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 Digital Payment Security Controls, 2021
Focal Document URL: https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12032
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-ind-rbi-dpsc-2021.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
Intro	Introduction	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
ChI	Preliminary	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
1	Short Title and Commencement	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
1.a	N/A	These directions shall be called the Reserve Bank of India (Digital Payment Security Controls) directions, 2021.	Functional	No Relationship	N/A	N/A	N/A	0		
1.b	N/A	These directions shall come into effect six months from the day they are placed on the official website of the Reserve Bank of India (RBI). However, in respect of instructions already issued either by Department of Payment and Settlement Systems (DPSS), Department of Regulation (DoR) or Department of Supervision (DoS) of RBI including those to select Regulated Entities (REs), by way of circular or advisory, the timeline would be with immediate effect or as per the timelines already prescribed.	Functional	No Relationship	N/A	N/A	N/A	0		
2	Applicability	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
2.a	N/A	Scheduled Commercial Banks (excluding Regional Rural Banks);	Functional	No Relationship	N/A	N/A	N/A	0		
2.b	N/A	Small Finance Banks;	Functional	No Relationship	N/A	N/A	N/A	0		
2.c	N/A	Payments Banks; and	Functional	No Relationship	N/A	N/A	N/A	0		
2.d	N/A	Credit card issuing NBFCs.	Functional	No Relationship	N/A	N/A	N/A	0		
3	N/A	All expressions unless defined herein shall have the same meaning as have been assigned to them under the Banking Regulation Act, 1949, Reserve Bank of India Act, 1934, Payment and Settlement Systems Act, 2007 or Information Technology Act, 2000/ Information Technology (Amendment) Act, 2008 and Rules made thereunder, any statutory modification or re-enactment thereto or as used in commercial parlance, as the case may be.	Functional	No Relationship	N/A	N/A	N/A	0		
ChII	General Controls	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
II.A	Governance and Management of Security Risks	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.	5		
4	Board Policy for Digital Payment Products and Services	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
4.a	N/A	Necessary controls to protect the confidentiality of customer data and integrity of data and processes associated with the digital product/ services offered;	Functional	Intersects With	Data Protection	DCH-02	Mechanisms exist to facilitate the implementation of data protection controls.	3		DCH-01
4.a	N/A	Necessary controls to protect the confidentiality of customer data and integrity of data and processes associated with the digital product/ services offered;	Functional	Intersects With	Implement Controls	GOV-11.2	Mechanisms exist to compel data and/or process owners to implement required security, compliance and resilience controls for Technology Assets, Applications, Services and/or Data (TAASD) under their control.	5		GOV-15.2
4.b	N/A	Availability of requisite infrastructure e.g. human resources, technology, etc. with necessary back up;	Functional	Intersects With	Operationalizing Security, Compliance & Resilience Capabilities	GOV-11	Mechanisms exist to compel data and/or process owners to operationalize security, compliance and resilience practices for Technology Assets, Applications, Services and/or Data (TAASD) under their control.	3		GOV-15
4.b	N/A	Availability of requisite infrastructure e.g. human resources, technology, etc. with necessary back up;	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.	5		PRM-03
4.c	N/A	Assurance that the payment product is built in a secure manner offering robust performance ensuring safety, consistency and rolled out after necessary testing for achieving desired FSP;	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
4.c	N/A	Assurance that the payment product is built in a secure manner offering robust performance ensuring safety, consistency and rolled out after necessary testing for achieving desired FSP;	Functional	Intersects With	Product Management	TDA-06	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	8		TDA-01.1
4.c	N/A	Assurance that the payment product is built in a secure manner offering robust performance ensuring safety, consistency and rolled out after necessary testing for achieving desired FSP;	Functional	Intersects With	Security, Compliance & Resilience Testing Throughout Development	TDA-17	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and (3) Document the results.	5		TDA-09
4.d	N/A	Capacity building and expansion with scalability (to meet the growth for efficient transaction processing);	Functional	Subset Of	Capacity & Performance Management	CAP-02	Mechanisms exist to facilitate the implementation of capacity management controls to ensure optimal system performance to meet expected and anticipated future capacity requirements.	10		CAP-01
4.d	N/A	Capacity building and expansion with scalability (to meet the growth for efficient transaction processing);	Functional	Intersects With	Capacity Planning	CAP-03	Mechanisms exist to conduct capacity planning so that necessary capacity for information processing, telecommunications and environmental support will exist during contingency operations.	5		CAP-03
4.e	N/A	Minimal customer service disruption with high availability of systems/ channels (to have minimal technical declines);	Functional	Subset Of	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.	10		BCD-01
4.e	N/A	Minimal customer service disruption with high availability of systems/ channels (to have minimal technical declines);	Functional	Intersects With	Failover Capability	BCD-22	Mechanisms exist to implement real-time or near-real-time failover capability to maintain availability of critical Technology Assets, Applications, Services and/or Data (TAASD).	3		BCD-12.2
4.f	N/A	Efficient and effective dispute resolution mechanism and handling of customer grievance; and	Functional	Subset Of	Grievances	CPL-22	Mechanisms exist to govern the intake and analysis of grievances related to the organization's cybersecurity and/or data protection practices.	10		CPL-07
4.f	N/A	Efficient and effective dispute resolution mechanism and handling of customer grievance; and	Functional	Intersects With	Grievance Response	CPL-22.1	Mechanisms exist to respond to legitimate grievances related to the organization's cybersecurity and/or data protection practices.	5		CPL-07.1
4.g	N/A	Adequate and appropriate review mechanism followed by swift corrective action, in case any one of the above requirements is hampered or having high potential to get hampered.	Functional	Intersects With	Non-Conformity Oversight	CPL-06	Mechanisms exist to identify and document instances of non-conformity with statutory, regulatory and/or contractual obligations, in order to develop appropriate risk mitigation actions.	5		CPL-01.1
4.g	N/A	Adequate and appropriate review mechanism followed by swift corrective action, in case any one of the above requirements is hampered or having high potential to get hampered.	Functional	Intersects With	Non-Conformity Corrective Action	CPL-06.1	Mechanisms exist to implement corrective action to remediate instances of non-conformity with applicable statutory, regulatory, and/or contractual compliance obligations.	5		CPL-02.3
5	N/A	REs shall incorporate appropriate processes into their governance and risk management programs for identifying, analysing, monitoring and managing the specific risks, including compliance risk and fraud risk, associated with the portfolio of digital payment products and services on a continual basis and in a holistic manner. The Board/ Senior Management of REs shall have appropriate performance monitoring systems/ key performance indicators for assessing whether the product or service offered through digital payment channels meet operational and security norms.	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
5	N/A	REs shall incorporate appropriate processes into their governance and risk management programs for identifying, analysing, monitoring and managing the specific risks, including compliance risk and fraud risk, associated with the portfolio of digital payment products and services on a continual basis and in a holistic manner. The Board/ Senior Management of REs shall have appropriate performance monitoring systems/ key performance indicators for assessing whether the product or service offered through digital payment channels meet operational and security norms.	Functional	Intersects With	Measures of Performance	GOV-12	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRP) measures of performance.	5		GOV-05

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 Digital Payment Security Controls, 2021**
Focal Document URL: https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12032
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-ind-rbi-dpsc-2021.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
5	N/A	REs shall incorporate appropriate processes into their governance and risk management programs for identifying, analysing, monitoring and managing the specific risks, including compliance risk and fraud risk, associated with the portfolio of digital payment products and services on a continual basis and in a holistic manner. The Board/ Senior Management of REs shall have appropriate performance monitoring systems/ key performance indicators for assessing whether the product or service offered through digital payment channels meet operational and security norms.	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
6	N/A	As part of this process, the REs shall define product-level limits on the level of acceptable security risk, document specific security objectives and performance criteria including quantitative benchmarks for evaluating the success of the security built into the digital payment product or service, periodically compare actual results with projections and qualitative benchmarks to detect and address adverse trends or concerns in a timely manner and modify the business plan/ strategy involving the product, when appropriate, based on the security performance of the product or service.	Functional	Intersects With	Key Performance Indicators (KPIs)	GOV-12.1	Mechanisms exist to develop, report and monitor Key Performance Indicators (KPIs) to assist organizational management in performance monitoring, trend analysis, and possible control redesign or replacement for the Security, Compliance & Resilience Program (SCRP).	5		GOV-05.1
6	N/A	As part of this process, the REs shall define product-level limits on the level of acceptable security risk, document specific security objectives and performance criteria including quantitative benchmarks for evaluating the success of the security built into the digital payment product or service, periodically compare actual results with projections and qualitative benchmarks to detect and address adverse trends or concerns in a timely manner and modify the business plan/ strategy involving the product, when appropriate, based on the security performance of the product or service.	Functional	Intersects With	Risk Tolerance	RSK-05.1	Mechanisms exist to define organizational risk tolerance, the specified range of acceptable results.	5		RSK-01.3
6	N/A	As part of this process, the REs shall define product-level limits on the level of acceptable security risk, document specific security objectives and performance criteria including quantitative benchmarks for evaluating the success of the security built into the digital payment product or service, periodically compare actual results with projections and qualitative benchmarks to detect and address adverse trends or concerns in a timely manner and modify the business plan/ strategy involving the product, when appropriate, based on the security performance of the product or service.	Functional	Subset Of	Product Management	TDA-06	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	10		TDA-01.1
7	N/A	REs shall have trained resources with necessary expertise to manage the digital payment infrastructure. Wherever the REs are dependent on third party service providers, adequate oversight and controls for monitoring the activities of the third party personnel, in line with RBI guidelines on outsourcing, shall be put in place.	Functional	Intersects With	Competency Requirements for Security, Compliance & Resilience-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security, compliance and resilience-related positions are staffed by qualified individuals who have the necessary skill set.	5		HRS-03.2
7	N/A	REs shall have trained resources with necessary expertise to manage the digital payment infrastructure. Wherever the REs are dependent on third party service providers, adequate oversight and controls for monitoring the activities of the third party personnel, in line with RBI guidelines on outsourcing, shall be put in place.	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.	5		SAT-03
7	N/A	REs shall have trained resources with necessary expertise to manage the digital payment infrastructure. Wherever the REs are dependent on third party service providers, adequate oversight and controls for monitoring the activities of the third party personnel, in line with RBI guidelines on outsourcing, shall be put in place.	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
8	Risk Assessment for Digital Payment Products and Services	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
8.a	N/A	The technology stack and solutions used;	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
8.b	N/A	Known vulnerabilities at each of the touchpoints of the digital product and the remedial action taken by the entity;	Functional	Intersects With	Vulnerability Ranking	VPM-05	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities using reputable outside sources for security vulnerability information.	3		VPM-03
8.b	N/A	Known vulnerabilities at each of the touchpoints of the digital product and the remedial action taken by the entity;	Functional	Intersects With	Vulnerability Remediation Process	VPM-06	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5		VPM-02
8.c	N/A	Dependence on third party service providers and oversight over such providers;	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
8.c	N/A	Dependence on third party service providers and oversight over such providers;	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
8.d	N/A	Risk arising out of integration of digital payment platform with other systems both internal and external to the RE, including core systems and systems of payment systems operators, etc.;	Functional	Intersects With	Interconnection Security Agreements (ISAs)	NET-05	Mechanisms exist to authorize connections from systems to other systems using Interconnection Security Agreements (ISAs), or similar methods, that document, for each interconnection: (1) Interface characteristics; (2) Security, compliance and resilience requirements; and; (3) The nature of the information communicated.	3		NET-05
8.d	N/A	Risk arising out of integration of digital payment platform with other systems both internal and external to the RE, including core systems and systems of payment systems operators, etc.;	Functional	Intersects With	Risk Assessment	RSK-13	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5		RSK-04
8.e	N/A	The customer experience, convenience and technology adoption required to use such products;	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).	3		RSK-04
8.f	N/A	Reconciliation process;	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).	3		RSK-04
8.g	N/A	Interoperability aspects;	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).	3		RSK-04
8.h	N/A	Data storage, security and privacy protection as per extant laws/ instructions;	Functional	Intersects With	Data Protection	DCH-02	Mechanisms exist to facilitate the implementation of data protection controls.	5		DCH-01
8.h	N/A	Data storage, security and privacy protection as per extant laws/ instructions;	Functional	Intersects With	Data Privacy Program	PRI-02	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	5		PRI-01
8.i	N/A	Operational risk including fraud risk;	Functional	Intersects With	Risk Identification	RSK-09	Mechanisms exist to identify and document risks, both internal and external.	3		RSK-03
