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 Regulation of Payment Aggregators (PA) (2025)
Focal Document URL: https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12896
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-ind-rbi-pa-2025.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 #
I	Preliminary	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
I.1	Short Title and Commencement	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
I.1.a	N/A	These Directions shall be called the Reserve Bank of India (Regulation of Payment Aggregators) Directions, 2025.	Functional	No Relationship	N/A	N/A	N/A	0		
I.2	Effective Date	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
I.2.a	N/A	These Directions shall be effective immediately unless indicated otherwise for any specific provision herein.	Functional	No Relationship	N/A	N/A	N/A	0		
I.3	Applicability	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
I.3.a	N/A	These Directions shall apply to all bank and non-bank entities undertaking the business of Payment Aggregator (PA) as defined herein. These Directions shall also apply to all Authorised Dealer banks as well as Scheduled Commercial Banks which engage with entities undertaking PA business, to the extent hereinafter specified.	Functional	No Relationship	N/A	N/A	N/A	0		
I.4	Definitions	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
I.4.a	N/A	Cash-on-delivery transaction: A merchant transaction wherein banknotes or currency notes, being legal tender in India, is offered or tendered, for and at the time of, delivery of goods and / or service(s).	Functional	No Relationship	N/A	N/A	N/A	0		
I.4.b	N/A	Contact Point Verification (CPV): Physical verification of the address or place of business of the merchant.	Functional	No Relationship	N/A	N/A	N/A	0		
I.4.c	N/A	E-commerce: Buying and selling of goods and services, including digital products, conducted over digital and electronic network. Explanation: For the purposes of this definition, the term 'digital & electronic network' shall include network of computers, television channels and any other internet application used in automated manner such as web pages, extranets, mobiles, etc.	Functional	No Relationship	N/A	N/A	N/A	0		
I.4.d	N/A	Inward transaction: Transaction involving the inflow of foreign exchange.	Functional	No Relationship	N/A	N/A	N/A	0		
I.4.e	N/A	Marketplace: An e-commerce entity which provides an information technology platform on a digital or electronic network to facilitate transactions between buyer(s) and seller(s).	Functional	No Relationship	N/A	N/A	N/A	0		
I.4.f	N/A	Merchant: An entity or a marketplace that sells goods, provides services, or offers investment products, and includes exporters and overseas sellers.	Functional	No Relationship	N/A	N/A	N/A	0		
I.4.g	N/A	Outward transaction: Transaction involving the outflow of foreign exchange.	Functional	No Relationship	N/A	N/A	N/A	0		
I.4.h	N/A	Payment channel: The method or manner through which payment instruction is initiated and processed in a payment system.	Functional	No Relationship	N/A	N/A	N/A	0		
I.4.i	N/A	Payment Aggregator (PA): An entity that facilitates aggregation of payments made by customers to the merchants through one or more payment channels through the merchant's interface (physical / virtual) for purchase of goods, services or investment products, and subsequently settles the collected funds to such merchants. PA is categorised as: (i) PA - Physical (PA - P): PA that facilitates transaction(s) where both the acceptance device and payment instrument are physically present in close proximity while making the transaction. (ii) PA - Cross Border (PA - CB): PA that facilitates aggregation of cross-border payments for current account transactions, that are not prohibited under FEMA, for its onboarded merchants through e-commerce mode. Sub-categories: a) PA-CB facilitating inward transaction; b) PA-CB facilitating outward transaction. Note: (1) A non-bank entity authorised as AD Category-II, and facilitating current account transactions not prohibited under FEMA (other than purchase or sale of goods or service), shall not fall within the purview of PA - CB business. (2) A card transaction, where the foreign exchange settlement is facilitated by a card network and the aggregator receives the payment in local currency, is not part of PA - CB activity. (iii) PA - Online (PA - O): PA that facilitates transaction(s) where the acceptance device and payment instrument are not present in close proximity while making the transaction.	Functional	No Relationship	N/A	N/A	N/A	0		
I.4.j	N/A	Payment Gateway (PG): An entity that provides technology infrastructure to route and facilitate processing of a payment transaction without any involvement in handling of funds.	Functional	No Relationship	N/A	N/A	N/A	0		
I.4.k	N/A	Central KYC Records Registry (CKYCR), Officially Valid Document (OVD), equivalent e-document, digital KYC, and Video-based Customer Identification Procedure (V-CIP) shall have the same meanings as defined in RBI Master Direction DBR.AML.BC.No.81/14.01.001/2015-16 dated February 25, 2016 on 'Master Direction - Know Your Customer (KYC) Direction, 2016', as amended from time to time (hereinafter referred to as 'MD on KYC').	Functional	No Relationship	N/A	N/A	N/A	0		
II	Authorisation and Capital Requirements	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
II.5	Authorisation for PA Business	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
II.5.a	N/A	A bank does not require authorisation to carry out PA business.	Functional	No Relationship	N/A	N/A	N/A	0		
II.5.b	N/A	A non-bank entity shall seek authorisation for operating as a PA by submitting an application through RBI's online portal. An entity, regulated by any of the financial sector regulator(s), shall apply along with a 'No Objection Certificate' (NOC) from such regulator(s), within 45 days of obtaining the NOC.	Functional	No Relationship	N/A	N/A	N/A	0		
II.5.c	N/A	A non-bank PA shall be a company incorporated in India under the Companies Act, 2013. The Memorandum of Association of the applicant entity should cover the proposed activity of operating as a PA.	Functional	No Relationship	N/A	N/A	N/A	0		
II.5.d	Directions Applicable from Date of Issue	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
II.5.d.i	PA with Existing Certificate of Authorisation	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
II.5.d.i.a	N/A	A PA having a Certificate of Authorisation (CoA) issued by RBI, and already carrying on business as a PA-P, shall intimate RBI. A revised CoA shall be issued to the PA.	Functional	No Relationship	N/A	N/A	N/A	0		
II.5.d.i.b	N/A	A PA having a Certificate of Authorisation (CoA) issued by RBI, and desirous of commencing business in another PA category, shall intimate RBI at least 30 days prior to commencing the new business.	Functional	No Relationship	N/A	N/A	N/A	0		
II.5.d.ii	N/A	An entity, whose application for grant of CoA for PA-O or PA - CB is under consideration of RBI, shall intimate the Reserve Bank about its existing PA-P business, if any, through the online portal, by December 31, 2025.	Functional	No Relationship	N/A	N/A	N/A	0		
II.5.d.iii	N/A	An entity carrying on only PA-P business shall apply for authorisation as prescribed in 5(b) above, by December 31, 2025. An entity which fails to apply by the due date shall intimate its banker(s) forthwith and wind up its business by February 28, 2026.	Functional	No Relationship	N/A	N/A	N/A	0		
II.5.e	N/A	Application of an entity, not meeting the minimum capital requirement, or which is incomplete / not in the prescribed form, shall be returned.	Functional	No Relationship	N/A	N/A	N/A	0		
II.6	Capital Requirements	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
II.6.a	N/A	An entity seeking authorisation to commence or carry on PA business shall have a minimum net-worth of Rs.15 crore at the time of tendering application for authorisation; and shall attain a minimum net-worth of Rs.25 crore by the end of third financial year of grant of authorisation.	Functional	No Relationship	N/A	N/A	N/A	0		
II.6.b	N/A	The minimum networth, as applicable, shall be maintained by a PA on an ongoing basis.	Functional	No Relationship	N/A	N/A	N/A	0		
II.6.c	N/A	For the purposes of this MD, computation of net worth of an entity shall be guided by the directions in RBI circular DPSS.CO.AD.No.1344 02.27.005/2014-15 dated January 16, 2015 on 'Computation of Net-worth', as amended from time to time. In addition to the items provided in the said circular, 'net worth' shall also include preference shares that are compulsorily convertible to equity. Compulsorily convertible preference shares can be either non-cumulative or cumulative, and they should be compulsorily convertible into equity shares and the shareholder agreements should specifically prohibit any withdrawal of this preference share capital at any time. Additionally, if Deferred Tax Assets have been included in any of the components, the same shall be deducted while arriving at the net-worth value.	Functional	No Relationship	N/A	N/A	N/A	0		
II.6.d	N/A	An entity, having Foreign Direct Investment (FDI), shall be guided by the Consolidated FDI Policy of the Government of India, and the relevant Foreign Exchange Management Regulations on this subject.	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 Regulation of Payment Aggregators (PA) (2025)
Focal Document URL: https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12896
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-ind-rbi-pa-2025.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 #
II.6.e	N/A	An entity seeking PA authorisation shall submit a certificate in the enclosed format (Annexure 2.1) from their statutory auditor evidencing compliance with the applicable net-worth requirement while submitting the application for authorisation. A newly incorporated non-bank entity which may not have an audited statement of financial accounts shall submit a certificate in the enclosed format from their statutory auditor regarding current networth along with a provisional balance sheet as of recent date.	Functional	No Relationship	N/A	N/A	N/A	0		
