NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document Secure Controls Framework (SCF) version 2025.4
STRM Guidance: https://securecontrolsframework.com/set-theory-relationship-mapping-strm/

Focal Document: **SEBI Cybersecurity and Cyber Resilience Framework (CSCRF)**
Focal Document URL: https://www.sebi.gov.in/legal/circulars/aug-2024/cybersecurity-and-cyber-resilience-framework-cscrf-for-sebi-regulated-entities-re
Published STRM URL: https://securecontrolsframework.com/content/strm/scf-strm-apac-india-sebi.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	Self Signed RE	Small Size RE	Mid Size RE	Qualified RE	Market Infrastructure
DE.CM.S1	Security Continuous Monitoring	SOC shall cover network endpoints physical environment personnel activities etc. SOC shall be up and running 24×7×365	Functional	Subset of	Security Operations Center (SOC)	OPS-04	Mechanisms exist to establish and maintain a Security Operations Center (SOC) that facilitates a 24x7 response capability.	10	SOC requirement. Establish 24x7x365 SOC covering: network monitoring (IDS/IPS), endpoint (EDR), log analysis (SIEM), threat intelligence, incident triage; define SOC roles, escalation procedures, SLAs.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
DE.CM.S2	Security Continuous Monitoring	Appropriate continuous security monitoring mechanisms shall be established in SOC for timely detection of anomalous or malicious activities	Functional	Subset of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	Continuous monitoring. Deploy: SIEM with correlation rules, behavioral analytics (UEBA), network traffic analysis (NTA), threat intelligence feeds; tune detection rules to reduce false positives.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
DE.CM.S3	Security Continuous Monitoring	All anomalies and alerts generated shall be properly monitored and investigated within stipulated time	Functional	Intersects With	Security Event Monitoring	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	8	Alert response. Define alert SLAs: Critical (15 min), High (1 hour), Medium (4 hours); automated initial triage; escalation if SLA breach imminent.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
DE.CM.S3	Security Continuous Monitoring	All anomalies and alerts generated shall be properly monitored and investigated within stipulated time	Functional	Intersects With	Event Log Analysis & Triage	MON-17	Mechanisms exist to ensure event log reviews include analysis and triage practices.	5	Log analysis. SOC analysts investigate all alerts; document findings in ticketing system; escalate true positives to incident response; periodic review of alert disposition.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
DE.CM.S4	Security Continuous Monitoring	Capacity utilization shall be monitored for all the critical systems in the organization	Functional	Subset of	Performance Monitoring	CAP-04	Automated mechanisms exist to centrally-monitor and alert on the operating state and health status of critical systems.	10	Capacity monitoring. Monitor critical systems: CPU, memory, disk, network util	Exempted	Exempted	Mandatory	Mandatory	Mandatory
DE.CM.S5	Security Continuous Monitoring	Cybersecurity audit configuration audit implementation audit change management audit and VAPT shall be conducted to detect vulnerabilities	Functional	Subset of	Periodic Audits	CPL-02.2	Mechanisms exist to conduct periodic audits of cybersecurity & data protection controls.	10	Audit coverage. Annual comprehensive IS audit covering: policy compliance, configuration review (CIS benchmarks), implementation effectiveness, change management adherence.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
DE.CM.S5	Security Continuous Monitoring	Cybersecurity audit configuration audit implementation audit change management audit and VAPT shall be conducted to detect vulnerabilities	Functional	Intersects With	Functional Review Of Cybersecurity & Data Protection Controls	CPL-03.2	Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for adherence to the organization's cybersecurity and data protection policies and	5	Vulnerability scanning. Quarterly authenticated scans (internal/external); continuous scanning for critical assets; validate findings before remediation.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
DE.CM.S5	Security Continuous Monitoring	Cybersecurity audit configuration audit implementation audit change management audit and VAPT shall be conducted to detect vulnerabilities	Functional	Intersects With	Periodic Review	CFG-03.1	Mechanisms exist to periodically review system configurations to identify and disable unnecessary and/or non-secure functions, ports,	5	Penetration testing. Annual pen testing for all critical systems and applications; use CERT-In empanelled auditors; retest after major changes; track remediation of findings.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
DE.DP.S1	Detection Process	Roles and responsibilities for detection are defined to ensure accountability	Functional	Intersects With	Position Categorization	HRS-02	Mechanisms exist to manage personnel security risk by assigning a risk designation to all positions and establishing screening criteria for individuals filling those positions.	8	Detection roles. Define SOC team structure: SOC Manager, L1/L2/L3 analysts, threat hunters, detection engineers; document in org chart and job descriptions.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
DE.DP.S1	Detection Process	Roles and responsibilities for detection are defined to ensure accountability	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	8	Role definition. RACI matrix for detection: SOC analysts (responsible), security architects (consulted), CISO (accountable), business owners (informed).	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
DE.DP.S2	Detection Process	REs shall ensure that detection processes are tested by developing playbooks and use-cases	Functional	Intersects With	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	8	Detection testing. Develop use-case-based playbooks (phishing, ransomware, data exfiltration, insider threat); test quarterly with purple team exercises; measure detection effectiveness (MTTD).	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
DE.DP.S2	Detection Process	REs shall ensure that detection processes are tested by developing playbooks and use-cases	Functional	Intersects With	Incident Response Testing	IRO-06	Mechanisms exist to formally test incident response capabilities through realistic exercises.	8	Detection testing. Develop use-case-based playbooks (phishing, ransomware, data exfiltration, insider threat); test quarterly with purple team exercises; measure detection effectiveness (MTTD).	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
DE.DP.S3	Detection Process	Event detection information shall be communicated as per the regulatory requirements and organizational policies	Functional	Subset of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable internal stakeholders affected clients & third-parties and regulatory authorities.	10	Event reporting. Communication matrix: Critical events → CISO immediately → Board within 24hrs; CERT-In notification per directions; customer notification per regulations; stakeholder updates per	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
DE.DP.S3	Detection Process	Event detection information shall be communicated as per the regulatory requirements and organizational policies	Functional	Intersects With	Cyber Incident Reporting for Sensitive / Regulated Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	5	Event reporting. Communication matrix: Critical events → CISO immediately → Board within 24hrs; CERT-In notification per directions; customer notification per regulations; stakeholder updates per	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
DE.DP.S4	Detection Process	MIIs and Qualified REs shall conduct goal-based adversarial simulation red teaming exercise on a periodic basis	Functional	Equal	Red Team Exercises	VPM-10	Mechanisms exist to utilize red team exercises to simulate attempts by adversaries to compromise systems.	10	Red team testing. Annual red team engagement for MIIs/Qualified REs; scope critical assets; use threat intelligence-driven scenarios; measure detection/response effectiveness; executive debrief with improvement plan.	Exempted	Exempted	Exempted	Mandatory	Mandatory
DE.DP.S5	Detection Process	REs shall conduct threat hunting and compromise assessment on a regular basis	Functional	Equal	Threat Hunting	THR-07	Mechanisms exist to perform cyber threat hunting that uses Indicators of Compromise (IoC).	10	Proactive threat hunting. Quarterly hypothesis-driven threat hunts; leverage threat intel (CERT-In, vendor feeds); hunt for: lateral movement, persistence mechanisms, data staging; document TTPs found; improve detection rules.	Exempted	Exempted	Exempted	Mandatory	Mandatory
EV.ST.S1	Strategies	REs shall formulate strategies to anticipate new attack vectors by removing or applying new controls to compensate for identified vulnerabilities	Functional	Intersects With	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	8		Exempted	Exempted	Mandatory	Mandatory	Mandatory
EV.ST.S1	Strategies	REs shall formulate strategies to anticipate new attack vectors by removing or applying new controls to compensate for identified vulnerabilities	Functional	Subset of	Threat Intelligence Program	THR-01	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability.	10	Proactive threat strategy. Threat intelligence-driven security: analyze emerging threats (CERT-In, vendor intel, sector ISACs), assess organizational susceptibility, implement preemptive controls, update detection rules, threat modeling for new systems.	Exempted	Exempted	Mandatory	Mandatory	Mandatory
EV.ST.S1	Strategies	REs shall formulate strategies to anticipate new attack vectors by removing or applying new controls to compensate for identified vulnerabilities	Functional	Intersects With	Threat Intelligence Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats.	5	Threat awareness. Operationalize threat intel: integrate feeds into SIEM, automated IoC blocking, threat actor profiling, attack surface management, vulnerability prioritization based on active exploitation.	Exempted	Exempted	Mandatory	Mandatory	Mandatory
EV.ST.S2	Strategies	REs shall demonstrate heterogeneity to minimize common mode failures particularly threat events exploiting common vulnerabilities	Functional	Equal	Heterogeneity	SEA-13	Mechanisms exist to utilize a diverse set of technologies for system components to reduce the impact of technical vulnerabilities.	10	Technology diversity. Avoid mono-culture: different vendors for security tools (firewalls, EDR, email security), diverse platforms (Windows/Linux), multiple ISPs, varied database platforms; reduces blast radius of vendor-specific vulnerabilities. Platform diversity. Use virtualization/containerization to support diverse OS platforms; implement security controls at multiple layers (network, host, application); avoid dependence on single control.	Exempted	Exempted	Mandatory	Mandatory	Mandatory
EV.ST.S3	Strategies	REs shall confirm post-incident modification of business functions and supporting processes to handle adversity and address environmental changes more effectively	Functional	Intersects With	IRP Update	IRO-04.2	Mechanisms exist to regularly review and modify incident response practices to incorporate lessons learned.	8	Incident improvements. Post-incident: revise business processes with security considerations, enhance resilience (redundancy, failover), update IT architecture (segmentation, monitoring), improved vendor management, staff augmentation where gaps	Exempted	Exempted	Mandatory	Mandatory	Mandatory
EV.ST.S3	Strategies	REs shall confirm post-incident modification of business functions and supporting processes to handle adversity and address environmental changes more effectively	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity & data privacy incidents.	8	Process evolution. Document process improvements post-incident; update policies/procedures; implement new controls; validate effectiveness through testing; measure improvement (reduced MTTD/MTTR, fewer repeat incidents).	Exempted	Exempted	Mandatory	Mandatory	Mandatory
EV.ST.S4	Strategies	MIIs and Qualified REs shall continuously adapt and evolve to counter new cybersecurity threats and challenges	Functional	Intersects With	Cybersecurity & Data Protection Controls Oversight	CPL-02	Mechanisms exist to provide a cybersecurity and data protection controls oversight function that reports to the organization's executive leadership.	3	Adaptive security. Continuous evolution cycle: monitor threat landscape → assess relevance → update defenses → test effectiveness → repeat; agile security program adapting to: new attack techniques, emerging technologies, regulatory changes, business transformations.	Exempted	Exempted	Mandatory	Mandatory	Mandatory
EV.ST.S4	Strategies	MIIs and Qualified REs shall continuously adapt and evolve to counter new cybersecurity threats and challenges	Functional	Intersects With	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	8	Adaptive security. Continuous evolution cycle: monitor threat landscape → assess relevance → update defenses → test effectiveness → repeat; agile security program adapting to: new attack techniques, emerging technologies, regulatory changes, business transformations.	Exempted	Exempted	Mandatory	Mandatory	Mandatory
EV.ST.S4	Strategies	MIIs and Qualified REs shall continuously adapt and evolve to counter new cybersecurity threats and challenges	Functional	Intersects With	Threat Intelligence Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging knowledge of attacker tactics.	5	Adaptive security. Continuous evolution cycle: monitor threat landscape → assess relevance → update defenses → test effectiveness → repeat; agile security program adapting to: new attack techniques, emerging technologies, regulatory changes, business transformations.	Exempted	Exempted	Mandatory	Mandatory	Mandatory
EV.ST.S5	Strategies	Mid-size and Small-size REs shall periodically evaluate their cyber resilience posture	Functional	Subset of	Cybersecurity & Data Protection Assessments	CPL-03	Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's cybersecurity and data protection policies, standards and other applicable requirements.	10	Resilience assessment. Periodic evaluation (at least annually for small/mid-size REs): maturity assessment against CSCRF, control effectiveness testing, gap analysis, resilience metrics (MTTD, MTTR, recovery capability), benchmarking against peers; action plan for improvements; track maturity progression over	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
GV.OC.S1	Organizational Context	Critical objectives, capabilities, and services that external stakeholders depend on or expect from the REs shall be understood and communicated.	Functional	Subset of	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	10	Core governance requirement. Implement stakeholder communication matrix documenting critical services, dependencies, and impact analysis.	Exempted	Exempted	Mandatory	Mandatory	Mandatory

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	Self Signed RE	Small Size RE	Mid Size RE	Qualified RE	Market Infrastructure
GV.OC.S1	Organizational Context	Critical objectives, capabilities, and services that external stakeholders depend on or expect from the REs shall be understood and communicated.	Functional	Intersects With	Authoritative Chain of Command	GOV-04.2	Mechanisms exist to establish an authoritative chain of command with clear lines of communication to remove ambiguity from individuals and teams related to managing data and technology-related risks.	5	Chain of command should be documented espescially if external parties are involved	Exempted	Exempted	Mandatory	Mandatory	Mandatory
GV.OC.S1	Organizational Context	Critical objectives, capabilities, and services that external stakeholders depend on or expect from the REs shall be understood and communicated.	Functional	Intersects With	Define Control Objectives	GOV-09	Mechanisms exist to establish control objectives as the basis for the selection, implementation and management of the organization's internal control system.	5		Exempted	Exempted	Mandatory	Mandatory	Mandatory
GV.OC.S2	Organizational Context	Legal and regulatory requirements regarding cybersecurity, including data protection and data privacy, shall be understood and managed.	Functional	Subset of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10		Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
GV.OC.S2	Organizational Context	Legal and regulatory requirements regarding cybersecurity, including data protection and data privacy, shall be understood and managed.	Functional	Intersects With	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	8		Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