8.i	N/A	Operational risk including fraud risk;	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

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 Digital Payment Security Controls, 2021**
Focal Document URL: https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12032
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-ind-rbi-dpsc-2021.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
8.j	N/A	Business continuity and service availability;	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
8.j	N/A	Business continuity and service availability;	Functional	Intersects With	Business Impact Analysis (BIA)	RSK-08	Mechanisms exist to conduct a Business Impact Analysis (BIA) to identify and assess security, compliance and resilience risks.	5		RSK-08
8.k	N/A	Compliance with extant cyber security requirements; and	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
8.l	N/A	Compatibility aspects.	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).	3		RSK-04
9	N/A	REs shall evaluate the risks associated with the chosen technology platforms, application architecture, both on the server and client side. Further, REs should undertake a review of the risk scenarios and existing security measures based on incidents affecting their services, before any major change to the infrastructure or procedures is made or, when, any new threats are identified through risk monitoring activities. Further, unused or unwanted features of the platform should be closely controlled to minimise risk.	Functional	Intersects With	Least Functionality	CFG-03	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	5		CFG-03
9	N/A	REs shall evaluate the risks associated with the chosen technology platforms, application architecture, both on the server and client side. Further, REs should undertake a review of the risk scenarios and existing security measures based on incidents affecting their services, before any major change to the infrastructure or procedures is made or, when, any new threats are identified through risk monitoring activities. Further, unused or unwanted features of the platform should be closely controlled to minimise risk.	Functional	Intersects With	Security Impact Analysis for Changes	CHG-06	Mechanisms exist to analyze proposed changes for potential security impacts, prior to the implementation of the change.	5		CHG-03
9	N/A	REs shall evaluate the risks associated with the chosen technology platforms, application architecture, both on the server and client side. Further, REs should undertake a review of the risk scenarios and existing security measures based on incidents affecting their services, before any major change to the infrastructure or procedures is made or, when, any new threats are identified through risk monitoring activities. Further, unused or unwanted features of the platform should be closely controlled to minimise risk.	Functional	Intersects With	Risk Assessment	RSK-13	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5		RSK-04
10	N/A	REs shall develop sound internal control systems and take into account the operational risk before offering digital payment products and related services. This would include ensuring that adequate safeguards are in place to protect integrity of data, customer confidentiality and security of data.	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
10	N/A	REs shall develop sound internal control systems and take into account the operational risk before offering digital payment products and related services. This would include ensuring that adequate safeguards are in place to protect integrity of data, customer confidentiality and security of data.	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.	3		RSK-01
10	N/A	REs shall develop sound internal control systems and take into account the operational risk before offering digital payment products and related services. This would include ensuring that adequate safeguards are in place to protect integrity of data, customer confidentiality and security of data.	Functional	Subset Of	Product Management	TDA-06	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	10		TDA-01.1
11	N/A	REs shall ensure that the digital payment architecture is robust and scalable, commensurate with the transaction volumes and customer growth. The IT strategy of the RE shall ensure that a robust capacity management plan is in place to meet evolving demand. REs shall also put in place review mechanism of IT/ IT Security architecture and technology platform overhaul on a periodic basis based on Board-approved policy.	Functional	Intersects With	Capacity & Performance Management	CAP-02	Mechanisms exist to facilitate the implementation of capacity management controls to ensure optimal system performance to meet expected and anticipated future capacity requirements.	5		CAP-01
11	N/A	REs shall ensure that the digital payment architecture is robust and scalable, commensurate with the transaction volumes and customer growth. The IT strategy of the RE shall ensure that a robust capacity management plan is in place to meet evolving demand. REs shall also put in place review mechanism of IT/ IT Security architecture and technology platform overhaul on a periodic basis based on Board-approved policy.	Functional	Intersects With	Capacity Planning	CAP-03	Mechanisms exist to conduct capacity planning so that necessary capacity for information processing, telecommunications and environmental support will exist during contingency operations.	5		CAP-03
11	N/A	REs shall ensure that the digital payment architecture is robust and scalable, commensurate with the transaction volumes and customer growth. The IT strategy of the RE shall ensure that a robust capacity management plan is in place to meet evolving demand. REs shall also put in place review mechanism of IT/ IT Security architecture and technology platform overhaul on a periodic basis based on Board-approved policy.	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.	3		SEA-02
12	N/A	REs shall have necessary capacity, systems and procedures in place to periodically test the backed-up data, application pertaining to digital products to ensure recovery without loss of transactions or audit-trails. These facilities should be tested at least on a half-yearly basis for digital payment products and services.	Functional	Intersects With	Transaction Recovery	BCD-26	Mechanisms exist to utilize specialized backup mechanisms that will allow transaction recovery for transaction-based Technology Assets, Applications and/or Services (TAAS) in accordance with Recovery Point Objectives (RPOs).	5		BCD-12.1
12	N/A	REs shall have necessary capacity, systems and procedures in place to periodically test the backed-up data, application pertaining to digital products to ensure recovery without loss of transactions or audit-trails. These facilities should be tested at least on a half-yearly basis for digital payment products and services.	Functional	Intersects With	Testing for Reliability & Integrity	BCD-32	Mechanisms exist to routinely test data backups to verify the reliability of the backup process, as well as the integrity and availability of the data.	8		BCD-11.1
II.B	Other Generic Security Controls	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
13	N/A	The communication protocol in the digital payment channels (especially over Internet) shall adhere to a secure standard. An appropriate level of encryption and security shall be implemented in the digital payment ecosystem.	Functional	Intersects With	Encrypting Data In Transit	CRY-05	Cryptographic mechanisms exist to prevent the unauthorized disclosure of data in transit.	5		CRY-03
13	N/A	The communication protocol in the digital payment channels (especially over Internet) shall adhere to a secure standard. An appropriate level of encryption and security shall be implemented in the digital payment ecosystem.	Functional	Intersects With	Safeguarding Data Over Open Networks	NET-37	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive and/or regulated data during transmission over open, public networks.	5		NET-12
14	N/A	Web applications providing the digital payment products and services should not store sensitive information in HTML hidden fields, cookies, or any other client-side storage to avoid any compromise in the integrity of the data.	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-05	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	3		TDA-06
14	N/A	Web applications providing the digital payment products and services should not store sensitive information in HTML hidden fields, cookies, or any other client-side storage to avoid any compromise in the integrity of the data.	Functional	Intersects With	Client-Facing Web Services	WEB-06	Mechanisms exist to deploy reasonably-expected security, compliance and resilience controls to protect the confidentiality and availability of client data that is stored, transmitted or processed by the Internet-based service.	5		WEB-04
15	N/A	REs shall implement Web Application Firewall (WAF) solution and DDoS mitigation techniques to secure the digital payment products and services offered over Internet.	Functional	Intersects With	Denial of Service (DoS) Protection	NET-21	Automated mechanisms exist to protect against or limit the effects of denial of service attacks.	5		NET-02.1
15	N/A	REs shall implement Web Application Firewall (WAF) solution and DDoS mitigation techniques to secure the digital payment products and services offered over Internet.	Functional	Intersects With	Web Application Firewall (WAF)	NET-34	Mechanisms exist to deploy Web Application Firewalls (WAFs) to provide defense-in-depth protection for application-specific threats.	5		WEB-03

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 Digital Payment Security Controls, 2021**
Focal Document URL: https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12032
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-ind-rbi-dpsc-2021.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
16	N/A	The key length (for symmetric/ asymmetric encryption, hashing), algorithms (for encryption, signing, exchange of keys, creation of message digest, random number generators), cipher suites, digital certificates and applicable protocols used in transmission channels, processing of data, authentication purpose, shall be strong, adopting internationally accepted and published standards that are not deprecated/ demonstrated to be insecure/ vulnerable and the configurations involved in implementing such controls are in general, compliant with extant instructions and the law of the land.	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.	8		CRY-01
16	N/A	The key length (for symmetric/ asymmetric encryption, hashing), algorithms (for encryption, signing, exchange of keys, creation of message digest, random number generators), cipher suites, digital certificates and applicable protocols used in transmission channels, processing of data, authentication purpose, shall be strong, adopting internationally accepted and published standards that are not deprecated/ demonstrated to be insecure/ vulnerable and the configurations involved in implementing such controls are in general, compliant with extant instructions and the law of the land.	Functional	Intersects With	Cryptographic Cipher Suites and Protocols Inventory	CRY-04	Mechanisms exist to identify, document and review deployed cryptographic cipher suites and protocols to proactively respond to industry trends regarding the continued viability of utilized cryptographic cipher suites and protocols.	5		CRY-01.5
17	N/A	REs shall renew their digital certificates used in digital payment ecosystem well in time.	Functional	Intersects With	Cryptographic Key Management	CRY-10	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5		CRY-09
17	N/A	REs shall renew their digital certificates used in digital payment ecosystem well in time.	Functional	Intersects With	Certificate Monitoring	CRY-13	Automated mechanisms exist to discover when new certificates are issued for organization-controlled domains.	3		CRY-12
18	N/A	The mobile application and internet banking application should have effective logging and monitoring capabilities to track user activity, security changes and identify anomalous behaviour and transactions.	Functional	Intersects With	Continuous Monitoring	MON-02	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	5		MON-01
18	N/A	The mobile application and internet banking application should have effective logging and monitoring capabilities to track user activity, security changes and identify anomalous behaviour and transactions.	Functional	Intersects With	Content of Event Logs	MON-09	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	3		MON-03
18	N/A	The mobile application and internet banking application should have effective logging and monitoring capabilities to track user activity, security changes and identify anomalous behaviour and transactions.	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
II.C	Application Security Life Cycle (ASLC)	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
19	N/A	REs shall implement multi-tier application architecture, segregating application, database and presentation layer in the digital payment products and services.	Functional	Intersects With	Network Segmentation (macrosegmentation)	NET-06	Mechanisms exist to implement network segmentation within network architectures to isolate Technology Assets, Applications and/or Services (TAAS) from other network resources.	3		NET-06
19	N/A	REs shall implement multi-tier application architecture, segregating application, database and presentation layer in the digital payment products and services.	Functional	Intersects With	Defense-In-Depth (DiD) Architecture	SEA-06	Mechanisms exist to implement security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.	5		SEA-03
20	N/A	REs shall follow a 'secure by design' approach in the development of digital payment products and services. REs shall ensure that digital payment applications are inherently more secure by embedding security within their development lifecycle.	Functional	Intersects With	Security, Compliance & Resilience Aware Design	SEA-02	Mechanisms exist to formally incorporate the organization's secure architecture principles into engineering, product and model design requirements to ensure security, compliance and resilience are built in by default and by design.	5		SEA-01.5
20	N/A	REs shall follow a 'secure by design' approach in the development of digital payment products and services. REs shall ensure that digital payment applications are inherently more secure by embedding security within their development lifecycle.	Functional	Subset Of	Secure Software Development Practices (SSDP)	TDA-05	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	10		TDA-06
21	N/A	REs shall explicitly define security objectives (including protection of customer information/ data) during (a) requirements gathering, (b) designing, (c) development, (d) testing including source code review, (e) implementation, maintenance & monitoring and (f) decommissioning phases of the digital payment applications.	Functional	Intersects With	Security, Compliance & Resilience Requirements Definition	PRM-09	Mechanisms exist to proactively govern Technology Assets, Applications and/or Services (TAAS) by: (1) Defining technical security, compliance and resilience requirements; and (2) Performing a criticality analysis at predefined decision points in the Secure Development Life Cycle (SDLC).	5		PRM-05
21	N/A	REs shall explicitly define security objectives (including protection of customer information/ data) during (a) requirements gathering, (b) designing, (c) development, (d) testing including source code review, (e) implementation, maintenance & monitoring and (f) decommissioning phases of the digital payment applications.	Functional	Intersects With	Security, Compliance & Resilience Testing Throughout Development	TDA-17	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and (3) Document the results.	5		TDA-09
22	N/A	REs (including those partnering with other entities to co-brand/ co-develop applications) shall adopt and incorporate a threat modelling approach during application lifecycle management into their policies, processes, guidelines and procedures.	Functional	Subset Of	Threat Modeling	TDA-05.2	Mechanisms exist to perform threat modelling and other secure design techniques, to ensure that threats to software and solutions are identified and accounted for.	10		TDA-06.2