III	Conduct of PA Business	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
III.7	Governance	N/A	Functional	Intersects With	Security, Compliance & Resilience Governance Policy	GOV-01	Mechanisms exist to establish a formal, documented security, compliance and resilience governance policy that: (1) Conveys executive management's intent; (2) Provides organizational direction and expected behaviors; (3) Is reviewed at least annually; and (4) Is updated, as necessary, to adapt to evolving risks, threats and other changes that affect the organization.	5		
III.7.a	Fit and Proper Criteria for Promoters and Directors	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
III.7.a.i	Record of Fairness and Integrity	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
III.7.a.i.a	N/A	Financial integrity.	Functional	Intersects With	Personnel Screening	HRS-05	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	5		HRS-04
III.7.a.i.b	N/A	Good reputation and character.	Functional	Intersects With	Personnel Screening	HRS-05	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	5		HRS-04
III.7.a.i.c	N/A	Honesty.	Functional	Intersects With	Personnel Screening	HRS-05	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	5		HRS-04
III.7.a.ii	Disqualifications	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
III.7.a.ii.a	N/A	Convicted by a court for any offence involving moral turpitude or any economic offence or any offence under the laws administered by the RBI.	Functional	Intersects With	Personnel Screening	HRS-05	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	5		HRS-04
III.7.a.ii.b	N/A	Adjudged insolvent and not discharged.	Functional	Intersects With	Personnel Screening	HRS-05	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	5		HRS-04
III.7.a.ii.c	N/A	An order, restraining, prohibiting or debarring the person from accessing / dealing in any financial system, passed by any regulatory authority, and the period specified in the order has not elapsed.	Functional	Intersects With	Personnel Screening	HRS-05	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	5		HRS-04
III.7.a.ii.d	N/A	Found to be of unsound mind by a court of competent jurisdiction and the finding is in force.	Functional	Intersects With	Personnel Screening	HRS-05	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	5		HRS-04
III.7.a.ii.e	N/A	Is financially not sound.	Functional	Intersects With	Personnel Screening	HRS-05	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	5		HRS-04
III.7.b	N/A	The promoters and directors of the applicant entity may submit a declaration in the enclosed format (Annexure 2.5). RBI may also check 'fit and proper' status of the applicant entity and management thereof by obtaining inputs from other regulators, government departments, etc., as deemed fit. As regards fulfilment of 'fit and proper' criteria, RBI's decision shall be final.	Functional	Intersects With	Personnel Screening	HRS-05	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	3		HRS-04
III.7.c	N/A	Any takeover or acquisition of control or change in the management of a non-bank PA shall adhere to RBI circular CO.DPSS.POLC.No.S-590/02-14-006/2022-23 dated July 4, 2022 on 'Requirement for obtaining prior approval in case of takeover / acquisition of control of non-bank PSOs and sale / transfer of payment system activity of non-bank PSO', as amended from time to time. This provision shall also apply to an entity whose application for authorisation as PA is pending with RBI.	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.	5		GOV-20
III.8	Dispute Management Framework	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
III.8.a	N/A	A PA shall have a dispute resolution mechanism to handle payment related disputes in transactions facilitated by it. The mechanism should also include timelines for processing refunds, etc. The policy shall ensure adherence to the instructions issued by RBI including on Turn Around Time (TAT) for resolution of failed transactions issued vide DPSS.CO.PD No.629/02.01.014/2019-20 dated September 20, 2019 (as amended from time to time). This includes assigning of proper reason codes, responding to chargeback, disputes raised against their onboarded merchants, etc.	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
III.8.a	N/A	A PA shall have a dispute resolution mechanism to handle payment related disputes in transactions facilitated by it. The mechanism should also include timelines for processing refunds, etc. The policy shall ensure adherence to the instructions issued by RBI including on Turn Around Time (TAT) for resolution of failed transactions issued vide DPSS.CO.PD No.629/02.01.014/2019-20 dated September 20, 2019 (as amended from time to time). This includes assigning of proper reason codes, responding to chargeback, disputes raised against their onboarded merchants, etc.	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
III.8.b	N/A	Agreements between a PA, its merchants, its acquiring banks, and all other stakeholders shall clearly delineate the roles and responsibilities of the involved parties, inter alia covering manner of refunds, treatment of failed transactions, return policy, grievance redressal, reconciliation, etc.	Functional	Intersects With	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-11	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for security, compliance and resilience controls between internal stakeholders and External Service Providers (ESPs).	3		TPM-05.4
III.8.b	N/A	Agreements between a PA, its merchants, its acquiring banks, and all other stakeholders shall clearly delineate the roles and responsibilities of the involved parties, inter alia covering manner of refunds, treatment of failed transactions, return policy, grievance redressal, reconciliation, 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
III.8.c	N/A	The PA shall disclose comprehensive information regarding its merchant policies, privacy policy and other terms and conditions on its website and / or its mobile application.	Functional	Intersects With	Data Privacy Notice	PRI-21	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations; (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	5		PRI-02
III.8.c	N/A	The PA shall disclose comprehensive information regarding its merchant policies, privacy policy and other terms and conditions on its website and / or its mobile application.	Functional	Intersects With	Conspicuous Link To Data Privacy Notice	PRI-21.2	Mechanisms exist to include a conspicuous link to the organization's data privacy notice on all consumer-facing websites and mobile applications.	3		PRI-17.1
III.8.d	N/A	The PA shall appoint an officer responsible for responding to issues raised by its merchants along with an escalation matrix for grievance redressal. Details of the officer and escalation matrix shall be prominently displayed on its website.	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
III.8.d	N/A	The PA shall appoint an officer responsible for responding to issues raised by its merchants along with an escalation matrix for grievance redressal. Details of the officer and escalation matrix shall be prominently displayed on its website.	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
III.8.d	N/A	The PA shall appoint an officer responsible for responding to issues raised by its merchants along with an escalation matrix for grievance redressal. Details of the officer and escalation matrix shall be prominently displayed on its website.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-05	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	3		GOV-04
III.9	Security, Fraud Prevention and Risk Management Framework	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 Regulation of Payment Aggregators (PA) (2025)**
Focal Document URL: https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12896
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-ind-rbi-pa-2025.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 #
III.9.a	N/A	A strong risk management system is necessary to meet the challenges of fraud and ensure customer protection. PA shall put in place adequate Information and Data Security infrastructure and systems for detection and prevention of frauds. PA shall ensure that infrastructure of the merchants is compliant with security standards like PCI-DSS and PCI-SSF, as may be applicable.	Functional	Intersects With	Continuous Monitoring	MON-02	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	3		MON-01
III.9.a	N/A	A strong risk management system is necessary to meet the challenges of fraud and ensure customer protection. PA shall put in place adequate Information and Data Security infrastructure and systems for detection and prevention of frauds. PA shall ensure that infrastructure of the merchants is compliant with security standards like PCI-DSS and PCI-SSF, as may be applicable.	Functional	Intersects With	Risk Management Program	RSK-02	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls that are aligned with: (1) The organization's Enterprise Risk Management (ERM); and (2) Industry-recognized cybersecurity risk management practices.	5		RSK-01
III.9.a	N/A	A strong risk management system is necessary to meet the challenges of fraud and ensure customer protection. PA shall put in place adequate Information and Data Security infrastructure and systems for detection and prevention of frauds. PA shall ensure that infrastructure of the merchants is compliant with security standards like PCI-DSS and PCI-SSF, as may be applicable.	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