GV.OC.S3	Organizational Context	REs shall understand and communicate the outcomes, capabilities, and services dependency on external resources such as third-party service providers	Functional	Subset of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10		Exempted	Exempted	Mandatory	Mandatory	Mandatory
GV.OC.S3	Organizational Context	REs shall understand and communicate the outcomes, capabilities, and services dependency on external resources such as third-party service providers	Functional	Intersects With	Third-Party Inventories	TPM-01.1	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data	5	Maintain comprehensive third-party register with criticality assessments per GV.SC.S2 requirements.	Exempted	Exempted	Mandatory	Mandatory	Mandatory
GV.OC.S3	Organizational Context	REs shall understand and communicate the outcomes, capabilities, and services dependency on external resources such as third-party service providers	Functional	Intersects With	Third-Party Criticality Assessments	TPM-02	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value	5	Third-party dependency management. Document service dependencies, criticality ratings, and alternative provider strategies.	Exempted	Exempted	Mandatory	Mandatory	Mandatory
GV.OC.S3	Organizational Context	REs shall understand and communicate the outcomes, capabilities, and services dependency on external resources such as third-party service providers	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to: (1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and (2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.	5		Exempted	Exempted	Mandatory	Mandatory	Mandatory
GV.OC.S3	Organizational Context	REs shall understand and communicate the outcomes, capabilities, and services dependency on external resources such as third-party service providers	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity and data protection requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data	8		Exempted	Exempted	Mandatory	Mandatory	Mandatory
GV.OC.S3	Organizational Context	REs shall understand and communicate the outcomes, capabilities, and services dependency on external resources such as third-party service providers	Functional	Intersects With	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity and data protection controls between internal stakeholders and External Service Providers (ESPs).	8		Exempted	Exempted	Mandatory	Mandatory	Mandatory
GV.OV.S1	Oversight	Cybersecurity risk management strategy outcomes shall be reviewed to inform and adjust strategy and directions.	Functional	Intersects With	Status Reporting To Governing Body	GOV-01.2	Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions.	8	Executive oversight requirement. Establish quarterly Board/Partners reporting on cybersecurity posture, incidents, and risk trends.	Exempted	Exempted	Mandatory	Mandatory	Mandatory
GV.OV.S2	Oversight	The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity data protection and business alignment through a steering committee.	8	Strategic alignment. Form steering committee with CISO, CIO, CFO, business heads; meet at least quarterly to review and adjust strategy.	Exempted	Exempted	Mandatory	Mandatory	Mandatory
GV.OV.S3	Oversight	Organizational cybersecurity risk management performance is evaluated and reviewed for adjustment needed.	Functional	Subset of	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity and data protection program measures of performance.	10	Performance monitoring. Define KPIs: patch compliance %, mean time to detect/respond, control effectiveness scores, training completion rates.	Exempted	Exempted	Mandatory	Mandatory	Mandatory
GV.OV.S4	Oversight	Organizations to assess their cyber resilience posture using CCI on a periodic basis.	Functional	Subset of	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity and data protection program measures of performance.	10	Resilience measurement. Use CERT-In Cyber Crisis Index (CCI) for assessment; conduct at least annually for small/mid-size REs, quarterly for MIIs.	Exempted	Exempted	Exempted	Mandatory	Mandatory
GV.PO.S1	Policy	A comprehensive cybersecurity and cyber resilience policy shall be documented and implemented after receiving approval from Board/ Partners/ Proprietor. The cybersecurity and cyber resilience policy shall include industry best practices, and encompass standards and guidelines mentioned in this	Functional	Subset of	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish maintain and disseminate cybersecurity & data protection policies standards and procedures.	10	Policy foundation. Ensure Board/Partners/Proprietor approval documented; policy covers all CSCRF domains (Govern, Identify, Protect, Detect, Respond, Recover, Evolve).	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
GV.PO.S2	Policy	The cybersecurity and cyber resilience policy shall be reviewed periodically by the REs.	Functional	Subset of	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity & privacy program including policies standards and procedures.	10	Policy maintenance. Review at least annually or when significant changes occur (regulatory updates, major incidents, technology changes).	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
GV.PO.S3	Policy	A policy for managing cybersecurity risks shall be established based on organizational context, cybersecurity strategy, and priorities and the same shall be communicated and enforced	Functional	Intersects With	Exception Management	GOV-02.1	Mechanisms exist to prohibit exceptions to standards except when formally assessed for risk impact.	5	Establish formal exception process with risk assessment and compensating controls approval by CISO/designated authority.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
GV.PO.S3	Policy	A policy for managing cybersecurity risks shall be established based on organizational context, cybersecurity strategy, and priorities and the same shall be communicated and enforced	Functional	Subset of	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity & privacy program including policies standards and procedures.	10	Risk-based policy. Document risk appetite, tolerance, and threshold; align with GV.RM.S4 requirements.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
GV.PO.S4	Policy	The policy for managing cybersecurity risks shall be reviewed updated communicated and enforced to reflect changes in requirements threats and technologies	Functional	Subset of	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity & privacy program including policies standards and procedures.	10	Policy currency. Track SEBI circulars, CERT-In advisories, IT Act amendments; update policy within 90 days of regulatory changes.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
GV.PO.S5	Policy	Clear definition of ownership, custodian of every asset and a proper chain of command for receiving approvals shall be established and followed	Functional	Subset of	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	10	Asset accountability. Document RACI matrix for all critical assets; define escalation paths from asset owner → CISO → Board/Partners.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
GV.PO.S5	Policy	Clear definition of ownership, custodian of every asset and a proper chain of command for receiving approvals shall be established and followed	Functional	Intersects With	Stakeholder Identification & Involvement	AST-01.2	Mechanisms exist to identify and involve pertinent stakeholders of critical Technology Assets, Applications, Services and/or Data (TAASD) to support the ongoing secure management of those assets.	8	Asset accountability. Document RACI matrix for all critical assets; define escalation paths from asset owner → CISO → Board/Partners.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
GV.PO.S5	Policy	Clear definition of ownership, custodian of every asset and a proper chain of command for receiving approvals shall be established and followed	Functional	Intersects With	Asset Ownership Assignment	AST-03	Mechanisms exist to ensure asset ownership responsibilities are assigned, tracked and managed at a team, individual, or responsible organization level to establish a common understanding of requirements for asset protection.	8	Asset accountability. Document RACI matrix for all critical assets; define escalation paths from asset owner → CISO → Board/Partners.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
GV.PO.S5	Policy	Clear definition of ownership, custodian of every asset and a proper chain of command for receiving approvals shall be established and followed	Functional	Intersects With	Authoritative Chain of Command	GOV-04.2	Mechanisms exist to establish an authoritative chain of command with clear lines of communication.	8	Asset accountability. Document RACI matrix for all critical assets; define escalation paths from asset owner → CISO → Board/Partners.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
GV.RM.S1	Risk Management	REs shall prepare a cyber risk management framework to identify assess mitigate and monitor risks and define security processes and procedures	Functional	Intersects With	Define Control Objectives	GOV-09	Mechanisms exist to establish control objectives as the basis for the selection implementation and management of the organization's internal control system.	5	Risk framework foundation. Adopt ISO 27005 or NIST RMF methodology; align with SEBI circular requirements and organizational risk management.	Exempted	Exempted	Mandatory	Mandatory	Mandatory
GV.RM.S1	Risk Management	REs shall prepare a cyber risk management framework to identify assess mitigate and monitor risks and define security processes and procedures	Functional	Subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk	10	Risk framework foundation. Adopt ISO 27005 or NIST RMF methodology; align with SEBI circular requirements and organizational risk management.	Exempted	Exempted	Mandatory	Mandatory	Mandatory
GV.RM.S2	Risk Management	Cybersecurity risk management activities and outcomes shall be included in risk management processes of the REs	Functional	Subset of	Operationalizing Cybersecurity & Data Protection Practices	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity & data	10	Risk integration. Include cybersecurity risks in enterprise risk register; report cyber risks to Board Risk Committee quarterly.	Exempted	Exempted	Mandatory	Mandatory	Mandatory

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	Self Signed RE	Small Size RE	Mid Size RE	Qualified RE	Market Infrastructure
GV.RM.S3	Risk Management	Different scenarios and their respective responses shall be documented and tested on a periodic basis to check the risk management plan of the REs.	Functional	Intersects With	Contingency Plan Testing & Exercises	BCD-04	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	5	This control mandates periodic testing of continuity and recovery scenarios, which is a critical component of risk management. Testing BCP/DRP scenarios validates the organization's ability to respond to risk events.	Exempted	Exempted	Mandatory	Mandatory	Mandatory
GV.RM.S3	Risk Management	Different scenarios and their respective responses shall be documented and tested on a periodic basis to check the risk management plan of the REs.	Functional	Subset of	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	10	This control requires documented incident response procedures and plans, which form the basis for scenarios that need to be tested. However, it focuses on plan development rather than periodic testing of scenarios.	Exempted	Exempted	Mandatory	Mandatory	Mandatory
GV.RM.S3	Risk Management	Different scenarios and their respective responses shall be documented and tested on a periodic basis to check the risk management plan of the REs.	Functional	Intersects With	Incident Response Testing	IRO-06	Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.	5	This control specifically requires periodic testing of incident response scenarios, documentation of responses, and validation of incident management capabilities. It directly aligns with the requirement to test different scenarios and their responses	Exempted	Exempted	Mandatory	Mandatory	Mandatory
GV.RM.S4	Risk Management	Risk tolerance and risk appetite statements shall be established, communicated, and maintained. REs shall determine and clearly express their risk tolerance and risk acceptance. The risk tolerance of the REs shall be informed by their role in critical infrastructure and/ or sector specific risk analysis. REs shall maintain a risk register which shall be periodically reviewed by their IT Committee for REs.	Functional	Intersects With	Risk Tolerance	RSK-01.3	Mechanisms exist to define organizational risk tolerance, the specified range of acceptable results.	8	Risk appetite definition. Document risk tolerance levels (e.g., accept risks <Rs 50L impact; mitigate >Rs 50L); Board approval required.	Exempted	Exempted	Mandatory	Mandatory	Mandatory
GV.RM.S4	Risk Management	Risk tolerance and risk appetite statements shall be established, communicated, and maintained. REs shall determine and clearly express their risk tolerance and risk acceptance. The risk tolerance of the REs shall be informed by their role in critical infrastructure and/ or sector specific risk analysis. REs shall maintain a risk register which shall be periodically reviewed by their IT Committee for REs.	Functional	Intersects With	Risk Appetite	RSK-01.5	Mechanisms exist to define organizational risk appetite, the degree of uncertainty the organization is willing to accept in anticipation of a reward.	8	Risk appetite definition. Document risk tolerance levels (e.g., accept risks <Rs 50L impact; mitigate >Rs 50L); Board approval required.	Exempted	Exempted	Mandatory	Mandatory	Mandatory
GV.RM.S4	Risk Management	Risk tolerance and risk appetite statements shall be established, communicated, and maintained. REs shall determine and clearly express their risk tolerance and risk acceptance. The risk tolerance of the REs shall be informed by their role in critical infrastructure and/ or sector specific risk analysis. REs shall maintain a risk register which shall be periodically reviewed by their IT Committee for REs.	Functional	Intersects With	Risk Register	RSK-04.1	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	8	Risk appetite definition. Document risk tolerance levels (e.g., accept risks <Rs 50L impact; mitigate >Rs 50L); Board approval required.	Exempted	Exempted	Mandatory	Mandatory	Mandatory
GV.RR.S1	Roles, Responsibilities and Authorities	The responsibility and accountability for cybersecurity risk lies with the REs’ leadership and the leadership is responsible for nurturing a culture that is risk-aware, cybersecurity conscious, and continually improving.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	3		Exempted	Exempted	Mandatory	Mandatory	Mandatory
GV.RR.S1	Roles & Responsibilities - Leadership Accountability	The responsibility and accountability for cybersecurity risk lies with the REs' leadership and the leadership is responsible for nurturing a culture that is risk-aware	Functional	Subset of	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity and data protection program.	10	Leadership commitment. Board/Partners to formally acknowledge accountability; integrate security metrics into leadership performance reviews. This control also maps to NIST CSF 2.0 GV.RR-01 and GV.RR-02	Exempted	Exempted	Mandatory	Mandatory	Mandatory
GV.RR.S1	Roles & Responsibilities - Leadership Accountability	The responsibility and accountability for cybersecurity risk lies with the REs' leadership and the leadership is responsible for nurturing a culture that is risk-aware	Functional	Intersects With	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered responsible and trained.	8	Leadership commitment. Board/Partners to formally acknowledge accountability; integrate security metrics into leadership performance reviews.	Exempted	Exempted	Mandatory	Mandatory	Mandatory
GV.RR.S1	Roles, Responsibilities and Authorities	The responsibility and accountability for cybersecurity risk lies with the REs’ leadership and the leadership is responsible for nurturing a culture that is risk-aware, cybersecurity conscious, and continually improving.	Functional	Intersects With	Business As Usual (BAU) Secure Practices	GOV-14	Mechanisms exist to incorporate cybersecurity and data protection principles into Business As Usual (BAU) practices through executive leadership involvement.	5	Leadership commitment. Board/Partners to formally acknowledge accountability; integrate security metrics into leadership performance reviews.	Exempted	Exempted	Mandatory	Mandatory	Mandatory
GV.RR.S2	Roles, Responsibilities and Authorities	Cybersecurity risk management roles, responsibilities, and authorities shall be developed, communicated, understood, and enforced.	Functional	Subset of	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity and data protection program.	10	Role clarity. Document roles: CISO, security team, IT operations, business process owners, compliance; define decision rights and escalation.	Exempted	Exempted	Mandatory	Mandatory	Mandatory
