Annexure - 2

Canara Robeco Asset Management Company Ltd.

SCOPE	SEBI Circular: SEBI/HO/ ITD-1/ITD_CSC_EXT/P/CIR/2024/113		Cyber Security Cyber Resilience Framework			
Sno	**CS Goal**	**CS Control**	**CS Domain**	**Standards**	**CSCRF guidelines**	**Applicability**
1	Anticipate	Governance	Organizational Context	GV.OC.S2, GV.OC.S3	1. Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners.	All REs except small-size, self-certification REs
2	Anticipate	Governance	Organizational Context	GV.OC.S2, GV.OC.S3	2. To ensure the goal of cybersecurity, REs shall define responsibilities of its own employees, third-party service providers' employees, and other entities, who may have privileged access or use their systems/ networks.	All REs except small-size, self-certification REs
3	Anticipate	Governance	Organizational Context	GV.OC.S2	1. All REs shall understand, manage and comply with relevant cybersecurity and data security/ protection requirements mentioned in government guidelines/ policies/ laws/ circulars/ regulations, etc. issued by SEBI/ GoI such as IT Act 2000, Digital Personal Data Protection Act (DPDP) 2023 or any other law/ circular/ regulation as and when issued.	All REs (Mandatory)
4	Anticipate	Governance	Organizational Context	GV.OC.S2	2. Conduct audits and inspections of IT resources of REs (and its sub-contractors/ third party service providers) or engage third-party auditor to conduct the same and check the adherence with SEBI and government guidelines/ policies/ laws/ circulars/ regulations, etc., and standard industry practices.	All REs (Mandatory)
5	Anticipate	Governance	Organizational Context	GV.OC.S2	3. SEBI/ any other government agency shall at any time perform search and seizure of RE's IT resources storing/ processing data and other relevant IT resources (including but not limited to logs, user details, etc.) pertaining to the RE. In this process, SEBI or SEBI authorized personnel/ agency may access RE's IT infrastructure, applications, data, documents, including other necessary information given to, stored or processed by third-party service providers.	All REs (Mandatory)
6	Anticipate	Governance	Organizational Context	GV.OC.S2	4. Engage a forensic auditor to identify the root cause of any incident (cybersecurity or other incidents) related to RE.	All REs (Mandatory)
7	Anticipate	Governance	Organizational Context	GV.OC.S2	5. SEBI shall seek the audit reports of the audits conducted by RE.	All REs (Mandatory)

8	Anticipate	Governance	Roles and Responsibilities	GV.RR.S3	1. REs shall designate a senior official as Chief Information Security Officer (CISO) whose function would be to assess, identify, and reduce cybersecurity risks, respond to incidents, establish appropriate standards and controls, and direct the establishment and implementation of processes and procedures as per the cybersecurity and cyber resilience policy approved by the Board/ Partners/ Proprietor of the MII and qualified REs. The reporting of the CISO of the MII and Qualified REs shall be directly to the MD & CEO of their organization. CISO shall possess sufficient qualification and capabilities to carry out his/ her responsibilities. REs shall establish a reporting procedure to facilitate communication of cybersecurity incidents/ unusual activities to the CISO or to the senior management in a time-bound manner as defined by guidelines/ policies/ laws/ circulars/ regulations, etc. MIIs and REs which have been identified as CII by NCIIPC shall define roles and responsibilities of CISO as per NCIIPC guidelines. The level, grade, and standing of CISO shall be atleast equivalent to CTO/ CIO.	MIIs, Qualified REs (Mandatory)
9	Anticipate	Governance	Roles and Responsibilities	GV.RR.S3	1. REs shall designate a senior official or management personnel (henceforth, referred to as the "Designated Officer") whose function would be to assess, identify, and reduce cybersecurity risks, respond to incidents, establish appropriate standards and controls, and direct the establishment and implementation of processes and procedures as per the cybersecurity and cyber resilience policy approved by the Board/ Partners/ Proprietor. REs shall establish a reporting procedure to facilitate communication of cybersecurity incidents/ unusual activities to Designated Officer in a time-bound manner as defined by guidelines/ policies/ laws/ circulars/ regulations, etc. issued by SEBI or GoI.	Mid-size, small- size, self-certification REs (Mandatory)
10	Anticipate	Governance	Roles and Responsibilities	GV.RR.S4	1. REs shall allocate adequate percentage of total IT budget to cybersecurity. Such allocation shall be mentioned under separate budgetary head for monitoring by the Board of directors/ top-level management.	All REs except small-size, self-certification REs
11	Anticipate	Governance	Roles and Responsibilities	GV.RR.S4	2. REs shall ensure that adequate resources are allocated and aligned with cybersecurity risk strategy, roles and responsibilities, and policies. Resources should be defined in terms of budgetary allocation, people, and material. Resourcing requirements should be revisited regularly based upon progress or shortfalls in the implementation of standards and shall reflect in the budgetary allocation.	All REs except small-size, self-certification REs

12	Anticipate	Governance	Roles and Responsibilities	GV.RR.S5, GV.RR.S6	1. REs shall ensure that every employee hired, irrespective of the department or role, present a low/ no threat to the REs' cybersecurity posture. This includes (but not limited to): a. Conducting due diligence b. Ensuring employees receive proper security training during onboarding and on regular basis c. Employment screening procedures, employment policies and agreement, employment termination procedures etc. are followed.	All REs except small-size, self-certification REs
13	Anticipate	Governance	Roles and Responsibilities	GV.RR.S5, GV.RR.S6	2. REs shall sign a confidentiality and integrity agreement with third-party service providers and conduct due diligence of all third-party service providers accessing their IT systems.	All REs except small-size, self-certification REs
14	Anticipate	Governance	Policy	GV.PO.S1, GV.PO.S2, GV.PO.S5	1. As part of the operational risk management framework to manage risks to systems, networks and databases from cyber-attacks and threats, REs shall formulate a comprehensive Cybersecurity and Cyber Resilience policy document encompassing CSCRF. In case of deviations from the CSCRF, reasons for such deviations, technical or otherwise, shall be provided in the policy document.	All REs (Mandatory)
15	Anticipate	Governance	Policy	GV.PO.S1, GV.PO.S2, GV.PO.S5	2. The policy document shall be approved by the Board/ Partners/ Proprietor of the REs. The policy document shall be reviewed by the aforementioned group periodically with a view to strengthen and improve cyber resilience posture.	All REs (Mandatory)
16	Anticipate	Governance	Policy	GV.PO.S1, GV.PO.S2, GV.PO.S5	3. REs shall have policies (including but not limited to) with respect to asset management, patch management, vulnerability management, VAPT policy, audit policy, monitoring of the networks and endpoints, configuration management, change management, secure software development life cycle management, authentication policies, authorization policies and processes, network segmentation/ isolation policies, commissioning internet facing assets, encryption policies, PII and privacy policies, cybersecurity control management policy, asset ownership documentation, etc., and chain of command for any approval process in the organization with respect to cybersecurity. The policies shall also contain do's and don'ts in the organization with respect to usage of information assets including desktops, laptops, BYOD, networks, internet, data, etc. The aforementioned policies may form a part of RE's cybersecurity policy or may be standalone policies.	All REs (Mandatory)

17	Anticipate	Governance	Policy	GV.PO.S1, GV.PO.S2, GV.PO.S5	4. REs shall formulate a policy for mobile and web applications and associated services with the approval of their Board/ Partners/ Proprietor. The contours of the policy, while discussing the parameters of any "new product" including its alignment with the overall business strategy and inherent risk of the product, risk management/ mitigation measures, compliance with regulatory instructions, customer experience, etc., shall explicitly include security requirements from Functionality, Security and Performance (FSP) angles	All REs (Mandatory)
18	Anticipate	Governance	Policy	GV.PO.S1, GV.PO.S2, GV.PO.S5	5. All information/ data (classified as *Regulatory Data* and *IT and Cybersecurity Data*) that is consumed/ handled by REs shall be made accessible to SEBI when required. If there is any dependency on external party, REs shall facilitate information sharing with SEBI by including it in their agreement with external party.	All REs (Mandatory)
19	Anticipate	Governance	Policy	GV.PO.S1, GV.PO.S2, GV.PO.S5	6. The Cybersecurity Policy shall include the following process to identify, assess, and manage cybersecurity risks associated with processes, information, networks and systems: a. 'Identify' critical IT assets and risks associated with such assets. b. 'Protect' assets by deploying suitable controls, tools and measures. c. 'Detect' incidents, anomalies and attacks through appropriate monitoring tools/processes. d. Respond' by taking immediate steps after identification of the incident, anomaly or attack. e. 'Recover' from incident through incident management and other appropriate recovery mechanism	All REs
20	Anticipate	Governance	Policy	GV.PO.S1, GV.PO.S2, GV.PO.S5	7. REs shall follow Plan-Do-Check-Act concept while creating and using the documented information. For example, activities under the 'Plan' phase shall be guided by Policies, the 'Do' phase will follow Procedures (SOPs), and the 'Check' and 'Act' phases will refer to the Policies and Procedures.	All REs except small-size, Self-certification REs
21	Anticipate	Governance	Policy	GV.PO.S1, GV.PO.S2, GV.PO.S5	8. As part of compliance management with respect to CSCRF, REs shall apply following key aspects (including but not limited to) for implementing compliance management: a. Assess Compliance with applicable guidelines/ policies/ laws/ circulars/ regulations, etc. issued by SEBI or GoI. b. Develop compliance policies and procedures c. Implement controls such as security measures d. Train employees e. Monitor and review compliance management processes f. Regular audits and reporting.	All REs except small-size, Self-certification REs

22	Anticipate	Governance	Policy	GV.PO.S1, GV.PO.S2, GV.PO.S5	9. The Board/ Partners/ Proprietor of the REs shall constitute an *IT Committee for REs* comprising experts proficient in technology. This IT Committee of REs shall meet on a periodic basis to review the implementation of the cybersecurity and cyber resilience policy approved by their Board/ Partners/ Proprietor, and such review shall include goal setting for a target level of cyber resilience, and establishing a plan to improve and strengthen cybersecurity and cyber resilience. The review shall be placed before the Board/ Partners/ Proprietor of REs for appropriate action.	All REs except small-size, Self-certification REs (Mandatory)
23	Anticipate	Governance	Policy	GV.PO.S1, GV.PO.S2, GV.PO.S5	10. The aforementioned committee and the senior management of the REs, including the CISO, shall periodically review instances of cybersecurity incidents/ attacks, if any, domestically and globally, and take steps to strengthen cybersecurity and cyber resilience.	All REs except small-size, Self-certification REs (Mandatory)
24	Anticipate	Governance	Policy	GV.PO.S1, GV.PO.S2, GV.PO.S5	11. The cybersecurity policy shall encompass the principles prescribed by National Critical Information Infrastructure Protection Centre (NCIIPC) of National Technical Research Organisation (NTRO), GoI in the report titled 'Guidelines for Protection of National Critical Information Infrastructure' and subsequent revisions, if any, from time to time.	All REs which have been identified as CII by NCIIPC (Mandatory)
25	Anticipate	Governance	Policy	GV.PO.S1, GV.PO.S2, GV.PO.S5	12. REs shall incorporate best practices from standards such as ISO 27001, ISO 27002, etc. or their subsequent revisions, if any, from time to time.	All REs except small-size, Self-certification REs
26	Anticipate	Governance	Oversight	GV.OV.S4	1. REs shall conduct third-party assessment (for MIIs) and self-assessment (for Qualified REs) of their cyber resilience using CCI and submit corresponding evidences to their submission authority on a periodic basis. CCI and its calculation methodology has been attached at **Annexure-K**. REs shall strive for building an automated tool and suitable dashboards (preferably integrated with log aggregator) for submitting compliance of CCI. A dashboard shall be available at the time of cyber audit, onsite inspection/ audit by SEBI or any agency appointed by SEBI.	MIIs and Qualified REs (Mandatory)