III.9.a	N/A	A strong risk management system is necessary to meet the challenges of fraud and ensure customer protection. PA shall put in place adequate Information and Data Security infrastructure and systems for detection and prevention of frauds. PA shall ensure that infrastructure of the merchants is compliant with security standards like PCI-DSS and PCI-SSF, as may be applicable.	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.	3		TPM-08
III.9.b	N/A	PA shall put in place a Board approved Information Security Policy for safety and security of the payment systems operated by it and implement security measures in accordance with the said policy to mitigate identified as well as emerging risks. PA shall ensure adherence to baseline technology-related recommendations as provided in Annexure 1.	Functional	Intersects With	Security, Compliance & Resilience Program (SCRP)	GOV-02	Mechanisms exist to facilitate the design, implementation, and monitoring of security, compliance and resilience governance controls.	5		GOV-01
III.9.b	N/A	PA shall put in place a Board approved Information Security Policy for safety and security of the payment systems operated by it and implement security measures in accordance with the said policy to mitigate identified as well as emerging risks. PA shall ensure adherence to baseline technology-related recommendations as provided in Annexure 1.	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
III.9.c	N/A	PA shall comply with data storage requirements as applicable to Payment System Operators (PSOs) as laid out in RBI circular DPSS.CO.OD No.2785/06.08.005/2017-2018 dated April 6, 2018 on 'Storage of Payment System Data', as amended from time to time.	Functional	Intersects With	Geographic Data Location	DCH-30	Mechanisms exist to inventory, document and maintain data flows for data that is resident (permanently or temporarily) within geographically distributed Technology Assets, Applications and/or Services (TAAS) (physical and virtual).	5		DCH-19
III.9.c	N/A	PA shall comply with data storage requirements as applicable to Payment System Operators (PSOs) as laid out in RBI circular DPSS.CO.OD No.2785/06.08.005/2017-2018 dated April 6, 2018 on 'Storage of Payment System Data', as amended from time to time.	Functional	Intersects With	Data Localization	DCH-31	Mechanisms exist to constrain the impact of "digital sovereignty laws," that require localized data within the host country, where data and processes may be subjected to arbitrary enforcement actions that potentially violate other applicable statutory, regulatory and/or contractual obligations.	5		DCH-26
III.9.d	N/A	An annual system audit, including cyber security audit, conducted by CERT-In empanelled auditors shall be carried out and report thereof shall be submitted to the respective Regional Office of DPSS, RBI within such timelines as may be prescribed by RBI.	Functional	Intersects With	Periodic Audits	CPL-07.2	Mechanisms exist to conduct periodic audits of security, compliance and resilience controls to evaluate conformity with the organization's documented policies, standards and procedures.	5		CPL-02.2
III.9.d	N/A	An annual system audit, including cyber security audit, conducted by CERT-In empanelled auditors shall be carried out and report thereof shall be submitted to the respective Regional Office of DPSS, RBI within such timelines as may be prescribed by RBI.	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
III.9.d	N/A	An annual system audit, including cyber security audit, conducted by CERT-In empanelled auditors shall be carried out and report thereof shall be submitted to the respective Regional Office of DPSS, RBI within such timelines as may be prescribed by 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
III.9.e	N/A	The PA shall also be guided by RBI circular CO.DPSS.OVRST.No.S447/06-26-002/2024-25 dated July 30, 2024 on 'Master Directions on Cyber Resilience and Digital Payment Security Controls for non-bank Payment System Operators', 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.	5		CPL-01
III.10	General Directions	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
III.10.a	N/A	A PA shall aggregate funds only for the merchant with whom it has a contractual relationship.	Functional	No Relationship	N/A	N/A	N/A	0		
III.10.b	N/A	A PA business shall not carry out marketplace business.	Functional	No Relationship	N/A	N/A	N/A	0		
III.10.c	N/A	A PA shall ensure that the extant instructions with regard to Merchant Discount Rate (MDR) are followed. A PA shall also ensure that any charges, other than the price of goods / service / investment amount, charged by a merchant, are distinctly displayed to the payer prior to the transaction.	Functional	No Relationship	N/A	N/A	N/A	0		
III.10.d	N/A	A PA shall not place limits on transaction amount for a particular payment mode. The responsibility thereof shall lie with the issuing bank / non-bank entity; for instance, the card issuing bank shall be responsible for placing transaction amount limits on cards issued by it based on the customer's credit worthiness, spending nature, profile, etc.	Functional	No Relationship	N/A	N/A	N/A	0		
III.10.e	N/A	A PA shall not give an option for ATM PIN as a factor of authentication for card-not-present transactions.	Functional	Intersects With	Authenticator Management	IAC-14	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	3		IAC-10
III.10.f	N/A	All refunds shall be made to the original method of payment, unless specifically instructed by the payer to credit the refund to an alternate mode belonging to the same payer.	Functional	No Relationship	N/A	N/A	N/A	0		
III.10.g	N/A	A PG, as defined in paragraph 4(j), shall not fall within the scope of this MD. However, a PG is encouraged to adopt the baseline technology recommendations of the Reserve Bank of India (appended as Annexure 1).	Functional	No Relationship	N/A	N/A	N/A	0		
III.10.h	N/A	A PA may avail services of a PG in terms of RBI circulars DoS.CO.CSITEG/SEC.1/31.01.015/2023-24 dated April 10, 2023 on 'Master Direction on Information Technology Services', CO.DPSS.POLC.No.S-384/02.32.001/2021-2022 dated August 3, 2021 on 'Framework for Outsourcing of Payment and Settlement-related Activities by Payment System Operators', and DBOD.NO.BP.40/21.04.158/2006-07 dated November 3, 2006 on 'Managing Risks and Code of Conduct in Outsourcing of Financial Services by banks', as applicable and amended from time to time.	Functional	Intersects With	Third-Party Management	TPM-02	Mechanisms exist to facilitate the implementation of third-party management controls.	5		TPM-01
III.10.h	N/A	A PA may avail services of a PG in terms of RBI circulars DoS.CO.CSITEG/SEC.1/31.01.015/2023-24 dated April 10, 2023 on 'Master Direction on Information Technology Services', CO.DPSS.POLC.No.S-384/02.32.001/2021-2022 dated August 3, 2021 on 'Framework for Outsourcing of Payment and Settlement-related Activities by Payment System Operators', and DBOD.NO.BP.40/21.04.158/2006-07 dated November 3, 2006 on 'Managing Risks and Code of Conduct in Outsourcing of Financial Services by banks', as applicable and amended from time to time.	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).	3		TPM-04.1
III.11	Specific Directions Applicable to PA - CB (Cross Border)	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
III.11.a	N/A	Funds related to inward and outward transactions as carried out by a PA-CB shall be kept separate. No co-mingling of funds or netting off for outward and inward transactions is permitted under any circumstance.	Functional	No Relationship	N/A	N/A	N/A	0		
III.11.b	N/A	For outward transactions, a PA - CB may directly on-board merchants located abroad or enter into agreement with e-commerce marketplaces or entities providing PA services abroad.	Functional	No Relationship	N/A	N/A	N/A	0		
III.11.c	N/A	Outward transactions can be carried out using any payment instrument provided by authorised payment systems in India, except small Prepaid Payment Instrument.	Functional	No Relationship	N/A	N/A	N/A	0		
III.11.d	N/A	A PA-CB shall not purchase foreign currency from, or sell it to, any entity other than an Authorised Dealer (AD). In respect of inward or outward transactions processed by a PA - CB, the maximum value per transaction shall be Rs.25 lakh.	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 Regulation of Payment Aggregators (PA) (2025)
Focal Document URL: https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12896
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-ind-rbi-pa-2025.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 #
III.11.e	N/A	AD-I banks maintaining Inward Collection Accounts (InCAs) / Outward Collection Accounts (OCAs), as defined in paragraph 16(a) of this MD, shall ensure that all requirements under FEMA are adhered to.	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
III.11.f	N/A	AD-I Bank shall have automated processes to fetch the requisite information from a PA - CB.	Functional	No Relationship	N/A	N/A	N/A	0		
III.11.g	N/A	To establish the bonafides of a transaction, the payment transaction (outward / inward) shall be identified as a cross-border transaction. A Payment System Provider shall make provisions for implementation of the same from such timelines as specified by RBI.	Functional	No Relationship	N/A	N/A	N/A	0		
III.11.h	N/A	PA - CB shall provide the documents / information required by the exporter / importer to the AD bank of the exporter / importer, for closure of their corresponding entry in Export Data Processing and Monitoring System (EDPMS) / Import Data Processing and Management System (IDPMS), wherever applicable, (for the respective inward / outward remittance), in compliance with the extant directions.	Functional	No Relationship	N/A	N/A	N/A	0		
III.11.i	N/A	Settlement in non-INR currencies shall be permitted only for those merchants (Indian exporters) which have been directly onboarded by the PA - CB facilitating inward transactions.	Functional	No Relationship	N/A	N/A	N/A	0		
