.	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-04	Mechanisms exist to: (1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and (2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.	3		TPM-03
7.11.b	N/A	The co-branding partner shall be a company incorporated in India under the Companies Act, 1956 / 2013. The co-branding partner can also be a Government department / ministry. In case the co-branding partner is a bank, the same shall be licensed by RBI.	Functional	No Relationship	N/A	N/A	N/A	0		
7.11.c	N/A	PPI issuer shall carry out due diligence of the co-branding partner to protect themselves against the reputation risk. In case of tie up with a financial entity, it may ensure that approval of co-branding partner's regulator for entering into such arrangement is available.	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	5		TPM-04.1
7.11.d	N/A	Instructions / Guidelines on KYC / AML / CFT (as indicated in paragraph 6) shall be adhered to in respect of all PPIs issued under the co-branding arrangement.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-02	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	3		CPL-01
7.11.d	N/A	Instructions / Guidelines on KYC / AML / CFT (as indicated in paragraph 6) shall be adhered to in respect of all PPIs issued under the co-branding arrangement.	Functional	Intersects With	Identity Proofing (Identity Verification)	IAC-05	Mechanisms exist to verify the identity of a user before issuing authenticators or modifying access permissions.	5		IAC-28
7.11.e	N/A	PPI issuer shall be liable for all acts of the co-branding partner. The issuer shall also be responsible for all customer-related aspects of the PPIs.	Functional	Intersects With	Third-Party Services	TPM-12	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-04
7.11.f	N/A	PPI issuer shall be permitted to co-brand such instruments with the name / logo of the company for whose customers / beneficiaries such co-branded instruments are to be issued.	Functional	No Relationship	N/A	N/A	N/A	0		
7.11.g	N/A	The name of PPI issuer shall be prominently visible on the payment instrument.	Functional	No Relationship	N/A	N/A	N/A	0		
7.11.h	N/A	In case of non-bank PPI issuer, where co-branding arrangement takes place between two non-bank PPI issuers, the agreement shall clearly indicate which partner is the PPI issuer.	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	3		TPM-05
7.11.i	N/A	Non-bank PPI issuer desirous of issuing co-branded PPIs shall seek one time approval from DPSS, CO, RBI, Mumbai.	Functional	No Relationship	N/A	N/A	N/A	0		
7.11.j	N/A	In case of co-branding arrangements between a bank and non-bank entity, the bank shall be the PPI issuer. Role of the non-bank entity shall be limited to marketing / distribution of the PPIs or providing access to the PPI holder to services that are offered.	Functional	No Relationship	N/A	N/A	N/A	0		
7.11.k	N/A	In case of co-branding arrangement between two banks, the PPI issuing bank shall ensure compliance to above instructions.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-02	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	3		CPL-01
7.11.l	N/A	Bank PPI issuer shall also adhere to instructions contained in circular DBR.No.FSD.BC.18/24.01.009/2015-16 dated July 1, 2015, as amended from time to time.	Functional	No Relationship	N/A	N/A	N/A	0		

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Reserve Bank of India (RBI) - Master Direction on Prepaid Payment Instruments (PPI), 2021
Focal Document URL: https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12156
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-ind-rbi-ppi-2021.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
7.12	N/A	There shall be no remittance without compliance to KYC requirements. The PPI issuer, including its agent/s, shall not create new PPIs every time for facilitating cash-based remittances to other PPIs / bank accounts. PPIs created for previous remittance by the same person shall be used.	Functional	No Relationship	N/A	N/A	N/A	0		
8	Cross-border transactions	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
8	N/A	The use of INR denominated PPIs for cross-border transactions shall not be permitted except as under:	Functional	No Relationship	N/A	N/A	N/A	0		
8.1	PPIs for cross-border outward transactions	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
8.1.a	N/A	Full-KYC PPIs issued by banks having AD-I licence shall be permitted to be used in cross-border outward transactions (only for permissible current account transactions under FEMA viz. purchase of goods and services), subject to adherence to extant norms governing such transactions;	Functional	No Relationship	N/A	N/A	N/A	0		
8.1.b	N/A	PPIs shall not be used for any cross-border outward fund transfer and / or for making payments under Liberalised Remittances Scheme (LRS). Prefunding of online merchant's account shall not be permitted using such Rupee denominated PPIs;	Functional	No Relationship	N/A	N/A	N/A	0		
8.1.c	N/A	PPI issuer shall enable the facility of cross-border outward transactions only on explicit request of the PPI holders and shall apply a per transaction limit not exceeding Rs.10,000/-, while per month limit shall not exceed Rs.50,000/- for such cross-border transactions;	Functional	No Relationship	N/A	N/A	N/A	0		
8.1.d	N/A	In case such PPIs are issued in card form, it shall be ensured that they are EMV Chip and PIN compliant; and	Functional	No Relationship	N/A	N/A	N/A	0		
8.1.e	N/A	Such PPIs may not be issued as a separate category of PPI.	Functional	No Relationship	N/A	N/A	N/A	0		
8.2	PPIs for credit towards cross-border inward remittances	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
8.2.a	N/A	Bank and non-bank PPI issuer, appointed as Indian agent of authorised overseas principals, shall be permitted to issue full-KYC PPIs to beneficiaries of inward remittances under the Money Transfer Services Scheme (MTSS) of RBI;	Functional	No Relationship	N/A	N/A	N/A	0		
8.2.b	N/A	Such PPIs shall be issued in adherence to extant norms under the MTSS Guidelines issued by Foreign Exchange Department (FED), RBI;	Functional	No Relationship	N/A	N/A	N/A	0		
8.2.c	N/A	Amounts only upto Rs.50,000/- from individual inward MTSS remittances shall be permitted to be loaded / reloaded in full-KYC PPIs issued to beneficiaries. Amount in excess of Rs.50,000/- shall be paid by credit to a bank account of the beneficiary. Full details of the transactions shall be maintained on record for scrutiny;	Functional	No Relationship	N/A	N/A	N/A	0		
8.2.d	N/A	Roles and responsibilities of PPI issuer shall be distinct from roles and responsibilities as Indian Agents under MTSS; and	Functional	No Relationship	N/A	N/A	N/A	0		
8.2.e	N/A	Such PPIs may not be issued as a separate category of PPI.	Functional	No Relationship	N/A	N/A	N/A	0		
8.3	N/A	Foreign Exchange PPIs: Entities authorised under FEMA to issue foreign exchange denominated PPIs shall be outside the purview of this MD.	Functional	No Relationship	N/A	N/A	N/A	0		
9	Types of PPIs	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
9.1	Small PPIs (or Minimum-detail PPIs)	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
9.1.i	PPIs upto Rs.10,000/- (with cash loading facility)	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
9.1.i.a	N/A	a) Bank and non-banks shall be permitted to issue such PPIs after obtaining minimum details of the PPI holder;	Functional	No Relationship	N/A	N/A	N/A	0		
9.1.i.b	N/A	b) Minimum details shall necessarily include a mobile number verified with One Time Password (OTP) and a self-declaration of name and unique identity / identification number of any 'mandatory document' or 'Officially Valid Document (OVD)' or any such document with any name listed for this purpose in the Master Direction on KYC, as amended from time to time;	Functional	No Relationship	N/A	N/A	N/A	0		
9.1.i.c	N/A	c) Such PPIs shall be reloadable in nature;	Functional	No Relationship	N/A	N/A	N/A	0		
9.1.i.d	N/A	d) Amount loaded in such PPIs during any month shall not exceed Rs.10,000/- and the total amount loaded during the financial year shall not exceed Rs.1,20,000/-;	Functional	No Relationship	N/A	N/A	N/A	0		
9.1.i.e	N/A	e) Amount outstanding at any point of time in such PPIs shall not exceed Rs.10,000/-;	Functional	No Relationship	N/A	N/A	N/A	0		
9.1.i.f	N/A	f) Total amount debited from such PPIs during any month shall not exceed Rs.10,000/;	Functional	No Relationship	N/A	N/A	N/A	0		
9.1.i.g	N/A	g) These PPIs shall be used only for purchase of goods and services. Cash withdrawal or funds transfer from such PPIs shall not be permitted;	Functional	No Relationship	N/A	N/A	N/A	0		
9.1.i.h	N/A	h) There shall be no separate limit for purchase of goods and services using PPIs; PPI issuer may decide limit for these purposes within the overall PPI limit;	Functional	No Relationship	N/A	N/A	N/A	0		
9.1.i.i	N/A	i) These PPIs shall be converted into full-KYC PPIs (as defined in paragraph 9.2) within a period of 24 months from the date of issue of the PPI, failing which no further credit shall be allowed in such PPIs. However, the PPI holder shall be allowed to use the balance available in the PPI;	Functional	No Relationship	N/A	N/A	N/A	0		
9.1.i.j	N/A	j) This category of PPI shall not be issued to the same user in future using the same mobile number and same minimum details;	Functional	No Relationship	N/A	N/A	N/A	0		
9.1.i.k	N/A	k) PPI issuer shall give an option to close the PPI at any time. The closure proceeds can be transferred 'back to source account' (payment source from where the PPI was loaded). Alternatively, the closure proceeds can be transferred to a bank account after complying with KYC requirements of PPI holder; and	Functional	No Relationship	N/A	N/A	N/A	0		
9.1.i.l	N/A	l) The features of such PPIs shall be clearly communicated to the PPI holder by SMS / e-mail / any other means at the time of issuance of the PPI / before the first loading of funds.	Functional	No Relationship	N/A	N/A	N/A	0		
9.1.ii	PPIs upto Rs.10,000/- (with no cash loading facility)	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
9.1.ii.a	N/A	a) Banks and non-banks shall be permitted to issue such PPIs after obtaining minimum details of the PPI holder;	Functional	No Relationship	N/A	N/A	N/A	0		
9.1.ii.b	N/A	b) Minimum details shall necessarily include a mobile number verified with OTP and a self-declaration of name and unique identity / identification number of any 'mandatory document' or OVD or any such document with any name listed for this purpose in the Master Direction on KYC, as amended from time to time;	Functional	No Relationship	N/A	N/A	N/A	0		
9.1.ii.c	N/A	c) Such PPIs shall be reloadable in nature. Loading / Reloading shall be from a bank account / credit card / full-KYC PPI;	Functional	No Relationship	N/A	N/A	N/A	0		
9.1.ii.d	N/A	d) The amount loaded in such PPIs during any month shall not exceed Rs.10,000 and the total amount loaded during the financial year shall not exceed Rs.1,20,000;	Functional	No Relationship	N/A	N/A	N/A	0		
9.1.ii.e	N/A	e) The amount outstanding at any point of time in such PPIs shall not exceed Rs.10,000;	Functional	No Relationship	N/A	N/A	N/A	0		
9.1.ii.f	N/A	f) These PPIs shall be used only for purchase of goods and services. Cash withdrawal or funds transfer from such PPIs shall not be permitted;	Functional	No Relationship	N/A	N/A	N/A	0		
9.1.ii.g	N/A	g) PPI issuer shall give an option to close the PPI at any time. The closure proceeds can be transferred 'back to source account' (payment source from where the PPI was loaded). Alternatively, the closure proceeds can be transferred to a bank account after complying with KYC requirements of PPI holder;	Functional	No Relationship	N/A	N/A	N/A	0		
9.1.ii.h	N/A	h) The features of such PPIs shall be clearly communicated to the PPI holder by SMS / e-mail / any other means at the time of issuance of the PPI / before the first loading of funds; and	Functional	No Relationship	N/A	N/A	N/A	0		
9.1.ii.i	N/A	i) The PPIs of paragraph 9.1(i) existing as on December 24, 2019 can be converted to this type of PPI, if desired by the PPI holder.	Functional	No Relationship	N/A	N/A	N/A	0		
9.2	Full-KYC PPIs	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
9.2.a	N/A	Banks and non-banks shall be permitted to issue such PPIs after completing KYC of the PPI holder (as indicated in paragraph 6);	Functional	No Relationship	N/A	N/A	N/A	0		
