5. Cyber Resilience Goal: WITHSTAND & CONTAIN | Cybersecurity function: RESPOND

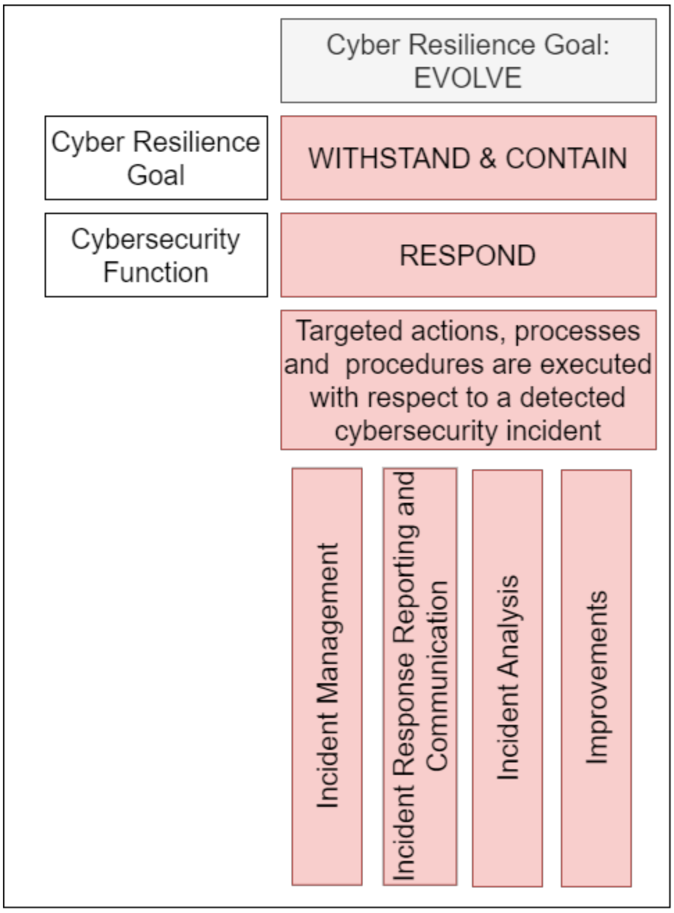
Cyber Resilience Goal: EVOLVE
Cyber Resilience Goal
WITHSTAND & CONTAIN
Cybersecurity Function
RESPOND
Targeted actions, processes and procedures are executed with respect to a detected cybersecurity incident
Incident Management
Incident Response Reporting and Communication
Incident Analysis
Improvements

Figure 6: Overview of Respond function

5.1. RS.MA: Incident Management

i. RS.MA: Objective:

Incident response plans and procedures are executed and maintained in order to ensure response to detected/ known cybersecurity incidents.

ii. RS.MA: Standard:

1. A comprehensive CCMP shall be documented with scenario-based SOP. Further, incident response management plan shall also be a part of CCMP. Additionally, response plan and execution of required SOP shall be triggered as soon as an incident occurs.
2. REs shall optimize their ability to respond in a timely and appropriate manner to adverse conditions, stresses, attacks, or indicators of these. This will maximize the REs' ability to maintain business operations, limit consequences, and avoid destabilization.
3. REs shall prepare contingency plans, COOP, training, exercises, and incident response and recovery plans for their systems and infrastructure and get them approved from their respective Board/ Partners/ Proprietor.

4. Cybersecurity incidents shall be contained and mitigated. Further, newly identified vulnerabilities shall be mitigated or documented as accepted risks.
5. MIIs and Qualified REs shall get onboarded to CSK (Cyber Swachhta Kendra) and other CERT-In initiatives as notified from time to time.

Box Item 12: Cybersecurity Incidents – Classification and Response

- *CSCRF has classified cybersecurity incidents into four categories:*
  1. *Low severity*
  2. *Medium severity*
  3. *High severity*
  4. *Critical severity*
- *Cybersecurity incident response process can be divided into several phases. Cyber incident response handling can be divided into four broad phases:*
  1. ***Preparation:** This phase covers not only establishment of incident response capabilities to ensure RE's readiness to respond to incidents but also prevention of incidents by having secure systems, networks, and applications. CSCRF has mandated REs to have an effective policy, response plan/strategy, communication, and documentation.*
  2. ***Detection and Analysis:** Detection and analysis phase involves:*
     i. *Collection of data and logs*
     ii. *Identification of IOAs*
     iii. *Identifying a baseline for normal behavior, and*
     iv. *Correlating events to check deviation in behavior.*
  3. ***Containment, Eradication & Recovery:** The objective of containment is to mitigate the incident before it overwhelms RE's resources and causes more damage. In eradication and recovery phase, all affected systems shall be isolated from the RE's network. Once the affected systems have been isolated, remediation steps should be taken to resume normal operations.*
  4. ***Post-incident activity:** Lessons learned should be shared within the organization to improve the RE's security measures and incident handling process.*
- *CSCRF covers aforementioned incident handling process through various standards and guidelines, and ensures that REs become more cyber resilient and provide a better response to cybersecurity incidents. Further, timelines for handling cyber incidents and report submission have also been provided in this framework.*

5.2. RS.CO: Incident Response Reporting and Communication

i. RS.CO: Objective:

Response activities are coordinated with internal and external stakeholders (e.g. external support from CERT-In, law enforcement agencies, etc.). Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness.

ii. RS.CO: Standard:

1. An SOP, documenting the roles and responsibilities of REs' personnel (with respect to cybersecurity incident response*),* shall be prepared and implemented.
2. Any cybersecurity incident falling under CERT-In Cybersecurity directions[21] shall be notified to SEBI, CERT-In, and NCIIPC (as

[21] Refer Q 30 in CERT-In Cybersecurity directions: https://www.cert-in.org.in/PDF/FAQs_on_CyberSecurityDirections_May2022.pdf

applicable) within a stipulated time. Any/ all other cybersecurity incident(s) shall be reported to SEBI, CERT-In and NCIIPC (as applicable) as per guidelines.

3. In the event of a cybersecurity incident, REs shall coordinate with stakeholders as per their CCMP.

5.3. RS.AN: Incident Analysis

i. RS.AN: Objective:

Incident analysis is conducted to ensure effective response and support recovery activities.

ii. RS.AN: Standard:

1. Processes shall be established to receive, analyze and respond to vulnerabilities/ incidents disclosed to the RE from internal and external sources (e.g. internal testing, security bulletins, or security researchers).
2. Cybersecurity incidents shall be categorized in-line with categorization given in RE's CCMP.
3. Detailed investigation of cybersecurity incidents, and alerts as well as a forensic analysis (as appropriate) shall be done to identify the root-cause of the incident, the modus operandi of the threat actor, lateral movement of the threat actor (if any), and to prevent the reoccurrence of similar incidents.
4. RCA shall be done to:
   a. Determine the gaps in terms of people, processes, and technology that led to the incident, and
   b. Further enhance the RE's security posture to prevent/ mitigate similar cybersecurity Incidents in the future.
5. Impact analysis of the incident shall be mandatorily conducted by the REs. Further, RCA and forensics analysis (as appropriate) shall be performed as per '*Classification and Handling of Cybersecurity Incidents*' SOP attached at **Annexure-O**.

5.4. RS.IM: Improvements

i. RS.IM: Objective:

RE's response activities are improved by incorporating lessons learned from current and previous detection/ response activities.

ii. RS.IM: Standard:

1. Lessons learned from incident handling activities shall be incorporated into incident response plans, training, and testing, and resulting changes shall be implemented accordingly.
2. Changes to the response plan shall be communicated to RE's designated key personnel.