III.12	N/A	An authorised PA shall submit reports as listed in Annexure 2 of this MD.	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
IV	KYC and Due Diligence	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
IV.13	Due Diligence by PA	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
IV.13.a	N/A	A PA shall undertake customer due diligence (CDD) of its merchants in accordance with MD on KYC. While onboarding, the PA shall, with the merchant's consent, retrieve the merchant's KYC record from CKYCR. The process defined in MD on KYC should be followed in case CKYCR record is found to be not updated.	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
IV.13.a	N/A	A PA shall undertake customer due diligence (CDD) of its merchants in accordance with MD on KYC. While onboarding, the PA shall, with the merchant's consent, retrieve the merchant's KYC record from CKYCR. The process defined in MD on KYC should be followed in case CKYCR record is found to be not updated.	Functional	Intersects With	Identity Evidence Validation & Verification	IAC-05.3	Mechanisms exist to require that the presented identity evidence be validated and verified through organizational-defined methods of validation and verification.	3		IAC-28.3
IV.13.b	Alternative CDD Process for Low-Turnover Merchants	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
IV.13.b.i	N/A	Obtain a copy of the PAN / Form 60 of the merchant and verify the PAN from issuing authority.	Functional	Intersects With	Identity Evidence	IAC-05.2	Mechanisms exist to require evidence of individual identification to be presented to the registration authority.	5		IAC-28.2
IV.13.b.i	N/A	Obtain a copy of the PAN / Form 60 of the merchant and verify the PAN from issuing authority.	Functional	Intersects With	Identity Evidence Validation & Verification	IAC-05.3	Mechanisms exist to require that the presented identity evidence be validated and verified through organizational-defined methods of validation and verification.	5		IAC-28.3
IV.13.b.ii	N/A	Conduct CPV of the merchant.	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
IV.13.b.ii	N/A	Conduct CPV of the merchant.	Functional	Intersects With	Address Confirmation	IAC-05.5	Mechanisms exist to require that a notice of proofing be delivered through an out-of-band channel to verify the user's address (physical or digital).	5		IAC-28.5
IV.13.b.iii	N/A	Obtain a certified copy of one officially valid document (OVD) of the proprietor or of the person holding power of attorney to operate the account, as applicable. One of the documents or the equivalent e-documents, as prescribed for CDD of sole-proprietary firms or legal entities, should be verified.	Functional	Intersects With	Identity Evidence	IAC-05.2	Mechanisms exist to require evidence of individual identification to be presented to the registration authority.	5		IAC-28.2
IV.13.b.iii	N/A	Obtain a certified copy of one officially valid document (OVD) of the proprietor or of the person holding power of attorney to operate the account, as applicable. One of the documents or the equivalent e-documents, as prescribed for CDD of sole-proprietary firms or legal entities, should be verified.	Functional	Intersects With	Identity Evidence Validation & Verification	IAC-05.3	Mechanisms exist to require that the presented identity evidence be validated and verified through organizational-defined methods of validation and verification.	5		IAC-28.3
IV.13.c	N/A	A PA shall undertake background and antecedent check of the merchant.	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
IV.13.d	N/A	In case a PA contracts with another PA that onboards the merchant, the latter is responsible for carrying out due diligence of the merchant.	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).	3		TPM-04.1
IV.13.e	N/A	PA shall facilitate allotment of appropriate Merchant Category Code and Merchant ID / Terminal ID to its merchants including those onboarded through an overseas PA. PA shall ensure that name of the merchant is captured appropriately for all transactions processed for it.	Functional	Intersects With	Standardized Identifier Management (User Names)	IAC-13.1	Mechanisms exist to govern naming standards for usernames and Technology Assets, Applications and/or Services (TAAS).	3		IAC-09
IV.13.f	N/A	A PA shall ensure that a marketplace onboarded by it does not accept payments for a seller not onboarded on to the marketplace's platform.	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.	3		TPM-08
IV.13.g	N/A	Necessary validation mechanisms shall be put in place by a PA to ensure that funds due to a merchant are credited in the merchant's bank account only.	Functional	Intersects With	Input Data Validation	TDA-12	Mechanisms exist to check the validity of information inputs.	3		TDA-18
IV.13.h	N/A	The PA must also monitor transactions subsequently undertaken by the merchants to ensure that these transactions are in line with latter's business profile and ensure adherence to other aspects of MD on KYC while conducting its operations.	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
IV.13.h	N/A	The PA must also monitor transactions subsequently undertaken by the merchants to ensure that these transactions are in line with latter's business profile and ensure adherence to other aspects of MD on KYC while conducting its operations.	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.	3		TPM-08
IV.13.i	N/A	Non-bank PA shall register itself with the Financial Intelligence Unit-India (FIU-IND) in compliance with MD on KYC and meet the reporting requirements listed therein.	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
IV.13.i	N/A	Non-bank PA shall register itself with the Financial Intelligence Unit-India (FIU-IND) in compliance with MD on KYC and meet the reporting requirements listed therein.	Functional	Intersects With	Contacts With Authorities	GOV-15	Mechanisms exist to identify and document appropriate contacts with relevant law enforcement and regulatory bodies.	3		GOV-06
IV.13.j	N/A	A PA, including an existing PA whose application is pending with Reserve Bank of India for authorisation, shall ensure that merchants onboarded till December 31, 2025, comply with the above due diligence requirements within one year from the date of this MD. From January 1, 2026, merchants should be onboarded in accordance with due diligence requirements prescribed in this MD.	Functional	No Relationship	N/A	N/A	N/A	0		
IV.14	Responsibilities of Acquiring Bank	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
IV.14.a	N/A	Acquiring bank shall have a policy for processing payments for merchants acquired through an authorised non-bank PA.	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
IV.14.a	N/A	Acquiring bank shall have a policy for processing payments for merchants acquired through an authorised non-bank PA.	Functional	Intersects With	Third-Party Management	TPM-02	Mechanisms exist to facilitate the implementation of third-party management controls.	3		TPM-01
IV.14.b	N/A	Acquiring bank need not undertake the customer due diligence of the merchant itself but should be able to obtain the required details whenever required.	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
IV.14.c	N/A	Acquiring Bank of a non-bank PA shall ensure that merchants onboarded by the PA are in compliance with acquiring bank's policy for merchant acquiring.	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
IV.14.c	N/A	Acquiring Bank of a non-bank PA shall ensure that merchants onboarded by the PA are in compliance with acquiring bank's policy for merchant acquiring.	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
IV.15	Due Diligence through Assisted Mode	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 Regulation of Payment Aggregators (PA) (2025)**
Focal Document URL: https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12896
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-ind-rbi-pa-2025.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 #
IV.15.a	Agent Activities Permitted for Due Diligence	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
IV.15.a.i	N/A	Digital KYC process as provided in Annex - I of MD - KYC (in lieu of Business Correspondents).	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
IV.15.a.i	N/A	Digital KYC process as provided in Annex - I of MD - KYC (in lieu of Business Correspondents).	Functional	Intersects With	Identity Evidence Validation & Verification	IAC-05.3	Mechanisms exist to require that the presented identity evidence be validated and verified through organizational-defined methods of validation and verification.	3		IAC-28.3
IV.15.a.ii	N/A	Assisted V-CIP, only by the agent assisting the individual / proprietor / power of attorney holder / beneficial owner / authorised signatory of the merchant, in terms of Paragraph 18 of MD on KYC. PA shall maintain the details of the agent assisting the merchant, where services of such agents are employed.	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
IV.15.a.ii	N/A	Assisted V-CIP, only by the agent assisting the individual / proprietor / power of attorney holder / beneficial owner / authorised signatory of the merchant, in terms of Paragraph 18 of MD on KYC. PA shall maintain the details of the agent assisting the merchant, where services of such agents are employed.	Functional	Intersects With	Identity Evidence Validation & Verification	IAC-05.3	Mechanisms exist to require that the presented identity evidence be validated and verified through organizational-defined methods of validation and verification.	3		IAC-28.3
IV.15.b	N/A	The non-bank PA shall carry out 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).	3		TPM-04.1
IV.15.b	N/A	The non-bank PA shall carry out due diligence of the persons appointed as authorised / designated agents.	Functional	Intersects With	Third-Party Personnel Security	TPM-13	Mechanisms exist to control personnel security requirements including security roles and responsibilities for third-party providers.	5		TPM-06
