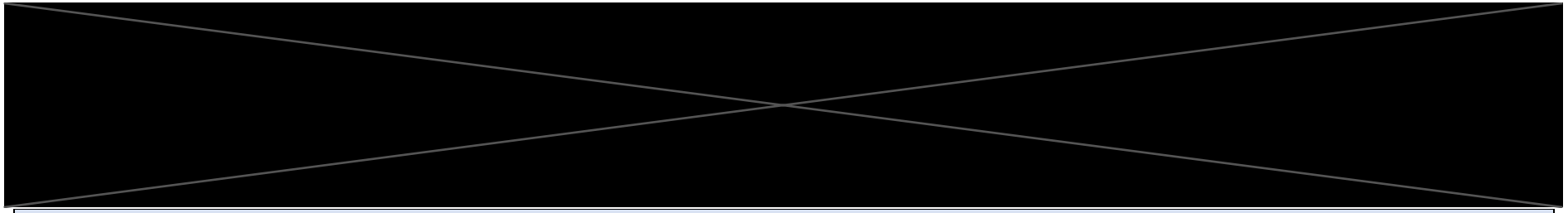

Cyber Resilience goal: RECOVER		
Cybersecurity control: RECOVER		
RC.RP: Guidelines		
RC.RP.S1	1. The response and recovery plans of the REs shall include scenario-based classifications. REs shall build their own response and recovery plan as per their business model and include the same in their CCMP. 2. The response and recovery plan of the REs shall have plans for the timely restoration of systems affected by incidents of cybersecurity incidents/ attacks or breaches (for instance, offering alternate services or systems to customers). Tests shall be designed to challenge the assumptions of response, resumption and recovery practices, including governance arrangements and communication plans. These tests shall include all stakeholders such as critical service providers, vendors, other linked REs, etc. 3. An indicative (but not exhaustive and limited to) recovery plan to be followed by the REs has been attached at **Annexure-C**.	All REs (Mandatory)
	4. REs shall maintain regularly updated *'golden images'* of *critical systems* at offsite location for rebuilding the systems (whenever required). This entails maintaining images "templates" that include a preconfigured operating system (OS), configuration setting backup and associated software applications that can be quickly deployed to rebuild a system, such as a virtual machine or server.	MIIs and Qualified REs (Mandatory)

Standards	CSCRF guidelines	Applicability
	5. REs shall explore the possibility of retaining spare hardware in an isolated environment to rebuild systems in an event that starting REs' operations from PDC and/ or DRS is not feasible. The REs shall also try to keep spare hardware in ready-to-use state for delivering critical services and such systems shall be updated as and when new changes (for example OS patches, security patches, etc.) are implemented in the primary systems. This spare hardware shall regularly undergo testing in-line with the response and recovery plan of the REs. 6. REs shall take all necessary precautions while updating the 'golden' server images and data backup to ensure that server images and data backups are undamaged/unbroken. 7. In case of ransomware attacks that specifically target backups, conventional data backups may not be effective. Therefore, REs shall create backups in an isolated and immutable (and/ or air-gapped) manner to ensure recovery if production system is compromised. 8. REs shall undertake regular business continuity drills to check the readiness of the organization and effectiveness of existing security controls at the ground level. One such drill scenario recommended to be tested is recovering from a ransomware attack considering both PDC and DRS have been impacted. This shall assess the effectiveness of people, processes and technologies to deal with such attacks.	
RC.RP.S2	1. In the event of disruption of any one or more of the *critical systems*, the RE shall, within 30 minutes of the incident, declare that incident as 'Disaster' based on the business impact analysis. Accordingly, the RTO shall be two (2) hours as recommended by IOSCO[33] for the resumption of critical operations. The RPO shall be 15 minutes for all	All REs (Mandatory)

[33] Refer https://www.bis.org/cpmi/publ/d146.pdf.

Standards	CSCRF guidelines	Applicability
	REs. The recovery plan shall be scenario-based and in line with the RTO and RPO specified.	
	2. REs shall conduct comprehensive scenario-based cyber resilience testing at least 2 times in a financial year (periodicity of such testing shall be of 6 months), to validate their ability to recover and resume operations following a cybersecurity incident/ attack within prescribed RTO and RPO defined by SEBI. In this regard, REs shall incorporate extreme plausible cyber-attack scenarios into their cyber response and recovery planning. The said scenarios may be devised by REs in consultation with their respective *IT Committee for REs* based on the learning from various sources such as past cybersecurity incidents, near-miss analysis, data from Security Operations Centre, honeypot logs analysis, etc. 3. REs shall periodically conduct backup testing and restore back-up data to check its usability. 4. For cyber resilience testing, REs shall also include stakeholders such as critical third-party service providers, market intermediaries, linked REs, etc. 5. The result of the Cyber resilience testing shall be placed before *IT Committee for REs*. The lessons learned from conducting such cyber resilience testing shall be shared with SEBI within 3 months from the end of the relevant period of conducting cyber resilience testing. Status of the observations found during the cyber resilience testing shall be monitored and tracked by *IT Committee for REs*.	MIIs and Qualified REs (Mandatory)
RC.RP.S3	1. All REs shall conduct suitable periodic drills to test the adequacy and effectiveness of the response and recovery plan.	All REs (Mandatory)

Standards	CSCRF guidelines	Applicability
RC.RP.S4	1. A backup and recovery plan shall be formulated by the REs and approved by their respective *IT Committee for REs*. The backup and recovery plan shall include policies and software solutions that work together to maintain business continuity in the event of a security incident. Such plan shall include guidance on restoration of data with the backup software used by the RE. 2. The backup and recovery policy shall include backup of data as well as backup of server images. 3. The backup of data and server images shall be maintained at off-site locations to keep backup copies intact and unbroken. 4. RTO and RPO, as prescribed by SEBI from time to time, shall be included in the recovery plan for the restoration of systems after cybersecurity incidents.	All REs (Mandatory)
	5. REs shall maintain offline, encrypted backups of data and shall regularly test these backups at least on a quarterly basis to ensure confidentiality, integrity and availability of data.	MIIs and Qualified REs (Mandatory)
RC.CO: Guidelines		
RC.CO.S1, RC.CO.S2, RC.CO.S3	1. Recovery plans shall be discussed with *IT Committee for REs* by the REs. Such plans shall include stakeholders' coordination in recovery process, and both internal and external communication.	All REs
RC.IM: Guidelines		
RC.IM.S1	1. While ensuring protection of data, and security of processes, RE's BCP-DR capabilities shall support its cyber resilience objectives, and rapid recovery and resumption of critical operations after cybersecurity incident.	All REs

Standards	CSCRF guidelines	Applicability
	2. REs shall try to incorporate lessons learned from incidents reported (if any) by other REs.	
RC.IM.S2	1. RE's RTO shall be met for all interconnected systems and networks through capacity upgradations and periodic coordinated resilience testing. 2. Recover lan shall be im roved after anal sin the learnin s from eriodic drills.	All REs (Mandatory)