9.2.b	N/A	The Video-based Customer Identification Process (V-CIP), as detailed in Department of Regulation's Master Direction on KYC dated February 25, 2016 (as amended from time to time), can be used to open full-KYC PPIs as well as to convert Small PPIs of paragraph 9.1 into full-KYC PPIs;	Functional	No Relationship	N/A	N/A	N/A	0		
9.2.c	N/A	Such PPIs shall be reloadable in nature;	Functional	No Relationship	N/A	N/A	N/A	0		

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Reserve Bank of India (RBI) - Master Direction on Prepaid Payment Instruments (PPI), 2021**
Focal Document URL: https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12156
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-ind-rbi-ppi-2021.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
9.2.d	N/A	The amount outstanding shall not exceed Rs.2,00,000/- at any point of time;	Functional	No Relationship	N/A	N/A	N/A	0		
9.2.e	N/A	The funds can be transferred 'back to source account' (payment source from where the PPI was loaded) or 'own bank account of the PPI holder' (duly verified by the PPI issuer). However, PPI issuer shall set the limits considering the risk profile of the PPI holders, other operational risks, etc.;	Functional	No Relationship	N/A	N/A	N/A	0		
9.2.f	N/A	PPI issuer shall provide the facility of 'pre-registered beneficiaries' whereby the PPI holder can register the beneficiaries by providing their bank account details, details of PPIs issued by same issuer (or different issuer as and when permitted), etc.;	Functional	No Relationship	N/A	N/A	N/A	0		
9.2.g	N/A	In case of such pre-registered beneficiaries, the funds transfer limit shall not exceed Rs.2,00,000/- per month per beneficiary. PPI issuer shall set the limits within this ceiling considering the risk profile of the PPI holders, other operational risks, etc.;	Functional	No Relationship	N/A	N/A	N/A	0		
9.2.h	N/A	Funds transfer limits for all other cases shall be restricted to Rs.10,000/- per month;	Functional	No Relationship	N/A	N/A	N/A	0		
9.2.i	N/A	Funds transfer from such PPIs shall also be permitted to other PPIs, debit cards and credit cards as per the limits given above;	Functional	No Relationship	N/A	N/A	N/A	0		
9.2.j	N/A	There is no separate limit on purchase of goods and services using PPIs and PPI issuer may decide limit for these purposes within the overall PPI limit;	Functional	No Relationship	N/A	N/A	N/A	0		
9.2.k	N/A	PPI issuer shall clearly indicate these limits to the PPI holders and provide necessary options to PPI holders to set their own fund transfer limits;	Functional	No Relationship	N/A	N/A	N/A	0		
9.2.l	N/A	PPI issuer shall also give an option to close the PPI and transfer the balance as per the applicable limits of this type of PPI. For this purpose, the issuer shall provide an option, including at the time of issuing the PPI, to the holder to provide details of pre-designated bank account or other PPIs of same issuer (or other issuer as and when permitted) to which the balance amount available in the PPI shall be transferred in the event of closure of PPI, expiry of validity period of such PPIs, etc.;	Functional	No Relationship	N/A	N/A	N/A	0		
9.2.m	N/A	In case of bank issued PPIs, cash withdrawal shall be permitted. However, cash withdrawal at PoS devices shall be subjected to a limit of Rs.2,000/- per transaction within an overall monthly limit of Rs.10,000/- across all locations (Tier 1 to 6 centres), subject to conditions stipulated in RBI circular DPSS.CO.PD.No.449/02.14.003/2015-16 dated August 27, 2015;	Functional	No Relationship	N/A	N/A	N/A	0		
9.2.n	N/A	In case of non-bank issued PPIs, cash withdrawal shall be permitted upto a maximum limit of Rs.2,000/- per transaction within an overall monthly limit of Rs.10,000/- per PPI across all channels (agents, ATMs, PoS devices, etc.); and	Functional	No Relationship	N/A	N/A	N/A	0		
9.2.o	N/A	Features of such PPIs shall be clearly communicated to the PPI holder by SMS / e-mail / any other means at the time of issuance of the PPI / before the first loading of funds.	Functional	Intersects With	Data Subject Communications	PRI-37	Mechanisms exist to craft disclosures and communications to data subjects in a manner that is concise, unambiguous and understandable by a reasonable person.	3		PRI-17
10	Specific categories of PPIs	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
10	N/A	Banks and non-banks shall not issue PPIs of any other category except as permitted under the following categories:	Functional	No Relationship	N/A	N/A	N/A	0		
10.1	Gift PPIs	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
10.1.a	N/A	Maximum value of each such prepaid gift instrument shall not exceed Rs.10,000/-;	Functional	No Relationship	N/A	N/A	N/A	0		
10.1.b	N/A	Such instrument shall not be reloadable;	Functional	No Relationship	N/A	N/A	N/A	0		
10.1.c	N/A	Cash-out or funds transfer shall not be permitted for such instrument. However, the funds may be transferred 'back to source account' (account from where Gift PPI was loaded) after receiving consent of the PPI holder;	Functional	No Relationship	N/A	N/A	N/A	0		
10.1.d	N/A	KYC (as indicated in paragraph 6) details of the purchaser of such instrument shall be maintained by the PPI issuer. Separate KYC shall not be required for customers who are issued such instrument against debit to their bank accounts and / or credit cards in India;	Functional	Intersects With	Media & Data Retention	DCH-27	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	3		DCH-18
10.1.d	N/A	KYC (as indicated in paragraph 6) details of the purchaser of such instrument shall be maintained by the PPI issuer. Separate KYC shall not be required for customers who are issued such instrument against debit to their bank accounts and / or credit cards in India;	Functional	Intersects With	Identity Proofing (Identity Verification)	IAC-05	Mechanisms exist to verify the identity of a user before issuing authenticators or modifying access permissions.	3		IAC-28
10.1.e	N/A	PPI issuer shall adopt a risk-based approach, duly approved by its Board, in deciding number of such instruments which can be issued to a customer, transaction limits, etc.;	Functional	Intersects With	Risk Assessment	RSK-13	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5		RSK-04
10.1.f	N/A	These PPIs shall be revalidated (including through issuance of new instrument) as and when requested by the PPI holder;	Functional	No Relationship	N/A	N/A	N/A	0		
10.1.g	N/A	Provisions of paragraph 13 on validity and redemption, as applicable, shall be adhered to; and	Functional	No Relationship	N/A	N/A	N/A	0		
10.1.h	N/A	Features of such PPIs shall be clearly communicated to the PPI holder by SMS / e-mail / any other means at the time of issuance of the PPI / before the first loading of funds.	Functional	Intersects With	Data Subject Communications	PRI-37	Mechanisms exist to craft disclosures and communications to data subjects in a manner that is concise, unambiguous and understandable by a reasonable person.	3		PRI-17
10.2	PPIs for Mass Transit Systems (PPI-MTS)	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
10.2.a	N/A	Banks / non-banks are permitted to issue such PPIs;	Functional	No Relationship	N/A	N/A	N/A	0		
10.2.b	N/A	Such PPIs shall contain the Automated Fare Collection application related to transit services, toll collection and parking;	Functional	No Relationship	N/A	N/A	N/A	0		
10.2.c	N/A	Such PPIs shall be enabled only for payments across various modes of public transport such as metro, buses, rail, & waterways, tolls and parking;	Functional	No Relationship	N/A	N/A	N/A	0		
10.2.d	N/A	These PPIs can be issued without KYC verification of the holders;	Functional	No Relationship	N/A	N/A	N/A	0		
10.2.e	N/A	These PPI can be reloadable in nature;	Functional	No Relationship	N/A	N/A	N/A	0		
10.2.f	N/A	The amount outstanding, in such PPIs shall not exceed Rs.3,000/- at any point of time;	Functional	No Relationship	N/A	N/A	N/A	0		
10.2.g	N/A	These PPIs can have perpetual validity, i.e., the provisions of validity and redemption given in Section 13 of this MD shall not apply to PPI-MTS; and	Functional	No Relationship	N/A	N/A	N/A	0		
10.2.h	N/A	Cash-withdrawal, refund or funds transfer shall not be permitted in such PPIs.	Functional	No Relationship	N/A	N/A	N/A	0		
10.3	PPIs to Foreign Nationals / Non-Resident Indians (NRIs) visiting India	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
10.3.a	N/A	Banks / Non-banks permitted to issue PPIs can issue INR denominated full-KYC PPIs to foreign nationals / NRIs visiting India (to start with, this facility will be extended to travellers from the G-20 countries, arriving at select international airports). Such PPIs can also be issued in co-branding arrangement with entities authorised to deal in Foreign Exchange under FEMA;	Functional	No Relationship	N/A	N/A	N/A	0		
10.3.b	N/A	The PPIs shall be issued after physical verification of Passport and Visa of the customers at the point of issuance. The PPI issuers shall ensure that such information and record thereof are maintained with them;	Functional	Intersects With	Media & Data Retention	DCH-27	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	3		DCH-18
10.3.b	N/A	The PPIs shall be issued after physical verification of Passport and Visa of the customers at the point of issuance. The PPI issuers shall ensure that such information and record thereof are maintained with them;	Functional	Intersects With	Identity Evidence	IAC-05.2	Mechanisms exist to require evidence of individual identification to be presented to the registration authority.	3		IAC-28.2
10.3.b	N/A	The PPIs shall be issued after physical verification of Passport and Visa of the customers at the point of issuance. The PPI issuers shall ensure that such information and record thereof are maintained with them;	Functional	Intersects With	In-Person Validation & Verification	IAC-05.4	Mechanisms exist to require that the validation and verification of identity evidence be conducted in person before a designated registration authority.	5		IAC-28.4
10.3.c	N/A	The PPIs can be issued in the form of wallets linked to UPI and can be used for merchant payments (P2M) only;	Functional	No Relationship	N/A	N/A	N/A	0		
10.3.d	N/A	Loading / Reloading of such PPIs shall be against receipt of foreign exchange by cash or through any payment instrument;	Functional	No Relationship	N/A	N/A	N/A	0		
10.3.e	N/A	The conversion to Indian Rupee shall be carried out only by entities authorised to deal in Foreign Exchange under FEMA;	Functional	No Relationship	N/A	N/A	N/A	0		
10.3.f	N/A	The amount outstanding at any point of time in such PPIs shall not exceed the limit applicable on full-KYC PPIs;	Functional	No Relationship	N/A	N/A	N/A	0		

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Reserve Bank of India (RBI) - Master Direction on Prepaid Payment Instruments (PPI), 2021**
Focal Document URL: https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12156
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-ind-rbi-ppi-2021.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
10.3.g	N/A	Provisions of paragraph 13 on validity and redemption, as applicable, shall be adhered to. The unutilised balances in such PPIs can be encashed in foreign currency or transferred 'back to source' (payment source from where the PPI was loaded), in compliance with foreign exchange regulations;	Functional	No Relationship	N/A	N/A	N/A	0		
11	Interoperability	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
11.1	N/A	Interoperability is the technical compatibility that enables a payment system to be used in conjunction with other payment systems.	Functional	No Relationship	N/A	N/A	N/A	0		
11.2	N/A	PPI issuer shall be guided by the technical specifications / standards / requirements for achieving interoperability through UPI and card networks as per the requirements of National Payments Corporation of India (NPCI) and the respective card networks. NPCI and card networks shall facilitate participation by PPI issuer in UPI and card networks.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-02	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5		CPL-01
11.3	N/A	PPI issuer shall have a Board approved policy for achieving PPI interoperability.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-04	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	3		GOV-02