GV.RR.S2	Roles, Responsibilities and Authorities	Cybersecurity risk management roles, responsibilities, and authorities shall be developed, communicated, understood, and enforced.	Functional	Intersects With	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing data and technology-related risks.	8	Role clarity. Document roles: CISO, security team, IT operations, business process owners, compliance; define decision rights and escalation.	Exempted	Exempted	Mandatory	Mandatory	Mandatory
GV.RR.S2	Roles & Responsibilities - Defined Roles	Cybersecurity risk management roles responsibilities and authorities shall be developed communicated understood and enforced	Functional	Intersects With	Position Categorization	HRS-02	Mechanisms exist to manage personnel security risk by assigning a risk designation to all positions and establishing screening criteria for individuals filling those positions.	8	Role clarity. Document roles: CISO, security team, IT operations, business process owners, compliance; define decision rights and escalation.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
GV.RR.S2	Roles & Responsibilities - Defined Roles	Cybersecurity risk management roles responsibilities and authorities shall be developed communicated understood and enforced	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	8	Role clarity. Document roles: CISO, security team, IT operations, business process owners, compliance; define decision rights and escalation.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
GV.RR.S3	Roles, Responsibilities and Authorities	A CISO/ Designated Officer shall be appointed and report to designated authority in the organization.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	8	Executive security leadership. CISO must report to CEO/MD/Board; ensure adequate budget, authority, and direct access to leadership.	Exempted	Exempted	Mandatory	Mandatory	Mandatory
GV.RR.S3	Roles, Responsibilities and Authorities	A CISO/ Designated Officer shall be appointed and report to designated authority in the organization.	Functional	Equal	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage coordinate develop implement and maintain an enterprise-wide cybersecurity & data protection program.	10	Executive security leadership. CISO must report to CEO/MD/Board; ensure adequate budget, authority, and direct access to leadership.	Exempted	Exempted	Mandatory	Mandatory	Mandatory
GV.RR.S4	Roles, Responsibilities and Authorities	Budgetary planning process shall be aligned with information security and privacy management objectives and processes. Adequate resources shall be allocated and aligned with cybersecurity risk strategy, roles and responsibilities, and policies.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	8	Resource planning. Annual security budget should align with risk assessment; include personnel, tools, training, audits, IR retainer.	Exempted	Exempted	Mandatory	Mandatory	Mandatory
GV.RR.S4	Roles, Responsibilities and Authorities	Budgetary planning process shall be aligned with information security and privacy management objectives and processes. Adequate resources shall be allocated and aligned with cybersecurity risk strategy, roles and responsibilities, and policies.	Functional	Intersects With	Cybersecurity & Data Protection Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of cybersecurity and data protection-related resource planning controls that define a viable plan for achieving cybersecurity and data protection objectives.	8	Resource planning. Annual security budget should align with risk assessment; include personnel, tools, training, audits, IR retainer.	Exempted	Exempted	Mandatory	Mandatory	Mandatory
GV.RR.S4	Roles, Responsibilities and Authorities	Budgetary planning process shall be aligned with information security and privacy management objectives and processes. Adequate resources shall be allocated and aligned with cybersecurity risk strategy, roles and responsibilities, and	Functional	Intersects With	Strategic Plan & Objectives	PRM-01.1	Mechanisms exist to establish a strategic cybersecurity and data protection-specific business plan and set of objectives to achieve that plan.	8	Resource planning. Annual security budget should align with risk assessment; include personnel, tools, training, audits, IR retainer.	Exempted	Exempted	Mandatory	Mandatory	Mandatory
GV.RR.S4	Roles, Responsibilities and Authorities	Budgetary planning process shall be aligned with information security and privacy management objectives and processes. Adequate resources shall be allocated and aligned with cybersecurity risk strategy, roles and responsibilities, and policies.	Functional	Intersects With	Allocation of Resources	PRM-03	Mechanisms exist to identify and allocate resources for management, operational, technical and data protection requirements within business process planning for projects / initiatives.	5	Resource planning. Annual security budget should align with risk assessment; include personnel, tools, training, audits, IR retainer.	Exempted	Exempted	Mandatory	Mandatory	Mandatory
GV.RR.S5	Roles, Responsibilities and Authorities	Employees and third-party service providers shall be allowed access to REs’ information systems once they have signed a confidentiality and integrity agreement	Functional	Subset of	Access Agreements	HRS-06	Mechanisms exist to require internal and third-party users to sign appropriate access agreements prior to being granted access.	10	Ensure employees and third-party providers sign confidentiality and integrity agreements prior to granting system access; document agreements and periodically review access rights.	Exempted	Exempted	Mandatory	Mandatory	Mandatory
GV.RR.S5	Roles, Responsibilities and Authorities	Employees and third-party service providers shall be allowed access to REs' information systems once they have signed a confidentiality and integrity agreement.	Functional	Intersects With	Confidentiality Agreements	HRS-06.1	Mechanisms exist to require Non-Disclosure Agreements (NDAs) or similar confidentiality agreements that reflect the needs to protect data and operational details, or both employees and third-parties.	8		Mandatory	Mandatory	Mandatory	Mandatory	Mandatory

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	Self Signed RE	Small Size RE	Mid Size RE	Qualified RE	Market Infrastructure
GV.RR.S6	Roles, Responsibilities and Authorities	Cybersecurity shall be included in human resources training programs.	Functional	Subset of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	Integrate cybersecurity topics into HR programs for all employees; include onboarding, role-specific training, and periodic refreshers to ensure understanding and compliance.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
GV.RR.S6	Roles, Responsibilities and Authorities	Cybersecurity shall be included in human resources training programs.	Functional	Intersects With	User Awareness	HRS-03.1	Mechanisms exist to communicate with users about their roles and responsibilities to maintain a safe and secure working environment.	8	Make sure assets are immediately returned after termination or end of contract.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
GV.RR.S6	Roles, Responsibilities and Authorities	Cybersecurity shall be included in human resources training programs.	Functional	Intersects With	Cybersecurity & Data Protection-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	8	Make sure assets are immediately returned after termination or end of contract.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
GV.SC.S1	Cybersecurity Supply Chain Risk Management	Cybersecurity supply chain risk management strategy/ process shall be identified, established, assessed, managed, and agreed to by organizational stakeholders.	Functional	Subset of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	Supply chain strategy. Classify vendors: critical (core banking), high (payment gateways), medium, low; define controls by tier.	Exempted	Exempted	Mandatory	Mandatory	Mandatory
GV.SC.S1	Cybersecurity Supply Chain Risk Management	Cybersecurity supply chain risk management strategy/process shall be identified established assessed managed and agreed to by organizational stakeholders	Functional	Intersects With	Third-Party Inventories	TPM-01.1	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data	5		Exempted	Exempted	Mandatory	Mandatory	Mandatory
GV.SC.S1	Cybersecurity Supply Chain Risk Management	Cybersecurity supply chain risk management strategy/process shall be identified established assessed managed and agreed to by organizational stakeholders	Functional	Intersects With	Third-Party Criticality Assessments	TPM-02	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value	5		Exempted	Exempted	Mandatory	Mandatory	Mandatory
GV.SC.S1	Cybersecurity Supply Chain Risk Management	Cybersecurity supply chain risk management strategy/process shall be identified established assessed managed and agreed to by organizational stakeholders	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to: (1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and (2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.	8		Exempted	Exempted	Mandatory	Mandatory	Mandatory
GV.SC.S2	Cybersecurity Supply Chain Risk Management	Suppliers and third-party service providers of information systems components and services shall be identified prioritized and assessed using a cyber-supply chain risk assessment process	Functional	Intersects With	Third-Party Inventories	TPM-01.1	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data	8	Supplier inventory. Maintain register with: vendor name, services provided, data access level, criticality rating, contract renewal dates.	Exempted	Exempted	Mandatory	Mandatory	Mandatory
GV.SC.S2	Cybersecurity Supply Chain Risk Management	Suppliers and third-party service providers of information systems components and services shall be identified prioritized and assessed using a cyber-supply chain risk assessment process	Functional	Intersects With	Third-Party Criticality Assessments	TPM-02	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value	8	Conduct due diligence before onboarding: financial health check	Exempted	Exempted	Mandatory	Mandatory	Mandatory
GV.SC.S3	Cybersecurity Supply Chain Risk Management	Contracts with suppliers and third-party service providers shall include appropriate measures to meet the objectives of the RE's cybersecurity program and cybersecurity supply chain risk management plan (including manpower adequacy in cybersecurity domain)	Functional	Subset of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity and data protection requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data	10	Contract requirements. Include SLAs for security (patch timelines, incident notification <6hrs), audit rights, data localization, liability.	Exempted	Exempted	Mandatory	Mandatory	Mandatory
GV.SC.S3	Cybersecurity Supply Chain Risk Management	Contracts with suppliers and third-party service providers shall include appropriate measures to meet the objectives of the RE's cybersecurity program and cybersecurity supply chain risk management plan (including manpower adequacy in cybersecurity domain)	Functional	Intersects With	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure cybersecurity and data protection requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	8	Ensure vendor contracts include subcontractor flow-down requirements; right to audit subcontractors processing RE data.	Exempted	Exempted	Mandatory	Mandatory	Mandatory
GV.SC.S3	Cybersecurity Supply Chain Risk Management	Contracts with suppliers and third-party service providers shall include appropriate measures to meet the objectives of the RE's cybersecurity program and cybersecurity supply chain risk management plan (including manpower adequacy in cybersecurity domain)	Functional	Subset of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity and data protection requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data	10	Include termination rights for material security breaches or failure to meet security SLAs; define breach notification penalties.	Exempted	Exempted	Mandatory	Mandatory	Mandatory
GV.SC.S3	Cybersecurity Supply Chain Risk Management	Contracts with suppliers and third-party service providers shall include appropriate measures to meet the objectives of the RE's cybersecurity program and cybersecurity supply chain risk management plan (including manpower adequacy in cybersecurity domain)	Functional	Intersects With	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity and data protection controls between internal stakeholders and External Service Providers (ESPs).	5	Include termination rights for material security breaches or failure to meet security SLAs; define breach notification penalties.	Exempted	Exempted	Mandatory	Mandatory	Mandatory
GV.SC.S3	Cybersecurity Supply Chain Risk Management	Contracts with suppliers and third-party service providers shall include appropriate measures to meet the objectives of the RE's cybersecurity program and cybersecurity supply chain risk management plan (including manpower adequacy in cybersecurity domain)	Functional	Intersects With	Break Clauses	TPM-05.7	Mechanisms exist to include "break clauses" within contracts for failure to meet contract criteria for cybersecurity and/or data protection controls.	5	Include termination rights for material security breaches or failure to meet security SLAs; define breach notification penalties.	Exempted	Exempted	Mandatory	Mandatory	Mandatory
GV.SC.S4	Cybersecurity Supply Chain Risk Management	REs shall monitor review and ensure compliance of third-party service providers performing critical activities for their respective organization on a periodic basis	Functional	Intersects With	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for cybersecurity and data protection controls.	8	Third-party monitoring. For critical vendors, review: quarterly SOC 2 reports, annual pen test results, monthly SLA compliance reports.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
GV.SC.S4	Cybersecurity Supply Chain Risk Management	REs shall monitor review and ensure compliance of third-party service providers performing critical activities for their respective organization on a periodic basis	Functional	Intersects With	Third-Party Deficiency Remediation	TPM-09	Mechanisms exist to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements.	8	Conduct at least annual vendor reviews: security posture reassessment; for critical vendors conduct quarterly reviews.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
GV.SC.S4	Cybersecurity Supply Chain Risk Management	REs shall monitor review and ensure compliance of third-party service providers performing critical activities for their respective organization on a periodic basis	Functional	Intersects With	Managing Changes To Third-Party Services	TPM-10	Mechanisms exist to control changes to services by suppliers, taking into account the criticality of business Technology Assets, Applications, Services and/or Data (TAASD) that are in scope by the third-party.	8	Track vendor remediation plans for identified deficiencies; escalate to procurement/legal if remediation timelines not met.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
GV.SC.S5	Cybersecurity Supply Chain Risk Management	SBOM shall be obtained for all new software procurements of core and critical activities and kept updated with every upgrade or change. In case the SBOM cannot be obtained for the legacy or proprietary systems, the Board/ Partners/ Proprietor of the organization shall approve the same with proper limitation, rationale, and risk management approach	Functional	Intersects With	Software Bill of Materials (SBOM)	TDA-04.2	Mechanisms exist to generate, or obtain, a Software Bill of Materials (SBOM) for Technology Assets, Applications and/or Services (TAAS) that lists software packages in use, including versions and applicable	5	SBOM requirement. Obtain SBOM for all COTS, custom developed software for core/critical systems; use CycloneDX or SPDX format.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
GV.SC.S6	Cybersecurity Supply Chain Risk Management	Response and recovery planning and testing shall be conducted along with third-party service providers	Functional	Intersects With	Coordinate With External Service Providers	BCD-01.2	Mechanisms exist to coordinate internal contingency plans with the contingency plans of external service providers to ensure that contingency requirements can be satisfied.	5	Contractual requirement: vendors must notify RE within 6 hours of security incident affecting RE data/services.	Exempted	Exempted	Mandatory	Mandatory	Mandatory
GV.SC.S6	Cybersecurity Supply Chain Risk Management	Response and recovery planning and testing shall be conducted along with third-party service providers	Functional	Intersects With	Correlation with External Organizations	IRO-02.5	Mechanisms exist to coordinate with approved third-parties to achieve a cross-organization perspective on incident awareness and more effective incident responses.	5	Joint response planning. Conduct annual tabletop exercises with critical vendors; test escalation procedures, communication channels.	Exempted	Exempted	Mandatory	Mandatory	Mandatory