23	N/A	For digital payment applications that are licensed by a third party vendor, REs shall have an escrow arrangement for the source code for ensuring continuity of services in case the vendor defaults or is unable to provide services.	Functional	Subset Of	Software Escrow	TDA-16.4	Mechanisms exist to escrow source code and supporting documentation to ensure software availability in the event the software provider goes out of business or is unable to provide support.	10		TDA-20.3
24	Security Testing of Digital Payment Applications	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
24.a	N/A	The VA shall be conducted at least on a half-yearly basis; PT shall be conducted at least on a yearly basis. In addition, VA/PT shall be conducted as and when any new IT Infrastructure or digital payment application is introduced or when any major change is performed in application or infrastructure;	Functional	Intersects With	Vulnerability Scanning	VPM-12	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5		VPM-06
24.a	N/A	The VA shall be conducted at least on a half-yearly basis; PT shall be conducted at least on a yearly basis. In addition, VA/PT shall be conducted as and when any new IT Infrastructure or digital payment application is introduced or when any major change is performed in application or infrastructure;	Functional	Intersects With	Penetration Testing	VPM-18	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	5		VPM-07
24.b	N/A	Testing related to review of source code/ certification shall be conducted/ obtained. This shall continue on a yearly basis, if changes/ upgrades have been made to the application during the year;	Functional	Intersects With	Static Code Analysis	TDA-17.1	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to employ static code analysis tools to identify and remediate common flaws and document the results of the analysis.	5		TDA-09.2
24.b	N/A	Testing related to review of source code/ certification shall be conducted/ obtained. This shall continue on a yearly basis, if changes/ upgrades have been made to the application during the year;	Functional	Intersects With	Manual Code Review	TDA-17.5	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to employ a manual code review process to identify and remediate unique flaws that require knowledge of the application's requirements and design.	5		TDA-09.7
24.c	N/A	Testing/ Certification should broadly address the objective that the product/ version/module(s) functions only in a manner that it is intended to do, is developed as per the best secure design/ coding practices and standards, addressing known flaws/threats due to insecure coding; and	Functional	Intersects With	Development Methods, Techniques & Processes	TDA-03	Mechanisms exist to require software developers to ensure that their software development processes employ industry-recognized secure practices for secure programming, engineering methods, quality control processes and validation techniques to minimize flawed and/or malformed software.	5		TDA-02.3
24.c	N/A	Testing/ Certification should broadly address the objective that the product/ version/module(s) functions only in a manner that it is intended to do, is developed as per the best secure design/ coding practices and standards, addressing known flaws/threats due to insecure coding; and	Functional	Intersects With	Security, Compliance & Resilience Testing Throughout Development	TDA-17	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and (3) Document the results.	5		TDA-09

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 Digital Payment Security Controls, 2021**
Focal Document URL: https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12032
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-ind-rbi-dpsc-2021.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
24.d	N/A	Penal provisions shall be included by the RE into third-party contractual arrangements for any non-compliance by the application provider.	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
24.d	N/A	Penal provisions shall be included by the RE into third-party contractual arrangements for any non-compliance by the application provider.	Functional	Intersects With	Break Clauses	TPM-19	Mechanisms exist to include "break clauses" within contracts for failure to meet contract criteria for security, compliance and/or resilience controls.	5		TPM-05.7
25	N/A	REs may also run automated VA scanning tools to automatically scan all systems on the network that are critical, public facing or store customer sensitive data on a continuous/ more frequent basis.	Functional	Subset Of	Vulnerability Scanning	VPM-12	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	10		VPM-06
26	N/A	REs shall compare the results from earlier vulnerability scans to verify/ ascertain that vulnerabilities are addressed either by patching, implementing a compensating control, or documenting and accepting the residual risk with necessary approval and that there is no recurrence of the known vulnerabilities. The identified vulnerabilities should be fixed in a time-bound manner.	Functional	Intersects With	Compensating Countermeasures	RSK-18	Mechanisms exist to identify and implement one, or more, compensating controls to reduce risk and threat exposure when the primary means of implementing the security function is unavailable or compromised.	3		RSK-06.2
26	N/A	REs shall compare the results from earlier vulnerability scans to verify/ ascertain that vulnerabilities are addressed either by patching, implementing a compensating control, or documenting and accepting the residual risk with necessary approval and that there is no recurrence of the known vulnerabilities. The identified vulnerabilities should be fixed in a time-bound manner.	Functional	Intersects With	Vulnerability Remediation Process	VPM-06	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5		VPM-02
26	N/A	REs shall compare the results from earlier vulnerability scans to verify/ ascertain that vulnerabilities are addressed either by patching, implementing a compensating control, or documenting and accepting the residual risk with necessary approval and that there is no recurrence of the known vulnerabilities. The identified vulnerabilities should be fixed in a time-bound manner.	Functional	Intersects With	Vulnerability Trend Analysis	VPM-13	Automated mechanisms exist to compare the results of vulnerability scans over time to determine trends in system vulnerabilities.	8		VPM-06.4
27	N/A	REs shall ensure that all vulnerability scanning is performed in authenticated mode either with agents running locally on the system to analyse the security configuration or with remote scanners that are given administrative rights on the system being tested.	Functional	Intersects With	Privileged Access For Vulnerability Scanning Tools	VPM-12.3	Mechanisms exist to implement privileged access authorization for selected vulnerability scanning activities.	8		VPM-06.3
28	N/A	REs shall verify and thoroughly test the functionality (to validate whether the system meets the functional requirements/ specifications) and security controls of payment products and services before its launch/ moving to the production environment.	Functional	Intersects With	Security Authorization	IAO-14	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.	5		IAO-07
28	N/A	REs shall verify and thoroughly test the functionality (to validate whether the system meets the functional requirements/ specifications) and security controls of payment products and services before its launch/ moving to the production environment.	Functional	Intersects With	Security, Compliance & Resilience Testing Throughout Development	TDA-17	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and (3) Document the results.	5		TDA-09
29	N/A	REs shall institute a mechanism to actively monitor for the non-genuine/ unauthorised/ malicious applications (with similar name/ features) on popular app-stores and the Web and respond accordingly to bring them down.	Functional	Intersects With	Threat Intelligence Program	THR-02	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	5		THR-01
29	N/A	REs shall institute a mechanism to actively monitor for the non-genuine/ unauthorised/ malicious applications (with similar name/ features) on popular app-stores and the Web and respond accordingly to bring them down.	Functional	Intersects With	Threat Intelligence Feeds	THR-04	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	3		THR-03
30	N/A	The server at the RE's end should have adequate checks and balances to ensure that no transaction is carried out through non-genuine/ unauthorised digital payment products/ applications and the authentication process is robust, secure and centralised.	Functional	Intersects With	Authenticate, Authorize and Audit (AAA)	IAC-03	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).	5		IAC-01.2
30	N/A	The server at the RE's end should have adequate checks and balances to ensure that no transaction is carried out through non-genuine/ unauthorised digital payment products/ applications and the authentication process is robust, secure and centralised.	Functional	Intersects With	Identification & Authentication for Devices	IAC-34	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) devices before establishing a connection using bidirectional authentication that is cryptographically- based and replay resistant.	3		IAC-04
31	N/A	The security controls for digital payment applications must focus on how these applications handle, store and protect payment data. The APIs for secure data storage and communication have to be implemented and used correctly in order to be effective. REs shall refer to standards such as OWASP-MASVS, OWASP-ASVS and other relevant OWASP standards, security and data protection guidelines in ISO 12812, threat catalogues and guides developed by NIST (including for Bluetooth and LTE security), for application security and other protection measures. Such testing has to necessarily verify for vulnerabilities including, but not limited to OWASP/ OWASP Mobile Top 10, application security guidelines/ requirements developed/ shared by operating system providers/ OEMs.	Functional	Intersects With	Development Methods, Techniques & Processes	TDA-03	Mechanisms exist to require software developers to ensure that their software development processes employ industry-recognized secure practices for secure programming, engineering methods, quality control processes and validation techniques to minimize flawed and/or malformed software.	3		TDA-02.3
31	N/A	The security controls for digital payment applications must focus on how these applications handle, store and protect payment data. The APIs for secure data storage and communication have to be implemented and used correctly in order to be effective. REs shall refer to standards such as OWASP-MASVS, OWASP-ASVS and other relevant OWASP standards, security and data protection guidelines in ISO 12812, threat catalogues and guides developed by NIST (including for Bluetooth and LTE security), for application security and other protection measures. Such testing has to necessarily verify for vulnerabilities including, but not limited to OWASP/ OWASP Mobile Top 10, application security guidelines/ requirements developed/ shared by operating system providers/ OEMs.	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
31	N/A	The security controls for digital payment applications must focus on how these applications handle, store and protect payment data. The APIs for secure data storage and communication have to be implemented and used correctly in order to be effective. REs shall refer to standards such as OWASP-MASVS, OWASP-ASVS and other relevant OWASP standards, security and data protection guidelines in ISO 12812, threat catalogues and guides developed by NIST (including for Bluetooth and LTE security), for application security and other protection measures. Such testing has to necessarily verify for vulnerabilities including, but not limited to OWASP/ OWASP Mobile Top 10, application security guidelines/ requirements developed/ shared by operating system providers/ OEMs.	Functional	Intersects With	Web Security Standard	WEB-03	Mechanisms exist to ensure the Open Web Application Security Project (OWASP) Application Security Verification Standard is incorporated into the organization's Secure Systems Development Lifecycle (SSDLC) process.	5		WEB-07
32	N/A	REs shall redact/ mask customer information such as account numbers/ card numbers/ other sensitive information when transmitted via SMS/ e-mails.	Functional	Intersects With	Masking Displayed Sensitive / Regulated Data	DCH-12	Mechanisms exist to apply data masking to sensitive and/or regulated information that is displayed or printed.	5		DCH-03.2
32	N/A	REs shall redact/ mask customer information such as account numbers/ card numbers/ other sensitive information when transmitted via SMS/ e-mails.	Functional	Intersects With	End-User Messaging Technologies	NET-40	Mechanisms exist to prohibit the transmission of unprotected sensitive and/or regulated data by end-user messaging technologies.	5		NET-12.2
II.D	Authentication Framework	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
33	N/A	In view of the proliferation of cyber-attacks and their potential consequences, REs should implement, except where explicitly permitted/ relaxed, multi-factor authentication for payments through electronic modes and fund transfers, including cash withdrawals from ATMs/ micro-ATMs/ business correspondents, through digital payment applications. At least one of the authentication methodologies should be generally dynamic or non-replicable. [e.g., Use of One Time Password, mobile devices (device binding and SIM), biometric/ PKI/ hardware tokens, EMV chip card (for Card Present Transactions) with server-side verification could be termed either in dynamic or non-replicable methodologies.].	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-37	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.	5		IAC-06

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 Digital Payment Security Controls, 2021**
Focal Document URL: https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12032
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-ind-rbi-dpsc-2021.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
33	N/A	In view of the proliferation of cyber-attacks and their potential consequences, REs should implement, except where explicitly permitted/ relaxed, multi-factor authentication for payments through electronic modes and fund transfers, including cash withdrawals from ATMs/ micro-ATMs/ business correspondents, through digital payment applications. At least one of the authentication methodologies should be generally dynamic or non-replicable. [e.g., Use of One Time Password, mobile devices (device binding and SIM), biometric/ PKI/ hardware tokens, EMV chip card (for Card Present Transactions) with server-side verification could be termed either in dynamic or non-replicable methodologies.].	Functional	Intersects With	Strong Customer Authentication (SCA)	WEB-07	Mechanisms exist to implement Strong Customer Authentication (SCA) for consumers to reasonably prove their identity.	8		WEB-06
34	Multi-Factor Authentication Objectives and Implementation	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
34.a	N/A	The implementation of appropriate authentication methodologies should be based on an assessment of the risk posed by the RE's digital payment products and services. The risk should be evaluated in light of the type of customer (e.g., retail/ corporate/ commercial); the customer transactional requirements/ pattern (e.g., bill payment, fund transfer), the sensitivity of customer information and the volume, value of transactions involved.	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.	5		IAC-10
34.a	N/A	The implementation of appropriate authentication methodologies should be based on an assessment of the risk posed by the RE's digital payment products and services. The risk should be evaluated in light of the type of customer (e.g., retail/ corporate/ commercial); the customer transactional requirements/ pattern (e.g., bill payment, fund transfer), the sensitivity of customer information and the volume, value of transactions involved.	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