11.4	Requirements for achieving interoperability: Common to wallets and cards	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
11.4.1	N/A	Where PPIs are issued in the form of wallets, interoperability across PPIs shall be enabled through UPI.	Functional	No Relationship	N/A	N/A	N/A	0		
11.4.2	N/A	Where PPIs are issued in the form of cards (physical or virtual), the cards shall be affiliated to the authorised card networks.	Functional	No Relationship	N/A	N/A	N/A	0		
11.4.3	N/A	PPI-MTS shall remain exempted from interoperability, while Gift PPI issuer (both banks and non-banks) have the option to offer interoperability.	Functional	No Relationship	N/A	N/A	N/A	0		
11.4.4	N/A	The interoperability shall be facilitated to all KYC-compliant PPIs and entire acceptance infrastructure. It shall be mandatory for PPI issuer to give the holders of full-KYC PPIs (KYC-compliant PPIs) interoperability through authorised card networks (for PPIs in the form of cards) and UPI (for PPIs in the form of wallets).	Functional	No Relationship	N/A	N/A	N/A	0		
11.4.5	N/A	Interoperability shall be mandatory on the acceptance side as well. QR codes in all modes shall be interoperable by March 31, 2022 vide RBI circular DPSS.CO.PD.No.497/02.14.003/2020-21 dated October 22, 2020. For other modes of acceptance, as also for issuance, the interoperability shall be achieved by March 31, 2022. Once a non-bank PPI entity becomes interoperable (on both issuing and acquiring side simultaneously), the entire merchant base, including those acquired by the banks, shall be accessible through the card networks and UPI.	Functional	No Relationship	N/A	N/A	N/A	0		
11.4.6	N/A	Technical requirements: PPI issuer shall adhere to all the requirements of card networks / UPI including membership type and criteria, merchant on-boarding, adherence to various standards, rules and regulations applicable to the specific payment system such as technical requirements, certifications and audit requirements, governance, etc.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-02	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5		CPL-01
11.4.7	Reconciliation, customer protection and grievance redressal	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
11.4.7.a	N/A	PPI issuer shall ensure adherence to all guidelines / requirements of card networks / UPI in terms of reconciliation of positions at daily / weekly / monthly or more frequent basis, as the case may be.	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	3		MON-16
11.4.7.b	N/A	PPI issuer shall adhere to all dispute resolution and customer grievance redressal mechanisms as prescribed by the card networks / NPCI.	Functional	Intersects With	Grievances	CPL-22	Mechanisms exist to govern the intake and analysis of grievances related to the organization's cybersecurity and/or data protection practices.	5		CPL-07
11.4.7.b	N/A	PPI issuer shall adhere to all dispute resolution and customer grievance redressal mechanisms as prescribed by the card networks / NPCI.	Functional	Intersects With	Grievance Response	CPL-22.1	Mechanisms exist to respond to legitimate grievances related to the organization's cybersecurity and/or data protection practices.	3		CPL-07.1
11.5	Requirements for achieving interoperability through card networks	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
11.5.1	N/A	Card networks are allowed to onboard PPI issuer to join their network. Non-bank PPI issuer is permitted to participate as member / associate member of authorised card networks.	Functional	No Relationship	N/A	N/A	N/A	0		
11.5.2	N/A	Settlement: For the purpose of settlement, a non-bank PPI issuer can participate directly or through a sponsor bank arrangement as the case may be. Non-bank PPI issuer shall adhere to the requirements of respective card network's settlement system.	Functional	No Relationship	N/A	N/A	N/A	0		
11.5.3	Safety and security	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
11.5.3.a	N/A	Banks and non-banks shall ensure that all new PPIs issued in the form of cards are EMV Chip and PIN compliant.	Functional	Intersects With	Secure Practices Alignment Justification	GOV-03.1	Mechanisms exist to align the organization's Security, Compliance & Resilience Program (SCRP) with one or more industry-recognized frameworks that: (1) Support external scrutiny; and (2) Provide defensible justification for secure practices.	3		GOV-01.4
11.5.3.a	N/A	Banks and non-banks shall ensure that all new PPIs issued in the form of cards are EMV Chip and PIN compliant.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-37	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.	5		IAC-06
11.5.3.b	N/A	Banks and non-banks shall ensure that all reissuance / renewal of PPIs in the form of cards are EMV Chip and PIN compliant.	Functional	Intersects With	Secure Practices Alignment Justification	GOV-03.1	Mechanisms exist to align the organization's Security, Compliance & Resilience Program (SCRP) with one or more industry-recognized frameworks that: (1) Support external scrutiny; and (2) Provide defensible justification for secure practices.	3		GOV-01.4
11.5.3.b	N/A	Banks and non-banks shall ensure that all reissuance / renewal of PPIs in the form of cards are EMV Chip and PIN compliant.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-37	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.	5		IAC-06
11.5.3.c	N/A	Gift PPIs may continue to be issued with or without EMV Chip and PIN enablement.	Functional	No Relationship	N/A	N/A	N/A	0		
11.6	Requirements for achieving interoperability through UPI	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
11.6.1	N/A	PPI issuer shall facilitate all basic / standard features of interoperability of UPI.	Functional	No Relationship	N/A	N/A	N/A	0		
11.6.2	N/A	PPI issuer shall act as Payment System Providers (PSP) in UPI. NPCI shall issue handle to the PPI issuer as per its policy / guidelines taking risk management aspects into consideration. Since *99# USSD is part of UPI, non-bank PPI issuer are also allowed to participate in the same.	Functional	No Relationship	N/A	N/A	N/A	0		
11.6.3	N/A	A PPI issuer shall enable holders of only its full-KYC PPIs to make UPI payments by linking its customer PPIs to its UPI handle. UPI transactions from PPI on the issuer's application shall be authenticated using the customer's existing PPI credentials. Such a transaction will, thus, be pre-approved before it reaches the UPI system. A PPI issuer, in its capacity as a PSP, shall not on-board customers of any bank or any other PPI issuer.	Functional	Intersects With	Strong Customer Authentication (SCA)	WEB-07	Mechanisms exist to implement Strong Customer Authentication (SCA) for consumers to reasonably prove their identity.	5		WEB-06
11.6.4	N/A	A PPI issuer may also facilitate discovery of its full-KYC PPIs on third-party UPI mobile applications, who, in turn shall enable such PPIs to be linked to their PSP handle/s. Such UPI transactions, from PPIs using third party UPI applications, shall be authenticated using the UPI credentials.	Functional	Intersects With	Strong Customer Authentication (SCA)	WEB-07	Mechanisms exist to implement Strong Customer Authentication (SCA) for consumers to reasonably prove their identity.	3		WEB-06

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Reserve Bank of India (RBI) - Master Direction on Prepaid Payment Instruments (PPI), 2021
Focal Document URL: https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12156
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-ind-rbi-ppi-2021.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
11.6.5	N/A	Settlement: For the purposes of settlement, a non-bank PPI issuer shall participate through a sponsor bank. Non-bank PPI issuer shall adhere to the requirements of sponsor bank arrangement in UPI as also meet all requirements of NPCI in this regard.	Functional	No Relationship	N/A	N/A	N/A	0		
12	Deployment of money collected	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
12.1	N/A	To ensure timely settlement, the non-bank PPI issuer shall invest the money collected against issuance of PPIs only as provided herein.	Functional	No Relationship	N/A	N/A	N/A	0		
12.2	N/A	For the schemes operated by banks, the outstanding balance shall be part of the 'net demand and time liabilities' for the purpose of maintenance of reserve requirements. This position will be computed on the basis of balances appearing in the books of the bank as on the date of reporting.	Functional	No Relationship	N/A	N/A	N/A	0		
12.3	Escrow account maintenance by non-bank PPI issuer	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
12.3.0	N/A	12.3 Non-bank PPI issuer is required to maintain the outstanding balance in an escrow account with any scheduled commercial bank. An additional escrow account may be maintained with a different scheduled commercial bank at the discretion of the PPI issuer. For the purpose of maintenance of escrow account, payment system operated by the non-bank PPI issuer for issuance of PPIs shall be deemed to be 'designated payment system' under Section 23A of the PSS Act. Non-bank PPI issuer that is member of Centralised Payment Systems operated by RBI shall maintain a Current Account with RBI. Maintenance of escrow balance shall be subject to the following conditions:	Functional	No Relationship	N/A	N/A	N/A	0		
12.3.i	N/A	(i) In case there is a need to shift the escrow account from one bank to another, the same shall be effected in a time-bound manner without unduly impacting the payment cycle to merchants. Migration shall be completed in the minimum possible time with prior intimation to RBI.	Functional	No Relationship	N/A	N/A	N/A	0		
12.3.ii	N/A	(ii) The balance in the escrow account shall not, at the end of the day, be lower than the value of outstanding PPIs and payments due to merchants. While as far as possible PPI issuer shall ensure immediate credit of funds to escrow on issue, load / reload of PPIs to the PPI holders, under no circumstance such credit to escrow account shall be later than the close of business day (the day on which the PPI has been issued, loaded / reloaded). This shall be monitored by the non-bank PPI issuer on daily basis and any shortfall shall be immediately reported to the respective Regional Office of DPSS, RBI.	Functional	No Relationship	N/A	N/A	N/A	0		
12.3.iii	Permitted debits and credits in escrow account	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
12.3.iii.a	N/A	Credits a. Payments received towards issue, load / reload of PPIs, including at agent locations;	Functional	No Relationship	N/A	N/A	N/A	0		
12.3.iii.b	N/A	Credits b. Refunds received for failed / disputed / returned / cancelled transactions; and	Functional	No Relationship	N/A	N/A	N/A	0		
12.3.iii.c	N/A	Credits c. Payments received from sponsor bank towards settlement obligations from participation in interoperable payment systems, as permitted by RBI from time to time;	Functional	No Relationship	N/A	N/A	N/A	0		
12.3.iii.d	N/A	Credits d. Transfers from Current Account maintained with RBI.	Functional	No Relationship	N/A	N/A	N/A	0		
12.3.iii.e	N/A	Debits e. Payments to various merchants / service providers towards reimbursement of claims received from them;	Functional	No Relationship	N/A	N/A	N/A	0		
12.3.iii.f	N/A	Debits f. Payment to sponsor bank for processing funds transfer instructions received from PPI holders as permitted by RBI from time to time;	Functional	No Relationship	N/A	N/A	N/A	0		
12.3.iii.g	N/A	Debits g. Payments made to sponsor bank towards settlement obligations from participation in interoperable payment systems, as permitted by RBI from time to time;	Functional	No Relationship	N/A	N/A	N/A	0		
12.3.iii.h	N/A	Debits h. Transfers to Current Account maintained with RBI.	Functional	No Relationship	N/A	N/A	N/A	0		
12.3.iii.i	N/A	Debits i. Payment towards applicable Government taxes (received along with PPI sale / reload amount from the buyers);	Functional	No Relationship	N/A	N/A	N/A	0		
12.3.iii.j	N/A	Debits j. Refunds towards cancellation of transactions in a PPI in case of PPIs loaded / reloaded erroneously or through fraudulent means (on establishment of erroneous transfer / fraud). The funds shall be credited back to the same source from where these were received. These funds are not to be forfeited till the disposal of the case;	Functional	No Relationship	N/A	N/A	N/A	0		
