Annexure-K: Cyber Capability Index (CCI)

REPORTING FORMAT FOR MIIs AND QUALIFIED REs TO SUBMIT THEIR CCI SCORE

NAME OF THE ORGANISATION: <Name>

ENTITY TYPE: <Intermediary Type>

ENTITY CATEGORY: <Category of the RE as per CSCRF>

RATIONALE FOR THE CATEGORY: <>

PERIOD: <>

NAME OF THE AUDITING ORGANISATION (applicable for MIIs): <Name>

RE’s Authorised signatory declaration:

I/ We hereby confirm that Cyber Capability Index (CCI) has been verified by me/ us and I/ We shall take the responsibility and ownership of the CCI report.

Signature:

Name of the signatory:

Designation (choose whichever applicable): <MD/ CEO/ Board member/ Partners/ Proprietor>

Company stamp:

Annexures:

1. CCI report as per the format given in Table 27 and CCI score

Cyber Capability Index (CCI)

A. **Background**-

CCI is an index-framework to rate the preparedness and resilience of the cybersecurity framework of the Market Infrastructure Institutions (MIIs) and Qualified REs. While MIIs are required to conduct third-party assessment of their cyber resilience on a half-yearly basis, Qualified REs are directed to conduct self-assessment of their cyber resilience on an annual basis.

B. **Index Calculation Methodology**-

1. The index is calculated on the basis of 23 parameters. These parameters have been given different weightages.
2. Implementation evidence to be submitted to SEBI only on demand.
3. All implementation evidences shall be verified by the auditor for conducting third-party assessment of MIIs.
4. The list of CCI parameters, their corresponding target and weightages in the index, is as follows:

Table 27: CCI parameters with corresponding measure, implementation evidence, target, and weightage

S No	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage	Self-assessment score	Auditor comments w.r.t. cyber audit (for MIIs)
1.	Security Budget Measure **[GV.RR.S4]**	Information Security Goal: Provide resources necessary for information systems.	Percentage (%) of the organisation's information system budget devoted to information security.	Impact	(Information security budget/ total organisation's information technology budget) ×100	10%	1. What is the total information security budget across all organization's systems? 2. What is the total information technology budget across all organization's systems? 3. Approval Document from Competent Authority for the same.	8%		
2.	Vulnerability Measure **[DE.CM.S5]**	Objective of this measure is to ensure that the vulnerabilities in organization's systems are identified and mitigated	Percentage of vulnerabilities mitigated pertaining to organization in a specified time frame.	Effectiveness Measure	(Number of vulnerabilities mitigated/ Number of vulnerabilities identified)×100	100 %	1. Confirmation that VAPT is done by CERT-In empanelled IS auditing organization and as per the scope prescribed by SEBI	18%		

S No	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage	Self-assessment score	Auditor comments w.r.t. cyber audit (for MIIs)
							2. VAPT report and its closure report. 3. Time taken to close the identified vulnerabilities.			
3.	Security Training Measure **[PR.AT.S 1]**	Information Security Goal: Ensure that organization's personnel are adequately trained to carry out their assigned information security- related duties and responsibilities	Percentage (%) of information system security personnel that have received security training within the past one years.	Implementation	(Number of information system security personnel that have completed security training within the past year/total number of information system security personnel) ×100	100 %	1. Details of the training/ awareness sessions scheduled within the past 1 year. 2. Cyber audit observation against Standard 1 mentioned in 'Protect: Awareness and Training' header in CSCRF Part-I and respective guidelines in Part-II.	5%		

S No	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage	Self-assessment score	Auditor comments w.r.t. cyber audit (for MIIs)
4.	Remote Access Control Measure **[PR.AA.S 12]**	Information Security Goal: Restrict access to information, systems, and components to individuals or machines that have been authenticated and are identifiable, known and credible.	Percentage (%) of remote users logging through MFA.	Effectiveness	(Number of remote users logging through MFA/ total number of remote users) ×100	100 %	1. Does the organization use automated tools to maintain an up-to-date record that identifies all remote access points? 2. How many remote access points exist in the organization's network? 3. Does the organisation employ IDS or IPS to monitor traffic traversing remote access points? 4. Does the organisation collect and review audit logs associated with all remote	2%		

S No	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage	Self-assessment score	Auditor comments w.r.t. cyber audit (for MIIs)
							access points? 5. Evidence of users who are allowed remote access through MFA, validated through Firewall, AD, or any dedicated system. 6. Based on reviews of the incident database, IDS/ IPS logs and alerts, and/ or appropriate remote access point log files, how many access points have been used to gain unauthorized access within the reporting period?			