GV.SC.S7	Cybersecurity Supply Chain Risk Management	Concentration risk on outsourced agencies shall be assessed and reviewed to achieve operational resiliency	Functional	Intersects With	Supply Chain Risk Assessment	RSK-09.1	Mechanisms exist to periodically assess supply chain risks associated with Technology Assets, Applications and/or Services (TAAS).	5	Supplier diversification. Avoid >40% dependency on single vendor for critical services; identify alternate vendors; test failover annually.	Exempted	Exempted	Mandatory	Mandatory	Mandatory
GV.SC.S8	Cybersecurity Supply Chain Risk Management	Third-party service providers shall also be mandated to follow similar standards of information security	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity and data protection requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data	5	Standards flow-down. Require vendors to implement controls equivalent to SEBI CSCRF or ISO 27001; verify through audits/certifications.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory

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	Self Signed RE	Small Size RE	Mid Size RE	Qualified RE	Market Infrastructure
GV.SC.S8	Cybersecurity Supply Chain Risk Management	Third-party service providers shall also be mandated to follow similar standards of information security	Functional	Intersects With	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure cybersecurity and data protection requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	5	Obtain annual self-attestation from vendors on compliance with contractual security requirements.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
ID.AM.S1	Asset Management	Physical devices digital assets (such as URLs domain names applications APIs etc.) shared resources and interfacing systems within the organization are inventoried	Functional	Subset of	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	10	Asset inventory baseline. Maintain comprehensive inventory: servers, workstations, network devices, applications, databases, cloud resources, APIs.	Exempted	Exempted	Mandatory	Mandatory	Mandatory
ID.AM.S2	Asset Management	Organizational communication data flows and encryption methods shall be mapped and inventoried with respect to all IT systems and network resources	Functional	Intersects With	Data Action Mapping	AST-02.8	Mechanisms exist to create and maintain a map of Technology Assets, Applications and/or Services (TAAS) where sensitive/regulated data is stored, transmitted or processed.	5		Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
ID.AM.S2	Asset Management	Organizational communication data flows and encryption methods shall be mapped and inventoried with respect to all IT systems and network resources	Functional	Equal	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and (3) Document all sensitive/regulated data flows.	10	Network documentation. Maintain: network topology diagrams, data flow diagrams showing data classification, encryption status at transit points.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
ID.AM.S3	Asset Management	REs shall ensure that no shadow IT assets are present in the organization	Functional	Intersects With	Approved Solutions	NET-04.11	Automated mechanisms exist to examine information for the presence of unsanctioned information and prohibits the transfer of such information, when transferring information between different security	5	Shadow IT prevention. Use CASB, network monitoring to detect unauthorized cloud services, applications; enforce procurement policy.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
ID.AM.S3	Asset Management	REs shall ensure that no shadow IT assets are present in the organization	Functional	Intersects With	Shadow Information Technology Detection	OPS-07	Mechanisms exist to detect the presence of unauthorized Technology Assets, Applications and/or Services (TAAS) in use.	8	Shadow IT prevention. Use CASB, network monitoring to detect unauthorized cloud services, applications; enforce procurement policy.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
ID.AM.S4	Asset Management	Board/Partners/Proprietor shall approve the list of critical systems	Functional	Intersects With	Identify Critical Assets	BCD-02	Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business functions.	8	Critical asset designation. Classify systems as critical (trading platform, payment system), high, medium, low; Board approval for critical list.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
ID.AM.S4	Asset Management	Board/Partners/Proprietor shall approve the list of critical systems	Functional	Subset of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of cybersecurity and data protection assessment and authorization controls.	10	Critical asset designation. Classify systems as critical (trading platform, payment system), high, medium, low; Board approval for critical list.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
ID.AM.S5	Asset Management	Inventories of data and corresponding metadata for designated data types are maintained	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	8	Data inventory. Document: data types (PII, financial, trading), locations (servers, databases, backups), owners, classification.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
ID.AM.S5	Asset Management	Inventories of data and corresponding metadata for designated data types are maintained	Functional	Intersects With	Sensitive Data Inventories	DCH-06.2	Mechanisms exist to maintain inventory logs of all sensitive media and conduct sensitive media inventories at least annually.	8	Classify data per PR.DS.S2 requirements: Regulatory Data vs IT/Cybersecurity Data; apply appropriate controls per classification.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
ID.AM.S6	Asset Management	All inventoried IT assets and data are managed throughout their lifecycles	Functional	Subset of	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	10	Lifecycle management. Track asset states: procurement, deployment, operation, maintenance, decommissioning; update CMDB at each stage.	Exempted	Exempted	Mandatory	Mandatory	Mandatory
ID.RA.S1	Risk Assessment	Asset vulnerabilities shall be identified validated and documented. Risk factors shall be assessed and managed for all IT assets of the REs	Functional	Intersects With	Risk Assessment	RSK-04	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	Vulnerability assessment. Conduct quarterly authenticated scans for all assets; prioritize remediation by CVSS score and asset criticality.	Exempted	Exempted	Mandatory	Mandatory	Mandatory
ID.RA.S1	Risk Assessment	Asset vulnerabilities shall be identified validated and documented. Risk factors shall be assessed and managed for all IT assets of the REs	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	Maintain risk register documenting: vulnerability details	Exempted	Exempted	Mandatory	Mandatory	Mandatory
ID.RA.S2	Risk Assessment	Risk assessment (including post-quantum risks) of REs' IT environment shall be done on a periodic basis	Functional	Subset of	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	10	Recurring risk assessment. Conduct comprehensive risk assessment at least annually; ad-hoc assessments for major changes, new threats.	Exempted	Exempted	Mandatory	Mandatory	Mandatory
ID.RA.S3	Risk Assessment	REs shall receive CTI from reliable/trusted information forums and sources. REs shall be on-boarded to CERT-In Intelligence platform	Functional	Equal	Threat Intelligence Feeds	THR-03	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	10	Threat intelligence integration. Register with CERT-In Intelligence platform; subscribe to NCIIPC advisories, SEBI circulars, industry ISACs.	Exempted	Exempted	Exempted	Mandatory	Mandatory
ID.RA.S4	Risk Assessment	Threats vulnerabilities their likelihoods and impacts shall be used to understand inherent risk and develop risk response prioritization	Functional	Subset of	Threat Analysis	THR-10	Mechanisms exist to identify, assess, prioritize and document the potential impact(s) and likelihood(s) of applicable internal and external	10	Dynamic risk assessment. Update risk assessment when: new CERT-In advisory, significant vulnerability discovered, threat landscape changes.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
ID.RA.S5	Risk Assessment	Risk responses shall be chosen prioritized planned tracked and communicated	Functional	Intersects With	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	8	Risk response actions. Document for each risk: accept (with justification), mitigate (controls), transfer (insurance), avoid (discontinue).	Exempted	Exempted	Mandatory	Mandatory	Mandatory
PR.AA.S1	Identity Management, Authentication, and Access Control	Identities and credentials are issued managed verified revoked and audited for authorized devices users and processes	Functional	Subset of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	IAM foundation. Implement centralized IAM (Active Directory, Azure AD); unique IDs for all users/devices; no shared accounts except approved.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory

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	Self Signed RE	Small Size RE	Mid Size RE	Qualified RE	Market Infrastructure
PR.AA.S1	Identity Management, Authentication, and Access Control	Identities and credentials are issued managed verified revoked and audited for authorized devices users and processes	Functional	Intersects With	Account Management	IAC-15	Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary	8	Establish account lifecycle: provisioning (with approval)	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.AA.S2	Identity Management, Authentication, and Access Control	Network integrity is protected (through measures such as network segregation network segmentation etc.)	Functional	Subset of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	Network protection. Implement: DMZ for public-facing systems, separate VLANs for trading/settlement/back-office, micro-segmentation.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.AA.S2	Identity Management, Authentication, and Access Control	Network integrity is protected (through measures such as network segregation network segmentation etc.)	Functional	Intersects With	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate Technology Assets, Applications and/or Services (TAAS) to protect from other network resources.	8	Deploy next-gen firewalls between network zones; implement network access controls; monitor inter-zone traffic.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.AA.S3	Identity Management, Authentication, and Access Control	While granting access permissions and authorizations Principle of Least Privilege shall be followed along with segregation of duties	Functional	Intersects With	Separation of Duties (SoD)	HRS-11	Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.	8	Least privilege enforcement. Grant minimum necessary access; implement RBAC; regular access reviews; SOD for critical functions (maker-checker).	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.AA.S3	Identity Management, Authentication, and Access Control	While granting access permissions and authorizations Principle of Least Privilege shall be followed along with segregation of duties	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business	5	Least privilege enforcement. Grant minimum necessary access; implement RBAC; regular access reviews; SOD for critical functions (maker-checker).	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.AA.S3	Identity Management, Authentication, and Access Control	While granting access permissions and authorizations Principle of Least Privilege shall be followed along with segregation of duties	Functional	Intersects With	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	8	Least privilege enforcement. Grant minimum necessary access; implement RBAC; regular access reviews; SOD for critical functions (maker-checker).	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.AA.S4	Identity Management, Authentication, and Access Control	REs shall follow Zero Trust Model to allow individuals devices and resources to access organization's resources	Functional	Subset of	Zero Trust Architecture (ZTA)	NET-01.1	Mechanisms exist to treat all users and devices as potential threats and prevent access to data and resources until the users can be properly authenticated and their access	10	Zero trust architecture. Implement: device authentication (802.1X), continuous authentication, micro-segmentation, assume breach mentality.	Exempted	Exempted	Mandatory	Mandatory	Mandatory
PR.AA.S5	Identity Management, Authentication, and Access Control	Access rights shall be reviewed and documented on a periodic basis. Maker-Checker framework shall be implemented for granting revoking and modifying user rights	Functional	Subset of	Periodic Review of Account Privileges	IAC-17	Mechanisms exist to periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as necessary.	10	Maker-checker: Access provisioning/modification requires approval workflow; two-person rule for privileged account creation/changes.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.AA.S6	Identity Management, Authentication, and Access Control	A comprehensive authentication policy shall be documented and implemented. Identities shall be proofed and bound to credentials	Functional	Subset of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	Authentication baseline. Policy covers: password complexity (12+ chars), MFA requirements, certificate management, biometric standards.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.AA.S6	Identity Management, Authentication, and Access Control	A comprehensive authentication policy shall be documented and implemented. Identities shall be proofed and bound to credentials	Functional	Intersects With	Authenticator Management	IAC-10	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	5	Identity proofing: verify government ID before account creation; re-verify for privileged access; annual re-verification for contractors.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.AA.S7	Identity Management, Authentication, and Access Control	All critical systems shall have MFA implemented for all users accessing from untrusted network to trusted network	Functional	Subset of	Multi-Factor Authentication (MFA)	IAC-06	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/regulated data.	10	MFA requirement. Enforce MFA for: all remote access, privileged accounts, critical system access; use phishing-resistant MFA (FIDO2, PKI).	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.AA.S8	Identity Management, Authentication, and Access Control	A comprehensive log management policy shall be documented and implemented	Functional	Subset of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	Logging policy. Log: authentication events, privileged actions, configuration changes, data access, security events; minimum fields per CSCRF.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.AA.S9	Identity Management, Authentication, and Access Control	User logs shall be uniquely identified and stored for a specified period	Functional	Intersects With	Content of Event Logs	MON-03	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.	5	User accountability. Logs must include unique user ID (not generic); link user actions to individual identity for forensics.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.AA.S9	Identity Management, Authentication, and Access Control	User logs shall be uniquely identified and stored for a specified period	Functional	Intersects With	Protection of Event Logs	MON-08	Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion.	5	Log retention. Retain logs: 365 days online, additional archival per regulatory requirements (typically 5-10 years for financial sector).	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.AA.S9	Identity Management, Authentication, and Access Control	User logs shall be uniquely identified and stored for a specified period	Functional	Intersects With	Event Log Retention	MON-10	Mechanisms exist to retain event logs for a time period consistent with records retention requirements to provide support for after-the-fact investigations of security incidents and to meet statutory, regulatory and contractual retention requirements.	8	Log retention. Retain logs: 365 days online, additional archival per regulatory requirements (typically 5-10 years for financial sector).	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.AA.S10	Identity Management, Authentication, and Access Control	Physical access to assets is managed monitored and protected. Physical access to critical systems shall be monitored and recorded on a continuous basis	Functional	Subset of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	Physical access control. Maintain authorized personnel list; issue access cards with photo ID; restrict data center access to authorized personnel	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.AA.S10	Identity Management, Authentication, and Access Control	Physical access to assets is managed monitored and protected. Physical access to critical systems shall be monitored and recorded on a continuous basis	Functional	Intersects With	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	8	Implement: biometric/card readers at entry points; mantrap for data center; escort visitors; lock server racks.