Cyber Resilience goal: ANTICIPATE		
Cybersecurity control: PROTECT		
PR.AA: Guidelines		
PR.AA.S1, PR.AA.S2, PR.AA.S3, PR.AA.S7, PR.AA.S9	1. <u>Access Controls, Password Policy/ Authentication Mechanism</u> a. No person by virtue of rank or position shall have any intrinsic right to access confidential data applications, system resources or facilities. 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. c. User access rights, delegated access and unused tokens, and privileged users' activities shall be reviewed on a periodic basis. d. Access to external cloud services such as Dropbox, google drive, iCloud, OneDrive, etc. shall be given as per RE's policy. 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. f. Account access lock policies after failure attempts shall be implemented for all accounts.	All REs (Mandatory)

Standards	CSCRF guidelines	Applicability
	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. 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to deactivate access privileges of users who are leaving the organization or whose access privileges have been withdrawn.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. i. All *critical systems* accessible over the internet shall have multi-factor security (such as VPNs, Firewall controls, etc.) and MFA. 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. 2. <u>Network Security Management</u> 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. 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. c. The LAN and wireless networks within REs' premises shall be secured with proper access controls.	

Standards	CSCRF guidelines	Applicability
	d. REs shall keep total and maximum connections to SMTP server limited.	
	3. Access Controls, Password Policy/ Authentication Mechanism a. PIM solution or PIM process shall be implemented to keep track of privileged access. 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**. 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. 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[27] 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. 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)

[27] Refer Table 15 in 'CSCRF Compliance, Audit Report Submission, and Timelines' section.

Standards	CSCRF guidelines	Applicability
	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. 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. 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. 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. f. Management of critical servers/ applications/ services/ network elements shall be restricted through enterprise identified intranet systems. g. REs shall implement SPF, DMARC, and DKIM for email security. 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. 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.	

Standards	CSCRF guidelines	Applicability
	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.	
PR.AA.S1, PR.AA.S2, PR.AA.S3	1. Stock Brokers who are providing algorithmic trading facilities shall take adequate measures to isolate and secure the perimeter and connectivity to the servers running algorithmic trading applications.	Stock Brokers/ Depository Participants (Mandatory)
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. 2. Delegated access and unused tokens shall be reviewed and cleaned at least on a quarterly basis.	MIIs and Qualified REs (Mandatory)
PR.AA.S6	1. Effective authentication policy shall be implemented with the defined complexity of the password. 2. All generic user IDs and email IDs which are not in use shall be removed after the use.	All REs (Mandatory)
	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. 4. The user credential data shall be stored using strong hashing algorithms.	All REs except small-size, self-certification REs (Mandatory)

Standards	CSCRF guidelines	Applicability
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. 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. 3. In order to identify unusual patterns and behaviours, monitoring of all logs of events and incidents shall be done.	All REs (Mandatory)
PR.AA.S10, PR.AA.S11, PR.AA.S12	1. <u>Physical Security</u> 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. 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. 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. 2. <u>Remote Support Service Security</u>	All REs (Mandatory)

Standards	CSCRF guidelines	Applicability
	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. 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. 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.	
	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)
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. 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)

Standards	CSCRF guidelines	Applicability
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. b. Solutions like IPS/ NG-IPS shall be used to continuously monitor the organizations' network for malicious activities. 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. 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. b. REs shall undertake the penetration testing activity for known AD Domain Controller abuse attacks. Weaknesses shall be remediated on topmost priority. 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)
	4. Secure Domain Controllers (DCs)	MIIs (Mandatory)

Standards	CSCRF guidelines	Applicability
	Threat actors often target and use DCs as a staging point to spread ransomware network-wide. a. REs shall ensure that DCs are patched as and when patch is released and it must be reviewed on a quarterly basis to ensure the implementation of the same. b. REs shall ensure that no unnecessary software is installed on DCs, as these can be leveraged to run arbitrary code on the system. c. REs shall ensure that access to DCs should be restricted to the Administrators group. Users within this group shall be limited and have separate accounts used for day-to-day operations with non-administrative permissions. d. REs shall ensure that DC host firewalls are configured to prevent direct internet access.	
PR.AA.S16, PR.AA.S17	1. <u>API security</u> 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. b. Proper access management, and effective authentication and authorization shall be done to ensure that only the desired entities have access to the APIs. c. OWASP documentation for developing APIs shall be followed and OWASP top 10 API security risks shall be mitigated. d. Connecting to entities via APIs shall be strictly on a whitelist-based approach.	All REs except small-size, Self-certification REs (Mandatory)

Standards	CSCRF guidelines	Applicability
	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 mirroring, active voice call, alert users, etc. to prevent online frauds. i. Mobile application shall require re-authentication whenever the device of the application remains unused for a designated period and also each time the investor/ user launches the application. j. Mobile application shall not store/ retain sensitive personal/ investor authentication information such as user IDs, passwords, keys, hashes, hard coded reference, etc.	

