Part I: CSCRF Objectives and Standards

The main objectives of CSCRF are to proactively strengthen the security posture of the REs and prepare the operations of the REs to withstand and recover from the cyber incidents. This section breaks down the objectives and standards as per the cyber resilience goals and cybersecurity functions that REs are expected to achieve.

1. Cyber Resilience Goal: ANTICIPATE | Cybersecurity function: GOVERNANCE

1.1. GV.OC: Organizational Context

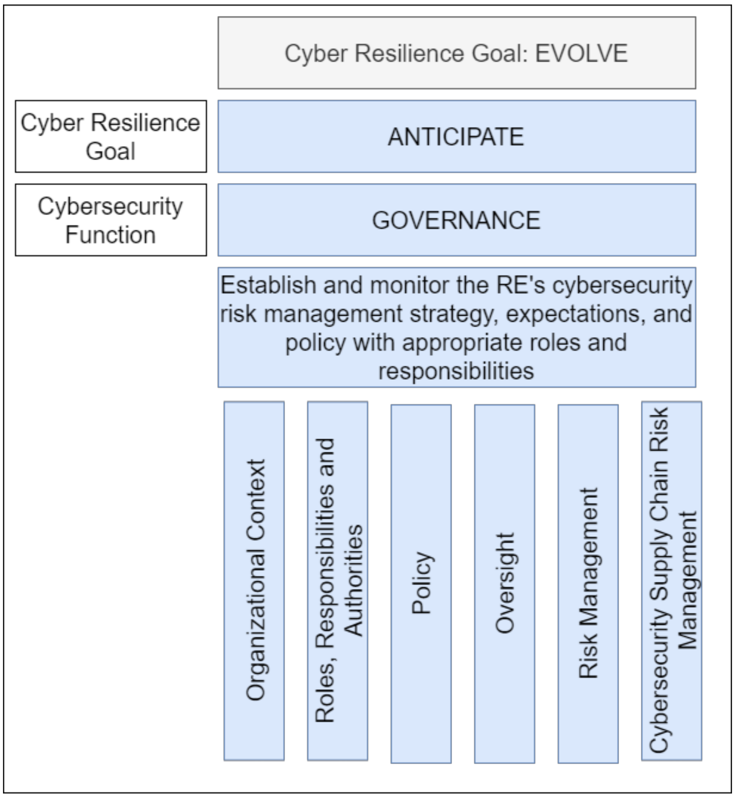
Cyber Resilience Goal: EVOLVE
Cyber Resilience Goal
ANTICIPATE
Cybersecurity Function
GOVERNANCE
Establish and monitor the RE's cybersecurity risk management strategy, expectations, and policy with appropriate roles and responsibilities
Organizational Context
Roles, Responsibilities and Authorities
Policy
Oversight
Risk Management
Cybersecurity Supply Chain Risk Management

Figure 2: Overview of Governance function

i. GV.OC: Objective

The essential concomitants surrounding the REs' cybersecurity risk management decisions are understood. This includes mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements.

ii. GV.OC: Standard

1. Critical objectives, capabilities, and services that external stakeholders depend on or expect from the REs shall be understood and communicated.
2. Legal and regulatory requirements regarding cybersecurity, including data protection and data privacy, shall be understood and managed.
3. REs shall understand and communicate the outcomes, capabilities, and services dependency on external resources such as third-party service providers.

1.2. GV.RR: Roles, Responsibilities and Authorities

i. GV.RR: Objective

Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated.

ii. GV.RR: Standard

1. The responsibility and accountability for cybersecurity risk lies with the REs' leadership and the leadership is responsible for nurturing a culture that is risk-aware, cybersecurity conscious, and continually improving.
2. Cybersecurity risk management roles, responsibilities, and authorities shall be developed, communicated, understood, and enforced.
3. A CISO/ Designated Officer shall be appointed and report to designated authority in the organization.
4. Budgetary planning process shall be aligned with information security and privacy management objectives and processes. Adequate resources shall be allocated and aligned with cybersecurity risk strategy, roles and responsibilities, and policies.
5. Employees and third-party service providers shall be allowed access to REs' information systems once they have signed a confidentiality and integrity agreement.
6. Cybersecurity shall be included in human resources training programs.

1.3. GV.PO: Policy

i. GV.PO: Objective

Organizational cybersecurity policy is established, communicated, and enforced.

ii. GV.PO: Standard

1. A comprehensive cybersecurity and cyber resilience policy shall be documented and implemented after receiving approval from Board/ Partners/ Proprietor. The cybersecurity and cyber resilience policy shall include industry best practices, and encompass standards and guidelines mentioned in this framework.
2. The cybersecurity and cyber resilience policy shall be reviewed periodically by the REs.
3. A policy for managing cybersecurity risks shall be established based on organizational context, cybersecurity strategy, and priorities and the same shall be communicated and enforced.
4. The above-mentioned policy for managing cybersecurity risks shall be reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, and technologies.
5. Clear definition of ownership, custodian of every asset and a proper chain of command for receiving approvals shall be established and followed.

1.4. GV.OV: Oversight

i. GV.OV: Objective

Results of organization-wide cybersecurity risk management activities, performance, and outcomes are used to inform, improve, and adjust the risk management strategy.

ii. GV.OV: Standard

1. Cybersecurity risk management strategy outcomes shall be reviewed to inform and adjust strategy and directions.
2. The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks.
3. Organizational cybersecurity risk management performance is evaluated and reviewed for adjustment needed.
4. Organizations to assess their cyber resilience posture using CCI on a periodic basis.