12.3.iii.k	N/A	Debits k. Any other payment due to the PPI issuer in the normal course of operating PPI business (for instance, service charges, forfeited amount, commissions, etc.); Note: (1) The payment towards service charges, commission and forfeited amount shall be at pre-determined rates / frequency. Such transfers shall only be effected to a designated bank account of the PPI issuer as indicated in the agreement with the bank where escrow account is maintained. (2) All these provisions shall be part of Service Level Agreement that will be signed between the PPI issuer and the bank maintaining escrow account.	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	3		TPM-05
12.3.iii.l	N/A	Debits l. Any other debit as directed by the regulator / courts / law enforcement agencies.	Functional	No Relationship	N/A	N/A	N/A	0		
12.3.iv	N/A	(iv) The agreement between the PPI issuer and the bank maintaining escrow account shall include a clause enabling the bank to use the money in the escrow account only for purposes mentioned in these Directions.	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	3		TPM-05
12.3.v	N/A	(v) Settlement of funds with merchants shall not be co-mingled with other business, if any, handled by the PPI issuer.	Functional	No Relationship	N/A	N/A	N/A	0		
12.3.vi	N/A	(vi) No interest shall be payable by the bank on such balances, except as indicated in paragraph 12.4 below.	Functional	No Relationship	N/A	N/A	N/A	0		
12.3.vii	N/A	(vii) PPI issuer shall be required to submit the list of merchants acquired by them to the bank and update the same from time to time. The bank shall be required to ensure that payments are made only to eligible merchants / purposes. There shall be an exclusive clause in the agreement signed between the PPI issuer and bank maintaining escrow account towards usage of balance in escrow account only for the purposes mentioned above.	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	3		TPM-05
12.3.viii	N/A	(viii) With the growing acceptance of PPIs in e-commerce payments, including in digital market places, the payment mechanism is often facilitated using the services of payment aggregators / payment gateways. In such a scenario, the emerging practice observed is that the PPI issuer has the necessary agreements with the digital market place and / or the payment aggregator / gateway rather than the individual merchants who are accepting the PPIs as a payment instrument. In view of the above, PPI issuer shall obtain an undertaking from the digital market place and / or payment aggregator / gateway that the payments made by the issuer are used for onward payments to the respective merchants. Such an undertaking shall be submitted by the PPI issuer to the bank maintaining the escrow account.	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	3		TPM-05
12.3.ix	N/A	(ix) A certificate (format enclosed Annex-5) signed by the auditor(s), shall be submitted by the authorised entities to the respective Regional Office of DPSS, RBI on a quarterly basis certifying that the entity has been maintaining adequate balance(s) in the escrow account(s) to cover outstanding value of PPIs issued and payments due to merchants. In case, an additional escrow account is being maintained, it shall be ensured that balances in both accounts are considered for the above certification. This shall also be indicated in the certificate. The same auditor shall be employed to audit both escrow accounts. The certificate shall be submitted within a fortnight from the end of quarter to which it pertains. Entities shall also submit an annual certificate (Annex-5), signed by the auditor, coinciding with accounting year of the entity to RBI.	Functional	No Relationship	N/A	N/A	N/A	0		
12.3.x	N/A	(x) Adequate records indicating the daily position of the value of instruments outstanding and payments due to merchants vis-a-vis balances maintained with the banks in the escrow accounts shall be made available for scrutiny to RBI or the bank where the account is maintained on demand.	Functional	No Relationship	N/A	N/A	N/A	0		
12.4	Core portion interest bearing account (exception to 12.3(vi))	N/A	Functional	No Relationship	N/A	N/A	N/A	0		

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Reserve Bank of India (RBI) - Master Direction on Prepaid Payment Instruments (PPI), 2021**
Focal Document URL: https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12156
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-ind-rbi-ppi-2021.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
12.4.0	N/A	12.4 As an exception to paragraph 12.3(vi), the non-bank PPI issuer can enter into an agreement with the bank maintaining the escrow account, to transfer 'core portion' of the amount, in the escrow account to a separate account on which interest is payable, subject to the following: Note - 'Core Portion' shall be computed as: Step 1: Compute lowest daily outstanding balance (LB) on a fortnightly (FN) basis, for one year (26 fortnights) from the preceding month. Step 2: Calculate the average of the lowest fortnightly outstanding balances [(LB1 of FN1 + LB2 of FN2 + ... + LB26 of FN26) divided by 26]. Step 3: The average balance so computed represents the 'Core Portion' eligible to earn interest.	Functional	No Relationship	N/A	N/A	N/A	0		
12.4.a	N/A	The bank shall satisfy itself that the amount deposited represents the 'core portion' after due verification of necessary documents.	Functional	No Relationship	N/A	N/A	N/A	0		
12.4.b	N/A	The amount shall be linked to the escrow account, i.e. the amounts held in the interest bearing account shall be available to the bank, to meet payment requirements of the entity, in case of any shortfall in the escrow account.	Functional	No Relationship	N/A	N/A	N/A	0		
12.4.c	N/A	This facility is permissible to entities who have been in business for at least one year (26 fortnights) and whose accounts have been duly audited for the full accounting year.	Functional	No Relationship	N/A	N/A	N/A	0		
12.4.d	N/A	No loan is permissible against such deposits. Banks shall not issue any deposit receipts or mark any lien on the amount held in such form of deposits.	Functional	No Relationship	N/A	N/A	N/A	0		
12.4.e	N/A	Core portion shall be calculated separately for each of the escrow accounts and will remain linked to the respective escrow account. Escrow balance and core portion maintained shall be clearly disclosed in the auditors' certificates submitted to RBI on quarterly and annual basis.	Functional	No Relationship	N/A	N/A	N/A	0		
13	Validity and redemption	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
13.1	N/A	All PPIs issued in the country shall have a minimum validity period of one year from the date of last loading / reloading in the PPI. PPIs can be issued with a longer validity as well. In case of PPIs issued in the form of card (with validity period mentioned on the card), the customer shall have the option to seek replacement of the card.	Functional	No Relationship	N/A	N/A	N/A	0		
13.2	N/A	PPI issuer shall caution the PPI holder at reasonable intervals, during the 45 days' period prior to expiry of the validity period of the PPI. The caution advice shall be sent by SMS / e-mail / any other means in the language preferred by the holder indicated at the time of issuance of the PPI.	Functional	No Relationship	N/A	N/A	N/A	0		
13.3	N/A	Non-bank PPI issuer cannot transfer the outstanding balance to its Profit & Loss account for at least three years from the expiry date of PPI. In case the PPI holder approaches the PPI issuer for refund of such amount, at any time after the expiry date of PPI, then the same shall be paid to the PPI holder in a bank account.	Functional	No Relationship	N/A	N/A	N/A	0		
13.4	N/A	Bank issuing PPIs shall be guided by the instructions on Depositor Education and Awareness Fund (DEA Fund) issued by Department of Banking Regulation, RBI, vide, circular DBOD.No.DEAF Cell.BC.101/30.01.002/2013-14 dated March 21, 2014, as amended from time to time.	Functional	No Relationship	N/A	N/A	N/A	0		
13.5	N/A	The PPI Issuer shall clearly indicate the expiry period of the PPI to the customer at the time of issuance of PPIs. Such information shall be clearly enunciated in the terms and conditions of sale of PPI. Where applicable, it shall also be clearly outlined on the website / mobile application of the PPI issuer.	Functional	No Relationship	N/A	N/A	N/A	0		
13.6	N/A	PPIs with no financial transaction for a consecutive period of one year shall be made inactive by the PPI issuer after sending a notice to the PPI holder/s. These can be reactivated only after validation and applicable due diligence. These PPIs shall be reported to RBI separately.	Functional	No Relationship	N/A	N/A	N/A	0		
13.7	N/A	The holders of PPIs shall be permitted to redeem the outstanding balance in the PPI, if for any reason the scheme is being wound-up or is directed by RBI to be discontinued.	Functional	No Relationship	N/A	N/A	N/A	0		
14	Transactions limits	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
14.1	N/A	The PPI holder is allowed to use the PPI for purposes within the overall PPI limit applicable. PPI issuer shall decide on limits considering the risk perception of the holders as per its risk management policy.	Functional	No Relationship	N/A	N/A	N/A	0		
14.2	N/A	All financial limits indicated against each type / category of the PPI shall be strictly adhered to.	Functional	No Relationship	N/A	N/A	N/A	0		
14.3	Handling refunds	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
14.3.a	N/A	Refunds in case of failed / returned / rejected / cancelled transactions shall be applied to the respective PPI immediately, to the extent that payment was made initially by debit to the PPI, even if such application of funds results in exceeding the limits prescribed for that type / category of PPI.	Functional	No Relationship	N/A	N/A	N/A	0		
14.3.b	N/A	However, refunds in case of failed / returned / rejected / cancelled transactions using any other payment instrument shall not be credited to PPI.	Functional	No Relationship	N/A	N/A	N/A	0		
14.3.c	N/A	PPI issuer shall be required to maintain complete details of such returns / refunds, etc., and be in readiness to provide them as and when called for.	Functional	No Relationship	N/A	N/A	N/A	0		
14.3.d	N/A	Further, PPIs issuer shall also put in place necessary systems that enable them to monitor frequent instances of refunds taking in place in specific PPIs and be in a position to substantiate with proof for audit / scrutiny purposes.	Functional	No Relationship	N/A	N/A	N/A	0		
15	Security, fraud prevention and risk management framework	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
15.1	N/A	A strong risk management system is necessary for PPI issuer to meet challenges of fraud and ensure customer protection. PPI issuer shall put in place adequate information and data security infrastructure and systems for prevention and detection of frauds.	Functional	No Relationship	N/A	N/A	N/A	0		
15.2	N/A	PPI issuer shall put in place Board approved Information Security policy for the safety and security of the payment systems operated by it, and implement security measures in accordance with this policy to mitigate identified risks. The PPI issuer shall review 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 its infrastructure or procedures.	Functional	No Relationship	N/A	N/A	N/A	0		
15.3	Security and fraud prevention framework	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
15.3.a	N/A	In case of wallets, PPI issuer shall ensure that if same login is provided for the PPI and other services offered by them, the same shall be clearly informed to the customer by SMS or email or any other means. The option to logout from the website / mobile account shall be provided prominently.	Functional	Intersects With	User-Initiated Logouts / Message Displays	CFG-04.6	Mechanisms exist to provide a logout capability and display an explicit logout message to users indicating the reliable termination of the session.	5		IAC-25.1
15.3.b	N/A	Issuer shall put in place appropriate mechanisms to restrict multiple invalid attempts to login / access to the PPI, inactivity, timeout features, etc.	Functional	Intersects With	Account Lockout	CFG-04.1	Mechanisms exist to enforce a limit for consecutive invalid login attempts by a user during an organization-defined time period and automatically locks the account when the maximum number of unsuccessful attempts is exceeded.	5		IAC-22
