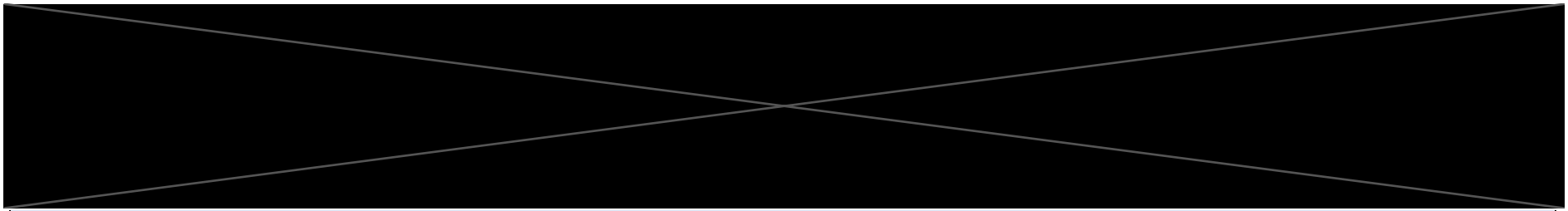

Cyber Resilience goal: WITHSTAND & CONTAIN		
Cybersecurity control: RESPOND		
RS.MA: Guidelines		
RS.MA.S1	1. All REs shall formulate an up-to-date CCMP in line with national CCMP of CERT-In. 2. CCMP shall be approved by Board/ Partners/ Proprietor of REs. 3. <u>Incident Response Management</u> a. All REs shall develop an Incident Response Management Plan as part of their CCMP. b. The response plan shall define responsibilities and actions to be performed by its employees and support/ outsourced staff in the event of a cyber-attack or cybersecurity incident. c. REs shall have a SOP for handling cybersecurity incident response and recovery for the various cybersecurity attacks. d. MIIs shall have a SOP for cybersecurity incidents reported to them by the REs under their supervision. e. SOP for reporting of cybersecurity incidents to SEBI is attached at **Annexure-O**. The same shall be adhered to.	All REs (Mandatory)
RS.MA.S2	1. In order to optimize the REs' ability to respond in a timely and appropriate manner, REs shall: a. Create cybersecurity awareness,	All REs except small-size, self-certification REs

Standards	CSCRF guidelines	Applicability
	b. Provide cybersecurity training to the relevant teams, c. Develop/ hire people with appropriate skill-sets, d. Prepare cyber playbooks, e. Create knowledge database for all known adverse conditions and attacks	
RS.MA.S5	1. REs shall collaborate with Cyber Swachhta Kendra (CSK) operated by CERT-In to trace bots and vulnerable service(s) running on their public IP addresses, and receive alerts regarding the same. The alerts received from CSK shall be closed in a time-bound manner. Observations (from CSK) which require a longer time to close shall be put up to the *IT Committee for REs* for their guidance and appropriate mitigation/ closure.	MIIs and Qualified REs (Mandatory)
RS.CO: Guidelines		
RS.CO.S1, RS.CO.S2, RS.CO.S3	1. Any cyber-attack, cybersecurity incident and/ or breach falling under CERT-In Cybersecurity directions[29] shall be notified to SEBI and CERT-In within 6 hours of noticing/ detecting such incidents or being brought to notice about such incidents. This information shall be shared with SEBI through the ***mkt_incidents@sebi.gov.in*** within 6 hours. However, necessary details of the incidents shall be reported on SEBI Incident Reporting Portal within 24 hours. Stock Brokers/ Depository Participants shall also report the incidents to Stock Exchanges/ Depositories along with SEBI and CERT-In within 6 hours of noticing/ detecting such incidents or being brought to notice about such incidents. All other cybersecurity incident(s) shall be reported to SEBI, CERT-In and NCIIPC (as applicable) within 24 hours. 2. REs shall share Threat Intelligence data that is collected, processed, and analysed to gain insights into the motives and behaviour (of the threat actor), target, attack pattern, etc. on SEBI Incident Reporting portal.	All REs (Mandatory)