S No	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage	Self-assessment score	Auditor comments w.r.t. cyber audit (for MIIs)
5.	Audit Record Review Measure **[DE.CM.S1]**	Information Security Goal: Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, suspicious or abnormal activity.	Percentage (%) of *critical systems* integrated with SIEM.	Efficiency	(Number of *critical systems* integrated with SIEM tool/total number of *critical systems*) ×100	100 %	1. Is logging activated on the system? 2. Does the organization have clearly defined criteria for what constitutes evidence of "suspicious or abnormal" activity within system audit logs? 3. For the reporting period, how many system audit logs have been reviewed for past six months for suspicious or abnormal activity.	2%		

S No	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage	Self-assessment score	Auditor comments w.r.t. cyber audit (for MIIs)
6.	Configuration Changes Measure **[DE.CM.S5]**	Information Security Goal: Establish and maintain baseline configuration and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	Percentage (%) approved and implemented configuration changes identified in the latest automated baseline configuration.	Implementation	(Number of approved and implemented configuration changes identified in the latest automated baseline configuration/ total number of configuration changes identified through automated or manual scans) × 100	100 %	1. Does the organization manage configuration changes to information systems using an organizationally approved process? 2. Does the organization use automated scanning to identify configuration changes that were implemented on its systems and networks? 3. If yes, how many configuration changes were identified through	2%		

S No	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage	Self-assessment score	Auditor comments w.r.t. cyber audit (for MIIs)
							automated scanning over the last reporting period? 4. How many change control requests were approved and implemented over the last reporting period? 5. Cyber audit observation against Standard 3 mentioned in ‘Detect: Continuous Security Monitoring’ header in CSCRF Part-I and respective guidelines in Part-II.			

S No	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage	Self-assessment score	Auditor comments w.r.t. cyber audit (for MIIs)
7.	Contingency Plan Testing Measure **[RS.MA.S3]**	Information Security Goal: Establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery of organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.	Percentage (%) of information systems that have conducted contingency plan testing at least once in a year.	Effectiveness	(Number of information systems that have conducted contingency plans testing at least once in a year/ number of information systems in the system inventory) ×100	100 %	1. How many information systems are in the system inventory? 2. How many information systems have an approved contingency plan? 3. How many contingency plans were successfully tested within the past 1 year? 4. Reports of the contingency plan testing conducted in past one year.	4%		

8.	User Accounts Measure **[PR.AA.S 7]**	Information Security Goal: All privilege users are identified and authenticated in accordance with information security policy.	Percentage (%) of privileged access through PIM.	Effectiveness	(Number of systems accessed through PIM/ total number of systems) ×100	100 %	1. Organization should have a documented and approved access control policy for systems, applications, networks, databases etc. 2. How many users have access to the system? 3. How many users have access to shared accounts? 4. Cyber audit observation against Standard 7 mentioned in ‘Protect: Identity Management, Authentication, and Access Control’ header in CSCRF Part-I and respective guidelines in Part-II.	3%		

S No	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage	Self-assessment score	Auditor comments w.r.t. cyber audit (for MIIs)
9.	Incident Response Measure **[RS.CO.S2]**	Information Security Goal: Track, document, and report incidents to appropriate organizational officials and/or authorities.	Percentage (%) of incidents reported within required time frame.	Effectiveness	(number of incidents reported on time/ total number of reported incidents) ×100	100 %	1. How many incidents were reported during the period? 2. Of the incidents reported, how many were reported within the prescribed time frame?	2%		

S No	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage	Self-assessment score	Auditor comments w.r.t. cyber audit (for MIIs)
10.	Maintenance Measure **[PR.MA.S 1]**	Information Security Goal: Perform periodic and timely maintenance on organizational information systems and provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.	Percentage (%) of system components that undergo maintenance in accordance with planned maintenance schedules.	Efficiency	(Number of system components that undergo maintenance according to planned maintenance schedules/ total number of system components) ×100	100 %	1. Does the system have a planned maintenance schedule? 2. How many components are contained within the system? 3. How many components underwent maintenance in accordance with the planned maintenance schedule?	5%		
11.	Media Sanitization Measure **[PR.AA.S 14]**	Information Security Goal: Sanitize or destroy information system media before disposal	Percentage (%) of media that passes sanitization procedures testing.	Effectiveness	(Number of media that passes sanitization procedures testing/total number of media disposed or	100 %	1.Policy/procedure for sanitizing media before it is discarded or reused. 2. Indicative proof that policy is being	2%		

