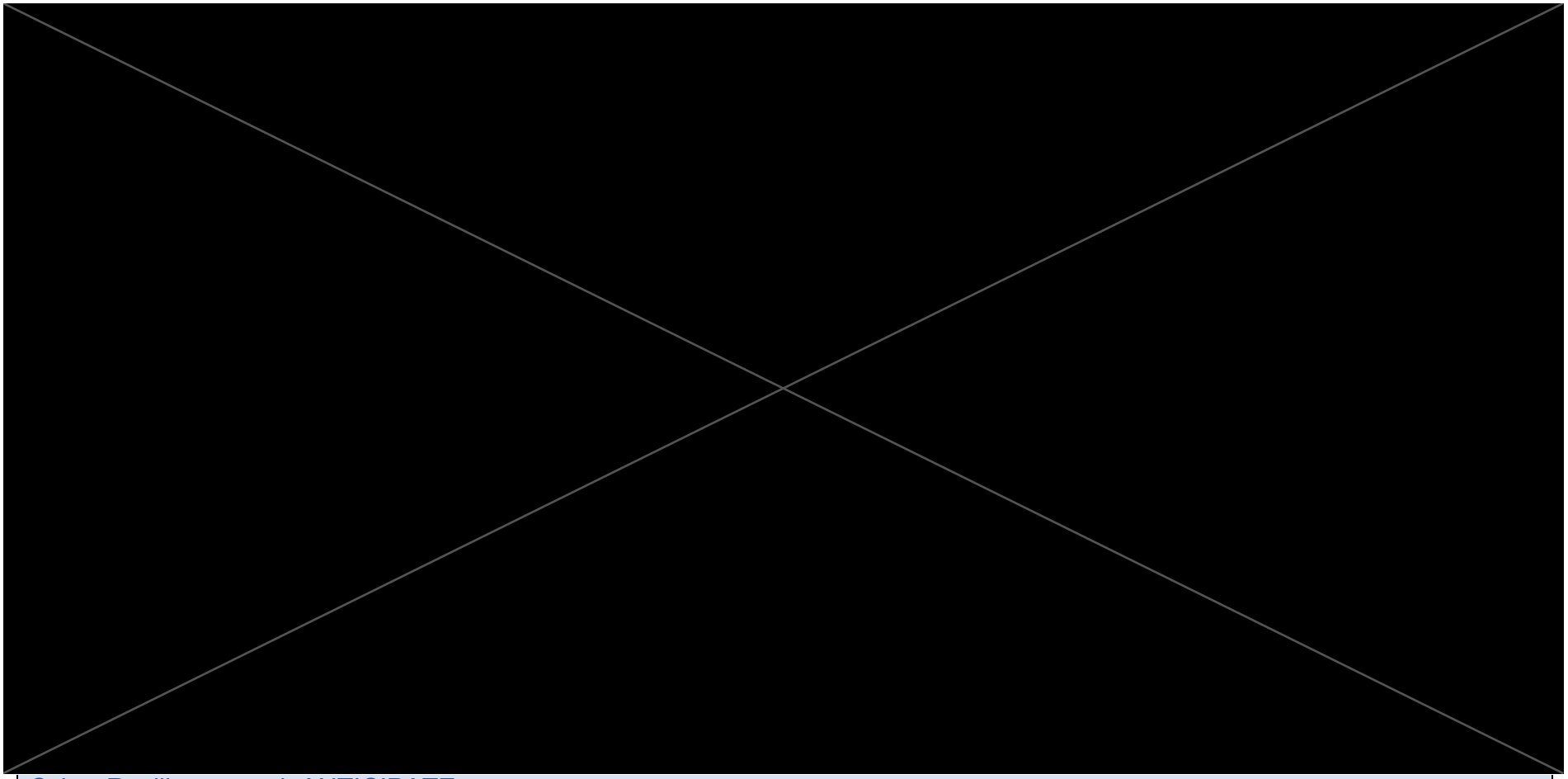

Cyber Resilience goal: ANTICIPATE		
Cybersecurity control: DETECT		
DE.CM: Guidelines		
DE.CM.S1, DE.CM.S2,	1. Security Continuous Monitoring	All REs (Mandatory)

Standards	CSCRF guidelines	Applicability
DE.CM.S3	a. REs shall establish appropriate security monitoring systems and processes to facilitate continuous monitoring of security events/ alerts and timely detection of unauthorized or malicious activities, unauthorized changes, unauthorized access and unauthorized copying and transmission of data/ information held in contractual or fiduciary capacity, by internal and external parties. The security logs of systems, applications and network devices exposed to the internet shall also be monitored for anomalies. b. Suitable alerts shall be generated in the event of detection of unauthorized or abnormal system activities, transmission errors or unusual online transactions. c. To enhance the security monitoring, REs (except client-based stock brokers having less than 100 clients) are mandated to employ SOC services for their systems. REs may choose any of the following models to use SOC services: i. RE's own SOC/ group SOC ii. Market SOC implemented mandatorily by NSE, BSE and optionally by NSDL and/ or CDSL iii. Any other third party managed SOC d. Small-Size and Self-certification category REs are mandated to be on-boarded on above-mentioned Market SOC.	
	2. <u>Functional efficacy of SOC</u> a. REs shall measure functional efficacy of their SOC using the quantifiable method given in **Annexure-N**. b. REs shall review the functional efficacy of SOC on a half-yearly basis.	MIIs and Qualified REs (Mandatory)