15.3.c	N/A	Issuer shall introduce a system where all wallet transactions involving debit to the wallet, including cash withdrawal transactions, shall be permitted only by validation through a Two Factor Authentication (2FA).	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-37	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.	5		IAC-06
15.3.d	N/A	The Additional Factor of Authentication (AFA) requirements for PPI Cards (physical or virtual) shall be same as required for debit cards.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-37	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.	3		IAC-06
15.3.e	N/A	2FA / AFA is not mandatory for PPIs issued under PPI-MTS and gift PPIs.	Functional	No Relationship	N/A	N/A	N/A	0		

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Reserve Bank of India (RBI) - Master Direction on Prepaid Payment Instruments (PPI), 2021**
Focal Document URL: https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12156
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-ind-rbi-ppi-2021.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
15.3.f	N/A	The transactions undertaken using PPIs through National Electronic Toll Collection (NETC) system can be performed as per the instructions given in DPSS circular DPSS.CO.PD.No.1227/02.31.001/2019-20 dated December 30, 2019, as amended from time to time.	Functional	No Relationship	N/A	N/A	N/A	0		
15.3.g	N/A	Processing of e-mandate for transactions undertaken using PPIs (cards and wallets) shall be performed, as per the instructions contained in DPSS circular DPSS.CO.PD.No.447/02.14.003/2019-20 dated August 21, 2019, as amended from time to time.	Functional	No Relationship	N/A	N/A	N/A	0		
15.3.h	N/A	Issuer shall provide customer induced options for fixing a cap on number of transactions and transaction value for different types of transactions / beneficiaries. Customers shall be allowed to change the caps, with additional authentication and validation.	Functional	Intersects With	Re-Authentication	IAC-43	Mechanisms exist to force users and devices to re-authenticate according to organization-defined circumstances that necessitate re-authentication.	3		IAC-14
15.3.i	N/A	Issuer shall put in place a limit on the number of beneficiaries that may be added in a day per PPI.	Functional	Intersects With	Unusual Transactions	MON-16.1	Mechanisms exist to define "normal business activities" to identify anomalous transaction activities that can reduce the opportunity for sending (outbound) and/or receiving (inbound) hostile and/or fraudulent actions.	5		DCH-25.1
15.3.j	N/A	Issuer shall introduce a system of alert when a beneficiary is added.	Functional	Intersects With	Automated Audit Actions	IAC-08.6	Automated mechanisms exist to audit account creation, modification, enabling, disabling and removal actions and notify organization-defined personnel or roles.	3		IAC-15.4
15.3.k	N/A	Issuer shall put in place suitable cooling period for funds transfer and cash withdrawal upon opening the PPI or loading / reloading of funds into the PPI or after adding a beneficiary so as to mitigate the fraudulent use of PPIs.	Functional	Intersects With	Unusual Transactions	MON-16.1	Mechanisms exist to define "normal business activities" to identify anomalous transaction activities that can reduce the opportunity for sending (outbound) and/or receiving (inbound) hostile and/or fraudulent actions.	3		DCH-25.1
15.3.l	N/A	Issuer shall put in place a mechanism to send alerts when transactions are done using the PPIs. In addition to the debit or credit amount intimation, the alert shall also indicate the balance available / remaining in the PPI after completion of the said transaction. For transactions undertaken in offline mode, as allowed from time to time, the transaction alert shall be sent as soon as the details of transaction are received by the PPI issuer. There is no compulsion to send separate alert for each transaction; however, details of each transaction shall be adequately conveyed as soon as such information reaches the PPI issuer.	Functional	Intersects With	Automated Incident Responder Alerting	MON-05.5	Mechanisms exist to automatically alert incident response personnel to inappropriate or anomalous activities that have potential security incident implications.	3		MON-01.12
15.3.m	N/A	Issuer shall put in place mechanism for velocity check on the number of transactions effected in a PPI per day / per beneficiary.	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	3		MON-16
15.3.m	N/A	Issuer shall put in place mechanism for velocity check on the number of transactions effected in a PPI per day / per beneficiary.	Functional	Intersects With	Unusual Transactions	MON-16.1	Mechanisms exist to define "normal business activities" to identify anomalous transaction activities that can reduce the opportunity for sending (outbound) and/or receiving (inbound) hostile and/or fraudulent actions.	5		DCH-25.1
15.3.n	N/A	Issuer shall also put in place suitable mechanism to prevent, detect and restrict occurrence of fraudulent transactions including loading / reloading funds into the PPI.	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	5		MON-16
15.3.n	N/A	Issuer shall also put in place suitable mechanism to prevent, detect and restrict occurrence of fraudulent transactions including loading / reloading funds into the PPI.	Functional	Intersects With	Unusual Transactions	MON-16.1	Mechanisms exist to define "normal business activities" to identify anomalous transaction activities that can reduce the opportunity for sending (outbound) and/or receiving (inbound) hostile and/or fraudulent actions.	5		DCH-25.1
15.3.o	N/A	Issuer shall put in place suitable internal and external escalation mechanisms in case of suspicious operations, besides alerting the customer in case of such transactions.	Functional	Intersects With	Incident Stakeholder Reporting	IRO-16	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5		IRO-10
15.3.o	N/A	Issuer shall put in place suitable internal and external escalation mechanisms in case of suspicious operations, besides alerting the customer in case of such transactions.	Functional	Intersects With	Event Log & Security-Relevant Telemetry Review Escalation Matrix	MON-05.3	Mechanisms exist to make event log and security-relevant telemetry review processes more efficient and effective by developing and maintaining an incident response escalation matrix.	3		MON-17.1
15.4	N/A	The requirements prescribed here are minimum and the entities may deploy additional checks and balances, as considered appropriate.	Functional	No Relationship	N/A	N/A	N/A	0		
15.5	N/A	PPI issuer shall put in place centralised database / management information system (MIS) to prevent multiple purchase of PPIs at different locations, leading to circumvention of limits, if any, prescribed for their issuance. In case of full-KYC PPIs issued by scheduled commercial banks for government departments, the limit of Rs.2,00,000/- shall be for each PPI, provided the PPIs are issued for expenses of the concerned government department and the loading is from the bank account of the government department.	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	3		MON-16
15.5	N/A	PPI issuer shall put in place centralised database / management information system (MIS) to prevent multiple purchase of PPIs at different locations, leading to circumvention of limits, if any, prescribed for their issuance. In case of full-KYC PPIs issued by scheduled commercial banks for government departments, the limit of Rs.2,00,000/- shall be for each PPI, provided the PPIs are issued for expenses of the concerned government department and the loading is from the bank account of the government department.	Functional	Intersects With	Unusual Transactions	MON-16.1	Mechanisms exist to define "normal business activities" to identify anomalous transaction activities that can reduce the opportunity for sending (outbound) and/or receiving (inbound) hostile and/or fraudulent actions.	3		DCH-25.1
15.6	N/A	Where direct interface is provided to its authorised / designated agents, PPI issuer shall ensure that compliance to regulatory requirements is strictly adhered to by these systems also.	Functional	Intersects With	Contract Flow-Down Requirements	TPM-14.1	Mechanisms exist to ensure applicable security, compliance and resilience requirements are included in contracts that flow-down to applicable subcontractors and suppliers.	3		TPM-05.2
15.6	N/A	Where direct interface is provided to its authorised / designated agents, PPI issuer shall ensure that compliance to regulatory requirements is strictly adhered to by these systems also.	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	5		TPM-08
15.7	N/A	PPI issuer 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, CO, RBI, Mumbai. It shall also be reported to CERT-IN as per the details notified by CERT-IN.	Functional	Intersects With	Incident Handling	IRO-06	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5		IRO-02
15.7	N/A	PPI issuer 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, CO, RBI, Mumbai. It shall also be reported to CERT-IN as per the details notified by CERT-IN.	Functional	Intersects With	Cyber Incident Reporting for Sensitive / Regulated Data	IRO-16.2	Mechanisms exist to report sensitive and/or regulated data incidents in a timely manner.	5		IRO-10.2
15.8	Guiding circulars on security	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
15.8.a	N/A	DPSS.CO.PD No.1343/02.14.003/2019-20 dated January 15, 2020 (as amended from time to time) on 'Enhancing Security of Card Transactions'. This circular, inter alia, gives the facility to card holders to switch on / off and set / modify the transaction limits across multiple channels.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-02	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	3		CPL-01
15.8.b	N/A	DPSS.CO.OD.No.1934/06.08.005/2019-20 dated June 22, 2020 (as amended from time to time) on Increasing Instances of Payment Frauds - Enhancing Public Awareness Campaigns Through Multiple Channels.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-02	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	3		CPL-01
15.8.c	N/A	CO.DPSS.POLC.No.S-384/02.32.001/2021-2022 dated August 03, 2021 (as amended from time to time) on Framework for Outsourcing of Payment and Settlement-related Activities by PSOs. The bank PPI issuer shall be guided by the outsourcing related instructions issued by their regulatory and supervisory departments.	Functional	Intersects With	Third-Party Management	TPM-02	Mechanisms exist to facilitate the implementation of third-party management controls.	5		TPM-01
16	Customer protection and grievance redressal framework	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
16.1	Disclosure of terms and conditions	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
16.1.a	N/A	All charges and fees associated with the use of the instrument; and	Functional	No Relationship	N/A	N/A	N/A	0		
16.1.b	N/A	The expiry period and the terms and conditions pertaining to expiration of the instrument.	Functional	No Relationship	N/A	N/A	N/A	0		

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Reserve Bank of India (RBI) - Master Direction on Prepaid Payment Instruments (PPI), 2021**
Focal Document URL: https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12156
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-ind-rbi-ppi-2021.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
16.2	Customer grievance redressal framework	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
16.2.a	N/A	PPI issuer shall disseminate the information of customer protection and grievance redressal policy in simple language (preferably in English, Hindi and the local language).	Functional	Intersects With	Grievances	CPL-22	Mechanisms exist to govern the intake and analysis of grievances related to the organization's cybersecurity and/or data protection practices.	5		CPL-07
16.2.a	N/A	PPI issuer shall disseminate the information of customer protection and grievance redressal policy in simple language (preferably in English, Hindi and the local language).	Functional	Intersects With	Data Subject Communications	PRI-37	Mechanisms exist to craft disclosures and communications to data subjects in a manner that is concise, unambiguous and understandable by a reasonable person.	3		PRI-17