34.b	N/A	Beyond the technology factor, the success of a particular authentication method depends on appropriate policies, procedures, and controls. An effective authentication method should take into consideration customer acceptance, ease of use, reliable performance, scalability to accommodate growth, customer profile, location, transaction, etc., and interoperability with other systems.	Functional	Intersects With	Identity & Access Management (IAM)	IAC-02	Mechanisms exist to facilitate the implementation of Identification and Access Management (IAM) controls.	5		IAC-01
34.c	N/A	To enhance online processing security, multi factor authentication and alerts (like SMS, e-mail, etc.) should be applied in respect of all payment transactions (including debits and credits), creation of new account linkages (addition/ modification/ deletion of beneficiaries), changing account details or revision to fund transfer limits. In devising these security features, REs should take into account their efficacy and differing customer preferences for additional online protection.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-37	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.	5		IAC-06
34.c	N/A	To enhance online processing security, multi factor authentication and alerts (like SMS, e-mail, etc.) should be applied in respect of all payment transactions (including debits and credits), creation of new account linkages (addition/ modification/ deletion of beneficiaries), changing account details or revision to fund transfer limits. In devising these security features, REs should take into account their efficacy and differing customer preferences for additional online protection.	Functional	Intersects With	Strong Customer Authentication (SCA)	WEB-07	Mechanisms exist to implement Strong Customer Authentication (SCA) for consumers to reasonably prove their identity.	5		WEB-06
34.d	N/A	The alerts and OTPs received by the customer for online transactions shall identify the merchant name, wherever applicable, rather than the payment aggregator through which the transaction was effected.	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
34.e	N/A	As an integral part of the multi factor authentication architecture, REs should also implement appropriate measures to minimise exposure to a middleman attack which is more commonly known as a man-in-the-middle attack (MITM), man-in-the browser (MITB) attack or man-in-the application attack. This is to ensure, among other things, that the data in transit is secured and the transactions are authenticated only by genuine/ authorised source/ process.	Functional	Intersects With	Encrypting Data In Transit	CRY-05	Cryptographic mechanisms exist to prevent the unauthorized disclosure of data in transit.	5		CRY-03
34.e	N/A	As an integral part of the multi factor authentication architecture, REs should also implement appropriate measures to minimise exposure to a middleman attack which is more commonly known as a man-in-the-middle attack (MITM), man-in-the browser (MITB) attack or man-in-the application attack. This is to ensure, among other things, that the data in transit is secured and the transactions are authenticated only by genuine/ authorised source/ process.	Functional	Intersects With	Replay-Resistant Authentication	IAC-03.1	Automated mechanisms exist to employ replay-resistant authentication.	5		IAC-02.2
34.e	N/A	As an integral part of the multi factor authentication architecture, REs should also implement appropriate measures to minimise exposure to a middleman attack which is more commonly known as a man-in-the-middle attack (MITM), man-in-the browser (MITB) attack or man-in-the application attack. This is to ensure, among other things, that the data in transit is secured and the transactions are authenticated only by genuine/ authorised source/ process.	Functional	Intersects With	Session Integrity	NET-29	Mechanisms exist to protect the authenticity and integrity of communications sessions.	5		NET-09
34.f	N/A	An authenticated session, together with its encryption protocol, should remain intact throughout the interaction with the customer. Else, in the event of interference or in case the customer closes the application, the session should be terminated, and the affected transactions resolved or reversed out. The customer should be promptly notified about the status of the transaction by email, SMS or through other means.	Functional	Intersects With	Transaction Recovery	BCD-26	Mechanisms exist to utilize specialized backup mechanisms that will allow transaction recovery for transaction-based Technology Assets, Applications and/or Services (TAAS) in accordance with Recovery Point Objectives (RPOs).	3		BCD-12.1
34.f	N/A	An authenticated session, together with its encryption protocol, should remain intact throughout the interaction with the customer. Else, in the event of interference or in case the customer closes the application, the session should be terminated, and the affected transactions resolved or reversed out. The customer should be promptly notified about the status of the transaction by email, SMS or through other means.	Functional	Intersects With	Session Termination	CFG-04.5	Automated mechanisms exist to log out users, both locally on the network and for remote sessions, at the end of the session or after an organization-defined period of inactivity.	5		IAC-25
34.f	N/A	An authenticated session, together with its encryption protocol, should remain intact throughout the interaction with the customer. Else, in the event of interference or in case the customer closes the application, the session should be terminated, and the affected transactions resolved or reversed out. The customer should be promptly notified about the status of the transaction by email, SMS or through other means.	Functional	Intersects With	Session Integrity	NET-29	Mechanisms exist to protect the authenticity and integrity of communications sessions.	5		NET-09
35	N/A	REs should set down the maximum number of failed log-in or authentication attempts after which access to the digital payment product/ service is blocked. They should have a secure procedure in place to re-activate the access to blocked product/ service. The customer shall be notified for failed log-in or authentication attempts.	Functional	Intersects With	Account Lockout	CFG-04.1	Mechanisms exist to enforce a limit for consecutive invalid login attempts by a user during an organization-defined time period and automatically locks the account when the maximum number of unsuccessful attempts is exceeded.	8		IAC-22
35	N/A	REs should set down the maximum number of failed log-in or authentication attempts after which access to the digital payment product/ service is blocked. They should have a secure procedure in place to re-activate the access to blocked product/ service. The customer shall be notified for failed log-in or authentication attempts.	Functional	Intersects With	Previous Logon Notification	SEA-29	Mechanisms exist to configure systems that process, store or transmit sensitive and/or regulated data to notify the user, upon successful logon, of the number of unsuccessful logon attempts since the last successful logon.	3		SEA-19
II.E	Fraud Risk Management	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
36	N/A	The REs shall document and implement the configuration aspects for identifying suspicious transactional behaviour in respect of rules, preventive, detective types of controls, mechanism to alert the customers in case of failed authentication, time frame for the same, etc.	Functional	Intersects With	Indicators of Compromise (IOC)	IRO-05	Mechanisms exist to define specific Indicators of Compromise (IOC) to identify the signs of potential cybersecurity events.	3		IRO-03
36	N/A	The REs shall document and implement the configuration aspects for identifying suspicious transactional behaviour in respect of rules, preventive, detective types of controls, mechanism to alert the customers in case of failed authentication, time frame for the same, etc.	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

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 Digital Payment Security Controls, 2021
Focal Document URL: https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12032
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-ind-rbi-dpsc-2021.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
37	N/A	System alerts shall be parameterised and monitored in terms of various applicable parameters. Such parameters, as applicable could be: transaction velocity (e.g., fund transfers, cash withdrawals, payments through electronic modes, adding new beneficiaries, etc.) in a short period, more so in the accounts of customers who've never used mobile app/ internet banking/ card ever (depending upon the type of payment channel), high risk merchant category codes (MCC) parameters, counterfeit card parameters (String of Invalid CVV/ PINs indicates an account generation attack), new account parameters (excessive activity on a new account), time zones, geo-locations, IP address origin (in respect of unusual patterns, prohibited zones/ rogue IPs), behavioural biometrics, transaction origination from point of compromise, transactions to mobile wallets/ mobile numbers/ VPAs on whom vishing fraud or other types of fraud is/are registered/ recorded, declined transactions, transactions with no approval code, etc.	Functional	Intersects With	System Generated Event Logs & Security-Relevant Telemetry	MON-04	Mechanisms exist to generate, monitor, correlate and respond to event logs and security-relevant telemetry from physical, cybersecurity, data protection and supply chain activities to achieve integrated situational awareness.	5		MON-01.4
37	N/A	System alerts shall be parameterised and monitored in terms of various applicable parameters. Such parameters, as applicable could be: transaction velocity (e.g., fund transfers, cash withdrawals, payments through electronic modes, adding new beneficiaries, etc.) in a short period, more so in the accounts of customers who've never used mobile app/ internet banking/ card ever (depending upon the type of payment channel), high risk merchant category codes (MCC) parameters, counterfeit card parameters (String of Invalid CVV/ PINs indicates an account generation attack), new account parameters (excessive activity on a new account), time zones, geo-locations, IP address origin (in respect of unusual patterns, prohibited zones/ rogue IPs), behavioural biometrics, transaction origination from point of compromise, transactions to mobile wallets/ mobile numbers/ VPAs on whom vishing fraud or other types of fraud is/are registered/ recorded, declined transactions, transactions with no approval code, etc.	Functional	Intersects With	Alert Threshold Tuning	MON-07	Mechanisms exist to "tune" event monitoring technologies through analyzing communications traffic/event patterns and developing profiles representing common traffic patterns and/or events.	5		MON-01.13
37	N/A	System alerts shall be parameterised and monitored in terms of various applicable parameters. Such parameters, as applicable could be: transaction velocity (e.g., fund transfers, cash withdrawals, payments through electronic modes, adding new beneficiaries, etc.) in a short period, more so in the accounts of customers who've never used mobile app/ internet banking/ card ever (depending upon the type of payment channel), high risk merchant category codes (MCC) parameters, counterfeit card parameters (String of Invalid CVV/ PINs indicates an account generation attack), new account parameters (excessive activity on a new account), time zones, geo-locations, IP address origin (in respect of unusual patterns, prohibited zones/ rogue IPs), behavioural biometrics, transaction origination from point of compromise, transactions to mobile wallets/ mobile numbers/ VPAs on whom vishing fraud or other types of fraud is/are registered/ recorded, declined transactions, transactions with no approval code, etc.	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
38	N/A	Fraud analysis shall be conducted to identify the reason for fraud occurrence and determine mechanism to prevent such frauds.	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.	5		IRO-13
38	N/A	Fraud analysis shall be conducted to identify the reason for fraud occurrence and determine mechanism to prevent such frauds.	Functional	Intersects With	Incident Pattern Analysis	IRO-17.1	Mechanisms exist to analyze historical incidents in aggregate to identify: (1) Patterns; (2) Trends; and (3) Other common root causes in order to address the vulnerability and risk.	5		IRO-09.4
39	Staff Education on Fraud Prevention Skills and Areas of Expertise	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
39.a	N/A	Fraud control tools and their usage;	Functional	Intersects With	Competency Requirements for Security, Compliance & Resilience-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security, compliance and resilience-related positions are staffed by qualified individuals who have the necessary skill set.	3		HRS-03.2
39.a	N/A	Fraud control tools and their usage;	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.	5		SAT-03
39.b	N/A	Investigative techniques and procedures;	Functional	Intersects With	Competency Requirements for Security, Compliance & Resilience-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security, compliance and resilience-related positions are staffed by qualified individuals who have the necessary skill set.	3		HRS-03.2
39.b	N/A	Investigative techniques and procedures;	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.	5		SAT-03
39.c	N/A	Cardholder and merchant education techniques to prevent fraud;	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.	5		SAT-03
39.d	N/A	Scheme/ Card operating regulations;	Functional	Intersects With	Competency Requirements for Security, Compliance & Resilience-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security, compliance and resilience-related positions are staffed by qualified individuals who have the necessary skill set.	3		HRS-03.2
39.d	N/A	Scheme/ Card operating regulations;	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.	5		SAT-03
39.e	N/A	Data processing and analysis and liaising or communicating with law enforcement agencies; and	Functional	Intersects With	Regulatory & Law Enforcement Contacts	IRO-15	Mechanisms exist to maintain incident response contacts with applicable regulatory and law enforcement agencies.	3		IRO-14
39.e	N/A	Data processing and analysis and liaising or communicating with law enforcement agencies; and	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.	5		SAT-03
39.f	N/A	The requisite skills required to (i) set and update appropriate rules, (ii) monitor the exceptions thrown based on the rules on a continuous basis and take necessary actions promptly, (iii) communicate/ escalate wherever required to appropriate authorities, and (iv) differentiate false positives from the rest.	Functional	Intersects With	Competency Requirements for Security, Compliance & Resilience-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security, compliance and resilience-related positions are staffed by qualified individuals who have the necessary skill set.	5		HRS-03.2
39.f	N/A	The requisite skills required to (i) set and update appropriate rules, (ii) monitor the exceptions thrown based on the rules on a continuous basis and take necessary actions promptly, (iii) communicate/ escalate wherever required to appropriate authorities, and (iv) differentiate false positives from the rest.	Functional	Intersects With	Alert Threshold Tuning	MON-07	Mechanisms exist to "tune" event monitoring technologies through analyzing communications traffic/event patterns and developing profiles representing common traffic patterns and/or events.	3		MON-01.13
39.f	N/A	The requisite skills required to (i) set and update appropriate rules, (ii) monitor the exceptions thrown based on the rules on a continuous basis and take necessary actions promptly, (iii) communicate/ escalate wherever required to appropriate authorities, and (iv) differentiate false positives from the rest.	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.	5		SAT-03

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 Digital Payment Security Controls, 2021**
Focal Document URL: https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12032
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-ind-rbi-dpsc-2021.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