27	Anticipate	Governance	Risk Management	GV.RM.S1, GV.RM.S2	1. Risk Management a. The design of the cyber risk management framework needs to consider the following (including but not limited to): i. Identification of the cybersecurity risk for the organization ii. Classification of identified and mapped business functions, supporting processes and information assets at risk. iii. Determination of risk appetite for IT and cybersecurity risks. iv. Definition of mitigation measures and controls to reduce the risks. v. Monitoring of the effectiveness of the above-mentioned measures and controls. vi. Evaluation of the effect of major changes and significant operational, technical or cybersecurity incident(s) on the risks.	All REs except small-size, self-certification REs (Mandatory)
28	Anticipate	Governance	Risk Management	GV.RM.S1, GV.RM.S2	b. REs shall consider using latest version of ISO 27005 as a guidance on design, implementation, and maintenance of information security risk management.	All REs except small-size, self-certification REs (Mandatory)
29	Anticipate	Governance	Risk Management	GV.RM.S1, GV.RM.S2	c. Risk management strategy of REs shall include (but not limited to) risk assessment, risk analysis, risk mitigation, risk monitoring and review, compliance with relevant laws and regulations, communication of risk management policies to all stakeholders, effective mitigation measures with options for compensatory controls wherever feasible, measures to reduce residual risk and ensuring that the cybersecurity risk tolerance is within acceptable limits.	All REs except small-size, self-certification REs (Mandatory)
30	Anticipate	Governance	Risk Management	GV.RM.S1, GV.RM.S2	d. REs shall use metrics like (including but not limited to) MTTD, MTTR, MTTC, number of cybersecurity incidents/ intrusion attempts detected and resolved within a specific period, number of false positives and false negatives generated by cybersecurity monitoring tools, number of successful cyber attacks occurred in the past year, and how these numbers are being reduced through continuous refinement of the monitoring process for measuring their cybersecurity maturity level.	All REs except small-size, self-certification REs (Mandatory)
31	Anticipate	Governance	Risk Management	GV.RM.S1, GV.RM.S2	e. REs shall periodically assess level of employee cybersecurity awareness, for e.g., through phishing test success rate, etc.	All REs except small-size, self-certification REs (Mandatory)
32	Anticipate	Governance	Risk Management	GV.RM.S1, GV.RM.S2	f. REs shall undertake periodic IT asset management for functions such as number of devices on the network running end-of-life (EOL) software, number of devices no longer receiving security updates, unidentified devices on the internal network, integration of third-party devices and services into the network, etc. Further, IT asset management may also be utilized for process of managing assets' access and permissions, patching cadence, security rating, third-party security rating, number of known vulnerabilities, etc.	All REs except small-size, self-certification REs (Mandatory)

33	Anticipate	Governance	Risk Management	GV.RM.S1, GV.RM.S2	g. Risk-based transaction monitoring or surveillance process shall be implemented as part of fraud risk management system across all delivery channels.	All REs except small-size, self-certification REs (Mandatory)
34	Anticipate	Governance	Risk Management	GV.RM.S3	1. Comprehensive scenario-based testing shall be done for assessing cybersecurity risks of the RE. A sample list of possible attack scenarios and possibilities for Stock Exchanges have been attached at **Annexure-E**. Other MIIs and REs shall prepare their own attack scenarios as per their business model and assess their risks accordingly.	All REs except small-size, self-certification REs (Mandatory)
35	Anticipate	Governance	CS Supply Chain Risk Management	GV.SC.S4	1. Where the systems (IBT, Back office and other customer facing applications, IT infrastructure, etc.) of a RE are managed by third-party service providers and in case the RE does not have direct control over the implementation of any of the guidelines, the RE shall instruct the third-party service providers to adhere to the applicable guidelines in the CSCRF and shall obtain the necessary cyber audit certifications from them to ensure compliance with the framework.	MIIs and Qualified REs (Mandatory)
36	Anticipate	Governance	CS Supply Chain Risk Management	GV.SC.S4	3. The responsibility, accountability and ownership of outsourced activities lies primarily with REs. Therefore, REs shall come up with appropriate monitoring mechanisms through a clearly defined framework to ensure that all the requirements as specified in CSCRF shall be complied with. The periodic reports submitted to SEBI shall highlight the critical activities handled by the third-party service providers and REs shall certify that the above-mentioned requirement is complied with.	All REs (Mandatory)
37	Anticipate	Governance	CS Supply Chain Risk Management	GV.SC.S4	4. REs shall conduct background checks and ensure signing of Non-Disclosure Agreement, and cybersecurity compliance for all third-party service providers.	All REs (Mandatory)
38	Anticipate	Governance	CS Supply Chain Risk Management	GV.SC.S5	1. REs shall obtain SBOM for existing their *critical systems* within 6 months (starting from the date of issuance of CSCRF).	All REs (Mandatory)
39	Anticipate	Governance	CS Supply Chain Risk Management	GV.SC.S5	2. REs shall obtain SBOMs for any new critical systems software products/ Software-as- a-Service applications (SaaS) at the time of procurement. SBOMs containing information such as all the open source and third-party components present in a codebase, versions of the components used in the codebase, and their patch status, etc. allow security teams to quickly identify any associated security or license risk.	All REs (Mandatory)
40	Anticipate	Governance	CS Supply Chain Risk Management	GV.SC.S5	3. MIIs shall include SBOM as part of their empanelment criteria for application software vendors.	All REs (Mandatory)

41	Anticipate	Governance	CS Supply Chain Risk Management	GV.SC.S5	4. SBOM shall include (but not limited to) the following: a. License information b. Name of the supplier c. All primary (top level) components with all their transitive dependencies (including third-party dependencies whether in-house or open-source components) and relationships d. Encryption used e. Cryptographic hash of the components f. Frequency of updates g. Known unknown (where a SBOM does not include a full dependency graph) h. Access control i. Methods for accommodating occasional incidental errors.	All REs (Mandatory)
42	Anticipate	Governance	CS Supply Chain Risk Management	GV.SC.S7	1. Any single third-party service provider, providing services to multiple REs, creates a concentration risk. When such third-party service providers encounter cybersecurity incidents/ attacks, it can led to systemic implications due to high concentration risk. Therefore, REs need to take into account concentration risk while outsourcing multiple critical services to the same third-party service provider.	All REs except small-size, self-certification REs (Mandatory)
43	Anticipate	Governance	CS Supply Chain Risk Management	GV.SC.S7	2. REs shall identify their third-party service providers posing a concentration risk and shall prescribe specific cybersecurity controls, including audit of their systems and protocols from independent auditors, to mitigate such concentration risk. REs shall also validate that such third-party service providers are meeting their goals of operational resiliency.	All REs except small-size, self-certification REs (Mandatory)
44	Anticipate	Governance	CS Supply Chain Risk Management	GV.SC.S7	3. Stock Exchanges/ Depositories shall take necessary steps to mitigate concentration risk of third-party service providers among Stock Brokers/ Depository Participants.	All REs except small-size, self-certification REs (Mandatory)
45	Anticipate	Governance	CS Supply Chain Risk Management	GV.SC.S7	4. SEBI circulars on outsourcing of activities, currently mandated and updated from time to time, shall be complied with by the respective REs. List of currently mandated SEBI circulars on outsourcing of activities has been attached at **Annexure-F**.	All REs except small-size, self-certification REs (Mandatory)
46	Anticipate	Identify	Asset Management	ID.AM.S1, ID.AM.S4	1. All REs shall identify and classify *critical systems* as defined in this framework based on their sensitivity and criticality for business operations, services and data management. The Board/ Partners/ Proprietor of the REs shall approve the list of *critical systems*.	All REs (Mandatory)
47	Anticipate	Identify	Asset Management	ID.AM.S1, ID.AM.S4	2. All REs shall maintain an up-to-date inventory of their (including but not limited to) hardware and systems, software, digital assets (such as URLs, domain names, application, APIs, etc.), shared resources (including cloud assets), interfacing systems (internal and external), details of its network resources, connections to its network and data flows.	All REs (Mandatory)
48	Anticipate	Identify	Asset Management	ID.AM.S1, ID.AM.S4	3. Any additions/ deletions or changes in existing assets shall be reflected in the asset inventory within 3 working days.	All REs (Mandatory)

49	Anticipate	Identify	Asset Management	ID.AM.S1, ID.AM.S4	4. For conducting criticality assessment of assets, REs shall take the following steps (including but not limited to): a. Maintain a comprehensive asset inventory b. Conduct threat modelling (based on risk assessment) c. Conduct vulnerability assessment	All REs (Mandatory)
50	Anticipate	Identify	Asset Management	ID.AM.S1, ID.AM.S4	5. REs shall prepare and maintain an up-to-date network architecture diagram at the organisational level including wired and wireless networks.	All REs (Mandatory)
51	Anticipate	Identify	Asset Management	ID.AM.S6	7. All IT assets shall be inventoried in ITSM tool.	All REs except small-size, self-certification REs (Mandatory)
52	Anticipate	Identify	Asset Management	ID.AM.S6	8. REs shall integrate cybersecurity considerations into product life cycles.	All REs except small-size, self-certification REs (Mandatory)
53	Anticipate	Identify	Risk Assessment	ID.RA.S1, ID.RA.S2	1. REs shall conduct a risk assessment (including post-quantum risks) of the IT environment of their organization on a half-yearly (for MIIs) and yearly (for qualified and mid-size REs) basis to acquire visibility and a reasonably accurate assessment of the overall cybersecurity risk posture. The above-mentioned risk assessment shall be utilized by the RE to develop a quantifiable cybersecurity risk score.	All REs except small-size, self-certification REs (Mandatory)
54	Anticipate	Identify	Risk Assessment	ID.RA.S1, ID.RA.S2	2. REs shall accordingly identify cyber risks that they may face, along with the likelihood of associated threats and their impact on their business, and deploy controls commensurate to their criticality.	All REs except small-size, self-certification REs (Mandatory)
55	Anticipate	Identify	Risk Assessment	ID.RA.S1, ID.RA.S2	3. Risk Assessment shall include (but not limited to): a. Technology stack and solutions used b. Known vulnerabilities c. Dependence on third-party service providers d. Data storage, security and privacy protection e. Threats, likelihoods and associated risks	All REs except small-size, self-certification REs (Mandatory)
56	Anticipate	Identify	Risk Assessment	ID.RA.S3	1. REs shall engage Dark web monitoring (for brand intelligence, customer protection, etc.), and takedown services as a cyber-defence strategy to check for any brand abuse, data/credentials leak, combating cyber abuse etc.	MIIs, Qualified REs (Mandatory)
57	Anticipate	Identify	Risk Assessment	ID.RA.S3	2. REs shall subscribe to anti-phishing/ anti-rogue app services to mitigate potential phishing or impersonation attacks.	MIIs, Qualified REs (Mandatory)
58	Anticipate	Identify	Risk Assessment	ID.RA.S3	3. REs shall devise SOPs to implement the advisories issued by CERT-In, NCIIPC or any other government agency in their IT environment within a defined timeframe.	MIIs, Qualified REs (Mandatory)
59	Anticipate	Identify	Risk Assessment	ID.RA.S3	4. REs shall have processes in place to manage and incorporate IOAs/ IOCs/ malware alerts/ vulnerability alerts (received from CERT-In or NCIIPC (as applicable) or any other government agencies) in their systems.	MIIs, Qualified REs (Mandatory)
60	Anticipate	Identify	Risk Assessment	ID.RA.S3	5. REs shall be onboarded to CERT-In intelligence platform to receive the advisories for necessary action and implementation.	MIIs, Qualified REs (Mandatory)

61	Anticipate	Identify	Risk Assessment	ID.RA.S4	1. Measures against Phishing websites and attacks a. REs need to proactively monitor the cyberspace to identify phishing websites w.r.t. REs' domains and report the same to CSIRT-Fin/CERT-In for taking appropriate action.	All REs (Mandatory)
62	Anticipate	Identify	Risk Assessment	ID.RA.S4	2. Risk assessment of authentication-based solutions shall be implemented to get insights about context behind every login. Further, when a user attempts to sign-in, risk-based authentication solution shall analyse factors such as device, location, network, sensitivity, etc.	All REs
63	Anticipate	Protect	Identity Mgmt, Authentication & Access	PR.AA.S1, PR.AA.S2, PR.AA.S3, PR.AA.S7, PR.AA.S9	1. Access Controls, Password Policy/ Authentication Mechanism a. No person by virtue of rank or position shall have any intrinsic right to access confidential data applications, system resources or facilities.	All REs (Mandatory)
64	Anticipate	Protect	Identity Mgmt, Authentication & Access	PR.AA.S1, PR.AA.S2, PR.AA.S3, PR.AA.S7, PR.AA.S9	b. Any access to REs' systems, applications, networks, databases, etc., shall be for a defined purpose and for a defined period. Access granted to IT systems, applications, databases and networks shall be on a need-to-use basis and based on the principle of least privilege. Such access shall be given for a specific duration and using effective authentication mechanisms.	All REs (Mandatory)
65	Anticipate	Protect	Identity Mgmt, Authentication & Access	PR.AA.S1, PR.AA.S2, PR.AA.S3, PR.AA.S7, PR.AA.S9	c. User access rights, delegated access and unused tokens, and privileged users' activities shall be reviewed on a periodic basis.	All REs (Mandatory)
66	Anticipate	Protect	Identity Mgmt, Authentication & Access	PR.AA.S1, PR.AA.S2, PR.AA.S3, PR.AA.S7, PR.AA.S9	d. Access to external cloud services such as Dropbox, google drive, iCloud, OneDrive, etc. shall be given as per RE's policy.	All REs (Mandatory)
67	Anticipate	Protect	Identity Mgmt, Authentication & Access	PR.AA.S1, PR.AA.S2, PR.AA.S3, PR.AA.S7, PR.AA.S9	e. REs shall ensure that records of user access to critical systems, wherever possible, are uniquely identified and logged for audit and review purposes. Such logs shall be maintained and stored in a secure location for a time period not less than two (2) years (atleast 6 months in online mode and rest in archival mode). REs also need to maintain records of users with access to shared accounts.	All REs (Mandatory)
68	Anticipate	Protect	Identity Mgmt, Authentication & Access	PR.AA.S1, PR.AA.S2, PR.AA.S3, PR.AA.S7, PR.AA.S9	f. Account access lock policies after failure attempts shall be implemented for all accounts.	All REs (Mandatory)
69	Anticipate	Protect	Identity Mgmt, Authentication & Access	PR.AA.S1, PR.AA.S2, PR.AA.S3, PR.AA.S7, PR.AA.S9	g. Existing user accounts and access rights shall be periodically reviewed by the owner of the system in order to detect dormant accounts, accounts with excessive privileges, unknown accounts or any type of discrepancy.	All REs (Mandatory)