16.2.b	N/A	PPI issuer shall clearly indicate the customer care contact details, including details of nodal officials for grievance redressal (telephone numbers, email address, postal address, etc.) on website, mobile wallet apps, and cards.	Functional	Intersects With	Grievances	CPL-22	Mechanisms exist to govern the intake and analysis of grievances related to the organization's cybersecurity and/or data protection practices.	5		CPL-07
16.2.c	N/A	PPI issuer's agents shall display proper signage of the PPI Issuer and the customer care contact details as at (b) above.	Functional	Intersects With	Grievances	CPL-22	Mechanisms exist to govern the intake and analysis of grievances related to the organization's cybersecurity and/or data protection practices.	3		CPL-07
16.2.d	N/A	PPI issuer shall provide specific complaint numbers for the complaints lodged along with the facility to track the status of the complaint by the customer.	Functional	Intersects With	Grievances	CPL-22	Mechanisms exist to govern the intake and analysis of grievances related to the organization's cybersecurity and/or data protection practices.	5		CPL-07
16.2.e	N/A	PPI issuer shall initiate action to resolve any customer complaint / grievance expeditiously, preferably within 48 hours and endeavour to resolve the same not later than 30 days from the date of receipt of such complaint / grievance.	Functional	Intersects With	Grievance Response	CPL-22.1	Mechanisms exist to respond to legitimate grievances related to the organization's cybersecurity and/or data protection practices.	5		CPL-07.1
16.2.f	N/A	PPI issuer shall display the detailed list of its authorised / designated agents (name, agent ID, address, contact details, etc.) on the website / mobile app.	Functional	Intersects With	Third-Party Inventories	TPM-08	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	3		TPM-01.1
16.3	N/A	PPI issuer shall create sufficient awareness and educate customers in the secure use of the PPIs, including the need for keeping passwords confidential, procedure to be followed in case of loss or theft of card or authentication data or if any fraud / abuse is detected, etc.	Functional	Intersects With	User Responsibilities for Account Management	IAC-22	Mechanisms exist to compel users to follow accepted practices in the use of authentication mechanisms (e.g., passwords, passphrases, physical or logical security tokens, smart cards and certificates).	5		IAC-18
16.3	N/A	PPI issuer shall create sufficient awareness and educate customers in the secure use of the PPIs, including the need for keeping passwords confidential, procedure to be followed in case of loss or theft of card or authentication data or if any fraud / abuse is detected, etc.	Functional	Intersects With	Incident Reporting Assistance	IRO-18	Mechanisms exist to provide incident response advice and assistance to users of Technology Assets, Applications and/or Services (TAAS) for the handling and reporting of actual and potential cybersecurity and data protection incidents.	5		IRO-11
16.3	N/A	PPI issuer shall create sufficient awareness and educate customers in the secure use of the PPIs, including the need for keeping passwords confidential, procedure to be followed in case of loss or theft of card or authentication data or if any fraud / abuse is detected, etc.	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-04	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	3		SAT-02
16.4	N/A	PPI issuer shall provide an option for the PPI holders to generate / receive account statements for at least past 6 months. The account statement shall, at the minimum, provide details such as date of transaction, debit / credit amount, net balance and description of transaction. Additionally, the PPI issuer shall provide transaction history for at least 10 transactions.	Functional	Intersects With	Data Subject Empowerment	PRI-39.1	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Obtain the source(s) of their PD; (4) Obtain the categories of their PD being collected, received, processed, stored and shared; (5) Request correction to their PD due to inaccuracies; (6) Request erasure of their PD; and (7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.	3		PRI-06
16.5	N/A	In case of PPIs issued by banks and non-banks, customers shall have recourse to the Reserve Bank - Integrated Ombudsman Scheme, 2021 (as amended from time to time) for grievance redressal.	Functional	No Relationship	N/A	N/A	N/A	0		
16.6	N/A	Non-bank PPI issuer shall report regarding the receipt of complaints and action taken status thereon in the enclosed format (Annex-6) on a Quarterly basis by the 10th of the following month to the respective Regional Office of DPSS, RBI. Banks shall submit the same report to DPSS, Mumbai Regional Office, RBI.	Functional	Intersects With	Grievances	CPL-22	Mechanisms exist to govern the intake and analysis of grievances related to the organization's cybersecurity and/or data protection practices.	3		CPL-07
16.6	N/A	Non-bank PPI issuer shall report regarding the receipt of complaints and action taken status thereon in the enclosed format (Annex-6) on a Quarterly basis by the 10th of the following month to the respective Regional Office of DPSS, RBI. Banks shall submit the same report to DPSS, Mumbai Regional Office, RBI.	Functional	Intersects With	Security, Compliance & Resilience Status Reporting	CPL-27	Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required.	3		GOV-17
16.7	Transparency in pricing and charge structure	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
16.7.a	N/A	Ensure uniformity in charges at agent level.	Functional	No Relationship	N/A	N/A	N/A	0		
16.7.b	N/A	Disclosure of charges for various types of transactions on its website, mobile app, agent locations, etc.	Functional	No Relationship	N/A	N/A	N/A	0		
16.7.c	N/A	Specific agreements with agents prohibiting them from charging any fee to the customers directly for services rendered by them on behalf of the PPI issuer.	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	3		TPM-05
16.7.d	N/A	Require each retail outlet / sub-agent to post a signage indicating their status as service providers for the PPI issuer and the fees for all services available at the outlet.	Functional	No Relationship	N/A	N/A	N/A	0		
16.7.e	N/A	The amount collected from the customer shall be acknowledged by issuing a receipt (printed or electronic) on behalf of the PPI issuer.	Functional	No Relationship	N/A	N/A	N/A	0		
16.8	N/A	PPI issuer shall be responsible for addressing all customer service aspects related to all PPIs (including co-branded PPIs) issued by them as well as their agents.	Functional	Intersects With	Grievances	CPL-22	Mechanisms exist to govern the intake and analysis of grievances related to the organization's cybersecurity and/or data protection practices.	3		CPL-07
16.8	N/A	PPI issuer shall be responsible for addressing all customer service aspects related to all PPIs (including co-branded PPIs) issued by them as well as their agents.	Functional	Intersects With	Third-Party Management	TPM-02	Mechanisms exist to facilitate the implementation of third-party management controls.	3		TPM-01
16.9	N/A	PPI issuer shall also display Frequently Asked Questions (FAQs) on its website / mobile app related to the PPIs.	Functional	No Relationship	N/A	N/A	N/A	0		
16.1	Guiding DPSS circulars on customer protection	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
16.10.a	N/A	Harmonisation of Turn Around Time (TAT) and customer compensation for failed transactions using authorised Payment Systems issued vide DPSS circular DPSS.CO.PD No.629/02.01.014/2019-20 dated September 20, 2019 (as amended from time to time);	Functional	No Relationship	N/A	N/A	N/A	0		
16.10.b	N/A	Online Dispute Resolution (ODR) system for resolving customer disputes and grievances pertaining to digital payments, using a system-driven and rule-based mechanism with zero or minimal manual intervention, issued vide DPSS circular DPSS.CO.PD No.116/02.12.004/2020-21 dated August 6, 2020 (as amended from time to time).	Functional	Intersects With	Grievances	CPL-22	Mechanisms exist to govern the intake and analysis of grievances related to the organization's cybersecurity and/or data protection practices.	5		CPL-07
16.10.b	N/A	Online Dispute Resolution (ODR) system for resolving customer disputes and grievances pertaining to digital payments, using a system-driven and rule-based mechanism with zero or minimal manual intervention, issued vide DPSS circular DPSS.CO.PD No.116/02.12.004/2020-21 dated August 6, 2020 (as amended from time to time).	Functional	Intersects With	Grievance Response	CPL-22.1	Mechanisms exist to respond to legitimate grievances related to the organization's cybersecurity and/or data protection practices.	3		CPL-07.1
17	Limiting liability of customers in unauthorised electronic payment transactions in PPIs issued by banks and non-banks	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
17.1	N/A	Bank PPI issuer shall continue to be guided by RBI circulars DBR.No.Leg.BC.78/09.07.005/2017-18 dated July 6, 2017 or DCBR.BPD.(PCB/RCB).Cir.No.06/12.05.001/2017-18 dated December 14, 2017, as applicable on Customer Protection - Limiting Liability of Customers in Unauthorised Electronic Banking Transactions.	Functional	No Relationship	N/A	N/A	N/A	0		

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Reserve Bank of India (RBI) - Master Direction on Prepaid Payment Instruments (PPI), 2021
Focal Document URL: https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12156
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-ind-rbi-ppi-2021.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
17.2	N/A	Non-bank PPI issuer, shall adhere to the following criteria for determining the customers' liability in unauthorised electronic payment transactions resulting in debit to its PPIs. PPIs issued under the arrangement of PPI-MTS as per paragraph 10.2 will be outside the purview of these paragraphs except for the cases of contributory fraud / negligence / deficiency on the part of the PPI-MTS issuer.	Functional	No Relationship	N/A	N/A	N/A	0		
17.3	Categories of electronic payment transactions	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
17.3.a	N/A	Remote / Online payment transactions: Transactions that do not require physical PPIs to be presented at the point of transactions e.g. wallets, card not present (CNP) transactions, etc.; and	Functional	No Relationship	N/A	N/A	N/A	0		
17.3.b	N/A	Face-to-face / Proximity payment transactions: Transactions that require physical PPIs to be present at the point of transactions e.g. transactions at ATMs, PoS devices, etc.	Functional	No Relationship	N/A	N/A	N/A	0		
17.4	Reporting of unauthorised payment transactions by customers to the non-bank PPI issuer	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
17.4.a	N/A	Non-bank PPI issuer shall ensure that its customers mandatorily register for SMS alerts and wherever available also register for e-mail alerts, for electronic payment transactions.	Functional	Intersects With	Automated Incident Responder Alerting	MON-05.5	Mechanisms exist to automatically alert incident response personnel to inappropriate or anomalous activities that have potential security incident implications.	3		MON-01.12
17.4.b	N/A	The SMS alert for any payment transaction in the account shall mandatorily be sent to the customers and e-mail alert may additionally be sent, wherever registered. The transaction alert should have a contact number and / or e-mail id on which a customer can report unauthorised transactions or notify the objection.	Functional	Intersects With	Incident Reporting Assistance	IRO-18	Mechanisms exist to provide incident response advice and assistance to users of Technology Assets, Applications and/or Services (TAAS) for the handling and reporting of actual and potential cybersecurity and data protection incidents.	3		IRO-11
17.4.b	N/A	The SMS alert for any payment transaction in the account shall mandatorily be sent to the customers and e-mail alert may additionally be sent, wherever registered. The transaction alert should have a contact number and / or e-mail id on which a customer can report unauthorised transactions or notify the objection.	Functional	Intersects With	Automated Incident Responder Alerting	MON-05.5	Mechanisms exist to automatically alert incident response personnel to inappropriate or anomalous activities that have potential security incident implications.	3		MON-01.12