40	N/A	REs shall maintain updated contact details of service providers, intermediaries, external agencies and other stakeholders (including other REs) for coordination in incident response. REs shall put in place a mechanism with the stakeholders to update and verify such contact details. REs shall also formulate specific SOPs to handle incidents related to payment ecosystem to mitigate the loss either to the customer or RE.	Functional	Intersects With	Correlation with External Organizations	IRO-06.1	Mechanisms exist to coordinate with approved third-parties to achieve a cross-organization perspective on incident awareness and more effective incident responses.	5		IRO-02.5
40	N/A	REs shall maintain updated contact details of service providers, intermediaries, external agencies and other stakeholders (including other REs) for coordination in incident response. REs shall put in place a mechanism with the stakeholders to update and verify such contact details. REs shall also formulate specific SOPs to handle incidents related to payment ecosystem to mitigate the loss either to the customer or RE.	Functional	Intersects With	Regulatory & Law Enforcement Contacts	IRO-15	Mechanisms exist to maintain incident response contacts with applicable regulatory and law enforcement agencies.	3		IRO-14
40	N/A	REs shall maintain updated contact details of service providers, intermediaries, external agencies and other stakeholders (including other REs) for coordination in incident response. REs shall put in place a mechanism with the stakeholders to update and verify such contact details. REs shall also formulate specific SOPs to handle incidents related to payment ecosystem to mitigate the loss either to the customer or RE.	Functional	Intersects With	Coordination With External Providers	IRO-19.1	Mechanisms exist to establish a direct, cooperative relationship between the organization's incident response capability and external service providers.	5		IRO-11.2
40	N/A	REs shall maintain updated contact details of service providers, intermediaries, external agencies and other stakeholders (including other REs) for coordination in incident response. REs shall put in place a mechanism with the stakeholders to update and verify such contact details. REs shall also formulate specific SOPs to handle incidents related to payment ecosystem to mitigate the loss either to the customer or RE.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-04	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	3		OPS-01.1
II.F	Reconciliation Mechanism	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
41	N/A	A real time/ near-real time (not later than 24 hours from the time of receipt of settlement file(s)) reconciliation framework for all digital payment transactions between RE and all other stakeholders such as payment system operators, business correspondents, card networks, payment system processors, payment aggregators, payment gateways, third party technology service providers, other participants, etc., shall be put in place for better detection and prevention of suspicious transactions. A mechanism shall be introduced to monitor the implementation and effectiveness of such framework.	Functional	Intersects With	Continuous Monitoring	MON-02	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	3		MON-01
41	N/A	A real time/ near-real time (not later than 24 hours from the time of receipt of settlement file(s)) reconciliation framework for all digital payment transactions between RE and all other stakeholders such as payment system operators, business correspondents, card networks, payment system processors, payment aggregators, payment gateways, third party technology service providers, other participants, etc., shall be put in place for better detection and prevention of suspicious transactions. A mechanism shall be introduced to monitor the implementation and effectiveness of such framework.	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	3		MON-16
II.G	Customer Protection, Awareness and Grievance Redressal Mechanism	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
42	N/A	REs shall incorporate secure, safe and responsible usage guidelines and training materials for end users within the digital payment applications. They shall also make it mandatory (i.e. not providing any option to circumvent/ avoid the material) for the consumer to go through secure usage guidelines (even in the consumer's preferred language) while obtaining and recording confirmation during the on-boarding procedure in the first instance and first use after each update of the digital payment application or after major updates to secure and safe usage guidelines.	Functional	Intersects With	Secure Practices Guidelines	OPS-06	Mechanisms exist to provide guidelines and recommendations for the secure use of Technology Assets, Applications and/or Services (TAAS) to assist in the configuration, installation and use of the product and/or service.	5		OPS-05
42	N/A	REs shall incorporate secure, safe and responsible usage guidelines and training materials for end users within the digital payment applications. They shall also make it mandatory (i.e. not providing any option to circumvent/ avoid the material) for the consumer to go through secure usage guidelines (even in the consumer's preferred language) while obtaining and recording confirmation during the on-boarding procedure in the first instance and first use after each update of the digital payment application or after major updates to secure and safe usage guidelines.	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-04	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	3		SAT-02
43	N/A	REs shall mention/ incorporate a section on the digital payment application clearly specifying the process and procedure (with forms/ contact information, etc.) to lodge consumer grievances. A mechanism to keep this information periodically updated shall also be put in place. The reporting facility on the application shall provide an option for registering a grievance. Customer dispute handling, reporting and resolution procedures, including the expected timelines for the RE's response should be clearly defined.	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
43	N/A	REs shall mention/ incorporate a section on the digital payment application clearly specifying the process and procedure (with forms/ contact information, etc.) to lodge consumer grievances. A mechanism to keep this information periodically updated shall also be put in place. The reporting facility on the application shall provide an option for registering a grievance. Customer dispute handling, reporting and resolution procedures, including the expected timelines for the RE's response should be clearly defined.	Functional	Intersects With	Grievance Response	CPL-22.1	Mechanisms exist to respond to legitimate grievances related to the organization's cybersecurity and/or data protection practices.	5		CPL-07.1
44	N/A	REs shall adhere to extant instructions, updated from time to time, to put in place system/s for online dispute resolution for resolving disputes and grievances of customers pertaining to digital payments.	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
44	N/A	REs shall adhere to extant instructions, updated from time to time, to put in place system/s for online dispute resolution for resolving disputes and grievances of customers pertaining to digital payments.	Functional	Intersects With	Grievance Response	CPL-22.1	Mechanisms exist to respond to legitimate grievances related to the organization's cybersecurity and/or data protection practices.	5		CPL-07.1
45	N/A	REs shall educate customers about the need to maintain the physical and logical security of their devices accessing digital payment products and services including recommending secure/ regular installation of operating system and application updates, downloading applications only from authorised sources, having anti-malware/ anti-virus applications on devices, etc.	Functional	Intersects With	Secure Practices Guidelines	OPS-06	Mechanisms exist to provide guidelines and recommendations for the secure use of Technology Assets, Applications and/or Services (TAAS) to assist in the configuration, installation and use of the product and/or service.	3		OPS-05
45	N/A	REs shall educate customers about the need to maintain the physical and logical security of their devices accessing digital payment products and services including recommending secure/ regular installation of operating system and application updates, downloading applications only from authorised sources, having anti-malware/ anti-virus applications on devices, etc.	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-04	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	5		SAT-02
46	N/A	REs shall ensure that its customers are provided information about the risks, benefits and liabilities of using digital payment products and its related services before they subscribe to them. Customers shall also be informed clearly and precisely on their rights, obligations and responsibilities on matters relating to digital payments, and, any problems that may arise from its service unavailability, processing errors and security breaches. The terms and conditions including customer privacy and security policy applying to digital payment products and services shall be readily available to customers within the product. All digital channels are to be offered on express willingness of customers and shall not be bundled without their knowledge.	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

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 Digital Payment Security Controls, 2021
Focal Document URL: https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12032
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-ind-rbi-dpsc-2021.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
46	N/A	REs shall ensure that its customers are provided information about the risks, benefits and liabilities of using digital payment products and its related services before they subscribe to them. Customers shall also be informed clearly and precisely on their rights, obligations and responsibilities on matters relating to digital payments, and, any problems that may arise from its service unavailability, processing errors and security breaches. The terms and conditions including customer privacy and security policy applying to digital payment products and services shall be readily available to customers within the product. All digital channels are to be offered on express willingness of customers and shall not be bundled without their knowledge.	Functional	Intersects With	Data Subject Consent	PRI-24	Mechanisms exist to enable data subjects to authorize the collection, receipt, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where the data subject is provided, prior to collection, with: (1) Plain language explaining the potential data privacy risks of the authorization; (2) A means to decline the authorization; and (3) Necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	5		PRI-03
46	N/A	REs shall ensure that its customers are provided information about the risks, benefits and liabilities of using digital payment products and its related services before they subscribe to them. Customers shall also be informed clearly and precisely on their rights, obligations and responsibilities on matters relating to digital payments, and, any problems that may arise from its service unavailability, processing errors and security breaches. The terms and conditions including customer privacy and security policy applying to digital payment products and services shall be readily available to customers within the product. All digital channels are to be offered on express willingness of customers and shall not be bundled without their knowledge.	Functional	Intersects With	Data Subject Communications	PRI-37	Mechanisms exist to craft disclosures and communications to data subjects in a manner that is concise, unambiguous and understandable by a reasonable person.	3		PRI-17
47	N/A	Whenever new operating features or functions, particularly those relating to security, integrity and authentication, are introduced to online delivery channels, clear and effective communication followed by sufficient instructions to properly utilise such new features should be provided to the customers.	Functional	Intersects With	Stakeholder Notification of Changes	CHG-08	Mechanisms exist to ensure stakeholders are made aware of and understand the impact of proposed changes.	5		CHG-05
47	N/A	Whenever new operating features or functions, particularly those relating to security, integrity and authentication, are introduced to online delivery channels, clear and effective communication followed by sufficient instructions to properly utilise such new features should be provided to the customers.	Functional	Intersects With	Secure Practices Guidelines	OPS-06	Mechanisms exist to provide guidelines and recommendations for the secure use of Technology Assets, Applications and/or Services (TAAS) to assist in the configuration, installation and use of the product and/or service.	5		OPS-05
48	N/A	REs may continuously create public awareness on the types of threats and attacks used against the consumers while using digital payment products and precautionary measures to safeguard against the same. Customers shall be cautioned against commonly known threats in recent times like phishing, vishing, reverse-phishing, remote access of mobile devices and educated to secure and safeguard their account details, credentials, PIN, card details, devices, etc.	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-04	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	3		SAT-02
48	N/A	REs may continuously create public awareness on the types of threats and attacks used against the consumers while using digital payment products and precautionary measures to safeguard against the same. Customers shall be cautioned against commonly known threats in recent times like phishing, vishing, reverse-phishing, remote access of mobile devices and educated to secure and safeguard their account details, credentials, PIN, card details, devices, etc.	Functional	Intersects With	Social Engineering & Mining	SAT-06.1	Mechanisms exist to include awareness training on recognizing and reporting potential and actual instances of social engineering and social mining.	5		SAT-02.2
49	N/A	REs shall provide digital payment products and services, to a customer only at her/ his option based on specific written or authenticated electronic requisition along with a positive acknowledgement of the terms and conditions.	Functional	Intersects With	Data Subject Consent	PRI-24	Mechanisms exist to enable data subjects to authorize the collection, receipt, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where the data subject is provided, prior to collection, with: (1) Plain language explaining the potential data privacy risks of the authorization; (2) A means to decline the authorization; and (3) Necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	5		PRI-03
49	N/A	REs shall provide digital payment products and services, to a customer only at her/ his option based on specific written or authenticated electronic requisition along with a positive acknowledgement of the terms and conditions.	Functional	Intersects With	Data Subject Opt-In Consent	PRI-27	Mechanisms exist to obtain consent from data subjects to opt-in for the following Personal Data (PD) actions: (1) Collecting; (2) Receiving; (3) Processing; (4) Storing; (5) Transmitting; (6) Sharing; and/or (7) Updating.	5		PRI-03.12
50	N/A	REs should provide a mechanism on their mobile and internet banking application for their customers to, with necessary authentication, identify/ mark a transaction as fraudulent for seamless and immediate notification to his RE. On such notification by the customer, the REs may endeavour to build the capability for seamless/ instant reporting of fraudulent transactions to the corresponding beneficiary/ counterparty's RE; vice-versa have mechanism to receive such fraudulent transactions reported from other REs. The objective of this mechanism is to accelerate early detection and enable the banking/ payment system to trace the transaction trail and mitigate the loss to the defrauded customer at the earliest possible time.	Functional	Intersects With	Correlation with External Organizations	IRO-06.1	Mechanisms exist to coordinate with approved third-parties to achieve a cross-organization perspective on incident awareness and more effective incident responses.	3		IRO-02.5