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.AA.S10	Identity Management, Authentication, and Access Control	Physical access to assets is managed monitored and protected. Physical access to critical systems shall be monitored and recorded on a continuous basis	Functional	Intersects With	Access To Critical Systems	PES-03.4	Physical access control mechanisms exist to enforce physical access to critical systems or sensitive/regulated data, in addition to the physical access controls for the facility.	8	CCTV monitoring 24x7 for critical areas; record and retain footage 90+ days; integrate access logs with SIEM; alarm monitoring.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.AA.S10	Identity Management, Authentication, and Access Control	Physical access to assets is managed monitored and protected. Physical access to critical systems shall be monitored and recorded on a continuous basis	Functional	Intersects With	Monitoring Physical Access	PES-05	Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.	8	CCTV monitoring 24x7 for critical areas; record and retain footage 90+ days; integrate access logs with SIEM; alarm monitoring.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.AA.S11	Identity Management, Authentication, and Access Control	Privileged users' activities shall be reviewed periodically. Access restriction shall be there for employees as well as third-party service providers	Functional	Intersects With	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	8	PAM implementation. Deploy PAM solution for: session recording, password vaulting, just-in-time access, privileged session monitoring.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.AA.S11	Identity Management, Authentication, and Access Control	Privileged users' activities shall be reviewed periodically. Access restriction shall be there for employees as well as third-party service providers	Functional	Intersects With	Auditing Use of Privileged Functions	IAC-21.4	Mechanisms exist to audit the execution of privileged functions.	8	Privileged activity monitoring. Review privileged user logs weekly; alert on anomalous behavior; restrict third-party vendor privileged access to specific maintenance windows only.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.AA.S12	Identity Management, Authentication, and Access Control	Remote access to assets shall be strictly tracked and administered	Functional	Subset of	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	10	Remote MFA. Enforce MFA for all remote access (VPN, RDP, SSH); no exceptions even for privileged users.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.AA.S13	Identity Management, Authentication, and Access Control	A comprehensive data-disposal and data-retention policy shall be documented and implemented	Functional	Intersects With	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	8	Data retention policy. Define retention periods: transactional data per RBI/SEBI (5-10 years), logs (1+ years), backups (per RPO); secure disposal after retention.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.AA.S13	Identity Management, Authentication, and Access Control	A comprehensive data-disposal and data-retention policy shall be documented and implemented	Functional	Intersects With	Information Disposal	DCH-21	Mechanisms exist to securely dispose of, destroy or erase information.	8	Data disposal: Use NIST 800-88 compliant wiping tools; certificate of destruction for physical media; maintain disposal logs.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.AA.S14	Identity Management, Authentication, and Access Control	Comprehensive SOPs shall be documented for handling storage media devices and their disposal	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5		Mandatory	Mandatory	Mandatory	Mandatory	Mandatory

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	Self Signed RE	Small Size RE	Mid Size RE	Qualified RE	Market Infrastructure
PR.AA.S14	Identity Management, Authentication, and Access Control	Comprehensive SOPs shall be documented for handling storage media devices and their disposal	Functional	Intersects With	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	5	Equipment disposal: Wipe all storage devices before disposal/reuse; verify data cannot be recovered; decommission tracking.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.AA.S14	Identity Management, Authentication, and Access Control	Comprehensive SOPs shall be documented for handling storage media devices and their disposal	Functional	Intersects With	Media Storage	DCH-06	Mechanisms exist to: (1) Physically control and securely store digital and non-digital media within controlled areas using organization-defined security measures; and (2) Protect system media until the media are destroyed or sanitized using approved equipment, techniques and	5	Media storage. SOP covers: secure storage location, access logging, encryption requirements, inventory tracking.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.AA.S14	Identity Management, Authentication, and Access Control	Comprehensive SOPs shall be documented for handling storage media devices and their disposal	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	8	Media storage. SOP covers: secure storage location, access logging, encryption requirements, inventory tracking.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.AA.S15	Identity Management, Authentication, and Access Control	Access control for using systems such as endpoint devices networks APIs removable media laptops mobiles etc. shall be defined and implemented	Functional	Subset of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	Endpoint access. Deploy EDR on all endpoints; enforce full disk encryption; disable USB ports or use whitelisting; MDM for mobile devices.	Exempted	Exempted	Mandatory	Mandatory	Mandatory
PR.AA.S15	Identity Management, Authentication, and Access Control	Access control for using systems such as endpoint devices networks APIs removable media laptops mobiles etc. shall be defined and implemented	Functional	Intersects With	Access Enforcement	IAC-20	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	8	Access controls: Network NAC for device authentication; API authentication/authorization (OAuth 2.0); removable media controls (encryption/disable).	Exempted	Exempted	Mandatory	Mandatory	Mandatory
PR.AA.S16	Identity Management, Authentication, and Access Control	Mobile applications shall be properly vetted against security requirements and thoroughly tested before deployment	Functional	Subset of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of cybersecurity and data protection assessment and authorization controls.	10	Mobile app testing. Test against OWASP Mobile Top 10; static/dynamic analysis; pen testing before production; re-test after major updates.	Exempted	Exempted	Mandatory	Mandatory	Mandatory
PR.AA.S16	Identity Management, Authentication, and Access Control	Mobile applications shall be properly vetted against security requirements and thoroughly tested before deployment	Functional	Intersects With	Assessments	IAO-02	Mechanisms exist to formally assess the cybersecurity and data protection controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	8	Mobile app testing. Test against OWASP Mobile Top 10; static/dynamic analysis; pen testing before production; re-test after major updates.	Exempted	Exempted	Mandatory	Mandatory	Mandatory
PR.AA.S17	Identity Management, Authentication, and Access Control	API security with proper authentication and authorization mechanisms shall be defined and implemented	Functional	Equal	Application Programming Interface (API) Security	CLD-04	Mechanisms exist to ensure support for secure interoperability between components with Application Programming Interfaces (APIs).	10	API security. Implement: OAuth 2.0/JWT authentication, rate limiting, input validation, API gateway, TLS 1.2+, API inventory/documentation.	Exempted	Exempted	Mandatory	Mandatory	Mandatory
PR.AT.S1	Awareness and Training	Mandatory programs for building awareness of cybersecurity cyber resilience and system hygiene among employees shall be established	Functional	Subset of	Cybersecurity & Data Protection-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	General awareness training. Annual mandatory training covering: phishing, password security, data handling, incident reporting; quarterly updates on emerging threats.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.AT.S2	Awareness and Training	REs shall ensure that privileged users understand their roles and responsibilities	Functional	Subset of	Role-Based Cybersecurity & Data Protection Training	SAT-03	Mechanisms exist to provide role-based cybersecurity and data protection-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	10	User role awareness. Document privileged user responsibilities; obtain signed acknowledgment; quarterly reminders.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.AT.S2	Awareness and Training	REs shall ensure that privileged users understand their roles and responsibilities	Functional	Equal	Privileged Users	SAT-03.5	Mechanisms exist to provide specific training for privileged users to ensure privileged users understand their unique roles and responsibilities	10	Privileged user training. Specialized training for admins: secure configuration, privilege management, logging requirements, incident escalation; refresher every 6 months.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.AT.S3	Awareness and Training	REs shall ensure that third-party stakeholders (e.g. suppliers customers/investors partners) understand their roles and responsibilities	Functional	Subset of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity and data protection requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data	10	Third-party awareness. Include security requirements in vendor onboarding; annual security awareness refresher for vendor staff with access.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.AT.S3	Awareness and Training	REs shall ensure that third-party stakeholders (e.g. suppliers customers/investors partners) understand their roles and responsibilities	Functional	Intersects With	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity and data protection controls between internal stakeholders and External Service Providers (ESPs).	8	Third-party personnel: Require vendors to provide security training certifications; conduct security orientation for vendor staff; background checks for critical vendor personnel.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.AT.S3	Awareness and Training	REs shall ensure that third-party stakeholders (e.g. suppliers customers/investors partners) understand their roles and responsibilities	Functional	Intersects With	Third-Party Personnel Security	TPM-06	Mechanisms exist to control personnel security requirements including security roles and responsibilities for third-party providers.	8	Third-party personnel: Require vendors to provide security training certifications; conduct security orientation for vendor staff; background checks for critical vendor personnel.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.AT.S4	Awareness and Training	REs shall ensure that senior executives/Board members understand their roles and responsibilities. Further a dedicated program on cybersecurity shall be made for Board members	Functional	Intersects With	Position Categorization	HRS-02	Mechanisms exist to manage personnel security risk by assigning a risk designation to all positions and establishing screening criteria for individuals filling those positions.	8	Executive awareness. Board briefings covering: cyber risk landscape, regulatory requirements, incident impact, fiduciary responsibilities.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.AT.S4	Awareness and Training	REs shall ensure that senior executives/Board members understand their roles and responsibilities. Further a dedicated program on cybersecurity shall be made for Board members	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	8	Executive training. Dedicated Board/executive program: quarterly briefings on cyber risk, annual tabletop exercises, SEBI compliance updates, cyber insurance implications.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.AT.S4	Awareness and Training	REs shall ensure that senior executives/Board members understand their roles and responsibilities. Further a dedicated program on cybersecurity shall be made for Board members	Functional	Intersects With	User Awareness	HRS-03.1	Mechanisms exist to communicate with users about their roles and responsibilities to maintain a safe and secure working environment.	8	Executive training. Dedicated Board/executive program: quarterly briefings on cyber risk, annual tabletop exercises, SEBI compliance updates, cyber insurance implications.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.AT.S5	Awareness and Training	REs shall ensure that physical and information security personnel understand their roles and responsibilities	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	8	Security role definition. Document security team roles: SOC analysts, incident responders, security architects, compliance officers; update job	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.AT.S5	Awareness and Training	REs shall ensure that physical and information security personnel understand their roles and responsibilities	Functional	Intersects With	User Awareness	HRS-03.1	Mechanisms exist to communicate with users about their roles and responsibilities to maintain a safe and secure working environment.	8	Security personnel training. Role-specific training: SOC analysts (threat hunting, SIEM), incident responders (forensics), security architects (secure design); industry certifications (CISSP, CEH); annual	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.DS.S1	Data Security	Data-at-rest and Data-in-transit shall be protected. Strong data protection measures with industry standard encryption algorithms shall be put in place	Functional	Subset of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	Encryption baseline. Use AES-256 for data at rest, TLS 1.2+ for data in transit; disable weak ciphers (RC4, 3DES); key management per CRY-09.	Exempted	Exempted	Mandatory	Mandatory	Mandatory
PR.DS.S1	Data Security	Data-at-rest and Data-in-transit shall be protected. Strong data protection measures with industry standard encryption algorithms shall be put in place	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	Data in transit. Enforce TLS 1.2+ for web, SFTP/SCP for file transfers, IPSec for site-to-site VPN; disable legacy protocols (Telnet, FTP, SSLv3).	Exempted	Exempted	Mandatory	Mandatory	Mandatory
PR.DS.S1	Data Security	Data-at-rest and Data-in-transit shall be protected. Strong data protection measures with industry standard encryption algorithms shall be put in place	Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5	Data at rest. Full disk encryption for laptops/mobile devices; database encryption (TDE); encrypt backups; encrypted file systems for sensitive data storage. MIIs: explore data-in-use encryption.	Exempted	Exempted	Mandatory	Mandatory	Mandatory
PR.DS.S2	Data Security	REs shall classify their data into Regulatory Data and IT and Cybersecurity Data. REs shall keep the data available and accessible within legal boundaries of India	Functional	Intersects With	Geolocation Requirements for Processing, Storage and Service Locations	CLD-09	Mechanisms exist to control the location of cloud processing/storage based on business requirements that includes statutory, regulatory and contractual obligations.	5	Data localization. Regulatory and IT/Cybersecurity Data must reside in India data centers; contractually restrict cloud providers from moving data outside India; audit data location annually.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.DS.S2	Data Security	REs shall classify their data into Regulatory Data and IT and Cybersecurity Data. REs shall keep the data available and accessible within legal boundaries of India	Functional	Intersects With	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	8	Data classification. Define taxonomy: Regulatory Data (customer data, transaction records, compliance records); IT/Cybersecurity Data (logs, configs, security tools data).	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.DS.S2	Data Security	REs shall classify their data into Regulatory Data and IT and Cybersecurity Data. REs shall keep the data available and accessible within legal boundaries of India	Functional	Intersects With	Data Localization	DCH-26	Mechanisms exist to constrain the impact of "digital sovereignty laws," that require localized data within the host country, where data and processes may be subjected to arbitrary enforcement actions that potentially violate other applicable statutory, regulatory and/or	8	Data classification. Define taxonomy: Regulatory Data (customer data, transaction records, compliance records); IT/Cybersecurity Data (logs, configs, security tools data).	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory

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	Self Signed RE	Small Size RE	Mid Size RE	Qualified RE	Market Infrastructure
PR.DS.S3	Data Security	Adequate capacity to ensure Availability of data shall be maintained	Functional	Intersects With	Capacity & Performance Management	CAP-01	Mechanisms exist to facilitate the implementation of capacity management controls to ensure optimal system performance to meet expected and anticipated future capacity requirements.	5	Capacity planning for availability. Monitor capacity metrics (CPU, memory, storage, network); forecast growth; maintain 30% headroom; annual capacity review; auto-scaling where applicable.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.DS.S4	Data Security	Measures against data leaks shall be implemented. Appropriate tools shall be put in place to prevent any data leakage	Functional	Subset of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	DLP controls. Deploy DLP: endpoint agents, network DLP, email DLP, cloud DLP (CASB); policies for PII, financial data, source code.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.DS.S4	Data Security	Measures against data leaks shall be implemented. Appropriate tools shall be put in place to prevent any data leakage	Functional	Intersects With	Prevent Unauthorized Exfiltration	NET-03.5	Automated mechanisms exist to prevent the unauthorized exfiltration of sensitive/regulated data across managed interfaces.	8	DLP controls. Deploy DLP: endpoint agents, network DLP, email DLP, cloud DLP (CASB); policies for PII, financial data, source code.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.DS.S4	Data Security	Measures against data leaks shall be implemented. Appropriate tools shall be put in place to prevent any data leakage	Functional	Intersects With	Data Loss Prevention (DLP)	NET-17	Automated mechanisms exist to implement Data Loss Prevention (DLP) to protect sensitive information as it is stored, transmitted and processed.	3	DLP implementation: Block/alert on sensitive data transfers; monitor cloud uploads; USB controls; print tracking; user education on DLP alerts.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.DS.S5	Data Security	The development and testing environment(s) shall be separated from the production environment	Functional	Equal	Separation of Development, Testing and Operational Environments	TDA-08	Mechanisms exist to manage separate development, testing and operational environments to reduce the risks of unauthorized access or changes to the operational environment and to ensure no impact to production Technology Assets, Applications and/or Services (TAAS).	10	Environment segregation. Physically/logically separate dev, test, UAT, production; no production data in non-prod (use data masking); separate access controls; network segmentation between environments.	Exempted	Exempted	Exempted	Mandatory	Mandatory
PR.DS.S6	Data Security	MIIs shall put in place integrity mechanisms to verify software firmware and information integrity of its critical systems and other systems connected to its critical systems	Functional	Intersects With	Configuration Enforcement	CFG-06	Automated mechanisms exist to monitor, enforce and report on configurations for endpoint devices.	8	FIM implementation. Deploy FIM on critical systems; baseline approved configurations; alert on unauthorized changes to: system files, configs,	Exempted	Exempted	Exempted	Mandatory	Mandatory
PR.DS.S6	Data Security	MIIs shall put in place integrity mechanisms to verify software firmware and information integrity of its critical systems and other systems connected to its critical systems	Functional	Intersects With	Integrity Assurance & Enforcement (IAE)	CFG-06.1	Automated mechanisms exist to identify unauthorized deviations from an approved baseline and implement automated resiliency actions to remediate the unauthorized change.	8	FIM implementation. Deploy FIM on critical systems; baseline approved configurations; alert on unauthorized changes to: system files, configs, binaries, registry keys.	Exempted	Exempted	Exempted	Mandatory	Mandatory
PR.DS.S6	Data Security	MIIs shall put in place integrity mechanisms to verify software firmware and information integrity of its critical systems and other systems connected to its critical systems	Functional	Intersects With	Endpoint File Integrity Monitoring (FIM)	END-06	Mechanisms exist to utilize File Integrity Monitor (FIM), or similar technologies, to detect and report on unauthorized changes to selected files and configuration settings.	8	FIM implementation. Deploy FIM on critical systems; baseline approved configurations; alert on unauthorized changes to: system files, configs, binaries, registry keys.	Exempted	Exempted	Exempted	Mandatory	Mandatory
PR.DS.S6	Data Security	MIIs shall put in place integrity mechanisms to verify software firmware and information integrity of its critical systems and other systems connected to its critical systems	Functional	Intersects With	Integrity Checks	END-06.1	Mechanisms exist to validate configurations through integrity checking of software and firmware.	8	Configuration integrity. Hash verification of software/firmware before deployment; code signing for custom applications; verify digital signatures.	Exempted	Exempted	Exempted	Mandatory	Mandatory
PR.IP.S1	Information Protection Processes and Procedures	A baseline configuration of IT systems shall be created and maintained incorporating security principles (e.g. concept of least functionality)	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening	8	Baseline hardening. Develop CIS Benchmark-aligned baselines for: Windows Server, Linux, network devices, databases; disable unnecessary services/ports.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.IP.S1	Information Protection Processes and Procedures	A baseline configuration of IT systems shall be created and maintained incorporating security principles (e.g. concept of least functionality)	Functional	Intersects With	Reviews & Updates	CFG-02.1	Mechanisms exist to review and update baseline configurations: (1) At least annually; (2) When required due to so; or (3) As part of system component installations and upgrades.	8	Baseline maintenance. Review baselines annually or after major OS/application updates; version control for baseline documents; test before deployment.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.IP.S1	Information Protection Processes and Procedures	A baseline configuration of IT systems shall be created and maintained incorporating security principles (e.g. concept of least functionality)	Functional	Intersects With	Least Functionality	CFG-03	Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports,	8	Minimal services. Disable unnecessary: protocols (SMBv1, TLS 1.0/1.1), services (Telnet, FTP), features; remove unused software; close unused ports.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.IP.S2	Information Protection Processes and Procedures	A System Development Life Cycle to manage systems shall be implemented	Functional	Equal	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	10	SDLC governance. Implement secure SDLC phases: requirements (security requirements), design (threat modeling), development (secure coding), testing (SAST/DAST), deployment (security hardening), maintenance (patch management).	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.IP.S3	Information Protection Processes and Procedures	REs shall put in place processes for configuration change control as well as change management	Functional	Intersects With	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	8	Change control process. Formal change request approval (CAB); impact assessment; testing in non-prod; rollback plan; post-implementation review.	Exempted	Exempted	Mandatory	Mandatory	Mandatory
PR.IP.S3	Information Protection Processes and Procedures	REs shall put in place processes for configuration change control as well as change management	Functional	Intersects With	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	8	Change control process. Formal change request approval (CAB); impact assessment; testing in non-prod; rollback plan; post-implementation review.	Exempted	Exempted	Mandatory	Mandatory	Mandatory
PR.IP.S3	Information Protection Processes and Procedures	REs shall put in place processes for configuration change control as well as change management	Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	8	Change control process. Formal change request approval (CAB); impact assessment; testing in non-prod; rollback plan; post-implementation review.	Exempted	Exempted	Mandatory	Mandatory	Mandatory
PR.IP.S4	Information Protection Processes and Procedures	REs shall thoroughly scan Critical software/applications to ensure that no malicious code is present	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	8	Malware scanning. Deploy: multi-engine antivirus, sandboxing for email attachments, web filtering; scan custom code before deployment; YARA rules for advanced threats.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.IP.S4	Information Protection Processes and Procedures	REs shall thoroughly scan Critical software/applications to ensure that no malicious code is present	Functional	Intersects With	Always On Protection	END-04.7	Mechanisms exist to ensure that anti-malware technologies are continuously running in real-time and cannot be disabled or altered by non-privileged users, unless specifically authorized by management on a case-by-case basis for a limited time period.	5	Malware scanning. Deploy: multi-engine antivirus, sandboxing for email attachments, web filtering; scan custom code before deployment; YARA rules for advanced threats.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.IP.S5	Information Protection Processes and Procedures	If the source code of software/application is not owned by the REs then REs shall obtain an undertaking/certificate from third-party service providers	Functional	Intersects With	Software Bill of Materials (SBOM)	TDA-04.2	Mechanisms exist to generate, or obtain, a Software Bill of Materials (SBOM) for Technology Assets, Applications and/or Services (TAAS) that lists software packages in use, including versions and applicable	5	Code verification. Obtain from vendor: attestation of secure development practices, vulnerability assessment results, malware scan certificate; conduct independent security review for critical systems.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.IP.S5	Information Protection Processes and Procedures	If the source code of software/application is not owned by the REs then REs shall obtain an undertaking/certificate from third-party service providers	Functional	Intersects With	First-Party Declaration (1PD)	TPM-05.6	Mechanisms exist to obtain a First-Party Declaration(1PD) from applicable External Service Providers (ESPs) that provides assurance of compliance with specified statutory, regulatory and contractual obligations for cybersecurity and data protection controls, including any flow-down requirements to subcontractors.	5	Code verification. Obtain from vendor: attestation of secure development practices, vulnerability assessment results, malware scan certificate; conduct independent security review for critical systems.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.IP.S6	Information Protection Processes and Procedures	Testing/certification of software/applications shall broadly address objectives such as product functions only in intended manner developed per best secure practices	Functional	Subset of	Cybersecurity & Data Protection Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with cybersecurity and data protection 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 security testing and evaluation process; and (3) Document the results of the security testing/evaluation and flaw remediation processes.	10	Security testing. Conduct: SAST (static code analysis), DAST (dynamic testing), SCA (software composition analysis), pen testing; security functionality testing; negative testing.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.IP.S7	Information Protection Processes and Procedures	REs shall document backup and recovery plan of data to ensure that there is no data loss	Functional	Intersects With	Data Backups	BCD-11	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	Backup procedures. Define backup schedule (full weekly, incremental daily); 3-2-1 rule (3 copies, 2 media types, 1 offsite); encrypt backups; RPO aligned with business needs.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.IP.S7	Information Protection Processes and Procedures	REs shall document backup and recovery plan of data to ensure that there is no data loss	Functional	Intersects With	Technology Assets, Applications and/or Services (TAAS) Recovery & Reconstitution	BCD-12	Mechanisms exist to ensure the secure recovery and reconstitution of Technology Assets, Applications and/or Services (TAAS) to a known state after a disruption, compromise	8	Recovery procedures. Document recovery steps; prioritize critical systems; define RTO per system; automated recovery where possible; maintain recovery runbooks.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory

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	Self Signed RE	Small Size RE	Mid Size RE	Qualified RE	Market Infrastructure
PR.IP.S7	Information Protection Processes and Procedures	REs shall document backup and recovery plan of data to ensure that there is no data loss	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	8		Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.IP.S8	Information Protection Processes and Procedures	REs shall implement test and maintain data backups. Further drills for restoration of backup data shall be conducted on a periodic basis	Functional	Intersects With	Data Backups	BCD-11	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).	8	Backup testing. Test backup restoration quarterly for critical systems, annually for others; verify data integrity; measure actual recovery time vs RTO; document test results.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.IP.S8	Information Protection Processes and Procedures	REs shall implement test and maintain data backups. Further drills for restoration of backup data shall be conducted on a periodic basis	Functional	Intersects With	Testing for Reliability & Integrity	BCD-11.1	Mechanisms exist to routinely test backups that verify the reliability of the backup process, as well as the integrity and availability of the data.	8	Backup testing. Test backup restoration quarterly for critical systems, annually for others; verify data integrity; measure actual recovery time vs RTO; document test results.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.IP.S9	Information Protection Processes and Procedures	Policies and regulations regarding the physical operating environment for REs' assets shall be defined and adhered to	Functional	Subset of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	Physical security planning. Site plan covers: access controls, CCTV coverage, environmental controls (HVAC, fire suppression, power backup), physical penetration testing results.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.IP.S9	Information Protection Processes and Procedures	Policies and regulations regarding the physical operating environment for REs' assets shall be defined and adhered to	Functional	Intersects With	Physical Security Plan (PSP)	PES-01.1	Mechanisms exist to document a Physical Security Plan (PSP), or similar document, to summarize the implemented security controls to protect physical access to technology assets, as well as applicable risks and threats.	8	Physical security planning. Site plan covers: access controls, CCTV coverage, environmental controls (HVAC, fire suppression, power backup), physical penetration testing results.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.IP.S10	Information Protection Processes and Procedures	Effectiveness of protective technologies shall be measured on a regular basis in line with the SLAs	Functional	Subset of	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity and data protection program measures of performance.	10	Control effectiveness. Measure: firewall block rate, AV detection rate, DLP policy violations, patch compliance %; quarterly reviews against SLAs.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.IP.S11	Information Protection Processes and Procedures	Response plans (incident response and business continuity) and recovery plans shall be put in place and regularly tested and updated	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR)	8	BC/DR planning. Develop comprehensive CCMP covering: incident response, business continuity, disaster recovery; define RTOs/RPOs; Board approval; annual testing.