17.4.c	N/A	Customers shall be advised to notify the non-bank PPI issuer of any unauthorised electronic payment transaction at the earliest and, shall also be informed that longer the time taken to notify the non-bank PPI issuer, higher will be the risk of loss to the non-bank PPI issuer / customer.	Functional	Intersects With	Incident Reporting Assistance	IRO-18	Mechanisms exist to provide incident response advice and assistance to users of Technology Assets, Applications and/or Services (TAAS) for the handling and reporting of actual and potential cybersecurity and data protection incidents.	5		IRO-11
17.4.d	N/A	To facilitate this, non-bank PPI issuer shall provide customers with 24x7 access via website / SMS / e-mail / a dedicated toll-free helpline for reporting unauthorised transactions that have taken place and / or loss or theft of the PPI.	Functional	Intersects With	Incident Reporting Assistance	IRO-18	Mechanisms exist to provide incident response advice and assistance to users of Technology Assets, Applications and/or Services (TAAS) for the handling and reporting of actual and potential cybersecurity and data protection incidents.	5		IRO-11
17.4.e	N/A	Further, a direct link for lodging of complaints, with specific option to report unauthorised electronic payment transactions shall be provided by non-bank PPI issuer on mobile app / home page of its website / any other evolving acceptance mode.	Functional	Intersects With	Grievances	CPL-22	Mechanisms exist to govern the intake and analysis of grievances related to the organization's cybersecurity and/or data protection practices.	3		CPL-07
17.4.e	N/A	Further, a direct link for lodging of complaints, with specific option to report unauthorised electronic payment transactions shall be provided by non-bank PPI issuer on mobile app / home page of its website / any other evolving acceptance mode.	Functional	Intersects With	Incident Reporting Assistance	IRO-18	Mechanisms exist to provide incident response advice and assistance to users of Technology Assets, Applications and/or Services (TAAS) for the handling and reporting of actual and potential cybersecurity and data protection incidents.	5		IRO-11
17.4.f	N/A	The loss / fraud reporting system so established shall also ensure that immediate response (including auto response) is sent to the customers acknowledging the complaint along with the registered complaint number. The communication systems used by non-bank PPI issuer to send alerts and receive their responses thereto shall record time and date of delivery of the message and receipt of customer's response, if any. This shall be important in determining the extent of a customer's liability. On receipt of report of an unauthorised payment transaction from the customer, non-bank PPI issuer shall take immediate action to prevent further unauthorised payment transactions in the PPI.	Functional	Intersects With	Grievances	CPL-22	Mechanisms exist to govern the intake and analysis of grievances related to the organization's cybersecurity and/or data protection practices.	3		CPL-07
17.4.f	N/A	The loss / fraud reporting system so established shall also ensure that immediate response (including auto response) is sent to the customers acknowledging the complaint along with the registered complaint number. The communication systems used by non-bank PPI issuer to send alerts and receive their responses thereto shall record time and date of delivery of the message and receipt of customer's response, if any. This shall be important in determining the extent of a customer's liability. On receipt of report of an unauthorised payment transaction from the customer, non-bank PPI issuer shall take immediate action to prevent further unauthorised payment transactions in the PPI.	Functional	Intersects With	Incident Handling	IRO-06	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5		IRO-02
17.4.f	N/A	The loss / fraud reporting system so established shall also ensure that immediate response (including auto response) is sent to the customers acknowledging the complaint along with the registered complaint number. The communication systems used by non-bank PPI issuer to send alerts and receive their responses thereto shall record time and date of delivery of the message and receipt of customer's response, if any. This shall be important in determining the extent of a customer's liability. On receipt of report of an unauthorised payment transaction from the customer, non-bank PPI issuer shall take immediate action to prevent further unauthorised payment transactions in the PPI.	Functional	Intersects With	Incident Reporting Assistance	IRO-18	Mechanisms exist to provide incident response advice and assistance to users of Technology Assets, Applications and/or Services (TAAS) for the handling and reporting of actual and potential cybersecurity and data protection incidents.	5		IRO-11
17.5	Customer liability limits for unauthorised payment transactions	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
17.5.a	N/A	(a) Contributory fraud / negligence / deficiency on the part of the non-bank PPI issuer, including PPI-MTS issuer (irrespective of whether or not the transaction is reported by the customer): Maximum Liability of Customer = Zero.	Functional	No Relationship	N/A	N/A	N/A	0		
17.5.b	N/A	(b) Third party breach where the deficiency lies neither with the non-bank PPI issuer nor with the customer but lies elsewhere in the system, and the customer notifies the non-bank PPI issuer regarding the unauthorised payment transaction: i. Within three days - Zero; ii. Within four to seven days - Transaction value or Rs.10,000/- per transaction, whichever is lower; iii. Beyond seven days - As per the Board approved policy of the non-bank PPI issuer. [Note: The number of days mentioned above shall be counted excluding the date of receiving the communication from the non-bank PPI issuer.]	Functional	No Relationship	N/A	N/A	N/A	0		
17.5.c	N/A	(c) In cases where the loss is due to negligence by a customer, such as where he / she has shared the payment credentials, the customer will bear the entire loss until he / she reports the unauthorised transaction to the non-bank PPI issuer. Any loss occurring after the reporting of the unauthorised transaction shall be borne by the non-bank PPI issuer.	Functional	No Relationship	N/A	N/A	N/A	0		
17.5.d	N/A	(d) Non-bank PPI issuer may also, at its discretion, decide to waive off any customer liability in case of unauthorised electronic payment transactions even in cases of customer negligence.	Functional	No Relationship	N/A	N/A	N/A	0		
17.6	N/A	The above shall be clearly communicated to all PPI holders.	Functional	No Relationship	N/A	N/A	N/A	0		
17.7	N/A	On being notified by the customer, the non-bank PPI issuer shall credit (notional reversal / shadow reversal) the amount involved in the unauthorised electronic payment transaction to the customer's PPI within 10 days from the date of such notification by the customer (without waiting for settlement of insurance claim, if any), even if such reversal breaches the maximum permissible limit applicable to that type / category of PPI. The credit shall be value-dated to be as of the date of the unauthorised transaction.	Functional	No Relationship	N/A	N/A	N/A	0		
17.8	N/A	Non-bank PPI issuer shall ensure that a complaint is resolved and liability of the customer, if any, established within such time, as may be specified in the non-bank PPI issuer's Board approved policy, but not exceeding 90 days from the date of receipt of the complaint, and the customer is compensated as per provisions of paragraph 17.5 above. In case the non-bank PPI issuer is unable to resolve the complaint or determine the customer liability, if any, within 90 days, the amount as prescribed in paragraph 17.5 shall be paid to the customer, irrespective of whether the negligence is on the part of customer or otherwise.	Functional	Intersects With	Grievance Response	CPL-22.1	Mechanisms exist to respond to legitimate grievances related to the organization's cybersecurity and/or data protection practices.	5		CPL-07.1

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Reserve Bank of India (RBI) - Master Direction on Prepaid Payment Instruments (PPI), 2021**
Focal Document URL: https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12156
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-ind-rbi-ppi-2021.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
17.9	N/A	Taking into account the risks arising out of unauthorised debits to PPIs owing to customer negligence / non-bank PPI issuer negligence / system frauds / third party breaches, non-bank PPI issuer needs to clearly define the rights and obligations of customers in case of unauthorised payment transactions in specified scenarios. Non-bank PPI issuer shall formulate / revise its customer relations policy, with approval of its Board, to cover aspects of customer protection, including the mechanism of creating customer awareness on the risks and responsibilities involved in electronic payment transactions and customer liability in such cases of unauthorised electronic payment transactions. The policy must be transparent, non-discriminatory and should stipulate the mechanism of compensating the customers for the unauthorised electronic payment transactions and also prescribe the timelines for effecting such compensation. Non-bank PPI issuer shall provide the details of its Board approved policy in regard to customers' liability formulated in pursuance of the provisions of these directions, to all customers at the time of issuing the PPI. Non-bank PPI issuer shall display its Board approved policy, along with the details of grievance handling / escalation procedure, in public domain / website / app for wider dissemination.	Functional	Intersects With	Grievances	CPL-22	Mechanisms exist to govern the intake and analysis of grievances related to the organization's cybersecurity and/or data protection practices.	3		CPL-07
17.9	N/A	Taking into account the risks arising out of unauthorised debits to PPIs owing to customer negligence / non-bank PPI issuer negligence / system frauds / third party breaches, non-bank PPI issuer needs to clearly define the rights and obligations of customers in case of unauthorised payment transactions in specified scenarios. Non-bank PPI issuer shall formulate / revise its customer relations policy, with approval of its Board, to cover aspects of customer protection, including the mechanism of creating customer awareness on the risks and responsibilities involved in electronic payment transactions and customer liability in such cases of unauthorised electronic payment transactions. The policy must be transparent, non-discriminatory and should stipulate the mechanism of compensating the customers for the unauthorised electronic payment transactions and also prescribe the timelines for effecting such compensation. Non-bank PPI issuer shall provide the details of its Board approved policy in regard to customers' liability formulated in pursuance of the provisions of these directions, to all customers at the time of issuing the PPI. Non-bank PPI issuer shall display its Board approved policy, along with the details of grievance handling / escalation procedure, in public domain / website / app for wider dissemination.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-04	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5		GOV-02
17.1	N/A	The burden of proving customer liability in case of unauthorised electronic payment transactions shall lie on the non-bank PPI issuer.	Functional	No Relationship	N/A	N/A	N/A	0		
17.11	N/A	Non-bank PPI issuer shall put in place a suitable mechanism and structure for reporting of the customer liability cases to the Board or one of its Committees. The reporting shall, inter-alia, include volume / number of cases and the aggregate value involved and distribution across various categories of cases. The Board or one of its Committees shall periodically review the unauthorised electronic payment transactions reported by customers or otherwise, as also the action taken thereon, the functioning of the grievance redressal mechanism and take appropriate measures to improve the systems and procedures.	Functional	Intersects With	Status Reporting To Governing Body	GOV-09.1	Mechanisms exist to provide governance oversight reporting and recommendations enabling executives to make decisions about matters considered material to the organization's Security, Compliance & Resilience Program (SCRP).	5		GOV-01.2