50	N/A	REs should provide a mechanism on their mobile and internet banking application for their customers to, with necessary authentication, identify/ mark a transaction as fraudulent for seamless and immediate notification to his RE. On such notification by the customer, the REs may endeavour to build the capability for seamless/ instant reporting of fraudulent transactions to the corresponding beneficiary/ counterparty's RE; vice-versa have mechanism to receive such fraudulent transactions reported from other REs. The objective of this mechanism is to accelerate early detection and enable the banking/ payment system to trace the transaction trail and mitigate the loss to the defrauded customer at the earliest possible time.	Functional	Intersects With	Incident Stakeholder Reporting	IRO-16	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	3		IRO-10
50	N/A	REs should provide a mechanism on their mobile and internet banking application for their customers to, with necessary authentication, identify/ mark a transaction as fraudulent for seamless and immediate notification to his RE. On such notification by the customer, the REs may endeavour to build the capability for seamless/ instant reporting of fraudulent transactions to the corresponding beneficiary/ counterparty's RE; vice-versa have mechanism to receive such fraudulent transactions reported from other REs. The objective of this mechanism is to accelerate early detection and enable the banking/ payment system to trace the transaction trail and mitigate the loss to the defrauded customer at the earliest possible time.	Functional	Intersects With	Incident Reporting Assistance	IRO-18	Mechanisms exist to provide incident response advice and assistance to users of Technology Assets, Applications and/or Services (TAAS) for the handling and reporting of actual and potential cybersecurity and data protection incidents.	5		IRO-11
ChIII	Internet Banking Security Controls	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
51	N/A	Internet banking websites are vulnerable to authentication related brute force attacks/ application layer Denial of Service (DoS) attacks. Based on the RE's individual risk/ vulnerability assessment on authentication-related attacks such as brute force/ DoS attacks, REs shall implement additional levels of authentication to internet banking website such as adaptive authentication, strong CAPTCHA (preferably with anti-bot features) with server-side validation, etc., in order to plug this vulnerability and prevent its exploitation. Appropriate measures shall be taken to prevent DNS cache poisoning attacks and for secure handling of cookies. Virtual keyboard option should be made available.	Functional	Intersects With	Domain Name Service (DNS) Resolution	NET-13	Mechanisms exist to ensure Domain Name Service (DNS) resolution is designed, implemented and managed to protect the security of name / address resolution.	5		NET-10
51	N/A	Internet banking websites are vulnerable to authentication related brute force attacks/ application layer Denial of Service (DoS) attacks. Based on the RE's individual risk/ vulnerability assessment on authentication-related attacks such as brute force/ DoS attacks, REs shall implement additional levels of authentication to internet banking website such as adaptive authentication, strong CAPTCHA (preferably with anti-bot features) with server-side validation, etc., in order to plug this vulnerability and prevent its exploitation. Appropriate measures shall be taken to prevent DNS cache poisoning attacks and for secure handling of cookies. Virtual keyboard option should be made available.	Functional	Intersects With	Denial of Service (DoS) Protection	NET-21	Automated mechanisms exist to protect against or limit the effects of denial of service attacks.	5		NET-02.1

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

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

Focal Document: **Reserve Bank of India (RBI) - Master Direction on Digital Payment Security Controls, 2021**
Focal Document URL: https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12032
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-ind-rbi-dpsc-2021.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
51	N/A	Internet banking websites are vulnerable to authentication related brute force attacks/ application layer Denial of Service (DoS) attacks. Based on the RE's individual risk/ vulnerability assessment on authentication-related attacks such as brute force/ DoS attacks, REs shall implement additional levels of authentication to internet banking website such as adaptive authentication, strong CAPTCHA (preferably with anti-bot features) with server-side validation, etc., in order to plug this vulnerability and prevent its exploitation. Appropriate measures shall be taken to prevent DNS cache poisoning attacks and for secure handling of cookies. Virtual keyboard option should be made available.	Functional	Intersects With	Strong Customer Authentication (SCA)	WEB-07	Mechanisms exist to implement Strong Customer Authentication (SCA) for consumers to reasonably prove their identity.	5		WEB-06
52	N/A	An online session shall be automatically terminated after a fixed period of inactivity.	Functional	Subset Of	Session Termination	CFG-04.5	Automated mechanisms exist to log out users, both locally on the network and for remote sessions, at the end of the session or after an organization-defined period of inactivity.	10		IAC-25
52	N/A	An online session shall be automatically terminated after a fixed period of inactivity.	Functional	Intersects With	Network Connection Termination	NET-28	Mechanisms exist to terminate network connections at the end of a session or after an organization-defined time period of inactivity.	5		NET-07
53	N/A	Secure delivery of password for login purpose shall be ensured. The password generated and dispatched by the RE should be valid for a limited period from the date of its creation. If the password is generated and dispatched by the RE, then, the user shall be compulsorily required to change the password, on the first login.	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.	5		IAC-10
53	N/A	Secure delivery of password for login purpose shall be ensured. The password generated and dispatched by the RE should be valid for a limited period from the date of its creation. If the password is generated and dispatched by the RE, then, the user shall be compulsorily required to change the password, on the first login.	Functional	Intersects With	Default Authenticators	IAC-14.4	Mechanisms exist to ensure default authenticators are changed as part of account creation or system installation.	5		IAC-10.8
54	N/A	When the internet banking application is accessed through external websites (eg: in case of payment of taxes, e-commerce transactions, etc.), the procedure for authentication and the appearance/ look and feel of the RE's internet banking site should be made uniform as far as possible.	Functional	Intersects With	Client-Facing Web Services	WEB-06	Mechanisms exist to deploy reasonably-expected security, compliance and resilience controls to protect the confidentiality and availability of client data that is stored, transmitted or processed by the Internet-based service.	3		WEB-04
ChIV	Mobile Payments Application Security Controls	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
55	N/A	On detection of any anomalies or exceptions for which the mobile application was not programmed, the customer shall be directed to remove the current copy/ instance of the application and proceed with installation of a new copy/ instance of the application. REs shall be able to verify the version of the mobile application before the transactions are enabled.	Functional	Intersects With	Logical Tampering Protection	AST-29.2	Mechanisms exist to assess the integrity of critical Technology Assets, Applications and/or Services (TAAS) to detect evidence of tampering, where: (1)Logical assessments evaluate the integrity of critical components (e.g., configuration settings); and (2)Physical assessments evaluate assets for evidence of unauthorized access and/or modifications.	3		AST-15
55	N/A	On detection of any anomalies or exceptions for which the mobile application was not programmed, the customer shall be directed to remove the current copy/ instance of the application and proceed with installation of a new copy/ instance of the application. REs shall be able to verify the version of the mobile application before the transactions are enabled.	Functional	Intersects With	Endpoint Integrity Checks	END-11.1	Mechanisms exist to validate configurations through integrity checking of software and firmware.	5		END-06.1
56	Specific Controls for Mobile Applications	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
56.a	N/A	Device policy enforcement (allowing app installation/ execution after baseline requirements are met);	Functional	Intersects With	Access Control For Mobile Devices	IAC-35	Automated mechanisms exist to enforce access control requirements for the connection of mobile devices to organizational Technology Assets, Applications and/or Services (TAAS).	5		MDM-02
56.a	N/A	Device policy enforcement (allowing app installation/ execution after baseline requirements are met);	Functional	Intersects With	Remote Access Endpoint Security Validation	NET-26.3	Automated mechanisms exist to validate the security posture of the endpoint devices (e.g., software versions and patch levels) prior to allowing devices to connect to organizational Technology Assets, Applications and/or Services (TAAS).	5		NET-14.7
56.b	N/A	Application secure download/ install;	Functional	Intersects With	Organization-Owned Mobile Devices	MDM-07	Mechanisms exist to prohibit the installation of non-approved applications or approved applications not obtained through the organization-approved application store.	3		MDM-07
56.b	N/A	Application secure download/ install;	Functional	Intersects With	Integrity Mechanisms for Software / Firmware Updates	TDA-06.4	Mechanisms exist to utilize integrity validation mechanisms for security updates.	5		TDA-01.2
56.c	N/A	Deactivating older application versions in a phased but time bound manner (not exceeding six months from the date of release of newer version) i.e., maintaining only one version (excluding the overlap period while phasing out older version) of the mobile application on a platform/ operating system;	Functional	Intersects With	Technology Lifecycle Management	AST-37	Mechanisms exist to manage the usable lifecycles of Technology Assets, Applications and/or Services (TAAS).	3		SEA-07.1
56.c	N/A	Deactivating older application versions in a phased but time bound manner (not exceeding six months from the date of release of newer version) i.e., maintaining only one version (excluding the overlap period while phasing out older version) of the mobile application on a platform/ operating system;	Functional	Intersects With	Removal of Previous Versions	AST-37.2	Mechanisms exist to remove old versions of software and firmware components after updated versions have been installed.	5		VPM-05.5
56.d	N/A	Storage of customer data;	Functional	Intersects With	Sensitive / Regulated Data Protection	DCH-07	Mechanisms exist to protect sensitive and/or regulated data wherever it is processed and/or stored.	5		DCH-01.2
56.d	N/A	Storage of customer data;	Functional	Intersects With	Mobile Device Data Retention Limitations	DCH-27.4	Mechanisms exist to limit data retention on mobile devices to the smallest usable dataset and timeframe.	3		MDM-08
56.e	N/A	Device or application encryption;	Functional	Intersects With	Encrypting Data At Rest	CRY-07	Cryptographic mechanisms exist to prevent the unauthorized disclosure of data at rest.	3		CRY-05
56.e	N/A	Device or application encryption;	Functional	Subset Of	Full Device & Container-Based Encryption	MDM-04	Cryptographic mechanisms exist to protect the confidentiality and integrity of information on mobile devices through full-device or container encryption.	10		MDM-03
56.f	N/A	Ensuring minimal data collection/ app permissions;	Functional	Intersects With	Minimize Sensitive / Regulated Data Exposure	DCH-27.1	Mechanisms exist to minimize sensitive and/or regulated data that is collected, received, processed, stored and/or transmitted throughout the information lifecycle to only those elements necessary to support necessary business processes.	5		DCH-18.1
56.f	N/A	Ensuring minimal data collection/ app permissions;	Functional	Intersects With	Restrict Collection, Processing & Sharing To Identified Purpose	PRI-31.1	Mechanisms exist to minimize the collection, processing and/or sharing of Personal Data (PD) to only what is adequate, relevant and limited to the purposes identified in the data privacy notice, including protections against collecting PD from minors without appropriate parental or legal guardian consent.	5		PRI-04
56.g	N/A	Application sandbox/ containerisation;	Functional	Intersects With	Process Isolation	SEA-09	Mechanisms exist to implement a separate execution domain for each executing process.	3		SEA-04
56.g	N/A	Application sandbox/ containerisation;	Functional	Subset Of	Application Container	SEA-31	Mechanisms exist to utilize an application container (virtualization approach) to isolate to a known set of dependencies, access methods and interfaces.	10		SEA-21
56.h	N/A	Ability to identify remote access applications (to the extent possible) and prohibit login access to the mobile application, as a matter of precaution; and	Functional	Intersects With	Unauthorized Activities	MON-21	Mechanisms exist to monitor for unauthorized activities, accounts, connections, devices and software.	3		MON-16.3
56.h	N/A	Ability to identify remote access applications (to the extent possible) and prohibit login access to the mobile application, as a matter of precaution; and	Functional	Intersects With	Remote Access Endpoint Security Validation	NET-26.3	Automated mechanisms exist to validate the security posture of the endpoint devices (e.g., software versions and patch levels) prior to allowing devices to connect to organizational Technology Assets, Applications and/or Services (TAAS).	5		NET-14.7
56.i	N/A	Code obfuscation.	Functional	Intersects With	Concealment & Misdirection	SEA-24	Mechanisms exist to utilize concealment and misdirection techniques for Technology Assets, Applications and/or Services (TAAS) to confuse and mislead adversaries.	3		SEA-14
56.i	N/A	Code obfuscation.	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-05	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	3		TDA-06
57	N/A	REs may consider to perform validation on the security and compatibility condition of the device/ operating system and the mobile application to ensure that activities relating to the account are put through the mobile application in a safe and secure manner.	Functional	Intersects With	Access Control For Mobile Devices	IAC-35	Automated mechanisms exist to enforce access control requirements for the connection of mobile devices to organizational Technology Assets, Applications and/or Services (TAAS).	3		MDM-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 Digital Payment Security Controls, 2021**
Focal Document URL: https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12032
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-ind-rbi-dpsc-2021.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
57	N/A	REs may consider to perform validation on the security and compatibility condition of the device/ operating system and the mobile application to ensure that activities relating to the account are put through the mobile application in a safe and secure manner.	Functional	Intersects With	Remote Access Endpoint Security Validation	NET-26.3	Automated mechanisms exist to validate the security posture of the endpoint devices (e.g., software versions and patch levels) prior to allowing devices to connect to organizational Technology Assets, Applications and/or Services (TAAS).	5		NET-14.7
58	N/A	REs may explore the feasibility of implementing a code that checks if the device is rooted/ jailbroken prior to the installation of the mobile application and disallow the mobile application to install/ function if the phone is rooted/ jailbroken.	Functional	Intersects With	Centralized Management Of Mobile Devices	MDM-02	Mechanisms exist to implement and govern Mobile Device Management (MDM) controls.	3		MDM-01