IV.15.c	N/A	The ultimate responsibility of due diligence shall lie on PA and agents can only be used for limited purposes as prescribed above.	Functional	Intersects With	Third-Party Management	TPM-02	Mechanisms exist to facilitate the implementation of third-party management controls.	3		TPM-01
V	Settlement of Funds and Escrow Accounts	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
V.16	Escrow Accounts of PA	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
V.16.a	N/A	A non-bank PA shall maintain the funds collected on behalf of its merchants in a separate escrow account with any Scheduled Commercial Bank (SCB) in India. In case of a PA - CB, such account shall also be referred to as Inward Collection Account (InCA) for inward transactions and Outward Collection Account (OCA) for outward transactions, as applicable. Details of operations in escrow accounts are incorporated in Table 1 (Escrow Account Requirements) which specifies general requirements, operational requirements (including pre-funding, additional accounts, inter-escrow transfers), permitted credits, permitted debits, day-end balance maintenance, interest provisions, and timelines for domestic escrow accounts, InCA, and OCA. Instructions therein must be adhered to by December 31, 2025. Such escrow accounts shall only be utilised for authorised PA business and not for any other business.	Functional	No Relationship	N/A	N/A	N/A	0		
V.16.b	N/A	For the purposes of maintenance of an escrow account, payment system operated by PA shall be deemed to be 'designated payment systems' under Section 23A of the Payment and Settlements Systems Act, 2007.	Functional	No Relationship	N/A	N/A	N/A	0		
V.17	Core Portion of Escrow Accounts	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
V.17.a	N/A	The core portion of escrow account shall continue to be maintained within the escrow account maintained for PA activity.	Functional	No Relationship	N/A	N/A	N/A	0		
V.17.b	N/A	This facility shall be permissible to entities who have been in business for twenty-six (26) fortnights and whose accounts have been duly audited for the full accounting year. For this purpose, the period of twenty-six fortnights shall be calculated from the date of actual business operation in the account.	Functional	No Relationship	N/A	N/A	N/A	0		
V.17.c	N/A	No loan is permissible against the core portion. Banks shall not issue any receipt for such deposits which may entitle PA to the funds available in the core portion or mark any lien on the amount held in such form of deposits.	Functional	No Relationship	N/A	N/A	N/A	0		
V.17.d	N/A	The core portion shall be calculated separately for each escrow account. The escrow balance maintained shall be clearly disclosed in the auditor's certificates to be submitted to RBI on quarterly and annual basis.	Functional	No Relationship	N/A	N/A	N/A	0		
V.18	General Directions on Escrow Account of PA	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
V.18.a	N/A	PA shall submit the list of merchants onboarded by it to the bank where it is maintaining the escrow account and update the list prior to initiating settlement to these merchants. This list includes eligible third parties to which PA - O or PA - P would be settling funds on the instructions of the merchant as detailed in permitted debits in Table 1 above. The bank shall ensure that payments are made only to eligible merchants and for permissible debits or credits as defined under this MD. There shall be an exclusive clause in the agreement signed between the PA and the bank maintaining escrow account towards usage of balance in escrow account only as per the permissible debits or credits as mentioned in Table 1 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
V.18.b	N/A	The escrow account shall not be operated for 'Cash-on-Delivery' transactions.	Functional	No Relationship	N/A	N/A	N/A	0		
V.18.c	N/A	Funds for an outward transaction may be received in the escrow account of the PA (and then transferred to the OCA of PA - CB) or directly in OCA of the PA - CB. Onward transfer to the foreign merchants shall be carried out only by debit to the OCA.	Functional	No Relationship	N/A	N/A	N/A	0		
V.18.d	N/A	In case a PA-CB also engages in domestic PA activity, InCA and OCA shall be kept separate from the escrow account(s) opened for such domestic PA activity.	Functional	No Relationship	N/A	N/A	N/A	0		
V.18.e	N/A	A certificate, signed by the statutory auditor(s), shall be submitted by the authorised entities to the respective Regional Office of DPSS, RBI, where registered office of PA is situated, certifying that the entity has been maintaining balance(s) in the escrow account(s) in compliance with these instructions, as per periodicity prescribed in Annexure 2. In case an additional escrow account is being maintained, it shall be ensured that balances in both accounts are considered for the above certification and that these are separately mentioned in the certificate. The certificates shall be submitted separately for domestic activity, i.e. PA - O / P and cross border activity, i.e. PA - CB.	Functional	No Relationship	N/A	N/A	N/A	0		
V.18.f	N/A	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 impacting the payment cycle to merchants, under advice to RBI.	Functional	No Relationship	N/A	N/A	N/A	0		
V.18.g	N/A	For banks, the outstanding balance in the escrow account shall be part of the 'net demand and time liabilities' (NDTL) for the purposes of maintenance of reserve requirements. This position shall 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		
V.18.h	N/A	Credits towards reversed transactions (where funds are received by PA) and refund transactions shall be routed back through the escrow account unless the refund is directly managed by the merchant and the payer has been made aware of the same, in terms of the contract between a PA and merchant. The chargeback rights of customers, as applicable, shall remain unaffected.	Functional	No Relationship	N/A	N/A	N/A	0		
VI	Repeal and Savings	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
VI.19	Circulars Repealed	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
VI.19.a	N/A	A.P. (DIR Series) Circular No. 17 dated November 16, 2010 on 'Processing and Settlement of Export related receipts facilitated by Online Payment Gateways' is hereby repealed except for an existing PA - CB which had applied for authorisation as PA - CB on or before April 30, 2024 and a decision thereon is pending with the Reserve Bank of India.	Functional	No Relationship	N/A	N/A	N/A	0		
VI.19.b	N/A	A.P. (DIR Series) Circular No. 109 dated June 11, 2013 on 'Processing and Settlement of Export related receipts facilitated by Online Payment Gateways - Enhancement of the value of transaction' is hereby repealed except for an existing PA - CB which had applied for authorisation as PA - CB on or before April 30, 2024 and a decision thereon is pending with the Reserve Bank of India.	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 Regulation of Payment Aggregators (PA) (2025)**
Focal Document URL: https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12896
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-ind-rbi-pa-2025.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 #
VI.19.c	N/A	A.P. (DIR Series) Circular No.16 dated September 24, 2015 on 'Processing and settlement of import and export related payments facilitated by Online Payment Gateway Service Providers' is hereby repealed except for an existing PA - CB which had applied for authorisation as PA - CB on or before April 30, 2024 and a decision thereon is pending with the Reserve Bank of India.	Functional	No Relationship	N/A	N/A	N/A	0		
VI.20	N/A	The circular DPSS.CO.PD.No.1102/02.14.08/2009-10 dated November 24, 2009 on 'Directions for opening and operation of Accounts and settlement of payments for electronic payment transactions involving intermediaries' is hereby repealed except only in relation to an existing PA - O which has sought authorisation and a decision thereon is pending with the Reserve Bank of India.	Functional	No Relationship	N/A	N/A	N/A	0		
VI.21	N/A	Save as provided herein, circulars listed in Annexure - 3 stands repealed with the issuance of this MD.	Functional	No Relationship	N/A	N/A	N/A	0		
VI.22	N/A	Notwithstanding such repeal as aforementioned, all authorisation / approvals granted, actions taken, and acknowledgements issued under the aforesaid circulars / Directions shall continue to be valid and shall be deemed to have been granted under this MD.	Functional	No Relationship	N/A	N/A	N/A	0		
VI.23	N/A	The circulars, directions and guidelines so repealed shall be deemed to have been in force until the date of coming into effect of this MD.	Functional	No Relationship	N/A	N/A	N/A	0		
Annex 1	Baseline Technology-related Recommendations	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
Annex 1.1	Security-related Recommendations	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
Annex 1.1.1	N/A	Information Security Governance: The entities at a minimum shall carry out comprehensive security risk assessment of their people, IT, business process environment, etc., to identify risk exposures with remedial measures and residual risks. These can be an internal security audit or an annual security audit by an independent security auditor or a CERT-In empanelled auditor. Reports on risk assessment, security compliance posture, security audit reports and security incidents shall be presented to the Board.	Functional	Intersects With	Periodic Audits	CPL-07.2	Mechanisms exist to conduct periodic audits of security, compliance and resilience controls to evaluate conformity with the organization's documented policies, standards and procedures.	3		CPL-02.2