Box Item 4: Cyber Capability Index

Under the guidance of SEBI's High Powered Steering Committing on Cybersecurity (HPSC-CS), SEBI has developed a Cyber Capability Index (CCI) for the securities market.

The above-mentioned CCI is calculated on the basis of 23 parameters with different weightages.

Based on the value of the index, the cybersecurity maturity level of the REs shall be determined as follows:

Table 24: Rating categories of REs based on CCI

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* *(RE has scored below the cut-off in at least one domain/ sub-domain)*

REs shall strive to build an automated tool and suitable dashboards (preferably integrated with log aggregator) for submitting CCI compliance.

1.5. GV.RM: Risk Management

i. GV.RM: Objective

The RE's priorities, constraints, risk tolerance and risk appetite statements, assumptions and constraints are established, communicated, and used to support operational risk decisions.

ii. GV.RM: Standard

1. REs shall prepare a cyber risk management framework to identify, assess, mitigate and monitor risks and define security processes and

procedures to address them. Cyber risk management objectives shall be agreed to by the REs' stakeholders.

2. Cybersecurity risk management activities and outcomes shall be included in risk management processes of the REs.
3. Different scenarios and their respective responses shall be documented and tested on a periodic basis to check the risk management plan of the REs.
4. Risk tolerance and risk appetite statements shall be established, communicated, and maintained. REs shall determine and clearly express their risk tolerance and risk acceptance. The risk tolerance of the REs shall be informed by their role in critical infrastructure and/ or sector specific risk analysis. REs shall maintain a risk register which shall be periodically reviewed by their *IT Committee for REs*.

Box Item 5: Cyber risk management

Cyber risk management enables an organization to identify, prioritize, manage and monitor risks to their IT/ information systems and infrastructure. Cyber risk management is a continuous and iterative process that necessitates continuous improvement and assessment of security controls by incorporating emerging new information and responding to latest threat landscape. Cyber risk management includes:

1. ***Identify:*** *Determine the threats that might affect and compromise an organization's cybersecurity. This also includes identifying cybersecurity vulnerabilities and the threats that might exploit them.*
2. ***Analyze:*** *Risk should be assessed with a measure of the likelihood of occurrence of a vulnerability and expected harmful impact that might result from the consequences of exploitation of the vulnerability.*
3. ***Evaluate:*** *Each risk should be evaluated against the threshold of acceptable risk.*
4. ***Prioritize:*** *High risk observations should be mitigated on priority.*
5. ***Respond:*** *Response to risks should be consistent with organization's Incident Response and Management Plan. Organizations may choose to treat, tolerate, terminate, transfer the risk based on their risk appetite.*
6. ***Monitor:*** *As cyber risk management is not a one-time activity but a continual process, organizations should monitor risks to ensure that they are below their pre-determined level of acceptable risk.*

1.6. GV.SC: Cybersecurity Supply Chain Risk Management

i. GV.SC: Objective

The RE's priorities, constraints, risk tolerance, and assumptions are established and used to support decisions associated with managing supply chain risks. The RE has established and implemented the processes to identify, assess and manage supply chain risks.

ii. GV.SC: Standard

1. Cybersecurity supply chain risk management strategy/ process shall be identified, established, assessed, managed, and agreed to by organizational stakeholders.
2. Suppliers and third-party service providers of information systems, components, and services shall be identified, prioritized, and assessed using a cyber-supply chain risk assessment process.

3. Contracts with suppliers and third-party service providers shall include appropriate measures to meet the objectives of the RE's cybersecurity program and cybersecurity supply chain risk management plan (including manpower adequacy in cybersecurity domain).
4. REs shall monitor, review and ensure compliance of third-party service providers performing critical activities for their respective organization on a periodic basis.
5. SBOM shall be obtained for all new software procurements of core and critical activities and kept updated with every upgrade or change. In case the SBOM cannot be obtained for the legacy or proprietary systems, the Board/ Partners/ Proprietor of the organization shall approve the same with proper limitation, rationale, and risk management approach.
6. Response and recovery planning, and testing shall be conducted along with third-party service providers.
7. Concentration risk on outsourced agencies shall be assessed and reviewed to achieve operational resiliency.
8. Third-party service providers shall also be mandated to follow similar standards of information security.

Box Item 6: Software Bill of Materials (SBOM)

Recent security breaches at third-party vendors like Apache (Log4j), Solarwinds, etc. have led to the introduction of Software Bill of Materials (SBOM) that enables an organization to identify possible vulnerabilities in the applications/ software solutions.

With introduction of SBOM, the following benefits are envisaged for REs:

1. ***Transparency:*** *REs will become more aware of components, versions, licenses, cryptographic hashes, etc. that they are using in their software applications. This will make the REs well-informed to make better security decisions.*
2. ***Tracking vulnerabilities:*** *REs will be able to track vulnerability status for each of the components as and when an update is made or a component is added/ deleted.*
3. ***Mitigate supply chain risks:*** *REs will be able to prevent and mitigate supply chain risks arising due to open-source or third-party dependencies (e.g. libraries, repositories, etc.) in software components.*
4. ***Audit:*** *REs will have the confidence that only authorized third-party dependencies have been used in their software applications and the same can be audited as and when required.*