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.IP.S11	Information Protection Processes and Procedures	Response plans (incident response and business continuity) and recovery plans shall be put in place and regularly tested and updated	Functional	Intersects With	Contingency Plan Testing & Exercises	BCD-04	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	8	RTO/RPO definition. Define per SEBI requirements: critical systems RTO ≤4 hours, RPO ≤1 hour; document in CCMP; test achievement through drills.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.IP.S12	Information Protection Processes and Procedures	A vulnerability management plan shall be developed and implemented	Functional	Equal	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	Vulnerability program. Comprehensive VPMP covering: asset inventory, vulnerability scanning schedule, prioritization criteria (CVSS + asset criticality), SLAs (critical: 7 days, high: 30 days), exception process, reporting.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.IP.S13	Information Protection Processes and Procedures	For applicable cloud instances of REs SEBI circular Framework for Adoption of Cloud Services by SEBI Regulated Entities (REs) shall be complied with	Functional	Intersects With	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	5	Cloud governance. Comply with SEBI Cloud Framework: Board approval for cloud adoption, data localization, security controls, audit rights, exit strategy, incident notification.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.IP.S13	Information Protection Processes and Procedures	For applicable cloud instances of REs SEBI circular Framework for Adoption of Cloud Services by SEBI Regulated Entities (REs) shall be complied with	Functional	Intersects With	Cloud Security Architecture	CLD-02	Mechanisms exist to ensure the cloud security architecture supports the organization's technology strategy to securely design, configure and maintain cloud employments.	5		Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.IP.S13	Information Protection Processes and Procedures	For applicable cloud instances of REs SEBI circular Framework for Adoption of Cloud Services by SEBI Regulated Entities (REs) shall be complied with	Functional	Subset of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	Cloud onboarding. Pre-onboarding assessment: CSP security review, data classification, compliance mapping, shared responsibility model understanding.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.IP.S14	Information Protection Processes and Procedures	Only CERT-In empanelled IS auditing organizations shall be onboarded for external audit of REs	Functional	Intersects With	Independent Assessors	CPL-03.1	Mechanisms exist to utilize independent assessors to evaluate cybersecurity and data protection controls at planned intervals or when the Technology Asset, Application and/or Service (TAAS) undergoes	5	Audit function. Maintain internal audit team for continuous monitoring; use CERT-In empanelled auditors for external IS audits per SEBI requirement.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.IP.S15	Information Protection Processes and Procedures	All software services shall be certified for application security and functional audit. COTS products empanelled by stock exchanges/depositories shall be certified	Functional	Subset of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	Software certification. Before production: application security testing (OWASP Top 10), functional audit; COTS from exchanges/depositories must have STQC certification; maintain certification records.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.IP.S15	Information Protection Processes and Procedures	All software services shall be certified for application security and functional audit. COTS products empanelled by stock exchanges/depositories shall be certified	Functional	Intersects With	Third-Party Attestation (3PA)	TPM-05.8	Mechanisms exist to obtain an attestation from an independent Third-Party Assessment Organization (3PAO) that provides assurance of conformity with specified statutory, regulatory and contractual obligations for cybersecurity and data protection controls, including any flow-down requirements to contractors and	8	Software certification. Before production: application security testing (OWASP Top 10), functional audit; COTS from exchanges/depositories must have STQC certification; maintain certification records.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.IP.S16	Information Protection Processes and Procedures	MIIs and Qualified REs shall obtain ISO 27001 certification	Functional	Subset of	Third-Party Attestation (3PA)	TPM-05.8	Mechanisms exist to obtain an attestation from an independent Third-Party Assessment Organization (3PAO) that provides assurance of conformity with specified statutory, regulatory and contractual obligations for cybersecurity and data protection controls, including any flow-down requirements to contractors and	10	ISO certification. MIIs and Qualified REs: obtain ISO 27001:2022 certification; maintain certification (annual surveillance, 3-year recertification); address non-conformities timely.	Exempted	Exempted	Exempted	Mandatory	Mandatory
PR.IP.S17	Information Protection Processes and Procedures	MIIs and Qualified REs shall follow globally recognized standards such as CIS Critical Security Controls to enhance their cyber resilience	Functional	Intersects With	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls.	8	CIS Controls adoption. Implement CIS Controls v8 (prioritize Implementation Groups based on organization size); use CIS-CAT for compliance	Exempted	Exempted	Exempted	Mandatory	Mandatory
PR.IP.S17	Information Protection Processes and Procedures	MIIs and Qualified REs shall follow globally recognized standards such as CIS Critical Security Controls to enhance their cyber resilience	Functional	Intersects With	Ability To Demonstrate Conformity	CPL-01.3	Mechanisms exist to ensure the organization is able to demonstrate conformity with applicable cybersecurity and data protection laws, regulations and/or contractual obligations.	8	Standards implementation: Map CSCRF to CIS Controls; implement controls by priority; measure implementation through metrics.	Exempted	Exempted	Exempted	Mandatory	Mandatory
PR.IP.S17	Information Protection Processes and Procedures	MIIs and Qualified REs shall follow globally recognized standards such as CIS Critical Security Controls to enhance their cyber resilience	Functional	Intersects With	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity & data	8	Secure engineering. Follow CIS Benchmarks for system hardening; implement defense-in-depth; security by design principles.	Exempted	Exempted	Exempted	Mandatory	Mandatory
PR.MA.S1	Maintenance	Maintenance and repair of REs' assets shall be performed and logged with approved and controlled tools	Functional	Intersects With	Test, Validate & Document Changes	CHG-02.2	Mechanisms exist to appropriately test and document proposed changes in a non-production environment before changes are implemented in a production environment.	8	Maintenance control. Maintenance procedures: approval workflow, maintenance windows, change control integration, supervised access for vendors, post-maintenance testing.	Exempted	Exempted	Mandatory	Mandatory	Mandatory
PR.MA.S1	Maintenance	Maintenance and repair of REs' assets shall be performed and logged with approved and controlled tools	Functional	Intersects With	Controlled Maintenance	MNT-02	Mechanisms exist to conduct controlled maintenance activities throughout the lifecycle of the Technology Asset, Application and/or	8	Maintenance automation. Use ITSM tools for maintenance tracking; automated patch deployment with testing; maintenance log integration with SIEM.	Exempted	Exempted	Mandatory	Mandatory	Mandatory
PR.MA.S2	Maintenance	Remote maintenance of REs' assets shall be approved logged and performed in a manner that prevents unauthorized access	Functional	Intersects With	Remote Maintenance	MNT-05	Mechanisms exist to authorize, monitor and control remote, non-local maintenance and diagnostic activities.	8	Remote maintenance security. Remote maintenance requires: advance approval, MFA, session recording, time-limited access, supervisor monitoring for critical systems, log review post-maintenance.	Exempted	Exempted	Mandatory	Mandatory	Mandatory
PR.MA.S2	Maintenance	Remote maintenance of REs' assets shall be approved logged and performed in a manner that prevents unauthorized access	Functional	Intersects With	Remote Maintenance Pre-Approval	MNT-05.5	Mechanisms exist to require maintenance personnel to obtain pre-approval and scheduling for remote, non-local maintenance sessions.	8	Remote maintenance security. Remote maintenance requires: advance approval, MFA, session recording, time-limited access, supervisor monitoring for critical systems, log review post-maintenance.	Exempted	Exempted	Mandatory	Mandatory	Mandatory
PR.MA.S3	Maintenance	Patches shall be identified and categorized based on their severity. Critical patches shall be implemented at the earliest	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	8	Patch program. Patch categorization: Critical (7 days), High (30 days), Medium (90 days); Emergency patching process for zero-days.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
PR.MA.S3	Maintenance	Patches shall be identified and categorized based on their severity. Critical patches shall be implemented at the earliest	Functional	Intersects With	Vulnerability Ranking	VPM-03	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities using reputable outside sources for security vulnerability information.	8	Patch remediation. Patch workflow: identification → testing (non-prod) → approval → deployment (prod) → verification; maintain patch compliance dashboard; exception process with compensating controls.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory

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	Self Signed RE	Small Size RE	Mid Size RE	Qualified RE	Market Infrastructure
PR.MA.S3	Maintenance	Patches shall be identified and categorized based on their severity. Critical patches shall be implemented at the earliest	Functional	Intersects With	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	8	Patch remediation. Patch workflow: identification → testing (non-prod) → approval → deployment (prod) → verification; maintain patch compliance dashboard; exception process with compensating controls.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
RC.CO.S1	Incident Recovery Communication	Public relations management as defined in the recovery plan shall be undertaken in the event of a cybersecurity incident	Functional	Subset of	Public Relations & Reputation Repair	IRO-16	Mechanisms exist to proactively manage public relations associated with incidents and employ appropriate measures to prevent further reputational damage and develop plans to repair any damage to the organization's reputation.	10	PR management. PR plan in CCMP: designated spokesperson, pre-approved messaging templates, media monitoring, social media strategy, customer communication channels, reputation repair actions; engage PR firm for major incidents.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
RC.CO.S2	Incident Recovery Communication	REs shall communicate recovery activities to internal and external stakeholders as well as executive and management teams	Functional	Equal	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	10	Recovery communication. Regular updates during recovery: internal (all hands emails, intranet), external (customer portal, website), executive (daily briefings), regulators (progress reports); communicate: systems restored, remaining work, revised ETAs.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
RC.CO.S3	Incident Recovery Communication	REs shall inform actions taken during recovery process to all related stakeholders	Functional	Subset of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	10	Action reporting. Communicate recovery actions: containment measures implemented, systems restored, security enhancements deployed, ongoing monitoring; tailor message to audience (technical for IT, business impact for executives).	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
RC.IM.S1	Improvements	Recovery plans shall be updated and improved to incorporate lessons learned from cybersecurity incidents	Functional	Intersects With	Contingency Plan Root Cause Analysis (RCA) & Lessons Learned	BCD-05	Mechanisms exist to conduct a Root Cause Analysis (RCA) and "lessons learned" activity every time the contingency plan is activated.	8	Lessons learned. Post-recovery: identify what worked well, what didn't, process improvements, tool enhancements, training needs; document in post-incident report; track implementation of	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
RC.IM.S1	Improvements	Recovery plans shall be updated and improved to incorporate lessons learned from cybersecurity incidents	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future	8	Plan updates. Post-incident: update recovery procedures based on actual recovery experience, adjust RTO/RPO if not met, additional resources/tools, improved coordination processes; version control; re-test updated procedures.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
RC.IM.S2	Improvements	REs cyber resilience capabilities shall be upgraded through periodic drills to ensure safe and timely restoration of critical operations	Functional	Intersects With	Contingency Plan Testing & Exercises	BCD-04	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	8	Resilience drills. Progressive testing: component testing (backup restore) → tabletop exercises (scenario walkthrough) → functional tests (partial failover) → full DR test (complete failover); measure improvement in recovery times; identify capability gaps; invest in tools/training to close gaps.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
RC.IM.S2	Improvements	REs cyber resilience capabilities shall be upgraded through periodic drills to ensure safe and timely restoration of critical operations	Functional	Intersects With	Contingency Plan Root Cause Analysis (RCA) & Lessons Learned	BCD-05	Mechanisms exist to conduct a Root Cause Analysis (RCA) and "lessons learned" activity every time the contingency plan is activated.	8	Resilience drills. Progressive testing: component testing (backup restore) → tabletop exercises (scenario walkthrough) → functional tests (partial failover) → full DR test (complete failover); measure improvement in recovery times; identify capability gaps; invest in tools/training to close gaps.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
RC.RP.S1	Incident Recovery Plan Execution	Recovery plan of REs shall have different cyber-scenario based classifications	Functional	Subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR)	10	Scenario-based recovery. Recovery plans for scenarios: ransomware (restore from backup), DDoS (alternate connectivity), data breach (forensics, notification), insider threat (HR coordination); scenario-specific procedures and priorities.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
RC.RP.S1	Incident Recovery Plan Execution	Recovery plan of REs shall have different cyber-scenario based classifications	Functional	Intersects With	Recovery Operations Criteria	BCD-01.5	Mechanisms exist to define specific criteria that must be met to initiate Business Continuity / Disaster Recover (BC/DR) plans that facilitate business continuity operations capable of meeting applicable Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	8	Scenario-based recovery. Recovery plans for scenarios: ransomware (restore from backup), DDoS (alternate connectivity), data breach (forensics, notification), insider threat (HR coordination); scenario-specific procedures and priorities.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
RC.RP.S2	Incident Recovery Plan Execution	RTO and RPO as specified by SEBI shall be mandated while executing recovery plan for the restoration of systems	Functional	Equal	Recovery Time / Point Objectives (RTO / RPO)	BCD-01.4	Mechanisms exist to facilitate recovery operations in accordance with Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	10	RTO/RPO compliance. SEBI requirements: Critical systems RTO ≤4 hours, RPO ≤1 hour; document system-specific RTO/RPO; design backup/recovery architecture to meet objectives; measure actual recovery times in tests.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
RC.RP.S3	Incident Recovery Plan Execution	REs shall periodically conduct drills for testing different recovery scenarios	Functional	Equal	Contingency Plan Testing & Exercises	BCD-04	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	10	Recovery testing. Conduct drills: quarterly tabletop exercises (all scenarios), annual full DR test (failover to DR site), bi-annual backup restore test (sample systems); document results, gaps, improvements.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