Annex 1.1.1	N/A	Information Security Governance: The entities at a minimum shall carry out comprehensive security risk assessment of their people, IT, business process environment, etc., to identify risk exposures with remedial measures and residual risks. These can be an internal security audit or an annual security audit by an independent security auditor or a CERT-In empanelled auditor. Reports on risk assessment, security compliance posture, security audit reports and security incidents shall be presented to the Board.	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
Annex 1.1.1	N/A	Information Security Governance: The entities at a minimum shall carry out comprehensive security risk assessment of their people, IT, business process environment, etc., to identify risk exposures with remedial measures and residual risks. These can be an internal security audit or an annual security audit by an independent security auditor or a CERT-In empanelled auditor. Reports on risk assessment, security compliance posture, security audit reports and security incidents shall be presented to the Board.	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
Annex 1.1.2	N/A	Data Security Standards: Data security standards and best practices like PCI-DSS, PCI-SSF, latest encryption standards, transport channel security, etc., shall be implemented.	Functional	Intersects With	Use of Cryptographic Controls	CRY-02	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	5		CRY-01
Annex 1.1.2	N/A	Data Security Standards: Data security standards and best practices like PCI-DSS, PCI-SSF, latest encryption standards, transport channel security, etc., shall be implemented.	Functional	Intersects With	Encrypting Data In Transit	CRY-05	Cryptographic mechaniams exist to prevent the unauthorized disclosure of data in transit.	3		CRY-03
Annex 1.1.2	N/A	Data Security Standards: Data security standards and best practices like PCI-DSS, PCI-SSF, latest encryption standards, transport channel security, etc., shall be implemented.	Functional	Intersects With	Data Protection	DCH-02	Mechanisms exist to facilitate the implementation of data protection controls.	5		DCH-01
Annex 1.1.3	N/A	Security Incident Reporting: The entities shall report security incidents / card holder data breaches to RBI within the stipulated timeframe to RBI. Monthly cyber security incident reports with root cause analysis and preventive actions undertaken shall be submitted to RBI.	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-14	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.	3		IRO-13
Annex 1.1.3	N/A	Security Incident Reporting: The entities shall report security incidents / card holder data breaches to RBI within the stipulated timeframe to RBI. Monthly cyber security incident reports with root cause analysis and preventive actions undertaken shall be submitted to RBI.	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
Annex 1.1.3	N/A	Security Incident Reporting: The entities shall report security incidents / card holder data breaches to RBI within the stipulated timeframe to RBI. Monthly cyber security incident reports with root cause analysis and preventive actions undertaken shall be submitted to RBI.	Functional	Intersects With	Serious Incident Reporting	IRO-16.3	Mechanisms exist to report any serious incident involving the organization's Technology Assets, Applications, Services and/or Data (TAASD) to relevant authorities in the locality where the incident occurred, in accordance with mandatory reporting: (1) Requirements; and (2) Timelines.	5		IRO-10.5
Annex 1.1.4	N/A	Merchant Onboarding: The entities shall undertake comprehensive security assessment during merchant onboarding process to ensure these minimal baseline security controls are adhered to by the merchants.	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
Annex 1.1.4	N/A	Merchant Onboarding: The entities shall undertake comprehensive security assessment during merchant onboarding process to ensure these minimal baseline security controls are adhered to by the merchants.	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
Annex 1.1.5	N/A	Cyber Security Audit and Reports: The entities shall carry out and submit to the IT Committee quarterly internal and annual external audit reports; bi-annual Vulnerability Assessment / Penetration Test (VAPT) reports; PCI-DSS including Attestation of Compliance (AOC) and Report of Compliance (ROC) compliance report with observations noted if any including corrective / preventive actions planned with action closure date; inventory of applications which store or process or transmit customer sensitive data; PCI-SSF compliance status of payment applications which stores or processes card holder data.	Functional	Intersects With	Compliance-Specific Asset Identification	AST-16.1	Mechanisms exist to create and maintain a current inventory of Technology Assets, Applications, Services and/or Data (TAASD) that are in scope for statutory, regulatory and/or contractual compliance obligations providing sufficient detail to determine control applicability, based on asset scope categorization.	3		AST-04.3
Annex 1.1.5	N/A	Cyber Security Audit and Reports: The entities shall carry out and submit to the IT Committee quarterly internal and annual external audit reports; bi-annual Vulnerability Assessment / Penetration Test (VAPT) reports; PCI-DSS including Attestation of Compliance (AOC) and Report of Compliance (ROC) compliance report with observations noted if any including corrective / preventive actions planned with action closure date; inventory of applications which store or process or transmit customer sensitive data; PCI-SSF compliance status of payment applications which stores or processes card holder data.	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
Annex 1.1.5	N/A	Cyber Security Audit and Reports: The entities shall carry out and submit to the IT Committee quarterly internal and annual external audit reports; bi-annual Vulnerability Assessment / Penetration Test (VAPT) reports; PCI-DSS including Attestation of Compliance (AOC) and Report of Compliance (ROC) compliance report with observations noted if any including corrective / preventive actions planned with action closure date; inventory of applications which store or process or transmit customer sensitive data; PCI-SSF compliance status of payment applications which stores or processes card holder data.	Functional	Intersects With	Vulnerability Scanning	VPM-12	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	3		VPM-06
Annex 1.1.5	N/A	Cyber Security Audit and Reports: The entities shall carry out and submit to the IT Committee quarterly internal and annual external audit reports; bi-annual Vulnerability Assessment / Penetration Test (VAPT) reports; PCI-DSS including Attestation of Compliance (AOC) and Report of Compliance (ROC) compliance report with observations noted if any including corrective / preventive actions planned with action closure date; inventory of applications which store or process or transmit customer sensitive data; PCI-SSF compliance status of payment applications which stores or processes card holder data.	Functional	Intersects With	Penetration Testing	VPM-18	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	5		VPM-07
Annex 1.1.6	N/A	Information Security: Board approved information security policy shall be reviewed at least annually. The policy shall consider aspects like: alignment with business objectives; the objectives, scope, ownership and responsibility for the policy; information security organisational structure; information security roles and responsibilities; maintenance of asset inventory and registers; data classification; authorisation; exceptions; knowledge and skill sets required; periodic training and continuous professional education; compliance review and penal measures for non-compliance of policies.	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

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 Regulation of Payment Aggregators (PA) (2025)**
Focal Document URL: https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12896
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-ind-rbi-pa-2025.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 #
Annex 1.1.6	N/A	Information Security: Board approved information security policy shall be reviewed at least annually. The policy shall consider aspects like: alignment with business objectives; the objectives, scope, ownership and responsibility for the policy; information security organisational structure; information security roles and responsibilities; maintenance of asset inventory and registers; data classification; authorisation; exceptions; knowledge and skill sets required; periodic training and continuous professional education; compliance review and penal measures for non-compliance of policies.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-04.1	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5		GOV-03
Annex 1.1.6	N/A	Information Security: Board approved information security policy shall be reviewed at least annually. The policy shall consider aspects like: alignment with business objectives; the objectives, scope, ownership and responsibility for the policy; information security organisational structure; information security roles and responsibilities; maintenance of asset inventory and registers; data classification; authorisation; exceptions; knowledge and skill sets required; periodic training and continuous professional education; compliance review and penal measures for non-compliance of policies.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-05	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	3		GOV-04
