6. Cyber Resilience Goal: RECOVER | Cybersecurity function: RECOVER

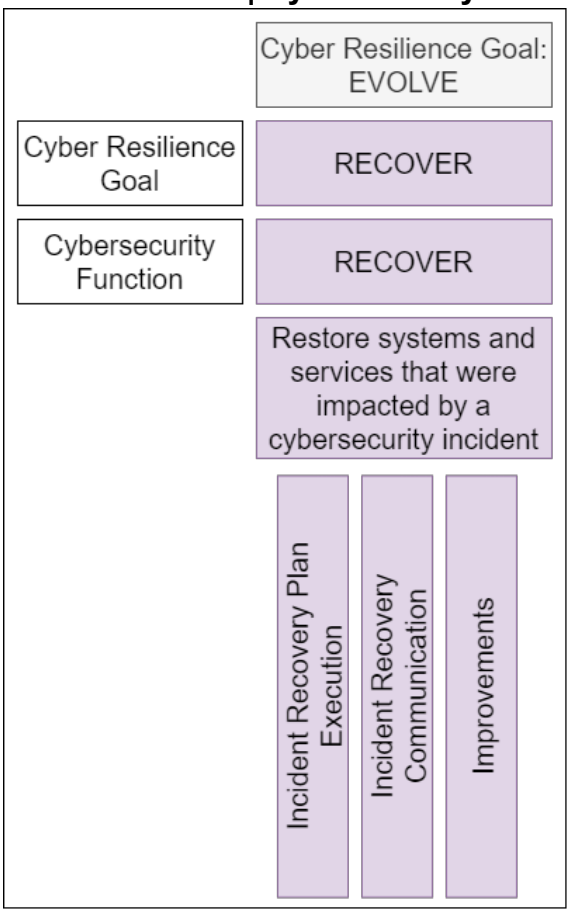

Figure 7: Overview of Recover function

6.1. RC.RP: Incident Recovery Plan Execution

i. RC.RP: Objective:

Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity incidents.

ii. RC.RP: Standard:

1. Recovery plan of REs shall have different cyber-scenario based classifications.
2. RTO and RPO, as specified by SEBI, shall be mandated while executing recovery plan for the restoration of systems after a cybersecurity incident.
3. REs shall periodically conduct drills for testing different recovery scenarios.
4. Backup and recovery plan of data shall be documented to ensure that there is no data loss.

6.2. RC.CO: Incident Recovery Communication

i. RC.CO: Objective:

Restoration activities are coordinated with internal and external stakeholders.

ii. RC.CO: Standard:

1. Public relations management as defined in the recovery plan shall be undertaken in the event of a cybersecurity incident.
2. REs shall communicate recovery activities to internal and external stakeholders as well as executive and management teams.
3. REs shall inform actions taken during recovery process to all related stakeholders.

6.3. RC.IM: Improvements

i. RC.IM: Objective:

Recovery planning and processes are improved by incorporating lessons learned from execution of recovery plans and processes.

ii. RC.IM: Standard:

1. Recovery plans shall be updated and improved to incorporate lessons learned from cybersecurity incidents.
2. REs cyber resilience capabilities shall be upgraded through periodic drills to ensure safe and timely restoration of critical operations.