Standards	CSCRF guidelines	Applicability
	c. REs shall deploy solutions such as BAS, CART, decoy, vulnerability management, etc. to enhance their cybersecurity posture.	
	d. Those REs who are utilizing third-party managed SOC services or market SOC shall obtain SOC efficacy report (using the quantifiable method given in **Annexure-N**) from their SOC provider on a yearly basis.	All REs having third-party managed SOC or market SOC (mandatory)
	3. MIIs shall have a cybersecurity Operations Centre (C-SOC) that would be a 24×7×365 set-up manned by dedicated security analysts to identify, respond, recover and protect from cybersecurity incidents[28]. The C-SOC for MIIs shall function in accordance with SEBI circular CIR/MRD/CSC/148/2018 dated December 07, 2018 which has been attached at **Annexure-M**.	MIIs (Mandatory)
DE.CM.S4	1. The use of IT assets/ resources shall be monitored, tuned and projections shall be made for future capacity requirements to ensure the required system performance for meeting the business objectives. 2. To ensure high resilience, high availability and timely detection of attacks on systems and networks, REs shall implement suitable mechanisms to monitor capacity utilization of its *critical systems* and networks. 3. Capacity management shall comprise of three primary types; Data storage capacity – (e.g. in database systems, file storage areas, etc.); Processing power capacity – (e.g. adequate computational power to ensure timely processing operations); and	All REs except small-size, Self-certification REs (Mandatory)

[28] Refer SEBI circular CIR/MRD/CSC/148/2018 dated December 07, 2018.

Standards	CSCRF guidelines	Applicability
	Communications capacity – ("bandwidth" to ensure communications are made in a timely manner). 4. Capacity management shall be; a. Pro-active – for example, using capacity considerations as part of change management; b. Reactive – e.g. triggers and alerts for when capacity usage is reaching a critical threshold so that timely increments (temporary or permanent) can be made.	
DE.CM.S5	1. The details of periodicity, timeline and report submission for cyber audit by REs have been provided in the *'CSCRF Compliance, Audit Report Submission, and Timelines'* section. 2. REs shall regularly conduct cybersecurity audit and VAPT with scope as mentioned in CSCRF in order to detect vulnerabilities in the IT environment. Further, REs shall conduct in-depth evaluation of the security posture of the system through simulations of actual attacks. An indicative (but not exhaustive and limited to) VAPT scope has been attached at **Annexure-L**. 3. The assets under these audits shall include (but not limited to) all *critical systems*, infrastructure components (like networking systems, security devices, load balancers, servers, databases, applications, remote access points, systems accessible through WAN, LAN as well as with Public IP's, websites, etc.), and other IT systems pertaining to the operations of REs. 4. REs shall perform VAPT prior to the commissioning of new systems, especially those which are part of *critical systems* or connected to *critical systems*.	All REs (Mandatory)

Standards	CSCRF guidelines	Applicability
	5. Revalidation of VAPT post closure of observations shall be done in a time bound manner to ensure that all the open vulnerabilities have been fixed.	
	6. In case of vulnerabilities being discovered in COTS (used for core business) or empanelled applications, REs shall report them to the vendors and the designated stock exchanges and/ or depositories in a timely manner.	Stock Brokers/ Depository Participants falling under Qualified REs and Mid-size REs (Mandatory)
DE.DP: Guidelines		
DE.DP.S4	1. REs shall conduct red teaming exercises as part of their cybersecurity framework on a half-yearly basis through use of red/ blue teams. 2. CART solution shall be deployed for continuous, automated process of testing the security of the systems, and achieving greater visibility on attack surfaces. 3. For red teaming exercise, a red team may consist of REs employees and/ or outside experts. Additionally, the red team shall be independent of the function being tested. 4. The results of the red teaming exercise shall be placed before *IT Committee for REs* and Governing board. The lessons learned from conducting such red team exercises shall be shared with SEBI within 3 months after completion of the exercise. Status of the remediation of the observation found during the red team exercise shall be monitored by *IT Committee for REs*.	MIIs and Qualified REs (Mandatory)

Standards	CSCRF guidelines	Applicability
DE.DP.S5	1. REs shall proactively search for hidden and undetected cyber threats in their network. 2. Threat hunting by leveraging threat intelligence, IOCs, IOAs, etc. shall be conducted on a quarterly basis.	MIIs and Qualified REs (Mandatory)