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

Standards	CSCRF guidelines	Applicability
	3. The incident shall also be reported to CERT-In in accordance with the guidelines/ directions issued by CERT-In from time to time. Additionally, the REs, whose systems have been identified as "Protected system" by NCIIPC shall also report the incident to NCIIPC. 4. The quarterly reports containing information on cyber-attacks, threats, cybersecurity incidents and breaches experienced by REs and measures taken to mitigate vulnerabilities, threats and attacks including information on bugs/ vulnerabilities, threats that may be useful for other REs and SEBI, shall be submitted to SEBI within 15 days from the quarter ended June, September, December and March of every year. 5. Such details, which are deemed useful for sharing with other REs, in a masked manner, shall be shared using mechanism to be specified by SEBI from time to time. While sharing the above-mentioned sensitive information, TLP may be followed with four levels of sensitivity: white, green, amber, or red. 6. During the processing of reported incidents by SEBI, REs shall provide regular reports (such as RCA, forensic analysis report, etc.) on the progress of the incident analysis.	
RS.CO.S2	1. *IT Committee for REs* shall discuss response plans, coordination with stakeholders for consistency in response actions, information sharing for better awareness, etc. 2. For the purpose of coordinating incident response, REs shall regularly update the contact details of service providers, intermediaries, and other stakeholders. 3. If the cyber-attack is of high impact[30] and has a broad reach, the RE shall give a press release which shall include (but not limited to) a brief of the incident, actions taken to	MIIs and Qualified REs (Mandatory)

[30] REs shall decide the impact of cyber-attack.

Standards	CSCRF guidelines	Applicability
	recover, normal operation resumption status (once achieved), etc. and inform all the affected customers/ stakeholders. 4. If the cyber-attack is of low impact[31] and has a narrow/low reach, the REs shall inform all the affected customers/ stakeholders.	
	5. REs shall notify the customer/ investor, through alternate communication channels, of all transactions including buy/ sell, payment or fund transfer above a specified value determined by the customer/ investor.	All REs (Mandatory)
RS.AN: Guidelines		
RS.AN.S1, RS.AN.S2, RS.AN.S3	1. Alerts generated from monitoring and detection systems shall be suitably investigated by the REs in order to determine activities that are to be performed to prevent spread of cybersecurity incidents/ attacks or breaches, mitigate their effects and resolve the incidents. 2. Data collection: REs shall collect and preserve data related to the incident, such as system logs, network traffic, and forensic images of affected systems. 3. Incident Analysis: REs shall analyse the data to understand the scope, cause, and impact of the incident, including how the incident occurred, what systems and data were affected, who was responsible, etc. 4. Evidence Preservation: REs shall preserve evidence related to the incident, including digital artefacts, network captures, and memory dumps, in a secure and forensically sound manner.	All REs (Mandatory)

[31] REs shall decide the impact of cyber-attack.

Standards	CSCRF guidelines	Applicability
RS.AN.S4, RS.AN.S5	1. Root Cause Analysis: REs shall perform a root cause analysis (RCA) to identify the specific control that has failed, underlying cause of the incident and the potential areas of improvement. 2. Forensic: Forensic analysis (as appropriate) shall be undertaken by the REs. 3. Any incident of loss or destruction of data or systems shall be thoroughly analysed and lessons learned from such incidents shall be incorporated to strengthen the security mechanisms and improve the recovery planning and processes. 4. Reporting: REs shall create a detailed incident report that includes information on the scope, cause, and impact of the incident, as well as recommendations for improving incident response and recovery capabilities. 5. REs shall conduct a compromise assessment through CERT-In empanelled IS auditing organizations.	All REs (Mandatory)
RS.IM: Guidelines		
RS.IM.S1	1. REs shall periodically[32] review and update their contingency plan, COOP, training exercises, and incident response and recovery plans (including CCMP) to incorporate lessons learned, and strengthen their response capabilities in the event of a future incident/ attack.	All REs except self-certification REs (Mandatory)
	2. Post occurrence of cybersecurity incident (if any), REs shall update their response and recovery plan (including CCMP) to improve their cyber resilience and incorporate the learnings from the cybersecurity incident.	All REs (Mandatory)

[32] Half-yearly for MIIs and Qualified REs. Once in two years for Mid-size and small-size REs.

Standards	CSCRF guidelines	Applicability
RS.IM.S2	3. The updates and changes in the contingency plan, COOP, training exercises, and incident response and recovery plan shall be communicated and approved by the Board/ Partners/ Proprietor.	All REs