Part II: CSCRF Guidelines

This section contains CSCRF guidelines that provides a direction to REs for the implementation of standards mentioned in CSCRF. There are certain guidelines which are mandatory in nature and have been written under '*Applicability*' column (Refer section 2 "*Thresholds for REs' categorization*").

Standards	CSCRF guidelines	Applicability
Cyber Resilience goal: ANTICIPATE		
Cybersecurity control: GOVERNANCE		
GV.OC: Guidelines		
GV.OC.S2, GV.OC.S3	1. Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners. 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
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. 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. 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	All REs (Mandatory)

Standards	CSCRF guidelines	Applicability
	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. 4. Engage a forensic auditor to identify the root cause of any incident (cybersecurity or other incidents) related to RE. 5. SEBI shall seek the audit reports of the audits conducted by RE.	
GV.RR: Guidelines		
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[22]. The level, grade, and standing of CISO shall be atleast equivalent to CTO/ CIO.	MIIs, Qualified REs (Mandatory)

[22] https://www.nciipc.gov.in/documents/Roles_Responsibilities-CISO.pdf

Standards	CSCRF guidelines	Applicability
	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)
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. 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
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	All REs except small-size, self-certification REs

Standards	CSCRF guidelines	Applicability
	c. Employment screening procedures, employment policies and agreement, employment termination procedures etc. are followed. 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.	
GV.PO: Guidelines		
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. 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)
	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	

Standards	CSCRF guidelines	Applicability
	aforementioned policies may form a part of RE's cybersecurity policy or may be standalone policies. 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. 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.	
	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

Standards	CSCRF guidelines	Applicability
	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
	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
	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[23] 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] Refer 'CSCRF Compliance, Audit Report Submission, and Timelines' section.

Standards	CSCRF guidelines	Applicability
	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)
	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)
	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
GV.OV: Guidelines		
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[24] 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)
GV.RM: Guidelines		

[24] Refer 'CSCRF Compliance, Audit Report Submission, and Timelines' section.

Standards	CSCRF guidelines	Applicability
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. b. REs shall consider using latest version of ISO 27005 as a guidance on design, implementation, and maintenance of information security risk management. 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. 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)

Standards	CSCRF guidelines	Applicability
	e. REs shall periodically assess level of employee cybersecurity awareness, for e.g., through phishing test success rate, etc. 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. g. Risk-based transaction monitoring or surveillance process shall be implemented as part of fraud risk management system across all delivery channels.	
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)
GV.SC: Guidelines		
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)

Standards	CSCRF guidelines	Applicability
	2. Where applications (for e.g.: NSE's NEAT, BSE's BOLT etc.) are offered to users over the internet by MIIs , the responsibility of ensuring cyber resilience of such applications resides with the MIIs and not with the users who are using the applications.	MIIs (Mandatory)
	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[25] 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. 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)
GV.SC.S5	1. REs shall obtain SBOM for existing their *critical systems* within 6 months (starting from the date of issuance of CSCRF). 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. 3. MIIs shall include SBOM as part of their empanelment criteria for application software vendors. 4. SBOM shall include (but not limited to) the following:	All REs (Mandatory)

[25] Refer 'CSCRF Compliance, Audit Report Submission, and Timelines' section.

Standards	CSCRF guidelines	Applicability
	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.	
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. 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. 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)

Standards	CSCRF guidelines	Applicability
	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**.