17.11	N/A	Non-bank PPI issuer shall put in place a suitable mechanism and structure for reporting of the customer liability cases to the Board or one of its Committees. The reporting shall, inter-alia, include volume / number of cases and the aggregate value involved and distribution across various categories of cases. The Board or one of its Committees shall periodically review the unauthorised electronic payment transactions reported by customers or otherwise, as also the action taken thereon, the functioning of the grievance redressal mechanism and take appropriate measures to improve the systems and procedures.	Functional	Intersects With	Recurring Incident Analysis	IRO-17.2	Mechanisms exist to periodically review incident response activities for the existence of recurring incidents.	3		IRO-09.2
18	Information system audit	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
18.1	N/A	Banks shall be guided by RBI circulars DBS.CO.ITC.BC.No.6/31.02.008/2010-11 dated April 29, 2011, DBS.CO/CSITE/BC.11/33.01.001/2015-16 dated June 02, 2016, DCBS.CO.PCB.Cir.No.1/18.01.000/2018-19 dated October 19, 2018 (as applicable) and other relevant circulars on the subject, as amended from time to time.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-02	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	3		CPL-01
18.2	N/A	Authorised non-bank PPI issuer shall submit a System Audit Report (SAR), including cyber security audit conducted by CERT-IN empaneled auditor, within two months of the close of its financial year to the respective Regional Office of DPSS, RBI. They shall also be guided by DPSS letter DPSS.CO.OD.No.1325/06.11.001/2019-20 dated January 10, 2020 (as amended from time to time) regarding System Audit of Payment Systems, as amended from time to time.	Functional	Intersects With	Independent Assessors	CPL-08	Mechanisms exist to utilize independent assessors to evaluate security, compliance and resilience at planned intervals or when the Technology Asset, Application and/or Service (TAAS) undergoes significant changes.	5		CPL-03.1
18.2	N/A	Authorised non-bank PPI issuer shall submit a System Audit Report (SAR), including cyber security audit conducted by CERT-IN empaneled auditor, within two months of the close of its financial year to the respective Regional Office of DPSS, RBI. They shall also be guided by DPSS letter DPSS.CO.OD.No.1325/06.11.001/2019-20 dated January 10, 2020 (as amended from time to time) regarding System Audit of Payment Systems, as amended from time to time.	Functional	Intersects With	Security, Compliance & Resilience Status Reporting	CPL-27	Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required.	5		GOV-17
18.3	Minimum information security framework	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
18.3.a	N/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.	Functional	Intersects With	Malware Testing Prior to Release	TDA-13.2	Mechanisms exist to utilize at least one(1) malware detection tool to identify if any known malware exists in the final binaries of the product or security update.	3		TDA-01.3
18.3.a	N/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.	Functional	Intersects With	Manual Code Review	TDA-17.5	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to employ a manual code review process to identify and remediate unique flaws that require knowledge of the application's requirements and design.	5		TDA-09.7
18.3.b	N/A	Security Operations Centre (SOC): Integration of system level (server), application level logs of mobile applications (PPIs) with SOC for centralised and co-ordinated monitoring and management of security related incidents.	Functional	Intersects With	Centralized Collection of Event Logs & Security-Relevant Telemetry	MON-05	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of event logs and security-relevant telemetry.	5		MON-02
18.3.b	N/A	Security Operations Centre (SOC): Integration of system level (server), application level logs of mobile applications (PPIs) with SOC for centralised and co-ordinated monitoring and management of security related incidents.	Functional	Intersects With	Security Operations Center (SOC)	OPS-07	Mechanisms exist to establish and maintain a Security Operations Center (SOC) that facilitates a 24x7 response capability.	5		OPS-04
18.3.c	N/A	Anti-Phishing: 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 mobile apps / phishing attacks.	Functional	Intersects With	Phishing & Spam Protection	NET-40.2	Mechanisms exist to utilize anti-phishing and spam protection technologies to detect and take action on unsolicited messages transported by electronic mail.	3		END-08
18.3.c	N/A	Anti-Phishing: 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 mobile apps / phishing attacks.	Functional	Intersects With	Threat Intelligence Program	THR-02	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	3		THR-01
18.3.d	N/A	Risk-based Transaction Monitoring: Risk-based transaction monitoring or surveillance process shall be implemented as part of fraud risk management system.	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	5		MON-16
18.3.d	N/A	Risk-based Transaction Monitoring: Risk-based transaction monitoring or surveillance process shall be implemented as part of fraud risk management system.	Functional	Intersects With	Unusual Transactions	MON-16.1	Mechanisms exist to define "normal business activities" to identify anomalous transaction activities that can reduce the opportunity for sending (outbound) and/or receiving (inbound) hostile and/or fraudulent actions.	5		DCH-25.1

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Reserve Bank of India (RBI) - Master Direction on Prepaid Payment Instruments (PPI), 2021**
Focal Document URL: https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12156
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-ind-rbi-ppi-2021.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
18.3.e	N/A	Vendor Risk Management: (i) 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 PPI provider, to be made accessible to RBI officials when sought, though the infrastructure / enabling resources may not physically be located in the premises of PPI provider; (iii) Adhere to the relevant legal and regulatory requirements relating to geographical location of infrastructure and movement of data out of borders; (iv) Review the security processes and controls being followed by service providers regularly; (v) Service agreements of PPI issuer 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.	Functional	Intersects With	Third-Party Processing, Storage and Service Locations	TPM-12.2	Mechanisms exist to restrict the location of information processing/storage based on business requirements.	3		TPM-04.4
18.3.e	N/A	Vendor Risk Management: (i) 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 PPI provider, to be made accessible to RBI officials when sought, though the infrastructure / enabling resources may not physically be located in the premises of PPI provider; (iii) Adhere to the relevant legal and regulatory requirements relating to geographical location of infrastructure and movement of data out of borders; (iv) Review the security processes and controls being followed by service providers regularly; (v) Service agreements of PPI issuer 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.	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-05
18.3.e	N/A	Vendor Risk Management: (i) 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 PPI provider, to be made accessible to RBI officials when sought, though the infrastructure / enabling resources may not physically be located in the premises of PPI provider; (iii) Adhere to the relevant legal and regulatory requirements relating to geographical location of infrastructure and movement of data out of borders; (iv) Review the security processes and controls being followed by service providers regularly; (v) Service agreements of PPI issuer 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.	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	5		TPM-08
18.3.e	N/A	Vendor Risk Management: (i) 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 PPI provider, to be made accessible to RBI officials when sought, though the infrastructure / enabling resources may not physically be located in the premises of PPI provider; (iii) Adhere to the relevant legal and regulatory requirements relating to geographical location of infrastructure and movement of data out of borders; (iv) Review the security processes and controls being followed by service providers regularly; (v) Service agreements of PPI issuer 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.	Functional	Intersects With	Security Compromise Notification Agreements	TPM-21.1	Mechanisms exist to compel External Service Providers (ESPs) to provide notification of actual or potential compromises in the supply chain that can potentially affect or have adversely affected Technology Assets, Applications and/or Services (TAAS) that the organization utilizes.	5		TPM-05.1
18.3.f	N/A	Disaster Recovery (DR): Consider having DR facility to achieve the Recovery Time Objective (RTO) / Recovery Point Objective (RPO) for the PPI 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.	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-02	Mechanisms exist to operate a Business Continuity Management System (BCMS) to achieve resilient Technology Assets, Applications, Services and/or Data (TAASD) during: (1) Routine operations; and (2) Adverse conditions.	5		BCD-01
18.3.f	N/A	Disaster Recovery (DR): Consider having DR facility to achieve the Recovery Time Objective (RTO) / Recovery Point Objective (RPO) for the PPI 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.	Functional	Intersects With	Recovery Time / Point Objectives (RTO / RPO)	BCD-04.1	Mechanisms exist to facilitate recovery operations in accordance with Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5		BCD-01.4
18.3.f	N/A	Disaster Recovery (DR): Consider having DR facility to achieve the Recovery Time Objective (RTO) / Recovery Point Objective (RPO) for the PPI 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.	Functional	Intersects With	Technology Assets, Applications and/or Services (TAAS) Recovery & Reconstitution	BCD-18	Mechanisms exist to ensure the secure recovery and reconstitution of Technology Assets, Applications and/or Services (TAAS) to a known state after a disruption, compromise or failure.	3		BCD-12
19	Reporting requirements	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
19.a	N/A	a) Net-worth Certificate (Annex-2);	Functional	No Relationship	N/A	N/A	N/A	0		
19.b	N/A	b) Declaration and Undertaking by the Director (Annex-3);	Functional	No Relationship	N/A	N/A	N/A	0		
19.c	N/A	c) PPI Statistics (Annex-4);	Functional	No Relationship	N/A	N/A	N/A	0		
19.d	N/A	d) Auditor Certificate on maintenance of balance in Escrow Account (Annex-5); and	Functional	No Relationship	N/A	N/A	N/A	0		
19.e	N/A	e) PPI Customer Grievance Report (Annex-6).	Functional	Intersects With	Grievances	CPL-22	Mechanisms exist to govern the intake and analysis of grievances related to the organization's cybersecurity and/or data protection practices.	3		CPL-07
19.e	N/A	e) PPI Customer Grievance Report (Annex-6).	Functional	Intersects With	Security, Compliance & Resilience Status Reporting	CPL-27	Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required.	3		GOV-17
20	Consolidated and other provisions	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
20.a	N/A	a) With issuance of these Directions, the instructions / guidelines issued by the RBI, contained in Table-1 of Annex-1 are consolidated.	Functional	No Relationship	N/A	N/A	N/A	0		
20.b	N/A	b) The instructions / guidelines issued by the RBI contained in Table-2 of Annex-1 are partially consolidated to the extent they are applicable to issuance and operations of PPIs.	Functional	No Relationship	N/A	N/A	N/A	0		