Annex 1.1.7	IT Governance	N/A	Functional	Intersects With	Security, Compliance & Resilience Governance Policy	GOV-01	Mechanisms exist to establish a formal, documented security, compliance and resilience governance policy that: (1) Conveys executive management's intent; (2) Provides organizational direction and expected behaviors; (3) Is reviewed at least annually; and (4) Is updated, as necessary, to adapt to evolving risks, threats and other changes that affect the organization.	5		
Annex 1.1.7.1	N/A	Involvement of Board: The major role of the Board / Top Management shall involve approving information security policies, establishing necessary organisational processes / functions for information security and providing necessary resources.	Functional	Intersects With	Security, Compliance & Resilience Program (SCRP)	GOV-02	Mechanisms exist to facilitate the design, implementation, and monitoring of security, compliance and resilience governance controls.	5		GOV-01
Annex 1.1.7.1	N/A	Involvement of Board: The major role of the Board / Top Management shall involve approving information security policies, establishing necessary organisational processes / functions for information security and providing necessary resources.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-09	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	3		GOV-01.1
Annex 1.1.7.1	N/A	Involvement of Board: The major role of the Board / Top Management shall involve approving information security policies, establishing necessary organisational processes / functions for information security and providing necessary resources.	Functional	Intersects With	Allocation of Resources	PRM-06	Mechanisms exist to identify and allocate resources for management, operational, technical and data protection requirements within business process planning for projects / initiatives.	3		PRM-03
Annex 1.1.7.2	N/A	IT Steering Committee: An IT Steering Committee shall be created with representations from various business functions as appropriate. The Committee shall assist the Executive Management in implementation of the IT strategy approved by the Board. It shall have well defined objectives and actions.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-09	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5		GOV-01.1
Annex 1.1.7.3	N/A	Enterprise Information Model: The entities shall establish and maintain an enterprise information model to enable applications development and decision-supporting activities, consistent with board approved IT strategy. The model shall facilitate optimal creation, use and sharing of information by a business, in a way that it maintains integrity, and is flexible, functional, timely, secure and resilient to failure.	Functional	Intersects With	Sensitive / Regulated Data Governance	DCH-03	Mechanisms exist to facilitate data governance so that sensitive and/or regulated data is effectively managed and maintained in accordance with applicable statutory, regulatory and contractual obligations.	3		GOV-10
Annex 1.1.7.3	N/A	Enterprise Information Model: The entities shall establish and maintain an enterprise information model to enable applications development and decision-supporting activities, consistent with board approved IT strategy. The model shall facilitate optimal creation, use and sharing of information by a business, in a way that it maintains integrity, and is flexible, functional, timely, secure and resilient to failure.	Functional	Intersects With	Alignment With Enterprise Architecture	SEA-04	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for security, compliance and resilience principles that addresses risk to organizational operations, assets, individuals and other organizations.	5		SEA-02
Annex 1.1.7.4	N/A	Cyber Crisis Management Plan: The entities shall prepare a comprehensive Cyber Crisis Management Plan approved by the IT strategic committee and shall include components such as Detection, Containment, Response and Recovery.	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.	3		BCD-01
Annex 1.1.7.4	N/A	Cyber Crisis Management Plan: The entities shall prepare a comprehensive Cyber Crisis Management Plan approved by the IT strategic committee and shall include components such as Detection, Containment, Response and Recovery.	Functional	Intersects With	Incident Response Plan (IRP)	IRO-08	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	8		IRO-04
Annex 1.1.8	N/A	Enterprise Data Dictionary: The entities shall maintain an 'enterprise data dictionary' incorporating the organisation's data syntax rules. This shall enable sharing of data across applications and systems, promote a common understanding of data across IT and business users and prevent creation of incompatible data elements.	Functional	Intersects With	Data Catalog	DCH-03.1	Mechanisms exist to identify and catalog the organization's data holdings in a structured format to document each sensitive and/or regulated data asset.	3		GOV-10.1
Annex 1.1.8	N/A	Enterprise Data Dictionary: The entities shall maintain an 'enterprise data dictionary' incorporating the organisation's data syntax rules. This shall enable sharing of data across applications and systems, promote a common understanding of data across IT and business users and prevent creation of incompatible data elements.	Functional	Intersects With	Standardized Terminology	GOV-03.2	Mechanisms exist to standardize technology and process terminology to reduce confusion amongst groups and departments.	3		SEA-02.1
Annex 1.1.9	N/A	Risk Assessment: The risk assessment shall, for each asset within its scope, identify the threat / vulnerability combinations and likelihood of impact on confidentiality, availability or integrity of that asset - from a business, compliance and / or contractual perspective.	Functional	Subset Of	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).	10		RSK-04
Annex 1.1.10	N/A	Access to Application: There shall be documented standards / procedures for administering an application system, which are approved by the application owner and kept up-to-date. Access to the application shall be based on the principle of least privilege and 'need to know' commensurate with the job responsibilities.	Functional	Intersects With	Least Privilege	IAC-30	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	5		IAC-21
Annex 1.1.10	N/A	Access to Application: There shall be documented standards / procedures for administering an application system, which are approved by the application owner and kept up-to-date. Access to the application shall be based on the principle of least privilege and 'need to know' commensurate with the job responsibilities.	Functional	Intersects With	System Administrative Processes	OPS-04.1	Mechanisms exist to develop, implement and govern system administration processes, with corresponding Standardized Operating Procedures (SOP), for operating and maintaining Technology Assets, Applications and/or Services (TAAS).	5		AST-26
Annex 1.1.11	N/A	Competency of Staff: Requirements for trained resources with requisite skill sets for the IT function need to be understood and assessed appropriately with a periodic assessment of the training requirements for human resources.	Functional	Intersects With	Identify Critical Skills & Gaps	HRS-16	Mechanisms exist to evaluate the critical security, compliance and resilience skills needed to support the organization's mission and identify gaps that exist.	5		HRS-13
Annex 1.1.11	N/A	Competency of Staff: Requirements for trained resources with requisite skill sets for the IT function need to be understood and assessed appropriately with a periodic assessment of the training requirements for human resources.	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-05	Mechanisms exist to provide role-based security, compliance and resilience-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	3		SAT-03
Annex 1.1.12	N/A	Vendor Risk Management: The Service Level Agreements (SLAs) for technology support, including BCP-DR and data management shall categorically include clauses permitting regulatory access to these set-ups.	Functional	Intersects With	Assessor Access	CPL-10	Mechanisms exist to grant assessors minimum necessary access to conduct conformity assessments, including: (1) Logical access to design, development, production, inspection and testing artifacts; and (2) Physical access to facilities.	3		CPL-03.3
Annex 1.1.12	N/A	Vendor Risk Management: The Service Level Agreements (SLAs) for technology support, including BCP-DR and data management shall categorically include clauses permitting regulatory access to these set-ups.	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
Annex 1.1.13	N/A	Maturity and Roadmap: The entities shall consider assessing their IT maturity level, based on well-known international standards, design an action plan and implement the plan to reach the target maturity level.	Functional	Intersects With	Targeted Capability Maturity Levels	PRM-03	Mechanisms exist to define and identify targeted capability maturity levels.	8		PRM-01.2
Annex 1.1.14	N/A	Cryptographic Requirement: The entities shall select encryption algorithms which are well established international standards and which have been subjected to rigorous scrutiny by an international community of cryptographers or approved by authoritative professional bodies, reputable security vendors or government agencies.	Functional	Subset Of	Use of Cryptographic Controls	CRY-02	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10		CRY-01

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 Regulation of Payment Aggregators (PA) (2025)**
Focal Document URL: https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12896
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-ind-rbi-pa-2025.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 #