70	Anticipate	Protect	Identity Mgmt, Authentication & Access	PR.AA.S1, PR.AA.S2, PR.AA.S3, PR.AA.S7, PR.AA.S9	h. Proper 'end of life' mechanisms shall be adopted for user management to deactivate access privileges of users who are leaving the organization or whose access privileges have been withdrawn. This includes named user IDs, default user IDs and generic email IDs.	All REs (Mandatory)
71	Anticipate	Protect	Identity Mgmt, Authentication & Access	PR.AA.S1, PR.AA.S2, PR.AA.S3, PR.AA.S7, PR.AA.S9	i. All critical systems accessible over the internet shall have multi-factor security (such as VPNs, Firewall controls, etc.) and MFA.	All REs (Mandatory)
72	Anticipate	Protect	Identity Mgmt, Authentication & Access	PR.AA.S1, PR.AA.S2, PR.AA.S3, PR.AA.S7, PR.AA.S9	j. MFA shall be enabled for all users and systems that connect using online/ internet facility and also particularly for VPNs, webmail, and accounts that access critical systems from non-trusted environments to trusted environments.	All REs (Mandatory)
73	Anticipate	Protect	Identity Mgmt, Authentication & Access	PR.AA.S1, PR.AA.S2, PR.AA.S3, PR.AA.S7, PR.AA.S9	2. Network Security Management a. Adequate controls shall be deployed to address virus/ malware/ ransomware attacks on servers and other IT systems. These controls may include host/ network/ application based IPS, customized kernels for Linux, anti-virus and anti-malware software, etc. Anti-virus definition files updates and automatic anti-virus scanning shall be done on a regular basis.	All REs (Mandatory)
74	Anticipate	Protect	Identity Mgmt, Authentication & Access	PR.AA.S1, PR.AA.S2, PR.AA.S3, PR.AA.S7, PR.AA.S9	b. All REs shall establish baseline standards to facilitate consistent application of security configurations to OS, databases, network devices, enterprise mobile devices, etc. within the IT environment. REs shall also conduct regular enforcement checks to ensure that baseline standards are applied uniformly.	All REs (Mandatory)
75	Anticipate	Protect	Identity Mgmt, Authentication & Access	PR.AA.S1, PR.AA.S2, PR.AA.S3, PR.AA.S7, PR.AA.S9	c. The LAN and wireless networks within REs' premises shall be secured with proper access controls.	All REs (Mandatory)
76	Anticipate	Protect	Identity Mgmt, Authentication & Access	PR.AA.S1, PR.AA.S2, PR.AA.S3, PR.AA.S7, PR.AA.S9	d. REs shall keep total and maximum connections to SMTP server limited.	All REs (Mandatory)
77	Anticipate	Protect	Identity Mgmt, Authentication & Access	PR.AA.S1, PR.AA.S2, PR.AA.S3, PR.AA.S7, PR.AA.S9	3. Access Controls, Password Policy/ Authentication Mechanism a. PIM solution or PIM process shall be implemented to keep track of privileged access.	All REs except small-size, self-certification REs (Mandatory)
78	Anticipate	Protect	Identity Mgmt, Authentication & Access	PR.AA.S1, PR.AA.S2, PR.AA.S3, PR.AA.S7, PR.AA.S9	b. REs shall implement an access policy which addresses strong password controls for users' access to systems, applications, networks and databases, etc. Illustrative examples for this are given in Annexure-G.	All REs except small-size, self-certification REs (Mandatory)
79	Anticipate	Protect	Identity Mgmt, Authentication & Access	PR.AA.S1, PR.AA.S2, PR.AA.S3, PR.AA.S7, PR.AA.S9	c. REs shall formulate an Internet access policy to monitor and regulate the use of internet and internet based services such as social media sites, cloud-based internet storage sites, etc. within the critical IT infrastructure of REs.	All REs except small-size, self-certification REs (Mandatory)

80	Anticipate	Protect	Identity Mgmt, Authentication & Access	PR.AA.S1, PR.AA.S2, PR.AA.S3, PR.AA.S7, PR.AA.S9	d. REs shall deploy controls and security measures to supervise staff with elevated system access entitlements (such as admin or privileged users). Such controls and measures shall inter-alia include restricting the number of privileged users, periodic review of privileged users' activities, disallow privileged users from accessing systems logs in which their activities are being captured, strong controls over remote access by privileged users, etc.	All REs except small-size, self-certification REs (Mandatory)
81	Anticipate	Protect	Identity Mgmt, Authentication & Access	PR.AA.S1, PR.AA.S2, PR.AA.S3, PR.AA.S7, PR.AA.S9	4. Network Security Management a. REs shall apply appropriate network segmentation/ isolation techniques to restrict access to the sensitive information, hosts and services. Segment to segment access shall be based on strong access control policy and principle of least privilege.	All REs except small-size, self-certification REs (Mandatory)
82	Anticipate	Protect	Identity Mgmt, Authentication & Access	PR.AA.S1, PR.AA.S2, PR.AA.S3, PR.AA.S7, PR.AA.S9	b. REs shall install network security devices, such as WAF, proxy servers, IPS, etc. to protect their IT infrastructure which is exposed to the internet, from security exposures originating from internal and external sources.	All REs except small-size, self-certification REs (Mandatory)
83	Anticipate	Protect	Identity Mgmt, Authentication & Access	PR.AA.S1, PR.AA.S2, PR.AA.S3, PR.AA.S7, PR.AA.S9	c. REs shall deploy web and email filters on the network. These devices shall be configured to scan for known bad domains, sources, and addresses, block these before receiving and downloading message and filter out emails with known malicious indicators, such as known malicious subject lines, and block suspicious Internet Protocol (IP) addresses, malicious domains/URLs at the firewall. All emails, attachments, and downloads both on the host and at the mail gateway shall be scanned with a reputable antivirus solution.	All REs except small-size, self-certification REs (Mandatory)
84	Anticipate	Protect	Identity Mgmt, Authentication & Access	PR.AA.S1, PR.AA.S2, PR.AA.S3, PR.AA.S7, PR.AA.S9	d. Network devices of REs shall be configured in line with whitelist approach of IPs, ports and services for inbound and outbound communication with proper ACL implementation.	All REs except small-size, self-certification REs (Mandatory)
85	Anticipate	Protect	Identity Mgmt, Authentication & Access	PR.AA.S1, PR.AA.S2, PR.AA.S3, PR.AA.S7, PR.AA.S9	e. REs shall implement DNS filtering services to ensure clean DNS traffic is allowed in the environment. DNS security extension for secure communication shall be used.	All REs except small-size, self-certification REs (Mandatory)
86	Anticipate	Protect	Identity Mgmt, Authentication & Access	PR.AA.S1, PR.AA.S2, PR.AA.S3, PR.AA.S7, PR.AA.S9	f. Management of critical servers/ applications/ services/ network elements shall be restricted through enterprise identified intranet systems.	All REs except small-size, self-certification REs (Mandatory)
87	Anticipate	Protect	Identity Mgmt, Authentication & Access	PR.AA.S1, PR.AA.S2, PR.AA.S3, PR.AA.S7, PR.AA.S9	g. REs shall implement SPF, DMARC, and DKIM for email security.	All REs except small-size, self-certification REs (Mandatory)
88	Anticipate	Protect	Identity Mgmt, Authentication & Access	PR.AA.S1, PR.AA.S2, PR.AA.S3, PR.AA.S7, PR.AA.S9	h. Email protection shall include (but not limited to) best practices like strong password protection, MFA, spam filtering, email encryption, secure email gateway, permissible attachments types, etc.	All REs except small-size, self-certification REs (Mandatory)

89	Anticipate	Protect	Identity Mgmt, Authentication & Access	PR.AA.S1, PR.AA.S2, PR.AA.S3, PR.AA.S7, PR.AA.S9	i. REs shall block malicious domains/IPs after diligently verifying them without impacting the operations. CSIRT-Fin/ CERT-In advisories which are published periodically shall be referred for latest malicious domains/ IPs, C&C DNS and links.	All REs except small-size, self-certification REs (Mandatory)
90	Anticipate	Protect	Identity Mgmt, Authentication & Access	PR.AA.S1, PR.AA.S2, PR.AA.S3, PR.AA.S7, PR.AA.S9	j. REs shall maintain an up-to-date and centralised inventory of authorised devices connected to REs' network (within/ outside RE's premises) and authorised devices enabling the REs' network. The REs may consider implementing solutions to automate network discovery and management.	All REs except small-size, self-certification REs (Mandatory)
91	Anticipate	Protect	Identity Mgmt, Authentication & Access	PR.AA.S4, PR.AA.S5	1. REs shall follow zero-trust security model in such a way that access (from within or outside REs' network) to their *critical systems* is by default denied by default and allowed only after proper authentication and authorization.	MIIs and Qualified REs (Mandatory)
92	Anticipate	Protect	Identity Mgmt, Authentication & Access	PR.AA.S4, PR.AA.S5	2. Delegated access and unused tokens shall be reviewed and cleaned at least on a quarterly basis.	MIIs and Qualified REs (Mandatory)
93	Anticipate	Protect	Identity Mgmt, Authentication & Access	PR.AA.S6	1. Effective authentication policy shall be implemented with the defined complexity of the password.	All REs (Mandatory)
94	Anticipate	Protect	Identity Mgmt, Authentication & Access	PR.AA.S6	2. All generic user IDs and email IDs which are not in use shall be removed after the use.	All REs (Mandatory)
95	Anticipate	Protect	Identity Mgmt, Authentication & Access	PR.AA.S6	3. REs shall implement strong password controls for users' access to systems, applications, networks, databases, etc. Password controls shall include (but not limited to) a change of password upon first login, minimum password length and history, password complexity as well as maximum validity period.	All REs except small-size, self-certification REs (Mandatory)
96	Anticipate	Protect	Identity Mgmt, Authentication & Access	PR.AA.S6	4. The user credential data shall be stored using strong hashing algorithms.	All REs except small-size, self-certification REs (Mandatory)
97	Anticipate	Protect	Identity Mgmt, Authentication & Access	PR.AA.S8	1. REs are advised to ensure that all logs sources are being identified and their respective logs are being collected. An indicative list of types of log data to be collected by REs is as follows: system logs, application logs, network logs, database logs, security logs, performance logs, audit trail logs, and event logs.	All REs (Mandatory)
98	Anticipate	Protect	Identity Mgmt, Authentication & Access	PR.AA.S8	2. Strong log retention policy shall be implemented as per government guidelines/ policies/ laws/ circulars/ regulations, etc. issued by SEBI/ GoI such as IT Act 2000, Digital Personal Data Protection Act (DPDP) 2023, and as required by CERT-In, NCIIPC or any other government agency.	All REs (Mandatory)
99	Anticipate	Protect	Identity Mgmt, Authentication & Access	PR.AA.S8	3. In order to identify unusual patterns and behaviours, monitoring of all logs of events and incidents shall be done.	All REs (Mandatory)