58	N/A	REs may explore the feasibility of implementing a code that checks if the device is rooted/ jailbroken prior to the installation of the mobile application and disallow the mobile application to install/ function if the phone is rooted/ jailbroken.	Functional	Intersects With	Remote Access Endpoint Security Validation	NET-26.3	Automated mechanisms exist to validate the security posture of the endpoint devices (e.g., software versions and patch levels) prior to allowing devices to connect to organizational Technology Assets, Applications and/or Services (TAAS).	5		NET-14.7
59	N/A	Checksum of current active version of application shall be hosted on public platform so that users can verify the same.	Functional	Intersects With	Cryptographic Hash	CRY-14	Mechanisms exist to utilize hash algorithms to generate a hash value that can be used to validate the integrity of data and/or software.	3		CRY-13
59	N/A	Checksum of current active version of application shall be hosted on public platform so that users can verify the same.	Functional	Subset Of	Software Release Integrity Verification	TDA-06.5	Mechanisms exist to publish integrity verification information for software releases.	10		TDA-20.1
60	N/A	REs shall ensure device binding of mobile application.	Functional	Intersects With	Identification & Authentication for Devices	IAC-34	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) devices before establishing a connection using bidirectional authentication that is cryptographically- based and replay resistant.	5		IAC-04
61	N/A	Considering that the additional factor of authentication and mobile application may reside on the same mobile device in the case of mobile banking, mobile payments, REs may consider implementing alternatives to SMS-based OTP authentication mechanisms.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-37	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.	3		IAC-06
61	N/A	Considering that the additional factor of authentication and mobile application may reside on the same mobile device in the case of mobile banking, mobile payments, REs may consider implementing alternatives to SMS-based OTP authentication mechanisms.	Functional	Intersects With	Out-of-Band (OOB) Multi-Factor Authentication (MFA)	IAC-37.3	Mechanisms exist to implement Out-of-Band (OOB) Multi-Factor Authentication (MFA) for access to privileged and non-privileged accounts such that one of the factors is independently provided by a device separate from the system being accessed.	5		IAC-06.4
62	N/A	The mobile application should require re-authentication whenever the device or application remains unused for a designated period and each time the user launches the application. Applications must be able to identify new network connections or connections from unsecured networks like unsecured Wi-Fi connections and must implement appropriate authentication/ checks/ measures to perform transactions under those circumstances.	Functional	Intersects With	Adaptive Identification & Authentication	IAC-41	Mechanisms exist to allow individuals to utilize alternative methods of authentication under specific circumstances or situations.	5		IAC-13
62	N/A	The mobile application should require re-authentication whenever the device or application remains unused for a designated period and each time the user launches the application. Applications must be able to identify new network connections or connections from unsecured networks like unsecured Wi-Fi connections and must implement appropriate authentication/ checks/ measures to perform transactions under those circumstances.	Functional	Intersects With	Re-Authentication	IAC-43	Mechanisms exist to force users and devices to re-authenticate according to organization-defined circumstances that necessitate re-authentication.	8		IAC-14
63	N/A	The mobile application should not store/ retain sensitive personal/ consumer authentication information such as user IDs, passwords, keys, hashes, hard coded references on the device and the application should securely wipe any sensitive customer information from memory when the customer/ user exits the application.	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
63	N/A	The mobile application should not store/ retain sensitive personal/ consumer authentication information such as user IDs, passwords, keys, hashes, hard coded references on the device and the application should securely wipe any sensitive customer information from memory when the customer/ user exits the application.	Functional	Intersects With	No Embedded Unencrypted Static Authenticators	IAC-14.3	Mechanisms exist to ensure that unencrypted, static authenticators are not embedded in applications, scripts or stored on function keys.	5		IAC-10.6
63	N/A	The mobile application should not store/ retain sensitive personal/ consumer authentication information such as user IDs, passwords, keys, hashes, hard coded references on the device and the application should securely wipe any sensitive customer information from memory when the customer/ user exits the application.	Functional	Intersects With	Non-Persistent Information	SEA-17.1	Mechanisms exist to: (1) Generate or refresh information per an organization-defined frequency; and (2) Delete information when no longer needed.	3		SEA-08.2
64	N/A	REs shall ensure that their mobile application limit the writing of sensitive information into 'temp' files. The sensitive information written in such files must be suitably encrypted/ masked/ hashed and stored securely.	Functional	Intersects With	Encrypting Data At Rest	CRY-07	Cryptographic mechanisms exist to prevent the unauthorized disclosure of data at rest.	5		CRY-05
64	N/A	REs shall ensure that their mobile application limit the writing of sensitive information into 'temp' files. The sensitive information written in such files must be suitably encrypted/ masked/ hashed and stored securely.	Functional	Intersects With	Temporary Files Containing Personal Data (PD)	PRI-30.2	Mechanisms exist to perform periodic checks of temporary files for the existence of Personal Data (PD).	5		DCH-18.3
65	N/A	REs may consider designing anti-malware capabilities into their mobile applications.	Functional	Intersects With	Malicious Code Protection (Antimalware)	END-04	Mechanisms exist to utilize antimalware, or similar technologies, to detect and eradicate malicious code.	5		END-04
66	N/A	REs shall ensure that the usage of raw (visible) SQL queries in mobile applications to fetch or update data from databases is avoided. Mobile applications should be secured from SQL injection type of vulnerabilities. Sensitive information should be written to the database in an encrypted form. Web content, as part of the mobile application's layout, should not be loaded if errors are detected during SSL/ TLS negotiation. Certificate errors on account of the certificate not being signed by a recognised certificate authority; expiry/ revocation of the certificate must be displayed to the user.	Functional	Intersects With	Database Encryption	CRY-08	Mechanisms exist to ensure that database servers utilize encryption to protect the confidentiality of the data within the databases.	5		CRY-05.3
66	N/A	REs shall ensure that the usage of raw (visible) SQL queries in mobile applications to fetch or update data from databases is avoided. Mobile applications should be secured from SQL injection type of vulnerabilities. Sensitive information should be written to the database in an encrypted form. Web content, as part of the mobile application's layout, should not be loaded if errors are detected during SSL/ TLS negotiation. Certificate errors on account of the certificate not being signed by a recognised certificate authority; expiry/ revocation of the certificate must be displayed to the user.	Functional	Intersects With	PKI-Based Authentication	IAC-18	Automated mechanisms exist to validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information for PKI-based authentication.	3		IAC-10.2
66	N/A	REs shall ensure that the usage of raw (visible) SQL queries in mobile applications to fetch or update data from databases is avoided. Mobile applications should be secured from SQL injection type of vulnerabilities. Sensitive information should be written to the database in an encrypted form. Web content, as part of the mobile application's layout, should not be loaded if errors are detected during SSL/ TLS negotiation. Certificate errors on account of the certificate not being signed by a recognised certificate authority; expiry/ revocation of the certificate must be displayed to the user.	Functional	Intersects With	Input Data Validation	TDA-12	Mechanisms exist to check the validity of information inputs.	5		TDA-18
66	N/A	REs shall ensure that the usage of raw (visible) SQL queries in mobile applications to fetch or update data from databases is avoided. Mobile applications should be secured from SQL injection type of vulnerabilities. Sensitive information should be written to the database in an encrypted form. Web content, as part of the mobile application's layout, should not be loaded if errors are detected during SSL/ TLS negotiation. Certificate errors on account of the certificate not being signed by a recognised certificate authority; expiry/ revocation of the certificate must be displayed to the user.	Functional	Intersects With	Web Application Input Validation & Sanitization	WEB-08	Mechanisms exist to ensure all input handled by a web application is validated and/or sanitized.	5		WEB-09
ChV	Card Payments Security	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
67	Payment Card Industry Standards for Comprehensive Card Security	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
67.a	N/A	PCI-PIN (secure management, processing, and transmission of personal identification number (PIN) data);	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
67.a	N/A	PCI-PIN (secure management, processing, and transmission of personal identification number (PIN) data);	Functional	Intersects With	Cryptographic Key Management	CRY-10	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5		CRY-09

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 Digital Payment Security Controls, 2021
Focal Document URL: https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12032
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-ind-rbi-dpsc-2021.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
67.a	N/A	PCI-PIN (secure management, processing, and transmission of personal identification number (PIN) data);	Functional	Intersects With	Secure Practices Alignment Justification	GOV-03.1	Mechanisms exist to align the organization's Security, Compliance & Resilience Program (SCRP) with one or more industry-recognized frameworks that: (1) Support external scrutiny; and (2) Provide defensible justification for secure practices.	3		GOV-01.4
67.b	N/A	PCI-PTS (security approval framework addresses the logical and/ or physical protection of cardholder and other sensitive data at point of interaction (POI) devices and hardware security modules (HSMs);	Functional	Intersects With	Kiosks & Point of Interaction (PoI) Devices	AST-21	Mechanisms exist to appropriately protect devices that capture sensitive and/or regulated data from tampering and substitution via direct physical interaction.	5		AST-07
67.b	N/A	PCI-PTS (security approval framework addresses the logical and/ or physical protection of cardholder and other sensitive data at point of interaction (POI) devices and hardware security modules (HSMs);	Functional	Intersects With	Secure Practices Alignment Justification	GOV-03.1	Mechanisms exist to align the organization's Security, Compliance & Resilience Program (SCRP) with one or more industry-recognized frameworks that: (1) Support external scrutiny; and (2) Provide defensible justification for secure practices.	3		GOV-01.4
67.c	N/A	PCI-HSM (securing cardholder-authentication applications and processes including key generation, key injection, PIN verification, secure encryption algorithm, etc.); and	Functional	Intersects With	Cryptographic Key Management	CRY-10	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5		CRY-09
67.c	N/A	PCI-HSM (securing cardholder-authentication applications and processes including key generation, key injection, PIN verification, secure encryption algorithm, etc.); and	Functional	Intersects With	Secure Practices Alignment Justification	GOV-03.1	Mechanisms exist to align the organization's Security, Compliance & Resilience Program (SCRP) with one or more industry-recognized frameworks that: (1) Support external scrutiny; and (2) Provide defensible justification for secure practices.	3		GOV-01.4
67.c	N/A	PCI-HSM (securing cardholder-authentication applications and processes including key generation, key injection, PIN verification, secure encryption algorithm, etc.); and	Functional	Intersects With	Hardware Security Modules (HSM)	IAC-39	Automated mechanisms exist to utilize Hardware Security Modules (HSM) to protect authenticators on which the component relies.	5		IAC-12.1
67.d	N/A	PCI-P2PE (security standard that requires payment card information to be encrypted instantly upon its initial swipe and then securely transferred directly to the payment processor).	Functional	Intersects With	Pre/Post Transmission Handling	CRY-03.2	Cryptographic mechanisms exist to ensure the confidentiality and integrity of information during preparation for transmission and during reception.	3		CRY-01.3
67.d	N/A	PCI-P2PE (security standard that requires payment card information to be encrypted instantly upon its initial swipe and then securely transferred directly to the payment processor).	Functional	Intersects With	Encrypting Data In Transit	CRY-05	Cryptographic mechanisms exist to prevent the unauthorized disclosure of data in transit.	5		CRY-03
67.d	N/A	PCI-P2PE (security standard that requires payment card information to be encrypted instantly upon its initial swipe and then securely transferred directly to the payment processor).	Functional	Intersects With	Secure Practices Alignment Justification	GOV-03.1	Mechanisms exist to align the organization's Security, Compliance & Resilience Program (SCRP) with one or more industry-recognized frameworks that: (1) Support external scrutiny; and (2) Provide defensible justification for secure practices.	3		GOV-01.4
68	N/A	REs should ensure that terminals installed at the merchants for capturing card details for payments or otherwise are validated against the PCI-P2PE program to use PCI-approved P2PE solutions; PoS terminals with PIN entry installed at the merchants for capturing card payments (including the double swipe terminals) are approved by the PCI-PTS program.	Functional	Intersects With	Kiosks & Point of Interaction (PoI) Devices	AST-21	Mechanisms exist to appropriately protect devices that capture sensitive and/or regulated data from tampering and substitution via direct physical interaction.	5		AST-07
68	N/A	REs should ensure that terminals installed at the merchants for capturing card details for payments or otherwise are validated against the PCI-P2PE program to use PCI-approved P2PE solutions; PoS terminals with PIN entry installed at the merchants for capturing card payments (including the double swipe terminals) are approved by the PCI-PTS program.	Functional	Intersects With	Information Assurance Enabled Products	TDA-06.6	Mechanisms exist to limit the use of commercially-provided Information Assurance (IA) and IA-enabled IT products to those products that have been successfully evaluated against a National Information Assurance Partnership (NIAP)-approved Protection Profile or the cryptographic module is FIPS-validated or NSA-approved.	3		TDA-02.2
69	N/A	Acquirers shall secure their card payment infrastructure (Unique Key Per Terminal - UKPT or Derived Unique Key Per Transaction - DUKPT/ Terminal Line Encryption - TLE).	Functional	Intersects With	Encrypting Data In Transit	CRY-05	Cryptographic mechanisms exist to prevent the unauthorized disclosure of data in transit.	5		CRY-03
69	N/A	Acquirers shall secure their card payment infrastructure (Unique Key Per Terminal - UKPT or Derived Unique Key Per Transaction - DUKPT/ Terminal Line Encryption - TLE).	Functional	Intersects With	Cryptographic Key Management	CRY-10	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5		CRY-09