Annex 1.1.15	N/A	Forensic Readiness: All security events from the entities infrastructure including but not limited to application, servers, middleware, endpoint, network, authentication events, database, web services, cryptographic events and log files shall be collected, investigated and analysed for proactive identification of security alerts.	Functional	Intersects With	Chain of Custody & Forensics	IRO-13	Mechanisms exist to perform digital forensics and maintain the integrity of the chain of custody, in accordance with applicable laws, regulations and industry-recognized secure practices.	3		IRO-08
Annex 1.1.15	N/A	Forensic Readiness: All security events from the entities infrastructure including but not limited to application, servers, middleware, endpoint, network, authentication events, database, web services, cryptographic events and log files shall be collected, investigated and analysed for proactive identification of security alerts.	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
Annex 1.1.15	N/A	Forensic Readiness: All security events from the entities infrastructure including but not limited to application, servers, middleware, endpoint, network, authentication events, database, web services, cryptographic events and log files shall be collected, investigated and analysed for proactive identification of security alerts.	Functional	Intersects With	Event Log & Security-Relevant Telemetry Analysis & Triage	MON-05.2	Mechanisms exist to ensure event log and security-relevant telemetry reviews include analysis and triage practices that integrate with the organization's established incident response processes.	5		MON-17
Annex 1.1.16	N/A	Data Sovereignty: The entities shall take preventive measures to ensure storing data in infrastructure that do not belong to external jurisdictions. Appropriate controls shall be considered to prevent unauthorised access to the data.	Functional	Intersects With	Geographic Data Location	DCH-30	Mechanisms exist to inventory, document and maintain data flows for data that is resident (permanently or temporarily) within geographically distributed Technology Assets, Applications and/or Services (TAAS) (physical and virtual).	3		DCH-19
Annex 1.1.16	N/A	Data Sovereignty: The entities shall take preventive measures to ensure storing data in infrastructure that do not belong to external jurisdictions. Appropriate controls shall be considered to prevent unauthorised access to the data.	Functional	Intersects With	Data Localization	DCH-31	Mechanisms exist to constrain the impact of "digital sovereignty laws," that require localized data within the host country, where data and processes may be subjected to arbitrary enforcement actions that potentially violate other applicable statutory, regulatory and/or contractual obligations.	5		DCH-26
Annex 1.1.16	N/A	Data Sovereignty: The entities shall take preventive measures to ensure storing data in infrastructure that do not belong to external jurisdictions. Appropriate controls shall be considered to prevent unauthorised access to the data.	Functional	Intersects With	Access To Sensitive / Regulated Data	IAC-25.1	Mechanisms exist to limit access to sensitive and/or regulated data to only those individuals whose job requires such access.	3		IAC-20.1
Annex 1.1.17	N/A	Data Security in Outsourcing: There shall be an outsourcing agreement providing 'right to audit' clause to enable the entities / their appointed agencies and regulators to conduct security audits. Alternatively, third parties shall submit annual independent security audit reports to the entities.	Functional	Intersects With	Assessor Access	CPL-10	Mechanisms exist to grant assessors minimum necessary access to conduct conformity assessments, including: (1) Logical access to design, development, production, inspection and testing artifacts; and (2) Physical access to facilities.	3		CPL-03.3
Annex 1.1.17	N/A	Data Security in Outsourcing: There shall be an outsourcing agreement providing 'right to audit' clause to enable the entities / their appointed agencies and regulators to conduct security audits. Alternatively, third parties shall submit annual independent security audit reports to the entities.	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
Annex 1.1.17	N/A	Data Security in Outsourcing: There shall be an outsourcing agreement providing 'right to audit' clause to enable the entities / their appointed agencies and regulators to conduct security audits. Alternatively, third parties shall submit annual independent security audit reports to the entities.	Functional	Intersects With	Third-Party Attestation (3PA)	TPM-23	Mechanisms exist to obtain an attestation from an independent Third-Party Assessment Organization (3PAO) that provides assurance of conformity with specified statutory, regulatory and contractual obligations for security, compliance and resilience controls, including any flow-down requirements to contractors and subcontractors.	3		TPM-05.8
Annex 1.1.18	N/A	Payment Application Security: Payment applications shall be developed as per PCI-SSF guidelines and complied with as required. The entities shall review PCI-DSS compliance status as part of merchant onboarding process.	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-05	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	5		TDA-06
Annex 1.1.18	N/A	Payment Application Security: Payment applications shall be developed as per PCI-SSF guidelines and complied with as required. The entities shall review PCI-DSS compliance status as part of merchant onboarding process.	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).	3		TPM-04.1
Annex 1.2	Other Recommendations	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
Annex 1.2.1	N/A	The customer card credentials shall not be stored within the database or the server accessed by the merchant.	Functional	Intersects With	Storing Authentication Data	DCH-15	Mechanisms exist to prohibit the storage of sensitive transaction authentication data after authorization.	5		DCH-06.5
Annex 1.2.2	N/A	Option for ATM PIN as a factor of authentication for card not present transactions shall not be given.	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
Annex 1.2.3	N/A	Instructions on storage of payment system data, as applicable to PSOs, shall apply.	Functional	Intersects With	Geographic Data Location	DCH-30	Mechanisms exist to inventory, document and maintain data flows for data that is resident (permanently or temporarily) within geographically distributed Technology Assets, Applications and/or Services (TAAS) (physical and virtual).	3		DCH-19
Annex 1.2.3	N/A	Instructions on storage of payment system data, as applicable to PSOs, shall apply.	Functional	Intersects With	Data Localization	DCH-31	Mechanisms exist to constrain the impact of "digital sovereignty laws," that require localized data within the host country, where data and processes may be subjected to arbitrary enforcement actions that potentially violate other applicable statutory, regulatory and/or contractual obligations.	5		DCH-26
Annex 1.2.4	N/A	All refunds shall be made to original method of payment unless specifically agreed by the customer to credit an alternate mode.	Functional	No Relationship	N/A	N/A	N/A	0		
Annex 2	Reports to be Submitted by Authorised Payment Aggregators	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
Annex 2.Annual	Annual Reports	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
Annex 2.Annual.1	N/A	Net-worth Certificate - Audited Annual report with statutory auditor certificate on Net-worth, to be submitted by September 30th (Annexure 2.1).	Functional	No Relationship	N/A	N/A	N/A	0		
Annex 2.Annual.2	N/A	IS Audit Report and Cyber Security Audit Report with observations noted, if any, including corrective / preventive action planned with closure date - Externally Audited - as prescribed by RBI. The scope of audit shall encompass all relevant areas of information system processes and applications.	Functional	Intersects With	Periodic Audits	CPL-07.2	Mechanisms exist to conduct periodic audits of security, compliance and resilience controls to evaluate conformity with the organization's documented policies, standards and procedures.	5		CPL-02.2
Annex 2.Annual.2	N/A	IS Audit Report and Cyber Security Audit Report with observations noted, if any, including corrective / preventive action planned with closure date - Externally Audited - as prescribed by RBI. The scope of audit shall encompass all relevant areas of information system processes and applications.	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
Annex 2.Annual.2	N/A	IS Audit Report and Cyber Security Audit Report with observations noted, if any, including corrective / preventive action planned with closure date - Externally Audited - as prescribed by RBI. The scope of audit shall encompass all relevant areas of information system processes and applications.	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
Annex 2.Quarterly	Quarterly Reports	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
Annex 2.Quarterly.1	N/A	Auditor's Certificate on Maintenance of Balance in Escrow Account - by 15th of the month following the quarter end (Annexure 2.2 and Annexure 2.3).	Functional	No Relationship	N/A	N/A	N/A	0		
Annex 2.Quarterly.2	N/A	Bankers' Certificate on Escrow Account Debits and Credits - Internally Audited - by 15th of the month following the quarter end in case of PA - O and PA - P.	Functional	No Relationship	N/A	N/A	N/A	0		
Annex 2.Quarterly.3	N/A	Bankers' Certificate on InCA / OCA Debits and Credits - Internally Audited - by 15th of the month following the quarter end in case of PA - CB.	Functional	No Relationship	N/A	N/A	N/A	0		
Annex 2.Monthly	Monthly Reports	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
Annex 2.Monthly.1	N/A	Statistics of Transactions Handled - by 7th of next month (Annexure 2.4).	Functional	No Relationship	N/A	N/A	N/A	0		
Annex 2.NonPeriodic	Non-periodic Reports	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
Annex 2.NonPeriodic.1	N/A	Declaration and Undertaking by the Director - Changes in Board of Directors - as and when happens (Annexure 2.5).	Functional	No Relationship	N/A	N/A	N/A	0		