100	Anticipate	Protect	Identity Mgmt, Authentication & Access	PR.AA.S10, PR.AA.S11, PR.AA.S12	1. Physical Security a. Physical access to the *critical systems* shall be restricted to a minimum and shall be provided only to authorized officials. Physical access provided to third-party service providers shall be properly supervised by ensuring at the minimum that third-party service providers are accompanied at all times by authorized employees.	All REs (Mandatory)
101	Anticipate	Protect	Identity Mgmt, Authentication & Access	PR.AA.S10, PR.AA.S11, PR.AA.S12	b. Employees of REs shall be screened before granting access to organizational information and information systems. Physical access to the critical systems shall be revoked immediately if the same is no longer required.	All REs (Mandatory)
102	Anticipate	Protect	Identity Mgmt, Authentication & Access	PR.AA.S10, PR.AA.S11, PR.AA.S12	c. All REs shall ensure that the perimeter of the critical equipment's room, if any, are physically secured and monitored by employing physical, human and procedural controls such as the use of security guards, CCTVs, card access systems, mantraps, bollards, etc. wherever appropriate.	All REs (Mandatory)
103	Anticipate	Protect	Identity Mgmt, Authentication & Access	PR.AA.S10, PR.AA.S11, PR.AA.S12	2. Remote Support Service Security a. As many OEMs and their service partners as well as System Integrators provide remote support services to organisations, REs shall ensure that these services are well-governed, controlled, logged and an oversight is maintained on all the activities done by remote support service providers. The above shall be complemented by regular monitoring and audit to ensure compliance of the defined policies for privileged users and remote access.	All REs (Mandatory)
104	Anticipate	Protect	Identity Mgmt, Authentication & Access	PR.AA.S10, PR.AA.S11, PR.AA.S12	b. REs shall ensure secure usage of RDP in IT systems. Further, it shall be implemented strictly on a need-to-use basis, and it must employ MFA. Remote access, if necessary, shall be given to authorised personnel from whitelisted IPs for a predefined time period, and with a provision to log all activities.	All REs (Mandatory)
105	Anticipate	Protect	Identity Mgmt, Authentication & Access	PR.AA.S10, PR.AA.S11, PR.AA.S12	c. Employees and third-party service providers who may be given authorized access to the critical systems, networks and other IT resources of REs shall be subject to stringent supervision, monitoring and access restrictions.	All REs (Mandatory)
106	Anticipate	Protect	Identity Mgmt, Authentication & Access	PR.AA.S10, PR.AA.S11, PR.AA.S12	d. Environmental controls (temperature, water, smoke, etc.), service availability alerts (power supply, servers, etc.), access logs, etc. shall be monitored.	All REs except small, self-certification REs (Mandatory)
107	Anticipate	Protect	Identity Mgmt, Authentication & Access	PR.AA.S13, PR.AA.S14	1. REs shall formulate a data-disposal and data retention policy to identify the value and lifetime of various parcels of data.	All REs (Mandatory)
108	Anticipate	Protect	Identity Mgmt, Authentication & Access	PR.AA.S13, PR.AA.S14	2. REs shall frame suitable policies for disposal of storage media and systems. The critical data/ information on such devices and systems shall be removed by using methods such as wiping/ cleaning/ overwrite, degauss/ crypto shredding/ physical destruction as applicable.	All REs (Mandatory)

109	Anticipate	Protect	Identity Mgmt, Authentication & Access	PR.AA.S15	1. Endpoint security a. Solutions like EPP, EDR, XDR, anti-malware software etc. shall be implemented to detect threats and attacks on endpoint devices, and to enable immediate response to such threats and attacks. Further, REs shall ensure that signatures are updated on all IT systems.	All REs except small-size, self-certification REs (Mandatory)
110	Anticipate	Protect	Identity Mgmt, Authentication & Access	PR.AA.S15	b. Solutions like IPS/ NG-IPS shall be used to continuously monitor the organizations' network for malicious activities.	All REs except small-size, self-certification REs (Mandatory)
111	Anticipate	Protect	Identity Mgmt, Authentication & Access	PR.AA.S15	c. PowerShell and local admin rights shall be disabled by default on endpoint machines and shall be used only for a specific purpose and for a limited time.	All REs except small-size, self-certification REs (Mandatory)
112	Anticipate	Protect	Identity Mgmt, Authentication & Access	PR.AA.S15	2. Guidance on usage of Active Directory (AD) servers a. REs shall regularly review the AD to locate and close existing backdoors such as compromised service accounts, which often have administrative privileges and are a potential target of attacks.	All REs except small-size, self-certification REs (Mandatory)
113	Anticipate	Protect	Identity Mgmt, Authentication & Access	PR.AA.S15	b. REs shall undertake the penetration testing activity for known AD Domain Controller abuse attacks. Weaknesses shall be remediated on topmost priority.	All REs except small-size, self-certification REs (Mandatory)
114	Anticipate	Protect	Identity Mgmt, Authentication & Access	PR.AA.S15	3. Restricted use of removable media and electronic devices a. REs shall define and implement policy for restriction and secure use of removable media (such as USB, external hard disks, etc.) and electronic devices (such as laptops, mobile devices, etc.). REs shall ensure secure erasure of data so that no data is in recoverable form on such media and electronic devices after use.	All REs except small-size, self-certification REs (Mandatory)
115	Anticipate	Protect	Identity Mgmt, Authentication & Access	PR.AA.S16, PR.AA.S17	1. API security a. API security protects against vulnerabilities and misconfigurations in the APIs and prevents their misuse. Thus, effective API security strategies like rate limiting, throttling, etc. shall be used while developing APIs to prevent overuse or abuse. If APIs have been provided by MIIs and consumed by REs then onus of ensuring API security shall be on MIIs. MIIs shall have API security solutions in place for securing services and data transmitted through APIs.	All REs except small-size, Self-certification REs (Mandatory)
116	Anticipate	Protect	Identity Mgmt, Authentication & Access	PR.AA.S16, PR.AA.S17	b. Proper access management, and effective authentication and authorization shall be done to ensure that only the desired entities have access to the APIs.	All REs except small-size, Self-certification REs (Mandatory)
117	Anticipate	Protect	Identity Mgmt, Authentication & Access	PR.AA.S16, PR.AA.S17	c. OWASP documentation for developing APIs shall be followed and OWASP top 10 API security risks shall be mitigated.	All REs except small-size, Self-certification REs (Mandatory)
118	Anticipate	Protect	Identity Mgmt, Authentication & Access	PR.AA.S16, PR.AA.S17	d. Connecting to entities via APIs shall be strictly on a whitelist-based approach.	All REs except small-size, Self-certification REs (Mandatory)

119	Anticipate	Protect	Identity Mgmt, Authentication & Access	PR.AA.S16, PR.AA.S17	2. Mobile Application Security a. The mobile application shall perform root detection and root cloaking detection. The application shall not work on emulators or virtual devices. b. REs shall explore the feasibility of implementing a code that checks if the device is rooted/ jailbroken prior to the installation of the mobile application and disallow the mobile application to install/ function if the phone is rooted/ jailbroken. c. Device Policy enforcement such as detection of developer option, USB debugging, Mock Location, time settings manipulation, etc. shall be configured. d. Mobile application shall check new network connections or connections for unsecured networks like VPN connection, proxy and unsecured Wi-Fi connections. e. Mobile application shall have anti-malware capabilities covering application spoofing, RAT, screen mirroring, overlay malwares, key loggers, tap jacking, etc. f. Controls to prevent reverse engineering and application tampering shall be implemented in the mobile applications. These controls shall also validate the signature during runtime for authenticity of the application. g. Mobile application shall perform checksum validation and the checksum of applications shall be published in public domain. h. Mobile application shall identify the presence of active remote access, screen	All REs except small-size, Self-certification REs (Mandatory)
120	Anticipate	Protect	Identity Mgmt, Authentication & Access	PR.AA.S16, PR.AA.S17	m. Mobile application shall implement device-binding solution to create a unique digital identity based on device, mobile number and SIM. n. OWASP – MASVS shall be referred for implementing mobile application security and other protection measures. o. REs shall consider implementing measures such as installing a "containerized" app on mobile/ smart phones for exclusive business use that is encrypted and separated from other smartphone data/ applications; implement measures to initiate a remote wipe on the containerized app, rendering the data unreadable, in case of requirement may also be considered.	All REs except small-size, self-certification REs
121	Anticipate	Protect	Identity Mgmt, Authentication & Access	PR.AA.S16, PR.AA.S17	3. Guidelines for Application Security and Emerging Technologies REs shall prepare SOPs for open source application security and concerns from emerging technologies like Generative AI security.	MIIs and Qualified REs
122	Anticipate	Protect	Awareness & Training	PR.AT.S1, PR.AT.S2	1. REs shall work on building awareness of cybersecurity, cyber resilience, and system hygiene among employees (with a focus on employees from non-technical disciplines).	All REs (Mandatory)
123	Anticipate	Protect	Awareness & Training	PR.AT.S1, PR.AT.S2	2. REs shall ensure that their employees are aware of potential risks including social engineering attacks, phishing, etc.	All REs (Mandatory)

124	Anticipate	Protect	Awareness & Training	PR.AT.S1, PR.AT.S2	3. Majority of the infections are primarily introduced via phishing emails, malicious adverts on websites, and third-party apps and programs. Hence, thoughtfully designed security awareness campaigns that stress the avoidance of clicking on links and attachments in email, shall be established as an essential pillar of defence. Additionally, the advisories issues by CERT-In/ CSIRT-Fin may be referred for assistance in conducting exercises for public awareness.	All REs (Mandatory)
125	Anticipate	Protect	Awareness & Training	PR.AT.S1, PR.AT.S2	4. REs shall conduct periodic training programs to enhance knowledge of IT/ cybersecurity policy and standards among the employees incorporating up-to-date cybersecurity threats. Wherever possible, this shall be extended to outsourced staff, third-party service providers, etc.	All REs (Mandatory)
126	Anticipate	Protect	Awareness & Training	PR.AT.S1, PR.AT.S2	5. The training programs shall be reviewed and updated to ensure that the contents of the program remain current and relevant.	All REs (Mandatory)
127	Anticipate	Protect	Awareness & Training	PR.AT.S3	1. REs shall mention/ incorporate a section on the mobile and web application clearly specifying the process and procedure (with forms/ contact information, etc.) to lodge customer/ investor grievances with respect to technology related issues and cybersecurity. A mechanism to keep this information periodically updated shall also be put in place. The reporting facility on the application shall provide an option for registering a grievance. Customers/ investors dispute handling, reporting and resolution procedures, including the expected timelines for the response should be clearly defined.	All REs (Mandatory)
128	Anticipate	Protect	Awareness & Training	PR.AT.S3	2. REs shall provide access to mobile and web applications to a customer only at her/ his option based on specific written or authenticated electronic requisition along with a positive acknowledgement of the terms and conditions.	All REs (Mandatory)
129	Anticipate	Protect	Awareness & Training	PR.AT.S3	3. REs shall provide a mechanism on their mobile and web application for their customers/ investors with necessary authentication to identify/ mark a transaction as fraudulent for seamless and immediate notification to his entities. On such notification by the customer/investor, they may endeavour to build the capability for seamless/ instant reporting of fraudulent transactions to the corresponding beneficiary/ counterparty's entities; vice-versa have mechanism to receive such fraudulent transactions reported from other entities.	All REs (Mandatory)
130	Anticipate	Protect	Awareness & Training	PR.AT.S3	4. Improve and maintain customer/ investor awareness and education with regard to cybersecurity risks.	All REs (Mandatory)
131	Anticipate	Protect	Awareness & Training	PR.AT.S3	5. Encourage customers/investors to report phishing mails/ phishing sites and on such reporting take effective remedial action.	All REs (Mandatory)

132	Anticipate	Protect	Awareness & Training	PR.AT.S3	6. Educate the customers/investors on the downside risk of sharing their login credentials/ passwords/ OTP etc. to any third-party and the consequences thereof.	All REs (Mandatory)
133	Anticipate	Protect	Data Security	PR.DS.S1, PR.DS.S2, PR.DS.S3	1. Data and Storage Devices security a. Data shall be encrypted in motion, at rest and in-use by using strong encryption methods. Data-in-use encryption shall be applicable for cloud deployment (refer **Annexure-J**). Layering of Full-disk Encryption (FDE) along with File-based Encryption (FBE) shall be used wherever possible. REs shall use industry standard, strong encryption algorithms (e.g., RSA, AES, etc.) wherever encryption is implemented. Illustrative measures in this regard are given in **Annexure-H** and **Annexure-I**.	All REs except small-size, self-certification REs (Mandatory)
134	Anticipate	Protect	Data Security	PR.DS.S1, PR.DS.S2, PR.DS.S3	1. Data and Storage Devices security b. REs shall deploy Data Loss Prevention (DLP) solutions/ processes.	All REs except small-size, self-certification REs (Mandatory)
135	Anticipate	Protect	Data Security	PR.DS.S1, PR.DS.S2, PR.DS.S3	1. Data and Storage Devices security c. REs shall implement measures to prevent unauthorized access, copying, transmission of data/ information held in contractual or fiduciary capacity. It shall be ensured that confidentiality of information is not compromised during the process of exchanging and transferring information with external parties. Illustrative measures to ensure security during transportation of data over the internet are given in Annexure-I.	All REs except small-size, self-certification REs (Mandatory)
136	Anticipate	Protect	Data Security	PR.DS.S1, PR.DS.S2, PR.DS.S3	1. Data and Storage Devices security d. The information security policy shall also cover use of devices such as mobile phones, photocopiers, scanners, etc., which can be used for capturing and transmission of sensitive data within their IT infrastructure. For instance, defining access policies for personnel, network connectivity for such devices, etc.	All REs except small-size, self-certification REs (Mandatory)
137	Anticipate	Protect	Data Security	PR.DS.S1, PR.DS.S2, PR.DS.S3	1. Data and Storage Devices security e. REs shall allow only authorized data storage device within their IT infrastructure through appropriate validation processes.	All REs except small-size, self-certification REs (Mandatory)