Standards	CSCRF guidelines	Applicability
	on the device and the application shall also securely wipe out any sensitive investor/ user information from memory when the investor/ user exits the application. k. Mobile application shall be secured against common vulnerabilities such as SQL injection, etc. l. REs shall ensure that the usage of raw SQL queries in mobile application to fetch or update data from databases is avoided. Additionally, sensitive information shall be written to the database in an encrypted form.	
	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
	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
PR.AT: Guidelines		
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). 2. REs shall ensure that their employees are aware of potential risks including social engineering attacks, phishing, etc.	All REs (Mandatory)

Standards	CSCRF guidelines	Applicability
	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. 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. 5. The training programs shall be reviewed and updated to ensure that the contents of the program remain current and relevant.	
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. 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. 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	All REs (Mandatory)

Standards	CSCRF guidelines	Applicability
	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. 4. Improve and maintain customer/ investor awareness and education with regard to cybersecurity risks. 5. Encourage customers/investors to report phishing mails/ phishing sites and on such reporting take effective remedial action. 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.	
PR.DS: Guidelines		
PR.DS.S1, PR.DS.S2, PR.DS.S3	1. <u>Data and Storage Devices security</u> 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**. b. REs shall deploy Data Loss Prevention (DLP) solutions/ processes. 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	All REs except small-size, self-certification REs (Mandatory)

Standards	CSCRF guidelines	Applicability
	exchanging and transferring information with external parties. Illustrative measures to ensure security during transportation of data over the internet are given in **Annexure-I**. 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. e. REs shall allow only authorized data storage device within their IT infrastructure through appropriate validation processes.	
	2. <u>Application Security in Customer Facing Applications:</u> 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)
	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. 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)

Standards	CSCRF guidelines	Applicability
	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. 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. 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)
PR.DS.S4	1. REs shall enforce effective data protection, backup, and recovery measures. 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)

Standards	CSCRF guidelines	Applicability
	3. Security controls for mobile and web applications shall focus on how these applications handle, store, and protect PII and other business related data. 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. 5. REs shall renew their digital certificates used in IT systems well in time. 6. REs shall implement measures to control usage of VBA/macros in office documents, control permissible attachment types in email systems. 7. REs shall have a documented data migration policy specifying SOPs and processes for data migration while ensuring data integrity, completeness and consistency.	
PR.DS.S5	1. For the development of all software/ applications and feature enhancements, there shall be separate production and non-production environments. 2. After development and/ or feature enhancement, SIT shall be done to ensure that the complete software/ application is working as required. 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)
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	MIIs and Qualified REs (Mandatory)

Standards	CSCRF guidelines	Applicability
	product updates and patches/ fixes are included in the source code escrow arrangement. 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. 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. 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.	
PR.IP: Guidelines		
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'. 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
	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)
	1. Hardening of Hardware and Software	All REs (Mandatory)

Standards	CSCRF guidelines	Applicability
	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. b. Hardening of OS shall be done to protect servers'/ endpoints' OS, and minimize attack surface and exposure to threats. 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. 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. 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. 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.	
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

Standards	CSCRF guidelines	Applicability
	2. Change Management process shall include (but not limited to) submission, planning (impact analysis, rollout plan), approval, and implementation, review (post-implementation), closure, etc. 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.	
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)
	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).	All REs

Standards	CSCRF guidelines	Applicability
	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.	
PR.IP.S14	1. <u>Periodic Audit</u> 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. 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. 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. 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**. 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. 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)

Standards	CSCRF guidelines	Applicability
	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. 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.	
	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)
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. b. Functional audit c. VAPT after every *major release* of the application/software d. All *critical systems* logs shall be integrated with RE's SOC. e. Audit of firewall configuration, WAF configuration, token configuration and channel identification shall be done.	All REs (Mandatory)

Standards	CSCRF guidelines	Applicability
	f. Software bill of material (SBOM) g. Requirement Traceability Matrix 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. 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. 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. 5. Inhouse developed software: a. REs shall ensure compliance with aforementioned point 1 is submitted by CERT-In empanelled IS auditing organization. 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.	

Standards	CSCRF guidelines	Applicability
	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.	
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)
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)
PR.MA: Guidelines		
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. 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. 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. 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)

Standards	CSCRF guidelines	Applicability
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. 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. 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. 4. All patches shall be tested first in non-production environment which shall be identical to the production environment. 5. Hardware and software of *critical systems* shall be replaced before they reach End-of-Life/End-of-Support. 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. 7. Procurement of hardware/software shall be aligned with technology refresh policy of the REs.	All REs (Mandatory)
	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	MIIs and Qualified REs

<table>
<tr><th>Standards</th><th>CSCRF guidelines</th><th>Applicability</th></tr>
<tr><td></td><td>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.
9. REs shall ensure that post application of any patch/ update, the resources deployed are adequate enough to deliver the expected performance.
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.
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.

<table>
<tr><th>S. No.</th><th>Criticality of Patch</th><th>Upper/ maximum Timeline</th></tr>
<tr><td>1</td><td>High</td><td>1 week</td></tr>
<tr><td>2</td><td>Moderate</td><td>2 weeks</td></tr>
<tr><td>3</td><td>Low</td><td>1 month</td></tr>
</table>
</td><td>(Mandatory)</td></tr>
</table>