69	N/A	Acquirers shall secure their card payment infrastructure (Unique Key Per Terminal - UKPT or Derived Unique Key Per Transaction - DUKPT/ Terminal Line Encryption - TLE).	Functional	Intersects With	Device Authorization Enforcement	IAC-34.2	Mechanisms exist to enforce cryptographic communications keys to prevent one key from being used to access multiple devices.	5		IAC-04.2
70	Security Controls at Hardware Security Module (HSM)	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
70.a	N/A	The HSMs should have logging enabled, the logs must themselves be tamper proof;	Functional	Intersects With	Content of Event Logs	MON-09	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	3		MON-03
70.a	N/A	The HSMs should have logging enabled, the logs must themselves be tamper proof;	Functional	Intersects With	Protection of Event Logs & Security-Relevant Telemetry	MON-12	Mechanisms exist to protect event logs, security-relevant telemetry and audit tools from unauthorized access, modification and deletion.	5		MON-08
70.b	N/A	HSM can become a single point of failure. This needs to be mitigated by 'clustering' for high availability and ensure secure backups;	Functional	Intersects With	Failover Capability	BCD-22	Mechanisms exist to implement real-time or near-real-time failover capability to maintain availability of critical Technology Assets, Applications, Services and/or Data (TAASD).	5		BCD-12.2
70.b	N/A	HSM can become a single point of failure. This needs to be mitigated by 'clustering' for high availability and ensure secure backups;	Functional	Intersects With	Data Backups	BCD-24	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5		BCD-11
70.c	N/A	Access to the HSM should be controlled through Access Control Lists (ACLs);	Functional	Intersects With	Access Enforcement	IAC-25	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	5		IAC-20
70.d	N/A	Separate ACLs should be maintained for each individual application to ensure application level isolation;	Functional	Intersects With	Access Enforcement	IAC-25	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	5		IAC-20
70.d	N/A	Separate ACLs should be maintained for each individual application to ensure application level isolation;	Functional	Intersects With	Security Function Isolation	SEA-10	Mechanisms exist to isolate security functions from non-security functions.	3		SEA-04.1
70.e	N/A	All access to HSM should be managed and monitored using a robust Privileged Identity and Access Management solution;	Functional	Subset Of	Privileged Account Management (PAM)	IAC-10	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	10		IAC-16
70.e	N/A	All access to HSM should be managed and monitored using a robust Privileged Identity and Access Management solution;	Functional	Intersects With	Privileged User Oversight	MON-14.2	Mechanisms exist to implement enhanced activity monitoring for privileged users.	3		MON-01.15
70.f	N/A	Decryption and validation of keys, PIN should be done at HSM;	Functional	Intersects With	Cryptographic Key Management	CRY-10	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5		CRY-09
70.f	N/A	Decryption and validation of keys, PIN should be done at HSM;	Functional	Intersects With	Hardware Security Modules (HSM)	IAC-39	Automated mechanisms exist to utilize Hardware Security Modules (HSM) to protect authenticators on which the component relies.	5		IAC-12.1
70.g	N/A	Card PIN generation and printing should be directly at system connected HSM;	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
70.g	N/A	Card PIN generation and printing should be directly at system connected HSM;	Functional	Intersects With	Hardware Security Modules (HSM)	IAC-39	Automated mechanisms exist to utilize Hardware Security Modules (HSM) to protect authenticators on which the component relies.	5		IAC-12.1
70.h	N/A	CVV generation and validation should be done at HSM;	Functional	Intersects With	Cryptographic Key Management	CRY-10	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	3		CRY-09
70.h	N/A	CVV generation and validation should be done at HSM;	Functional	Intersects With	Hardware Security Modules (HSM)	IAC-39	Automated mechanisms exist to utilize Hardware Security Modules (HSM) to protect authenticators on which the component relies.	5		IAC-12.1
70.i	N/A	Ensure HSM is implemented with secure PIN block format with controls to disable outputting PIN block in weaker format;	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

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 Digital Payment Security Controls, 2021**
Focal Document URL: https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12032
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-ind-rbi-dpsc-2021.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
70.i	N/A	Ensure HSM is implemented with secure PIN block format with controls to disable outputting PIN block in weaker format;	Functional	Intersects With	Hardware Security Modules (HSM)	IAC-39	Automated mechanisms exist to utilize Hardware Security Modules (HSM) to protect authenticators on which the component relies.	3		IAC-12.1
70.j	N/A	Secure key management for HSMs (such as LMKs, etc.); and	Functional	Subset Of	Cryptographic Key Management	CRY-10	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	10		CRY-09
70.j	N/A	Secure key management for HSMs (such as LMKs, etc.); and	Functional	Intersects With	Control & Distribution of Cryptographic Keys	CRY-10.4	Mechanisms exist to facilitate the secure distribution of symmetric and asymmetric cryptographic keys using industry recognized key management technology and processes.	5		CRY-09.4
70.k	N/A	Security of the physical keys of the HSM device should be properly maintained.	Functional	Intersects With	Control & Distribution of Cryptographic Keys	CRY-10.4	Mechanisms exist to facilitate the secure distribution of symmetric and asymmetric cryptographic keys using industry recognized key management technology and processes.	3		CRY-09.4
70.k	N/A	Security of the physical keys of the HSM device should be properly maintained.	Functional	Intersects With	Physical Access Device Inventories	PES-08.1	Mechanisms exist to maintain an accurate inventory of all physical access devices (e.g., RFID cards, access fobs and door keys).	3		PES-19
71	ATM Security Measures	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
71.a	N/A	Implement security measures such as BIOS password, disabling USB ports, disabling auto-run facility, applying the latest patches of operating system and other softwares, terminal security solution, time-based admin access, etc;	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02
71.a	N/A	Implement security measures such as BIOS password, disabling USB ports, disabling auto-run facility, applying the latest patches of operating system and other softwares, terminal security solution, time-based admin access, etc;	Functional	Intersects With	Endpoint Protection Mechanisms	END-03	Mechanisms exist to protect the confidentiality, integrity, availability and safety of endpoint devices.	3		END-02
71.a	N/A	Implement security measures such as BIOS password, disabling USB ports, disabling auto-run facility, applying the latest patches of operating system and other softwares, terminal security solution, time-based admin access, etc;	Functional	Intersects With	Software & Firmware Patching	VPM-08	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5		VPM-05
71.b	N/A	Implement anti-skimming and whitelisting solution; and	Functional	Intersects With	Kiosks & Point of Interaction (PoI) Devices	AST-21	Mechanisms exist to appropriately protect devices that capture sensitive and/or regulated data from tampering and substitution via direct physical interaction.	5		AST-07
71.b	N/A	Implement anti-skimming and whitelisting solution; and	Functional	Intersects With	Explicitly Allow / Deny Applications	CFG-14.1	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	5		CFG-03.3
71.c	N/A	Upgrade all the ATMs with supported versions of operating system. Use of ATMs that have unsupported operating systems shall be prohibited.	Functional	Subset Of	Unsupported Technology Assets, Applications and/or Services (TAAS)	AST-39	Mechanisms exist to prevent unsupported Technology Assets, Applications and/or Services (TAAS) by: (1) Removing and/or replacing TAAS when support for the components is no longer available from the developer, vendor or manufacturer; and (2) Requiring justification and documented approval for the continued use of unsupported TAAS required to satisfy mission/business needs.	10		TDA-17
72	N/A	REs shall ensure robust surveillance/ monitoring of card transactions (especially overseas cash withdrawals) and setting up of rules and limits commensurate with their risk appetites. REs shall take up with the card network and/ or ATM network as the case may be, to put in place transaction limits at Card, BIN as well as at the RE level. Such limits shall be mandatorily set at the card network switch itself. Limits could be mandated both for domestic as well as international transactions separately. REs shall put in place transaction control mechanisms with necessary caps (restrictions on transactions), if any of the limits set as per the above requirement is breached. A periodic review mechanism of such limits set as per the risk appetite of the RE shall be put in place as per the Board-approved policy. REs shall institute a mechanism to monitor breaches, if any, on a 24x7 basis, including weekends, long holidays and put in place a robust incident response mechanism to mitigate the fraud loss, on account of suspicious transactions, if any. REs shall ensure that card details of the customers are not stored in plain text at the RE and its vendor(s) locations, systems and applications. REs shall also ensure that the processing of card details in readable format is performed in a secure manner to strictly avoid data leakage of sensitive customer information.	Functional	Intersects With	Incident Handling	IRO-06	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	3		IRO-02
72	N/A	REs shall ensure robust surveillance/ monitoring of card transactions (especially overseas cash withdrawals) and setting up of rules and limits commensurate with their risk appetites. REs shall take up with the card network and/ or ATM network as the case may be, to put in place transaction limits at Card, BIN as well as at the RE level. Such limits shall be mandatorily set at the card network switch itself. Limits could be mandated both for domestic as well as international transactions separately. REs shall put in place transaction control mechanisms with necessary caps (restrictions on transactions), if any of the limits set as per the above requirement is breached. A periodic review mechanism of such limits set as per the risk appetite of the RE shall be put in place as per the Board-approved policy. REs shall institute a mechanism to monitor breaches, if any, on a 24x7 basis, including weekends, long holidays and put in place a robust incident response mechanism to mitigate the fraud loss, on account of suspicious transactions, if any. REs shall ensure that card details of the customers are not stored in plain text at the RE and its vendor(s) locations, systems and applications. REs shall also ensure that the processing of card details in readable format is performed in a secure manner to strictly avoid data leakage of sensitive customer information.	Functional	Intersects With	Continuous Monitoring	MON-02	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	3		MON-01
72	N/A	REs shall ensure robust surveillance/ monitoring of card transactions (especially overseas cash withdrawals) and setting up of rules and limits commensurate with their risk appetites. REs shall take up with the card network and/ or ATM network as the case may be, to put in place transaction limits at Card, BIN as well as at the RE level. Such limits shall be mandatorily set at the card network switch itself. Limits could be mandated both for domestic as well as international transactions separately. REs shall put in place transaction control mechanisms with necessary caps (restrictions on transactions), if any of the limits set as per the above requirement is breached. A periodic review mechanism of such limits set as per the risk appetite of the RE shall be put in place as per the Board-approved policy. REs shall institute a mechanism to monitor breaches, if any, on a 24x7 basis, including weekends, long holidays and put in place a robust incident response mechanism to mitigate the fraud loss, on account of suspicious transactions, if any. REs shall ensure that card details of the customers are not stored in plain text at the RE and its vendor(s) locations, systems and applications. REs shall also ensure that the processing of card details in readable format is performed in a secure manner to strictly avoid data leakage of sensitive customer information.	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
73	Card Data Scanning Tools Safety Measures	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
73.a	N/A	Any tool (procured by/ from a third-party) for the purpose of scanning of unencrypted card data should first be tested in a test environment to understand the scope and impact of the tool's capabilities;	Functional	Intersects With	Test, Validate & Document Changes	CHG-07	Mechanisms exist to appropriately test and document proposed changes in a non-production environment before changes are implemented into production.	5		CHG-02.2
73.a	N/A	Any tool (procured by/ from a third-party) for the purpose of scanning of unencrypted card data should first be tested in a test environment to understand the scope and impact of the tool's capabilities;	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
73.b	N/A	The scanning tool should be installed only in the RE's premises on their devices;	Functional	Intersects With	Periodic Scans for Sensitive / Regulated Data	DCH-05.1	Mechanisms exist to periodically scan unstructured data sources for sensitive and/or regulated data or data requiring special protection measures by statutory, regulatory or contractual obligations.	5		DCH-06.3
73.b	N/A	The scanning tool should be installed only in the RE's premises on their devices;	Functional	Intersects With	Third-Party Processing, Storage and Service Locations	TPM-12.2	Mechanisms exist to restrict the location of information processing/storage based on business requirements.	3		TPM-04.4
73.c	N/A	Card data scanning should not be done remotely;	Functional	Intersects With	Periodic Scans for Sensitive / Regulated Data	DCH-05.1	Mechanisms exist to periodically scan unstructured data sources for sensitive and/or regulated data or data requiring special protection measures by statutory, regulatory or contractual obligations.	3		DCH-06.3

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 Digital Payment Security Controls, 2021**
Focal Document URL: https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12032
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-ind-rbi-dpsc-2021.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
73.c	N/A	Card data scanning should not be done remotely;	Functional	Intersects With	Remote Access	NET-26	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	3		NET-14
73.d	N/A	The discovered data, if any, must preferably reside in the scanning tool. Exportable card data must be appropriately masked. (No data, even masked, must be taken out of the RE's premises/ infrastructure); and	Functional	Intersects With	Limitations on Use & Distribution of Sensitive / Regulated Data	DCH-08	Mechanisms exist to restrict the use and distribution of sensitive and/or regulated data.	5		DCH-10.1
73.d	N/A	The discovered data, if any, must preferably reside in the scanning tool. Exportable card data must be appropriately masked. (No data, even masked, must be taken out of the RE's premises/ infrastructure); and	Functional	Intersects With	Masking Displayed Sensitive / Regulated Data	DCH-12	Mechanisms exist to apply data masking to sensitive and/or regulated information that is displayed or printed.	5		DCH-03.2
73.e	N/A	Limited access to service providers to conduct the scan or analyse the data, if at all, must be provided only on the RE's devices.	Functional	Intersects With	Third-Party Remote Access Governance	NET-30	Mechanisms exist to proactively control and monitor third-party accounts used to access, support, or maintain system components via remote access.	3		NET-14.6
73.e	N/A	Limited access to service providers to conduct the scan or analyse the data, if at all, must be provided only on the RE's devices.	Functional	Intersects With	Third-Party Services	TPM-12	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-04