138	Anticipate	Protect	Data Security	PR.DS.S1, PR.DS.S2, PR.DS.S3	2. Application Security in Customer Facing Applications: a. Application security for Customer facing applications offered over the Internet such as IBTs (Internet Based Trading applications), portals containing sensitive or private information and Back office applications (repository of financial and personal information offered by REs to Customers) are paramount as they carry significant attack surfaces by virtue of being available publicly over the Internet for mass use. An illustrative list of measures for ensuring security in such applications is provided in **Annexure-G**.	All REs except self-certification REs (Mandatory)
139	Anticipate	Protect	Data Security	PR.DS.S1, PR.DS.S2, PR.DS.S3	1. REs shall implement suitable mechanisms, including generation of appropriate alerts, to monitor capacity utilisation on a real-time basis and shall proactively address issues pertaining to their capacity needs.	All REs except self-certification REs (Mandatory)
140	Anticipate	Protect	Data Security	PR.DS.S1, PR.DS.S2, PR.DS.S3	. 2. For capacity planning and monitoring, REs shall comply with circulars/ guidelines on capacity planning issued by SEBI (and updated from time to time).	All REs except self-certification REs (Mandatory)
141	Anticipate	Protect	Data Security	PR.DS.S1, PR.DS.S2, PR.DS.S3	1. REs shall keep the *Regulatory Data* available and easily accessible in legible and usable form, within the legal boundaries of India. However, for the investors whose country of incorporation is outside India, the REs shall keep the original data, available and easily accessible in legible and usable form, within the legal boundaries of India. Further, if the *Regulatory Data* retained within India is not in readable form, the REs must maintain an application/system to read/ analyse the retained data.	All REs (Mandatory)
142	Anticipate	Protect	Data Security	PR.DS.S1, PR.DS.S2, PR.DS.S3	2. The *IT and Cybersecurity Data* which is sent to/ consumed by global/ international SOC of the REs and SaaS based cybersecurity solutions have been exempted from being maintained within the legal boundaries of India. For above mentioned SaaS based cybersecurity solutions and SOC offerings utilized by REs where the data is not processed/stored within the legal boundaries of India, such data shall be classified, assessed and periodically reviewed (at least once in a year) by the respective *IT Committee for REs* or equivalent body of the RE. Additionally, such *IT and Cybersecurity Data* shall be approved by the Board/ Partners/ Proprietor annually. Further, such data shall be made available to SEBI/ CERT-In/ any other government agency whenever required within a reasonable time not exceeding 48 hours from the time of request.	All REs (Mandatory)

143	Anticipate	Protect	Data Security	PR.DS.S1, PR.DS.S2, PR.DS.S3	3. While doing data classification, REs shall adhere to data security standards and guidelines and other government guidelines/ policies/ laws/ circulars/ regulations, etc. issued by SEBI/ GoI such as IT Act 2000, Digital Personal Data Protection Act (DPDP) 2023 or any other law/ circular/ regulation as and when issued.	All REs (Mandatory)
144	Anticipate	Protect	Data Security	PR.DS.S4	1. REs shall enforce effective data protection, backup, and recovery measures.	All REs (Mandatory)
145	Anticipate	Protect	Data Security	PR.DS.S4	2. REs shall block administrative rights on end user workstations/ PCs/ laptops by default and provide access rights on need basis as per the established process and approvals and for specific duration for which it is required.	All REs (Mandatory)
146	Anticipate	Protect	Data Security	PR.DS.S4	3. Security controls for mobile and web applications shall focus on how these applications handle, store, and protect PII and other business related data.	All REs (Mandatory)
147	Anticipate	Protect	Data Security	PR.DS.S4	4. Web and mobile applications shall not store sensitive information in HTML hidden fields, cookies, or any other client-side storage to avoid any compromise in the integrity of the data.	All REs (Mandatory)
148	Anticipate	Protect	Data Security	PR.DS.S4	5. REs shall renew their digital certificates used in IT systems well in time.	All REs (Mandatory)
149	Anticipate	Protect	Data Security	PR.DS.S4	6. REs shall implement measures to control usage of VBA/macros in office documents, control permissible attachment types in email systems.	All REs (Mandatory)
150	Anticipate	Protect	Data Security	PR.DS.S4	7. REs shall have a documented data migration policy specifying SOPs and processes for data migration while ensuring data integrity, completeness and consistency.	All REs (Mandatory)
151	Anticipate	Protect	Data Security	PR.DS.S5	1. For the development of all software/ applications and feature enhancements, there shall be separate production and non-production environments.	MIIs and Qualified REs (Mandatory)
152	Anticipate	Protect	Data Security	PR.DS.S5	2. After development and/ or feature enhancement, SIT shall be done to ensure that the complete software/ application is working as required.	MIIs and Qualified REs (Mandatory)
153	Anticipate	Protect	Data Security	PR.DS.S5	3. During the development phase of any software/application to be used by the REs or customers of REs, it shall be ensured that vulnerabilities identified by best practices baselines such as OWASP, top 25 software security vulnerabilities identified by SANS, etc. are addressed. It is recommended that REs should adopt methodologies like DevSecOps for secure development of their applications/ software.	MIIs and Qualified REs (Mandatory)

154	Anticipate	Protect	Data Security	PR.DS.S6	1. REs shall obtain the source codes for all critical applications from their third-party service providers. Where obtaining of the source code is not possible, REs shall put in place a source code escrow arrangement or other equivalent arrangements to adequately mitigate the risk of default by the third-party service provider. REs shall ensure that all product updates and patches/ fixes are included in the source code escrow arrangement.	MIIs and Qualified REs (Mandatory)
155	Anticipate	Protect	Data Security	PR.DS.S6	2. For all the software and applications, where vulnerabilities will be identified at a later date, REs shall ensure that the vulnerabilities shall be mitigated in a time bound manner. REs shall also stipulate timelines in their SLA with their third-party service providers for the timely compliance and closure of identified vulnerabilities.	MIIs and Qualified REs (Mandatory)
156	Anticipate	Protect	Data Security	PR.DS.S6	3. REs shall put in place appropriate third-party service providers (including software vendors) risk assessment process and controls proportionate to their criticality/ risk in order to manage supply chain risks effectively.	MIIs and Qualified REs (Mandatory)
157	Anticipate	Protect	Data Security	PR.DS.S6	4. REs shall ensure that maintenance and necessary support for applications/ software is provided by the third-party service providers (including software vendors) and the same is enforced through a formal agreement.	MIIs and Qualified REs (Mandatory)
158	Anticipate	Protect	Information Protection Procedures	PR.IP.S1	1. REs shall ensure that IT, OT and IS infrastructure is 'secure by design', 'secure by engineering/ implementation' and the infrastructure has appropriate elements to ensure 'secure IT operations'.	All REs
159	Anticipate	Protect	Information Protection Procedures	PR.IP.S1	2. For implementation of principle of least functionality, measures such as configuring only essential capabilities by disabling unnecessary and/or unsecured functions, ports, protocols, services, etc. within an information systems shall be implemented.	All REs
160	Anticipate	Protect	Information Protection Procedures	PR.IP.S1	3. REs shall use application directory whitelisting on all assets to ensure that only authorized software are run and all unauthorized software are blocked from installation/ execution.	All REs except small-size, self-certification REs (Mandatory)
161	Anticipate	Protect	Information Protection Procedures	PR.IP.S1	1. Hardening of Hardware and Software a. REs shall deploy only hardened and vetted hardware/ software. During the hardening process, REs shall, inter-alia, ensure that default usernames and passwords are replaced with non-standard usernames and strong passwords and all unnecessary services are removed or disabled in software/ system.	All REs (Mandatory)
162	Anticipate	Protect	Information Protection Procedures	PR.IP.S1	b. Hardening of OS shall be done to protect servers'/ endpoints' OS, and minimize attack surface and exposure to threats.	All REs (Mandatory)

163	Anticipate	Protect	Information Protection Procedures	PR.IP.S1	c. For running services, non-default ports shall be used wherever applicable. Open ports on networks and systems, which are not in use or can be potentially used for exploitation of data, shall be blocked. All open ports shall be monitored and appropriate measures shall be taken to secure them.	All REs (Mandatory)
164	Anticipate	Protect	Information Protection Procedures	PR.IP.S1	d. Practice of whitelisting of ports based (at firewall level) on business usage shall be implemented rather than blacklisting of certain ports. Traffic on all other ports which have not been whitelisted shall be blocked by default.	All REs (Mandatory)
165	Anticipate	Protect	Information Protection Procedures	PR.IP.S1	e. REs shall restrict execution of "PowerShell" and "wscript" in their environment, if not required. Additionally, REs shall also ensure installation and use of latest version of PowerShell, with enhanced logging enabled, script block logging and transcription enabled. Send the associated logs to a centralized log repository for monitoring and analysis.	All REs (Mandatory)
166	Anticipate	Protect	Information Protection Procedures	PR.IP.S1	f. REs shall utilize host based firewall to prevent Remote Procedure Call (RPC) and Server Message Block (SMB) communications among endpoints wherever possible to limit lateral movement as well as other attack activities.	All REs (Mandatory)
167	Anticipate	Protect	Information Protection Procedures	PR.IP.S3	1. The change management process shall be part of all agreements with third-party service providers to ensure that changes to the system are implemented in a controlled and coordinated manner.	All REs except small-size, self-certification REs
168	Anticipate	Protect	Information Protection Procedures	PR.IP.S3	2. Change Management process shall include (but not limited to) submission, planning (impact analysis, rollout plan), approval, and implementation, review (post-implementation), closure, etc.	All REs except small-size, self-certification REs
169	Anticipate	Protect	Information Protection Procedures	PR.IP.S3	3. REs shall have a clearly defined framework for change management including requirements justifying exception(s), duration of exception(s), process of granting exception(s), and authority for approving and for periodic review of exception(s) given.	All REs except small-size, self-certification REs
170	Anticipate	Protect	Information Protection Procedures	PR.IP.S4, PR.IP.S6	3. Secure Software Development Life Cycle (SSDLC) a. All REs shall ensure that regression testing is undertaken before new or modified systems are implemented. The scope of tests shall cover business logic, security controls and system performance under various stress-load scenarios, and recovery conditions. b. For any production release, vulnerability assessment shall be undertaken. For all *major release*, VAPT shall be conducted by the REs to assess the risk and vulnerabilities generated from recent additions/ modifications in applications/ software.	All REs except small-size, self-certification REs (Mandatory)

171	Anticipate	Protect	Information Protection Procedures	PR.IP.S4, PR.IP.S6	4. Secure Software Development Cycle (SSDLC) a. REs shall prepare business requirement document with clear mentioning of security requirements, session management, audit trail, logging, data integrity, security event tracking, exception handling, etc. b. For secure rollout of software and applications, threat modelling and application security testing shall be conducted during development. c. REs shall refer to standards, security guidelines for application security and other protection measures given by OWASP (for e.g. OWASP-ASVS). d. REs shall adopt the principle of defence-in-depth to provide a layered security mechanism. e. Before introducing new technologies for critical systems, REs shall ensure that IT/ security team has assessed evolving security concerns and achieved fair level of maturity with such technologies before incorporating them into IT infrastructure.	All REs
172	Anticipate	Protect	Information Protection Procedures	PR.IP.S14	1. Periodic Audit a. REs shall engage only CERT-In empanelled IS auditing organizations for conducting external audits including cyber audit to audit the implementation of all standards mentioned in this framework.	All REs except self-certification REs (Mandatory)
173	Anticipate	Protect	Information Protection Procedures	PR.IP.S14	b. A CERT-In empanelled IS auditing organisation can audit the RE for a maximum period of three consecutive years. Subsequently, the said IS auditing organisation shall be eligible for auditing the RE again only after a cooling off period of two years.	All REs except self-certification REs (Mandatory)
174	Anticipate	Protect	Information Protection Procedures	PR.IP.S14	c. The details of periodicity, timeline and report submission for cyber audit by REs have been provided in the 'CSCRF Compliance, Audit Report Submission, and Timelines' section.	All REs except self-certification REs (Mandatory)
175	Anticipate	Protect	Information Protection Procedures	PR.IP.S14	d. Along with the cyber audit reports, henceforth, all REs shall also submit a declaration from the Managing Director (MD)/ Chief Executive Officer (CEO) as mentioned in Annexure-B.	All REs except self-certification REs (Mandatory)
176	Anticipate	Protect	Information Protection Procedures	PR.IP.S14	e. To ensure that all the open vulnerabilities in the IT assets of REs have been fixed, revalidation VAPT and cyber audit shall also be done in a time bound manner.	All REs except self-certification REs (Mandatory)
177	Anticipate	Protect	Information Protection Procedures	PR.IP.S14	f. Audit Management process of the REs shall include (but not limited to) audit program/ calendar, planning, preparation, delivery, evaluation, reporting, and follow- up, etc.	All REs except self-certification REs (Mandatory)
178	Anticipate	Protect	Information Protection Procedures	PR.IP.S14	g. For conducting audits, CERT-In 'IT Security Auditing Guidelines for Auditee Organizations' may be followed by REs. Additionally, CERT-In 'Guidelines for CERT-In Empanelled IS Auditing Organizations' (attached at Annexure-D) may be mandated for empanelled IS auditing organizations.	All REs except self-certification REs (Mandatory)