S No	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage	Self-assessment score	Auditor comments w.r.t. cyber audit (for MIIs)
		or release for reuse.			released for reuse) × 100		followed. 3. Cyber audit observation against Standard 14 mentioned in 'Protect: Identity Management, Authentication, and Access Control' header in CSCRF Part-I and respective guidelines in Part-II.			
12.	Physical Security Incidents Measure **[PR.AA.S 10]**	Information Security Goal: Integrate physical and information security protection mechanisms to ensure appropriate protection of the organization's	Percentage (%) of physical security incidents allowing unauthorized entry into facilities containing information systems.	Effectiveness	(Number of physical security incidents allowing unauthorized entry into facilities containing information systems/total number of physical security incidents) ×100	0%	1.Policy/procedure ensuring the secure physical access to *critical systems*? 2. How many physical security incidents occurred during the specified period? 3. How many of the physical	1%		

S No	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage	Self-assessment score	Auditor comments w.r.t. cyber audit (for MIIs)
		information resources.					security incidents allowed unauthorized entry into facilities containing information systems? 4. Cyber audit Observation against Standard 10 mentioned in 'Protect: Identity Management, Authentication, and Access Control' header in CSCRF Part-I and respective guidelines in Part-II.			

S No	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage	Self-assessment score	Auditor comments w.r.t. cyber audit (for MIIs)
13.	Planning Measure **[GV.RR.S5]**	Information Security Goal: Develop, document, periodically update, and implement security measures for authorised access to the information systems of the organisation.	Percentage of employees who get authorized access to information systems only after they sign an acknowledgement that they have read and understood confidentiality and integrity agreement.	Implementation	(Number of users who are granted system access after signing confidentiality and integrity agreement/total number of users who are granted system access) ×100	100 %	1. How many users accessed the system? 2. How many users signed confidentiality and integrity agreement acknowledgements? 3. How many users have been granted access to the information system only after signing confidentiality and integrity agreement acknowledgements?	1%		

S No	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage	Self-assessment score	Auditor comments w.r.t. cyber audit (for MIIs)
14.	Personnel Security Screening Measure **[PR.AA.S10]**	Information Security Goal: Ensure that individuals occupying positions of responsibility within organizations are trustworthy and meet established security criteria for those positions.	Percentage (%) of individuals screened before being granted access to organizational information and information systems.	Implementation	(Number of individuals screened/total number of individuals having access to organization's information and information systems) ×100	100 %	1. How many individuals have been granted access to organizational information and information systems? 2. What is the number of individuals who have completed personnel screening?	1%		
15.	Risk Assessment Measure **[ID.RA.S2]**	Objective of this measure is to periodically assess the risk to organization's IT assets and operations. Cybersecurity risks to the organization's	Percentage of organization's information systems, and assets covered under risk assessment.	Implementation Measure	(Number of organization's information systems, and assets covered under risk assessment/Total number of organization information	100 %	1. Has the organization completed a cyber-risk assessment? 3. Cyber Audit observation against this Standard 2 mentioned in 'Identify: Risk	5%		

S No	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage	Self-assessment score	Auditor comments w.r.t. cyber audit (for MIIs)
		information systems, and assets are understood and assessed.			systems, and assets) ×100		Assessment' header in CSCRF Part-I and respective guidelines in Part-II.			
16.	Service Acquisition Contract Measure **[GV.SC.S3]**	Information Security Goal: Ensure third-party providers employ adequate security measures to protect information, applications, and/or services outsourced by the organization.	Percentage (%) of system and service acquisition contracts that include security requirements and/or specifications.	Implementation	(Number of system and service acquisition contracts that include security requirements and specifications/ total number of system and service acquisition contracts) ×100	100 %	1. How many active service acquisition contracts does the organization have? 2. How many active service acquisition contracts include security requirements and specifications? 3. How many contracts includes integration of systems with SOC technologies?	3%		

S No	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage	Self-assessment score	Auditor comments w.r.t. cyber audit (for MIIs)
							4. Whether the acquisition contract includes SLA for vulnerabilities closure and timely implementation of patches? 5. Contracts for adoption of Cloud includes implementation of 'security of the cloud' , etc.			
17.	System and Communication Protection Measure **[PR.DS.S 4]**	Information Security Goal: Allocate sufficient resources to adequately protect electronic information infrastructure.	Percentage of mobile computers and devices that perform all cryptographic operations.	Implementation	(Number of mobile computers and devices that perform all cryptographic operations/total number of mobile computers and devices) ×100	100 %	1. How many mobile computers and devices are used in the organization? 2. How many mobile computers and devices employ cryptography? 3. How many mobile	1%		

S No	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage	Self-assessment score	Auditor comments w.r.t. cyber audit (for MIIs)
							computers and devices have cryptography implementation waivers?			

