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) - Storage of Payment System Data - Data Localization, 2018**
Focal Document URL: https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11244
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-ind-rbi-data-localization-2018.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
1	N/A	Please refer to paragraph 4 of the Statement on Development and Regulatory Policies of the First Bi-monthly Monetary Policy Statement for 2018-19 dated April 5, 2018. In recent times, there has been considerable growth in the payment ecosystem in the country. Such systems are also highly technology dependent, which necessitate adoption of safety and security measures, which are best in class, on a continuous basis.	Functional	No Relationship	N/A	N/A	N/A	0		
2	Data Storage Requirements	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
2	N/A	It is observed that not all system providers store the payments data in India. In order to ensure better monitoring, it is important to have unfettered supervisory access to data stored with these system providers as also with their service providers / intermediaries / third party vendors and other entities in the payment ecosystem. It has, therefore, been decided that:	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.	5		CPL-03.3
2	N/A	It is observed that not all system providers store the payments data in India. In order to ensure better monitoring, it is important to have unfettered supervisory access to data stored with these system providers as also with their service providers / intermediaries / third party vendors and other entities in the payment ecosystem. It has, therefore, been decided that:	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
2.i	N/A	All system providers shall ensure that the entire data relating to payment systems operated by them are stored in a system only in India. This data should include the full end-to-end transaction details / information collected / carried / processed as part of the message / payment instruction. For the foreign leg of the transaction, if any, the data can also be stored in the foreign country, if required.	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
2.i	N/A	All system providers shall ensure that the entire data relating to payment systems operated by them are stored in a system only in India. This data should include the full end-to-end transaction details / information collected / carried / processed as part of the message / payment instruction. For the foreign leg of the transaction, if any, the data can also be stored in the foreign country, if required.	Functional	Intersects With	Geolocation Requirements for Processing, Storage and Service Locations	DCH-30.1	Mechanisms exist to control the location of Technology Assets, Applications and/or Services (TAAS) processing and/or storage based on business requirements that includes statutory, regulatory and contractual obligations.	5		CLD-09
2.i	N/A	All system providers shall ensure that the entire data relating to payment systems operated by them are stored in a system only in India. This data should include the full end-to-end transaction details / information collected / carried / processed as part of the message / payment instruction. For the foreign leg of the transaction, if any, the data can also be stored in the foreign country, if required.	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.	8		DCH-26
2.i	N/A	All system providers shall ensure that the entire data relating to payment systems operated by them are stored in a system only in India. This data should include the full end-to-end transaction details / information collected / carried / processed as part of the message / payment instruction. For the foreign leg of the transaction, if any, the data can also be stored in the foreign country, if required.	Functional	Intersects With	Third-Party Processing, Storage and Service Locations	TPM-12.2	Mechanisms exist to restrict the location of information processing/storage based on business requirements.	5		TPM-04.4
2.ii	N/A	System providers shall ensure compliance of (i) above within a period of six months and report compliance of the same to the Reserve Bank latest by October 15, 2018.	Functional	Intersects With	Ability To Demonstrate Conformity	CPL-04	Mechanisms exist to ensure the organization is able to demonstrate security, compliance and/or resilience capability conformity with applicable cybersecurity and data protection laws, regulations and/or contractual obligations.	5		CPL-01.3
2.iii	N/A	System providers shall submit the System Audit Report (SAR) on completion of the requirement at (i) above. The audit should be conducted by CERT-IN empaneled auditors certifying completion of activity at (i) above. The SAR duly approved by the Board of the system providers should be submitted to the Reserve Bank not later than December 31, 2018.	Functional	Intersects With	Declaration of Conformity	CPL-04.4	Mechanisms exist to generate a declaration of conformity for each conformity assessment, where the document: (1) Is concise; (2) Unambiguously reflects the current status; (3) Is physically or electronically signed; and (4) Where possible, is machine readable.	5		CPL-01.5
2.iii	N/A	System providers shall submit the System Audit Report (SAR) on completion of the requirement at (i) above. The audit should be conducted by CERT-IN empaneled auditors certifying completion of activity at (i) above. The SAR duly approved by the Board of the system providers should be submitted to the Reserve Bank not later than December 31, 2018.	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
2.iii	N/A	System providers shall submit the System Audit Report (SAR) on completion of the requirement at (i) above. The audit should be conducted by CERT-IN empaneled auditors certifying completion of activity at (i) above. The SAR duly approved by the Board of the system providers should be submitted to the Reserve Bank not later than December 31, 2018.	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).	3		GOV-01.2
3	N/A	The directive is issued under Section 10(2) read with Section 18 of Payment and Settlement Systems Act 2007, (Act 51 of 2007).	Functional	No Relationship	N/A	N/A	N/A	0		