179	Anticipate	Protect	Information Protection Procedures	PR.IP.S14	h. Due diligence with respect to the audit process and the tools used for such audits shall be undertaken by REs to ensure competence and effectiveness of audits.	All REs except self-certification REs (Mandatory)
180	Anticipate	Protect	Information Protection Procedures	PR.IP.S14	i. REs shall strive for building an automated tool and suitable dashboards (preferably integrated with log aggregator) for submitting compliance with CSCRF. A dashboard shall be available at the time of cyber audit, onsite inspection/ audit by SEBI or any agency appointed by SEBI.	MIIs and Qualified REs (Mandatory)
181	Anticipate	Protect	Information Protection Procedures	PR.IP.S15	1. All the categories of software solutions/ applications/ products for *critical systems* used by REs shall mandatorily pass-through the following tests/ audits and compliances: a. Application security testing: i. Dynamic Application Security Testing (DAST) for scanning software applications in real-time against leading vulnerability sources, such as OWASP Top 10, SANS Top 25 CWE, etc. to find security flaws or open vulnerabilities. ii. Static Application Security Testing (SAST) for analyzing program source code to identify security vulnerabilities such as SQL injection, buffer overflows, XML external entity (XXE) attacks, OWASP Top 10 security risks, etc.	All REs (Mandatory)
182	Anticipate	Protect	Information Protection Procedures	PR.IP.S15	b. Functional audit	All REs (Mandatory)
183	Anticipate	Protect	Information Protection Procedures	PR.IP.S15	c. VAPT after every major release of the application/software	All REs (Mandatory)
184	Anticipate	Protect	Information Protection Procedures	PR.IP.S15	d. All critical systems logs shall be integrated with RE's SOC.	All REs (Mandatory)
185	Anticipate	Protect	Information Protection Procedures	PR.IP.S15	e. Audit of firewall configuration, WAF configuration, token configuration and channel identification shall be done.	All REs (Mandatory)
186	Anticipate	Protect	Information Protection Procedures	PR.IP.S15	f. Software bill of material (SBOM)	All REs (Mandatory)
187	Anticipate	Protect	Information Protection Procedures	PR.IP.S15	g. Requirement Traceability Matrix	All REs (Mandatory)
188	Anticipate	Protect	Information Protection Procedures	PR.IP.S15	2. Tests/ audits stated above at point 1 (a-b) shall be limited to cybersecurity aspects. Application security testing shall also include API security and API discovery. Scope of functional audit shall cover data integrity, report integrity, and transaction integrity, etc.	All REs (Mandatory)
189	Anticipate	Protect	Information Protection Procedures	PR.IP.S15	3. With respect to empanelled COTS used by Stock Brokers and Depository Participants: a. Before empaneling any COTS solutions for supplying software/ products to their respective stock brokers and depository participants, Stock Exchanges and Depositories shall conduct tests/ audits stated above at point 1 (a-b) through STQC. b. The Stock Exchanges and Depositories shall prepare a SOP for inclusion of tests/ audits in their vendor empanelment process for COTS solutions. c. The empanelment shall be approved by the Stock Exchanges and Depositories only after receipt of compliance reports from STQC and VAPT report from the COTS vendor.	All REs (Mandatory)

190	Anticipate	Protect	Information Protection Procedures	PR.IP.S15	4. Customized COTS: a. REs shall ensure that the compliance with tests/ audits stated above at point 1 (a-d) by CERT-In empanelled IS auditing organization for any customized COTS.	All REs (Mandatory)
191	Anticipate	Protect	Information Protection Procedures	PR.IP.S15	5. Inhouse developed software: a. REs shall ensure compliance with aforementioned point 1 is submitted by CERT-In empanelled IS auditing organization.	All REs (Mandatory)
192	Anticipate	Protect	Information Protection Procedures	PR.IP.S15	6. Software services in form of SaaS/ hosted services used by REs: i. REs shall be required to submit compliance with the technical specification mentioned in hosted services definition for the SaaS/ hosted services used by them.	All REs (Mandatory)
193	Anticipate	Protect	Information Protection Procedures	PR.IP.S15	6. Software services in form of SaaS/ hosted services used by REs: ii. REs shall also submit compliance with adoption of hosted services and SaaS as per the various functions of CSCRF including Governance, Identify, Protect, Detect, Respond, and Recover.	All REs (Mandatory)
194	Anticipate	Protect	Information Protection Procedures	PR.IP.S16	1. ISO 27001 certification shall be mandatory for REs as it provides essential security standards with respect to ISMS. The scope for ISO 27001 certification shall include (but not limited to) PDC site, DR site, NDR site, SOC, and Colocation facility.	MIIs and qualified REs (Mandatory)
195	Anticipate	Protect	Information Protection Procedures	PR.IP.S17	1. REs shall follow the latest version of CIS Controls or equivalent standards which are prioritized set of safeguards and actions for cyber defence and provide specific and actionable ways to mitigate prevalent cybersecurity incidents/ attacks.	MIIs and qualified REs (Mandatory)
196	Anticipate	Protect	Maintenance	PR.MA.S2	1. REs shall ensure proper remote access policy framework incorporating the specific requirements of accessing the enterprise resources (located in the data centre) securely from home using internet connection.	All REs except small-size, self-certification REs (Mandatory)
197	Anticipate	Protect	Maintenance	PR.MA.S2	2. REs shall ensure that only trusted client machines shall be permitted to access enterprise IT resources remotely. REs shall put in place appropriate security control measures such as (including but not limited to) host integrity check, binding of MAC address of the device with the IP address, etc. for remote access and telecommuting.	All REs except small-size, self-certification REs (Mandatory)
198	Anticipate	Protect	Maintenance	PR.MA.S2	3. REs shall ensure that appropriate risk mitigation mechanisms are put in place whenever remote access of data centre resources is permitted for third-party service providers.	All REs except small-size, self-certification REs (Mandatory)
199	Anticipate	Protect	Maintenance	PR.MA.S2	4. REs shall ensure that remote access shall be monitored continuously for any abnormal/ unauthorized access, and appropriate alerts and alarms shall be generated to address this breach before any damage is done.	All REs except small-size, self-certification REs (Mandatory)

200	Anticipate	Protect	Maintenance	PR.MA.S3	1. REs shall establish and ensure that the patch management procedures include the identification, categorization and prioritization of patches and updates. An implementation timeframe for each category of patches shall be established to apply them in a timely manner.	All REs (Mandatory)
201	Anticipate	Protect	Maintenance	PR.MA.S3	2. All operating systems and applications shall be updated with the latest patches on a regular basis. As an interim measure for zero-day vulnerabilities, and where patches are not available, virtual patching may be considered for protecting systems and networks. This measure hinders cybercriminals from gaining access to any system through vulnerabilities in end-of-support and end-of-life applications and software. Patches shall be sourced only from the authorized sites of the OEM.	All REs (Mandatory)
202	Anticipate	Protect	Maintenance	PR.MA.S3	3. REs shall perform comprehensive and rigorous testing of security patches and updates, wherever possible, before deployment into the production environment so as to ensure that application of patches does not impact other systems.	All REs (Mandatory)
203	Anticipate	Protect	Maintenance	PR.MA.S3	4. All patches shall be tested first in non-production environment which shall be identical to the production environment.	All REs (Mandatory)
204	Anticipate	Protect	Maintenance	PR.MA.S3	5. Hardware and software of *critical systems* shall be replaced before they reach End-of-Life/End-of-Support.	All REs (Mandatory)
205	Anticipate	Protect	Maintenance	PR.MA.S3	6. Compensatory controls like virtual patching shall be implemented for legacy systems for a maximum period of 6 months. Further, the constraints due to which virtual patching is done shall be legitimate and documented.	All REs (Mandatory)
206	Anticipate	Protect	Maintenance	PR.MA.S3	7. Procurement of hardware/software shall be aligned with technology refresh policy of the REs.	All REs (Mandatory)
207	Anticipate	Protect	Maintenance	PR.MA.S3	8. REs shall establish a patch management policy to ensure that all applicable patches (at both PDC and DR Site are identified, assessed, tested and applied to all IT systems/applications in a timely manner. The policy shall be approved by IT Committee for REs. Additionally, the above-mentioned policy on patch management shall be reviewed by IT Committee for REs atleast on an annual basis.	MIIs and Qualified REs (Mandatory)
208	Anticipate	Protect	Maintenance	PR.MA.S3	9. REs shall ensure that post application of any patch/ update, the resources deployed are adequate enough to deliver the expected performance.	MIIs and Qualified REs (Mandatory)
209	Anticipate	Protect	Maintenance	PR.MA.S3	10. REs shall also establish processes for tracking patch compliance across all IT systems/ applications and reporting the same to their respective *IT Committee for REs* on a quarterly basis.	MIIs and Qualified REs (Mandatory)

210	Anticipate	Protect	Maintenance	PR.MA.S3	11. Based on the criticality of the patches, REs shall ensure that patches are implemented at both PDC and DR site within the upper/ maximum time limit as defined below. However, for emergency patching, patches shall be deployed within timelines as stipulated by the OEMs.	MIIs and Qualified REs (Mandatory)
211	Anticipate	Detect	Security Continuous Montitoring	DE.CM.S1, DE.CM.S2, DE.CM.S3	1. Security Continuous Monitoring a. REs shall establish appropriate security monitoring systems and processes to facilitate continuous monitoring of security events/ alerts and timely detection of unauthorized or malicious activities, unauthorized changes, unauthorized access and unauthorized copying and transmission of data/ information held in contractual or fiduciary capacity, by internal and external parties. The security logs of systems, applications and network devices exposed to the internet shall also be monitored for anomalies.	All REs (Mandatory)
212	Anticipate	Detect	Security Continuous Montitoring	DE.CM.S1, DE.CM.S2, DE.CM.S3	1. Security Continuous Monitoring b. Suitable alerts shall be generated in the event of detection of unauthorized or abnormal system activities, transmission errors or unusual online transactions.	All REs (Mandatory)
213	Anticipate	Detect	Security Continuous Montitoring	DE.CM.S1, DE.CM.S2, DE.CM.S3	1. Security Continuous Monitoring c. To enhance the security monitoring, REs (except client-based stock brokers having less than 100 clients) are mandated to employ SOC services for their systems. REs may choose any of the following models to use SOC services: i. RE's own SOC/ group SOC ii. Market SOC implemented mandatorily by NSE, BSE and optionally by NSDL and/ or CDSL iii. Any other third party managed SOC	All REs (Mandatory)
214	Anticipate	Detect	Security Continuous Montitoring	DE.CM.S1, DE.CM.S2, DE.CM.S3	1. Security Continuous Monitoring d. Small-Size and Self-certification category REs are mandated to be on-boarded on above-mentioned Market SOC.	All REs (Mandatory)
215	Anticipate	Detect	Security Continuous Montitoring	DE.CM.S1, DE.CM.S2, DE.CM.S3	2. Functional efficacy of SOC a. REs shall measure functional efficacy of their SOC using the quantifiable method given in **Annexure-N**.	MIIs and Qualified REs (Mandatory)
216	Anticipate	Detect	Security Continuous Montitoring	DE.CM.S1, DE.CM.S2, DE.CM.S3	2. Functional efficacy of SOC b. REs shall review the functional efficacy of SOC on a half-yearly basis.	MIIs and Qualified REs (Mandatory)
217	Anticipate	Detect	Security Continuous Montitoring	DE.CM.S1, DE.CM.S2, DE.CM.S3	2. Functional efficacy of SOC c. REs shall deploy solutions such as BAS, CART, decoy, vulnerability management, etc. to enhance their cybersecurity posture.	MIIs and Qualified REs (Mandatory)
218	Anticipate	Detect	Security Continuous Montitoring	DE.CM.S1, DE.CM.S2, DE.CM.S3	2. Functional efficacy of SOC d. Those REs who are utilizing third-party managed SOC services or market SOC shall obtain SOC efficacy report (using the quantifiable method given in **Annexure-N**) from their SOC provider on a yearly basis.	All REs having third-party managed SOC or market SOC (mandatory)