RC.RP.S4	Incident Recovery Plan Execution	Backup and recovery plan of data shall be documented to ensure that there is no data loss	Functional	Subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR)	10	Backup documentation. Backup plan covers: scope (all critical data), schedule (full/incremental/differential), retention (per RPO), storage locations (primary/DR site/cloud), encryption, testing frequency, restoration procedures.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
RC.RP.S4	Incident Recovery Plan Execution	Backup and recovery plan of data shall be documented to ensure that there is no data loss	Functional	Intersects With	Data Backups	BCD-11	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).	8	Backup documentation. Backup plan covers: scope (all critical data), schedule (full/incremental/differential), retention (per RPO), storage locations (primary/DR site/cloud), encryption, testing frequency, restoration procedures.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
RC.RP.S4	Incident Recovery Plan Execution	Backup and recovery plan of data shall be documented to ensure that there is no data loss	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	8	Backup documentation. Backup plan covers: scope (all critical data), schedule (full/incremental/differential), retention (per RPO), storage locations (primary/DR site/cloud), encryption, testing frequency, restoration procedures.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
RS.AN.S1	Incident Analysis	Processes shall be established to receive analyze and respond to vulnerabilities/incidents disclosed to the RE from internal and external sources	Functional	Intersects With	Threat Intelligence Feeds	THR-03	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	8	Vulnerability intake. Establish: security@domain email, vulnerability disclosure page, bug bounty ; triage within 24 hours; acknowledge researcher; coordinate disclosure timeline.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
RS.AN.S1	Incident Analysis	Processes shall be established to receive analyze and respond to vulnerabilities/incidents disclosed to the RE from internal and external sources	Functional	Intersects With	Threat Intelligence Reporting	THR-03.1	Mechanisms exist to utilize external threat intelligence feeds to generate and disseminate organization-specific security alerts, advisories and/or directives.	8	VDP implementation. Publish VDP policy (in-scope systems, disclosure timeline, recognition); respond to researchers professionally; fix verified vulnerabilities; coordinate public disclosure.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
RS.AN.S2	Incident Analysis	Cybersecurity incidents shall be categorized in-line with categorization given in RE's CCMP	Functional	Subset of	Incident Classification & Prioritization	IRO-02.4	Mechanisms exist to identify classes of incidents and actions to take to ensure the continuation of organizational missions and business	10	Incident classification. CCMP categorization (per SEBI Annexure-O): Critical (trading halt, major data breach), High, Medium, Low; priority determines response timeline and escalation.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
RS.AN.S3	Incident Analysis	Detailed investigation of cybersecurity incidents and alerts as well as a forensic analysis shall be done to identify the root-cause of the incident	Functional	Intersects With	Chain of Custody & Forensics	IRO-08	Mechanisms exist to perform digital forensics and maintain the integrity of the chain of custody, in accordance with applicable laws, regulations and industry-recognized secure practices.	8	Lateral movement detection. Use EDR logs to identify: lateral movement techniques, privilege escalation, persistence mechanisms, data staging; timeline analysis.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
RS.AN.S3	Incident Analysis	Detailed investigation of cybersecurity incidents and alerts as well as a forensic analysis shall be done to identify the root-cause of the incident	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future	8	Forensic investigation. For significant incidents: preserve evidence (chain of custody), forensic imaging, memory analysis, log correlation, malware analysis; use forensic tools; document methodology; legal admissibility considerations.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
RS.AN.S4	Incident Analysis	RCA shall be done to:	Functional	Intersects With	Contingency Plan Root Cause Analysis (RCA) & Lessons Learned	BCD-05	Mechanisms exist to conduct a Root Cause Analysis (RCA) and "lessons learned" activity every time the contingency plan is activated.	8	BC/DR RCA. For incidents requiring BC/DR activation: assess plan effectiveness, identify gaps (people/process/technology), update plans; post-incident report to Board.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
RS.AN.S4	Incident Analysis	RCA shall be done to:	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future	8	Incident RCA. Use structured RCA methodology (5 Whys, Fishbone); categorize gaps: people (training needs), process (procedure updates), technology (control implementation); assign remediation owners with deadlines.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
RS.AN.S4a	Incident Analysis	Determine the gaps in terms of people processes and technology that led to the incident	Functional	Intersects With	Contingency Plan Root Cause Analysis (RCA) & Lessons Learned	BCD-05	Mechanisms exist to conduct a Root Cause Analysis (RCA) and "lessons learned" activity every time the contingency plan is activated.	8	BC/DR RCA. For incidents requiring BC/DR activation: assess plan effectiveness, identify gaps (people/process/technology), update plans; post-incident report to Board.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory

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	Self Signed RE	Small Size RE	Mid Size RE	Qualified RE	Market Infrastructure
RS.AN.S4a	Incident Analysis	Determine the gaps in terms of people processes and technology that led to the incident	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future	8	Incident RCA. Use structured RCA methodology (5 Whys, Fishbone); categorize gaps: people (training needs), process (procedure updates), technology (control implementation); assign remediation owners with deadlines.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
RS.AN.S4b	Incident Analysis	Further enhance the RE's security posture to prevent/ mitigate similar cybersecurity Incidents in the future.	Functional	Intersects With	Contingency Plan Root Cause Analysis (RCA) & Lessons Learned	BCD-05	Mechanisms exist to conduct a Root Cause Analysis (RCA) and "lessons learned" activity every time the contingency plan is activated.	8	BC/DR RCA. For incidents requiring BC/DR activation: assess plan effectiveness, identify gaps (people/process/technology), update plans; post-incident report to Board.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
RS.AN.S4b	Incident Analysis	Further enhance the RE's security posture to prevent/ mitigate similar cybersecurity Incidents in the future.	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future	8	Incident RCA. Use structured RCA methodology (5 Whys, Fishbone); categorize gaps: people (training needs), process (procedure updates), technology (control implementation); assign remediation owners with deadlines.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
RS.AN.S5	Incident Analysis	Impact analysis of the incident shall be mandatorily conducted by the REs	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future	8	BIA process. Assess incident impact using pre-defined BIA: RTO/RPO breach analysis, financial quantification, regulatory penalty exposure, customer impact, brand reputation.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
RS.CO.S1	Incident Response Reporting and Communication	An SOP documenting the roles and responsibilities of REs' personnel with respect to cybersecurity incident response shall be prepared and implemented	Functional	Intersects With	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	8	Response roles. Document roles in IRP: Incident Commander, CISO, SOC lead, IT operations, legal, communications, business continuity, HR (insider threats).	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
RS.CO.S1	Incident Response Reporting and Communication	An SOP documenting the roles and responsibilities of REs' personnel with respect to cybersecurity incident response shall be prepared and implemented	Functional	Intersects With	Position Categorization	HRS-02	Mechanisms exist to manage personnel security risk by assigning a risk designation to all positions and establishing screening criteria for individuals filling those positions.	8	Response SOP. Detailed SOPs for: incident triage, evidence collection, forensics, communication (internal/external/regulatory), legal hold, vendor engagement, post-incident review.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
RS.CO.S1	Incident Response Reporting and Communication	An SOP documenting the roles and responsibilities of REs' personnel with respect to cybersecurity incident response shall be prepared and implemented	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	8	Response SOP. Detailed SOPs for: incident triage, evidence collection, forensics, communication (internal/external/regulatory), legal hold, vendor engagement, post-incident review.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
RS.CO.S2	Incident Response Reporting and Communication	Any cybersecurity incident falling under CERT-In Cybersecurity directions shall be notified to SEBI CERT-In and NCIIPC within stipulated time	Functional	Subset of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	10	Executive reporting. Board notification: immediate for critical incidents, quarterly summary for all incidents; include impact, response actions, lessons learned.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
RS.CO.S2	Incident Response Reporting and Communication	Any cybersecurity incident falling under CERT-In Cybersecurity directions shall be notified to SEBI CERT-In and NCIIPC within stipulated time	Functional	Intersects With	Cyber Incident Reporting for Sensitive / Regulated Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	8	Regulatory reporting. Report to CERT-In within 6 hours per directions; SEBI notification per circular requirements; NCIIPC for critical infrastructure incidents; maintain reporting log with timestamps.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
RS.CO.S3	Incident Response Reporting and Communication	In the event of a cybersecurity incident REs shall coordinate with stakeholders as per their CCMP	Functional	Intersects With	Correlation with External Organizations	IRO-02.5	Mechanisms exist to coordinate with approved third-parties to achieve a cross-organization perspective on incident awareness and more effective incident responses.	5	External coordination. Coordinate per CCMP: law enforcement (for criminal activity), forensics partner, legal counsel, PR firm, insurance carrier, affected vendors/customers.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
RS.CO.S3	Incident Response Reporting and Communication	In the event of a cybersecurity incident REs shall coordinate with stakeholders as per their CCMP	Functional	Intersects With	Situational Awareness For Incidents	IRO-09	Mechanisms exist to document, monitor and report the status of cybersecurity and data protection incidents to internal stakeholders all the way through the resolution of the incident.	5	Team coordination. Activate cross-functional ISIRT: cybersecurity, IT ops, business continuity, legal, HR, communications; define decision-making authority; daily standups during incidents.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
RS.CO.S3	Incident Response Reporting and Communication	In the event of a cybersecurity incident REs shall coordinate with stakeholders as per their CCMP	Functional	Intersects With	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	8	Team coordination. Activate cross-functional ISIRT: cybersecurity, IT ops, business continuity, legal, HR, communications; define decision-making authority; daily standups during incidents.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
RS.CO.S3	Incident Response Reporting and Communication	In the event of a cybersecurity incident REs shall coordinate with stakeholders as per their CCMP	Functional	Intersects With	Supply Chain Coordination	IRO-10.4	Mechanisms exist to provide cybersecurity and data protection incident information to the provider of the Technology Assets, Applications and/or Services (TAAS) and other organizations involved in the supply chain for TAAS related to the incident.	5	Status communication. Maintain incident status dashboard; regular updates to stakeholders per communication plan; situation reports (SITREP) for extended incidents.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
RS.IM.S1	Improvements	Lessons learned from incident handling activities shall be incorporated into incident response plans training and testing	Functional	Intersects With	Contingency Plan Root Cause Analysis (RCA) & Lessons Learned	BCD-05	Mechanisms exist to conduct a Root Cause Analysis (RCA) and "lessons learned" activity every time the contingency plan is activated.	8	BC/DR improvements. Update BCP/DRP based on lessons learned; enhance recovery procedures; additional resources/tools; updated contact lists.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
RS.IM.S1	Improvements	Lessons learned from incident handling activities shall be incorporated into incident response plans training and testing	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future	8	Continuous improvement. Post-incident: update IRP/playbooks, enhance detection rules, additional controls, staff training, vendor management changes; track implementation; re-test.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
RS.IM.S2	Improvements	Changes to the response plan shall be communicated to RE's designated key personnel	Functional	Intersects With	IRP Update	IRO-04.2	Mechanisms exist to regularly review and modify incident response practices to incorporate lessons learned, business process changes and industry developments, as	5	Change notification. Document plan changes: change log, effective date, rationale; distribute to: ISIRT, Board, key business owners; acknowledgment required.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
RS.IM.S2	Improvements	Changes to the response plan shall be communicated to RE's designated key personnel	Functional	Intersects With	Incident Response Training	IRO-05	Mechanisms exist to train personnel in their incident response roles and responsibilities.	8	Plan communication. Version control for CCMP/IRP; communicate updates via: email to ISIRT members, training sessions, updated documentation in accessible repository.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
RS.MA.S1	Incident Management	A comprehensive CCMP shall be documented with scenario-based SOP. Further incident response management plan shall also be part of CCMP	Functional	Subset of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	10	CCMP foundation. Comprehensive Cyber Crisis Management Plan (CCMP) includes: incident classification, escalation matrix, communication plan, recovery procedures, scenario-based playbooks (ransomware, DDoS, data breach, insider threat).	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
RS.MA.S1	Incident Management	A comprehensive CCMP shall be documented with scenario-based SOP. Further incident response management plan shall also be part of CCMP	Functional	Intersects With	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	8	IRP documentation. CCMP must include detailed IRP covering: preparation, detection, analysis, containment, eradication, recovery, post-incident; Board-approved; accessible to response team 24x7.	Mandatory	Mandatory	Mandatory	Mandatory	Mandatory
RS.MA.S2	Incident Management	REs shall optimize their ability to respond in a timely and appropriate manner to adverse conditions stresses attacks or indicators	Functional	Subset of	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	10	Incident handling process. Optimize response through: automated playbooks (SOAR), pre-positioned tools (forensics, backup restore), retainer with IR firm, war room procedures, defined communication templates.	Exempted	Exempted	Mandatory	Mandatory	Mandatory
RS.MA.S3	Incident Management	REs shall prepare contingency plans COOP training exercises and incident response and recovery plans approved by Board/Partners/Proprietor	Functional	Subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR)	10	Response planning. Contingency plans: incident response (cyber attacks), business continuity (operational disruption), disaster recovery (site failure); integrated testing.	Exempted	Exempted	Mandatory	Mandatory	Mandatory