S No	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage	Self-assessment score	Auditor comments w.r.t. cyber audit (for MIIs)
18.	Risk Management **[GV.RM.S1, GV.RM.S2]**	Based on risk appetite of the organization, cybersecurity risks are identified, analysed, evaluated, prioritized, responded, and monitored.	Percentage (%) of organization information systems, and assets covered under risk management.	Effectiveness	(Number of organization information systems, and assets covered under risk management/Total number of organization information systems, and assets) ×100	100 %	1. Does organization have a cyber-risk management framework? 2. Has the organization established, communicated, and maintained its risk appetite and risk tolerance statements? 3. Has organization responded to risk observations based on its risk appetite?	8%		

S No	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage	Self-assessment score	Auditor comments w.r.t. cyber audit (for MIIs)
19.	Critical Assets Identified **[ID.AM.S1, ID.AM.S2]**	Objective of this measure is to ensure identification and management of assets in accordance with their relative importance to the organizational objectives and the organization's risk strategy.	Percentage (%) of the *critical systems* identified by REs among all other IT systems.	Implementation Measure	(Number of critical systems Identified/ Total IT systems integrated with SOC) ×100	50%	1. Process to identify and approve the list of critical assets. 2. List of critical assets identified as per the ID.AM.S1. 3. Auditors reports on identification of assets as critical/ non-critical.	9%		
20.	CSK Events **[RS.MA.S5]**	Objective of this measure is to mitigate threats upon external IPs	Number of CSK reported events closed in timely manner.	Effectiveness Measure	(Total number of CSK reported events closed in 15 days/ Total number of CSK reported events to the organization)×100	100%	1. Summary report of the events reported by CSK.	4%		

S No	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage	Self-assessment score	Auditor comments w.r.t. cyber audit (for MIIs)
21.	Cybersecurity Policy Document **[GV.PO.S1]**	Develop, document, periodically update, and implement cybersecurity policies and procedures for organizational information systems that describe the security controls in place or planned for information systems.			Non quantifiable measure		1. Cybersecurity Policy document of the organization. 2. Frequency of the revision of the policy document. 3. Approval of the policy document. 4. Cyber audit observation against Standard 1 mentioned in 'Governance: Policy' header in CSCRF Part-I and respective guidelines in Part-II.	4%		

Annexure-K

S No	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage	Self-assessment score	Auditor comments w.r.t. cyber audit (for MIIs)
22.	SOC efficacy	How effective is our SOC operational?	SOC efficacy score	Effectiveness	As specified in SOC efficacy (**Annexure-N**)	100 %	1. How effective is the functioning of RE's SOC?	5%		
23.	Automated compliance with CSCRF	Develop an automated tool (preferably integrated with log aggregator) to submit compliance with CSCRF.	Percentage (%) of standards compliance automated	Maturity measure	(Number of standards for which compliance has been automated for CSCRF compliance/Total number of CSCRF standards)×100	100 %	1. Automated dashboard to get detailed reports of CSCRF standards compliance.	5%		

5. Based on the value of the index, the cybersecurity maturity level of the MIIs and Qualified REs shall be determined as follows:

SN.	Rating	Index Score Rating
1	Exceptional Cybersecurity Maturity	100-91
2	Optimal Cybersecurity Maturity	90-81
3	Manageable Cybersecurity Maturity	80-71
4	Developing Cybersecurity Maturity	70-61
5	Bare Minimum Cybersecurity Maturity	60-51
6	Fail	< =50 (The RE has scored below the cut-off in at least one domain/ sub-domain)

6. MIIs and Qualified REs shall strive for building an automated tool and suitable dashboards (preferably integrated with log aggregator) for submitting compliance. A dashboard shall be available at the time of cyber audit, onsite inspection/ audit by SEBI or any agency appointed by SEBI.