219	Anticipate	Detect	Security Continuous Montitoring	DE.CM.S4	1. The use of IT assets/ resources shall be monitored, tuned and projections shall be made for future capacity requirements to ensure the required system performance for meeting the business objectives.	All REs except small-size, Self-certification REs (Mandatory)
220	Anticipate	Detect	Security Continuous Montitoring	DE.CM.S4	2. To ensure high resilience, high availability and timely detection of attacks on systems and networks, REs shall implement suitable mechanisms to monitor capacity utilization of its critical systems and networks.	All REs except small-size, Self-certification REs (Mandatory)
221	Anticipate	Detect	Security Continuous Montitoring	DE.CM.S4	3. Capacity management shall comprise of three primary types; Data storage capacity – (e.g. in database systems, file storage areas, etc.); Processing power capacity – (e.g. adequate computational power to ensure timely processing operations); and Communications capacity – ("bandwidth" to ensure communications are made in a timely manner).	All REs except small-size, Self-certification REs (Mandatory)
222	Anticipate	Detect	Security Continuous Montitoring	DE.CM.S4	4. Capacity management shall be; a. Pro-active – for example, using capacity considerations as part of change management; b. Reactive – e.g. triggers and alerts for when capacity usage is reaching a critical threshold so that timely increments (temporary or permanent) can be made.	All REs except small-size, Self-certification REs (Mandatory)
223	Anticipate	Detect	Security Continuous Montitoring	DE.CM.S5	1. The details of periodicity, timeline and report submission for cyber audit by REs have been provided in the *'CSCRF Compliance, Audit Report Submission, and Timelines'* section.	All REs (Mandatory)
224	Anticipate	Detect	Security Continuous Montitoring	DE.CM.S5	2. REs shall regularly conduct cybersecurity audit and VAPT with scope as mentioned in CSCRF in order to detect vulnerabilities in the IT environment. Further, REs shall conduct in-depth evaluation of the security posture of the system through simulations of actual attacks. An indicative (but not exhaustive and limited to) VAPT scope has been attached at **Annexure-I**.	All REs (Mandatory)
225	Anticipate	Detect	Security Continuous Montitoring	DE.CM.S5	3. The assets under these audits shall include (but not limited to) all *critical systems*, infrastructure components (like networking systems, security devices, load balancers, servers, databases, applications, remote access points, systems accessible through WAN, LAN as well as with Public IP's, websites, etc.), and other IT systems pertaining to the operations of REs.	All REs (Mandatory)
226	Anticipate	Detect	Security Continuous Montitoring	DE.CM.S5	4. REs shall perform VAPT prior to the commissioning of new systems, especially those which are part of *critical systems* or connected to *critical systems*.	All REs (Mandatory)
227	Anticipate	Detect	Security Continuous Montitoring	DE.CM.S5	5. Revalidation of VAPT post closure of observations shall be done in a time bound manner to ensure that all the open vulnerabilities have been fixed.	All REs (Mandatory)

228	Anticipate	Detect	Security Continuous Montitoring	DE.CM.S5	6. In case of vulnerabilities being discovered in COTS (used for core business) or empanelled applications, REs shall report them to the vendors and the designated stock exchanges and/ or depositories in a timely manner.	Stock Brokers/ Depository Participants falling under Qualified REs and Mid-size REs (Mandatory)
229	Anticipate	Detect	Detection Process	DE.DP.S4	1. REs shall conduct red teaming exercises as part of their cybersecurity framework on a half-yearly basis through use of red/ blue teams.	MIIs and Qualified REs (Mandatory)
230	Anticipate	Detect	Detection Process	DE.DP.S4	2. CART solution shall be deployed for continuous, automated process of testing the security of the systems, and achieving greater visibility on attack surfaces.	MIIs and Qualified REs (Mandatory)
231	Anticipate	Detect	Detection Process	DE.DP.S4	3. For red teaming exercise, a red team may consist of REs employees and/ or outside experts. Additionally, the red team shall be independent of the function being tested.	MIIs and Qualified REs (Mandatory)
232	Anticipate	Detect	Detection Process	DE.DP.S4	4. The results of the red teaming exercise shall be placed before *IT Committee for REs* and Governing board. The lessons learned from conducting such red team exercises shall be shared with SEBI within 3 months after completion of the exercise. Status of the remediation of the observation found during the red team exercise shall be monitored by *IT Committee for REs*.	MIIs and Qualified REs (Mandatory)
233	Anticipate	Detect	Detection Process	DE.DP.S5	1. REs shall proactively search for hidden and undetected cyber threats in their network.	MIIs and Qualified REs (Mandatory)
234	Anticipate	Detect	Detection Process	DE.DP.S5	2. Threat hunting by leveraging threat intelligence, IOCs, IOAs, etc. shall be conducted on a quarterly basis.	MIIs and Qualified REs (Mandatory)
235	Withstand & Contain	Respond	Incident Management	RS.MA.S1	1. All REs shall formulate an up-to-date CCMP in line with national CCMP of CERT-In.	All REs (Mandatory)
236	Withstand & Contain	Respond	Incident Management	RS.MA.S1	2. CCMP shall be approved by Board/ Partners/ Proprietor of REs.	All REs (Mandatory)
237	Withstand & Contain	Respond	Incident Management	RS.MA.S1	3. Incident Response Management a. All REs shall develop an Incident Response Management Plan as part of their CCMP.	All REs (Mandatory)
238	Withstand & Contain	Respond	Incident Management	RS.MA.S1	3. Incident Response Management b. The response plan shall define responsibilities and actions to be performed by its employees and support/ outsourced staff in the event of a cyber-attack or cybersecurity incident.	All REs (Mandatory)
239	Withstand & Contain	Respond	Incident Management	RS.MA.S1	3. Incident Response Management c. REs shall have a SOP for handling cybersecurity incident response and recovery for the various cybersecurity attacks.	All REs (Mandatory)
240	Withstand & Contain	Respond	Incident Management	RS.MA.S1	3. Incident Response Management d. MIIs shall have a SOP for cybersecurity incidents reported to them by the REs under their supervision.	All REs (Mandatory)

241	Withstand & Contain	Respond	Incident Management	RS.MA.S1	3. Incident Response Management e. SOP for reporting of cybersecurity incidents to SEBI is attached at **Annexure-O**. The same shall be adhered to.	All REs (Mandatory)
242	Withstand & Contain	Respond	Incident Management	RS.MA.S2	1. In order to optimize the REs' ability to respond in a timely and appropriate manner, REs shall: a. Create cybersecurity awareness,	All REs except small-size, self-certification REs
243	Withstand & Contain	Respond	Incident Management	RS.MA.S2	1. In order to optimize the REs' ability to respond in a timely and appropriate manner, REs shall: b. Provide cybersecurity training to the relevant teams,	All REs except small-size, self-certification REs
244	Withstand & Contain	Respond	Incident Management	RS.MA.S2	1. In order to optimize the REs' ability to respond in a timely and appropriate manner, REs shall: c. Develop/ hire people with appropriate skill-sets,	All REs except small-size, self-certification REs
245	Withstand & Contain	Respond	Incident Management	RS.MA.S2	1. In order to optimize the REs' ability to respond in a timely and appropriate manner, REs shall: d. Prepare cyber playbooks,	All REs except small-size, self-certification REs
246	Withstand & Contain	Respond	Incident Management	RS.MA.S2	1. In order to optimize the REs' ability to respond in a timely and appropriate manner, REs shall: e. Create knowledge database for all known adverse conditions and attacks	All REs except small-size, self-certification REs
247	Withstand & Contain	Respond	Incident Management	RS.MA.S5	1. REs shall collaborate with Cyber Swachhta Kendra (CSK) operated by CERT-In to trace bots and vulnerable service(s) running on their public IP addresses, and receive alerts regarding the same. The alerts received from CSK shall be closed in a time-bound manner. Observations (from CSK) which require a longer time to close shall be put up to the *IT Committee for REs* for their guidance and appropriate mitigation/ closure.	MIIs and Qualified REs (Mandatory)
248	Withstand & Contain	Respond	Incident Communication	RS.CO.S1, RS.CO.S2, RS.CO.S3	1. Any cyber-attack, cybersecurity incident and/ or breach falling under CERT-In Cybersecurity directions shall be notified to SEBI and CERT-In within 6 hours of noticing/ detecting such incidents or being brought to notice about such incidents. This information shall be shared with SEBI through the mkt_incidents@sebi.gov.in within 6 hours. However, necessary details of the incidents shall be reported on SEBI Incident Reporting Portal within 24 hours. Stock Brokers/ Depository Participants shall also report the incidents to Stock Exchanges/ Depositories along with SEBI and CERT-In within 6 hours of noticing/ detecting such incidents or being brought to notice about such incidents. All other cybersecurity incident(s) shall be reported to SEBI, CERT-In and NCIIPC (as applicable) within 24 hours.	All REs (Mandatory)
249	Withstand & Contain	Respond	Incident Communication	RS.CO.S1, RS.CO.S2, RS.CO.S3	2. REs shall share Threat Intelligence data that is collected, processed, and analysed to gain insights into the motives and behaviour (of the threat actor), target, attack pattern, etc. on SEBI Incident Reporting portal.	All REs (Mandatory)

250	Withstand & Contain	Respond	Incident Communication	RS.CO.S1, RS.CO.S2, RS.CO.S3	3. The incident shall also be reported to CERT-In in accordance with the guidelines/ directions issued by CERT-In from time to time. Additionally, the REs, whose systems have been identified as "Protected system" by NCIIPC shall also report the incident to NCIIPC.	All REs (Mandatory)
251	Withstand & Contain	Respond	Incident Communication	RS.CO.S1, RS.CO.S2, RS.CO.S3	4. The quarterly reports containing information on cyber-attacks, threats, cybersecurity incidents and breaches experienced by REs and measures taken to mitigate vulnerabilities, threats and attacks including information on bugs/ vulnerabilities, threats that may be useful for other REs and SEBI, shall be submitted to SEBI within 15 days from the quarter ended June, September, December and March of every year.	All REs (Mandatory)
252	Withstand & Contain	Respond	Incident Communication	RS.CO.S1, RS.CO.S2, RS.CO.S3	5. Such details, which are deemed useful for sharing with other REs, in a masked manner, shall be shared using mechanism to be specified by SEBI from time to time. While sharing the above-mentioned sensitive information, TLP may be followed with four levels of sensitivity: white, green, amber, or red.	All REs (Mandatory)
253	Withstand & Contain	Respond	Incident Communication	RS.CO.S1, RS.CO.S2, RS.CO.S3	6. During the processing of reported incidents by SEBI, REs shall provide regular reports (such as RCA, forensic analysis report, etc.) on the progress of the incident analysis.	All REs (Mandatory)
254	Withstand & Contain	Respond	Incident Communication	RS.CO.S2	1. *IT Committee for REs* shall discuss response plans, coordination with stakeholders for consistency in response actions, information sharing for better awareness, etc.	MIIs and Qualified REs (Mandatory)
255	Withstand & Contain	Respond	Incident Communication	RS.CO.S2	2. For the purpose of coordinating incident response, REs shall regularly update the contact details of service providers, intermediaries, and other stakeholders.	MIIs and Qualified REs (Mandatory)
256	Withstand & Contain	Respond	Incident Communication	RS.CO.S2	3. If the cyber-attack is of high impact and has a broad reach, the RE shall give a press release which shall include (but not limited to) a brief of the incident, actions taken to recover, normal operation resumption status (once achieved), etc. and inform all the affected customers/ stakeholders.	MIIs and Qualified REs (Mandatory)
257	Withstand & Contain	Respond	Incident Communication	RS.CO.S2	4. If the cyber-attack is of low impact and has a narrow/low reach, the REs shall inform all the affected customers/ stakeholders.	MIIs and Qualified REs (Mandatory)
258	Withstand & Contain	Respond	Incident Communication	RS.CO.S2	5. REs shall notify the customer/ investor, through alternate communication channels, of all transactions including buy/ sell, payment or fund transfer above a specified value determined by the customer/ investor.	All REs (Mandatory)

259	Withstand & Contain	Respond	Incident Analysis	RS.AN.S1, RS.AN.S2, RS.AN.S3	1. Alerts generated from monitoring and detection systems shall be suitably investigated by the REs in order to determine activities that are to be performed to prevent spread of cybersecurity incidents/ attacks or breaches, mitigate their effects and resolve the incidents.	All REs (Mandatory)
260	Withstand & Contain	Respond	Incident Analysis	RS.AN.S1, RS.AN.S2, RS.AN.S3	2. Data collection: REs shall collect and preserve data related to the incident, such as system logs, network traffic, and forensic images of affected systems.	All REs (Mandatory)
261	Withstand & Contain	Respond	Incident Analysis	RS.AN.S1, RS.AN.S2, RS.AN.S3	3. Incident Analysis: REs shall analyse the data to understand the scope, cause, and impact of the incident, including how the incident occurred, what systems and data were affected, who was responsible, etc.	All REs (Mandatory)
262	Withstand & Contain	Respond	Incident Analysis	RS.AN.S1, RS.AN.S2, RS.AN.S3	4. Evidence Preservation: REs shall preserve evidence related to the incident, including digital artefacts, network captures, and memory dumps, in a secure and forensically sound manner.	All REs (Mandatory)
263	Withstand & Contain	Respond	Incident Analysis	RS.AN.S4, RS.AN.S5	1. Root Cause Analysis: REs shall perform a root cause analysis (RCA) to identify the specific control that has failed, underlying cause of the incident and the potential areas of improvement.	All REs (Mandatory)
264	Withstand & Contain	Respond	Incident Analysis	RS.AN.S4, RS.AN.S5	2. Forensic: Forensic analysis (as appropriate) shall be undertaken by the REs.	All REs (Mandatory)
265	Withstand & Contain	Respond	Incident Analysis	RS.AN.S4, RS.AN.S5	3. Any incident of loss or destruction of data or systems shall be thoroughly analysed and lessons learned from such incidents shall be incorporated to strengthen the security mechanisms and improve the recovery planning and processes.	All REs (Mandatory)
266	Withstand & Contain	Respond	Incident Analysis	RS.AN.S4, RS.AN.S5	4. Reporting: REs shall create a detailed incident report that includes information on the scope, cause, and impact of the incident, as well as recommendations for improving incident response and recovery capabilities.	All REs (Mandatory)
267	Withstand & Contain	Respond	Incident Analysis	RS.AN.S4, RS.AN.S5	5. REs shall conduct a compromise assessment through CERT-In empanelled IS auditing organizations.	All REs (Mandatory)
268	Withstand & Contain	Respond	Improvements	RS.IM.S1	1. REs shall periodically review and update their contingency plan, COOP, training exercises, and incident response and recovery plans (including CCMP) to incorporate lessons learned, and strengthen their response capabilities in the event of a future incident/ attack.	All REs except self-certification REs (Mandatory)
269	Withstand & Contain	Respond	Improvements	RS.IM.S1	2. Post occurrence of cybersecurity incident (if any), REs shall update their response and recovery plan (including CCMP) to improve their cyber resilience and incorporate the learnings from the cybersecurity incident.	All REs (Mandatory)
270	Withstand & Contain	Respond	Improvements	RS.IM.S2	3. The updates and changes in the contingency plan, COOP, training exercises, and incident response and recovery plan shall be communicated and approved by the Board/ Partners/ Proprietor.	All REs

271	Recover	Recover	Incident Recovery Execution	RC.RP.S1	1. The response and recovery plans of the REs shall include scenario-based classifications. REs shall build their own response and recovery plan as per their business model and include the same in their CCMP.	All REs (Mandatory)
272	Recover	Recover	Incident Recovery Execution	RC.RP.S1	2. The response and recovery plan of the REs shall have plans for the timely restoration of systems affected by incidents of cybersecurity incidents/ attacks or breaches (for instance, offering alternate services or systems to customers). Tests shall be designed to challenge the assumptions of response, resumption and recovery practices, including governance arrangements and communication plans. These tests shall include all stakeholders such as critical service providers, vendors, other linked REs, etc.	All REs (Mandatory)
273	Recover	Recover	Incident Recovery Execution	RC.RP.S1	3. An indicative (but not exhaustive and limited to) recovery plan to be followed by the REs has been attached at **Annexure-C**.	All REs (Mandatory)
274	Recover	Recover	Incident Recovery Execution	RC.RP.S1	4. REs shall maintain regularly updated *'golden images'* of *critical systems* at offsite location for rebuilding the systems (whenever required). This entails maintaining images "templates" that include a preconfigured operating system (OS), configuration setting backup and associated software applications that can be quickly deployed to rebuild a system, such as a virtual machine or server.	MIIs and Qualified REs (Mandatory)
275	Recover	Recover	Incident Recovery Execution	RC.RP.S1	5. REs shall explore the possibility of retaining spare hardware in an isolated environment to rebuild systems in an event that starting REs' operations from PDC and/ or DRS is not feasible. The REs shall also try to keep spare hardware in ready-to-use state for delivering critical services and such systems shall be updated as and when new changes (for example OS patches, security patches, etc.) are implemented in the primary systems. This spare hardware shall regularly undergo testing in-line with the response and recovery plan of the REs.	MIIs and Qualified REs (Mandatory)
276	Recover	Recover	Incident Recovery Execution	RC.RP.S1	6. REs shall take all necessary precautions while updating the 'golden' server images and data backup to ensure that server images and data backups are undamaged/unbroken.	MIIs and Qualified REs (Mandatory)
277	Recover	Recover	Incident Recovery Execution	RC.RP.S1	7. In case of ransomware attacks that specifically target backups, conventional data backups may not be effective. Therefore, REs shall create backups in an isolated and immutable (and/ or air-gapped) manner to ensure recovery if production system is compromised.	MIIs and Qualified REs (Mandatory)

278	Recover	Recover	Incident Recovery Execution	RC.RP.S1	8. REs shall undertake regular business continuity drills to check the readiness of the organization and effectiveness of existing security controls at the ground level. One such drill scenario recommended to be tested is recovering from a ransomware attack considering both PDC and DRS have been impacted. This shall assess the effectiveness of people, processes and technologies to deal with such attacks.	MIIs and Qualified REs (Mandatory)
279	Recover	Recover	Incident Recovery Execution	RC.RP.S2	1. In the event of disruption of any one or more of the *critical systems*, the RE shall, within 30 minutes of the incident, declare that incident as 'Disaster' based on the business impact analysis. Accordingly, the RTO shall be two (2) hours as recommended by IOSCO for the resumption of critical operations. The RPO shall be 15 minutes for all REs. The recovery plan shall be scenario-based and in line with the RTO and RPO specified.	All REs (Mandatory)
280	Recover	Recover	Incident Recovery Execution	RC.RP.S2	2. REs shall conduct comprehensive scenario-based cyber resilience testing at least 2 times in a financial year (periodicity of such testing shall be of 6 months), to validate their ability to recover and resume operations following a cybersecurity incident/ attack within prescribed RTO and RPO defined by SEBI. In this regard, REs shall incorporate extreme plausible cyber-attack scenarios into their cyber response and recovery planning. The said scenarios may be devised by REs in consultation with their respective *IT Committee for REs* based on the learning from various sources such as past cybersecurity incidents, near-miss analysis, data from Security Operations Centre, honeypot logs analysis, etc.	MIIs and Qualified REs (Mandatory)
281	Recover	Recover	Incident Recovery Execution	RC.RP.S2	3. REs shall periodically conduct backup testing and restore back-up data to check its usability.	MIIs and Qualified REs (Mandatory)
282	Recover	Recover	Incident Recovery Execution	RC.RP.S2	4. For cyber resilience testing, REs shall also include stakeholders such as critical third- party service providers, market intermediaries, linked REs, etc.	MIIs and Qualified REs (Mandatory)
283	Recover	Recover	Incident Recovery Execution	RC.RP.S2	5. The result of the Cyber resilience testing shall be placed before *IT Committee for REs*. The lessons learned from conducting such cyber resilience testing shall be shared with SEBI within 3 months from the end of the relevant period of conducting cyber resilience testing. Status of the observations found during the cyber resilience testing shall be monitored and tracked by *IT Committee for REs*.	MIIs and Qualified REs (Mandatory)
284	Recover	Recover	Incident Recovery Execution	RC.RP.S3	1. All REs shall conduct suitable periodic drills to test the adequacy and effectiveness of the response and recovery plan.	All REs (Mandatory)

285	Recover	Recover	Incident Recovery Execution	RC.RP.S4	1. A backup and recovery plan shall be formulated by the REs and approved by their respective *IT Committee for REs* . The backup and recovery plan shall include policies and software solutions that work together to maintain business continuity in the event of a security incident. Such plan shall include guidance on restoration of data with the backup software used by the RE.	All REs (Mandatory)
286	Recover	Recover	Incident Recovery Execution	RC.RP.S4	2. The backup and recovery policy shall include backup of data as well as backup of server images.	All REs (Mandatory)
287	Recover	Recover	Incident Recovery Execution	RC.RP.S4	3. The backup of data and server images shall be maintained at off-site locations to keep backup copies intact and unbroken.	All REs (Mandatory)
288	Recover	Recover	Incident Recovery Execution	RC.RP.S4	4. RTO and RPO, as prescribed by SEBI from time to time, shall be included in the recovery plan for the restoration of systems after cybersecurity incidents.	All REs (Mandatory)
289	Recover	Recover	Incident Recovery Execution	RC.RP.S4	5. REs shall maintain offline, encrypted backups of data and shall regularly test these backups at least on a quarterly basis to ensure confidentiality, integrity and availability of data.	MIIs and Qualified REs (Mandatory)
290	Recover	Recover	Incident Recovery Communication	RC.CO.S1, RC.CO.S2, RC.CO.S3	1. Recovery plans shall be discussed with *IT Committee for REs* by the REs. Such plans shall include stakeholders' coordination in recovery process, and both internal and external communication.	All REs
291	Recover	Recover	Incident Recovery Improvements	RC.IM.S1	1. While ensuring protection of data, and security of processes, RE's BCP-DR capabilities shall support its cyber resilience objectives, and rapid recovery and resumption of critical operations after cybersecurity incident.	All REs
292	Recover	Recover	Incident Recovery Improvements	RC.IM.S1	2. REs shall try to incorporate lessons learned from incidents reported (if any) by other REs.	All REs
293	Recover	Recover	Incident Recovery Improvements	RC.IM.S2	1. RE's RTO shall be met for all interconnected systems and networks through capacity upgradations and periodic coordinated resilience testing.	All REs (Mandatory)
294	Recover	Recover	Incident Recovery Improvements	RC.IM.S2	2. Recovery plan shall be improved after analysing the learnings from periodic drills.	All REs (Mandatory)
295	Evolve	Evolve	Evolve	EV.ST.S1, EV.ST.S2, EV.ST.S3	1. REs shall anticipate new attack vectors through threat modelling (based on risk assessment) and work to defend them.	All REs except small, self-certification REs
296	Evolve	Evolve	Evolve	EV.ST.S1, EV.ST.S2, EV.ST.S3	2. REs shall strive for reducing their attack surfaces.	All REs except small, self-certification REs
297	Evolve	Evolve	Evolve	EV.ST.S1, EV.ST.S2, EV.ST.S3	3. RE shall proactively examine controls, practices, and capabilities for prospective, emerging or potential threats.	All REs except small, self-certification REs

298	Evolve	Evolve	Evolve	EV.ST.S1, EV.ST.S2, EV.ST.S3	4. RE shall proactively assess and take necessary actions with respect to its system's requirements, architecture, design, configuration, acquisition processes, or operational processes as a strategy for adaptation to the identified and prospective threats and vulnerabilities.	All REs except small, self-certification REs
299	Evolve	Evolve	Evolve	EV.ST.S1, EV.ST.S2, EV.ST.S3	5. RE shall continuously improve upon the ability to quickly deploy and integrate existing and new services, both on-premises and in the cloud.	All REs except small, self-certification REs
300	Evolve	Evolve	Evolve	EV.ST.S1, EV.ST.S2, EV.ST.S3	6. RE shall strive to rapidly correlate data using mathematical models and machine learning in order to make data-driven decisions.	All REs except small, self-certification REs
301	Evolve	Evolve	Evolve	EV.ST.S1, EV.ST.S2, EV.ST.S3	7. REs shall use auditing/ logging systems on different OS to acquire and store audit/logging data.	All REs except small, self-certification REs
302	Evolve	Evolve	Evolve	EV.ST.S1, EV.ST.S2, EV.ST.S3	8. In order to include heterogeneity, apply different audit/logging regimes at different architectural layers.	All REs except small, self-certification REs
303	Evolve	Evolve	Evolve	EV.ST.S1, EV.ST.S2, EV.ST.S3	9. REs shall look for feasibility of deploying diverse operating systems. Attack or compromise on one type of OS may not affect other OS deployed.	All REs except small, self-certification REs
304	Evolve	Evolve	Evolve	EV.ST.S1, EV.ST.S2, EV.ST.S3	10. RE shall maintain extra capacity of IT assets for information storage, processing, or communications.	All REs except small, self-certification REs