Deloitte.

Tax alert: Consultation Paper on Consolidated Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI Regulated Entities

11 July 2023

The Securities and Exchange Board of India (SEBI) released a consultation paper which examines the implementation of a 'Consolidated Cyber Security and Cyber Resilience Framework' (CSCRF) for its Regulated Entities (REs). It aims to establish a unified framework that encompasses various strategies to safeguard REs and Market Infrastructure Institutions (MIIs) against cyber risks and incidents.

The consolidated CSCRF proposes to supersede the previously issued SEBI cybersecurity circulars between 2015 to 2023 to be complied by MIIs, Stockbrokers/Depository Participants, Mutual Funds/Asset Management Companies (AMC), KYC Registration Agencies (KRAs), Qualified Registrars to an Issue / Share Transfer Agents (QRTAs), Portfolio Managers.

In a nutshell

Key provisions under the CSCRF Framework as envisioned under the consultation paper:

- A comprehensive Cybersecurity Guidelines aimed to **address cybersecurity challenges, strengthen cyber resilience, and establish standardized guidelines** for all REs.

- **Graded approach**
  - REs
  - Specified REs* and
  - Market Infrastructure Institutions (MIIs).

- Covers obligations and processes across 5 functions of REs and mandates ISO and cyber audit certifications
- Obligations for **log retention**, **access control**, **encryption**, **incident response management**, and communication with stakeholders including cyber security agencies emphasised.

Scroll down to read the detailed alert

Key Highlights:

The Paper relies upon the five concurrent and continuous functions of cybersecurity – Identify, Protect, Detect, Respond, and Recover and suggests security controls, to be followed by REs, Specified REs and MIIs across various functions and reporting requirements. The same is outlined as under:

<table>
<tr><th></th><th rowspan="2">Basic obligations All REs</th><th colspan="2">Additional obligations</th></tr>
<tr><th>Specified REs</th><th>MIIs</th></tr>
<tr><td colspan="4">STAGE I – IDENTIFY</td></tr>
<tr><td>Asset Management</td><td>Identify critical assets, updated inventory, criticality assessment of assets, network architecture diagram, third party with similar standards</td><td colspan="2">Specific controls to address Cyber Risk</td></tr>
<tr><td rowspan="2">Governance – A Comprehensive cybersecurity & cyber resilience Policy</td><td rowspan="2">Approved by the Board covering overseen by Technology Committee and appoints Designated officer of compliance. It would contain aspects of asset mgt, VAPT, management change, policies on authentication & authorization, encryption, privacy etc., and obligations of third party</td><td colspan="2">Policy to cover principles prescribed by NCIIPC, CISO being senior cybersecurity expert to oversee global and domestic cyber security attacks and remediate, practices from international standards – ISO27001, 27002, COBIT 5.</td></tr>
<tr><td></td><td>Oversight standing Committee and Cyber Capability index for self - assessment bi-annually</td></tr>
<tr><td>Risk Assessment and Risk management</td><td colspan="3">Quantified bi-annual risk assessment, ISO27005:2022 standards compliance, use of matrices such as incidents detected and resolved, employee security weakness etc., evaluate authentication-based server, use of Cyber Threat Intelligence provided by CISO, CERT_IN or third-party vendor and comprehensive scenario-based testing</td></tr>
<tr><td>Supply chain risk management</td><td colspan="3">Consideration of concentration risk for third party service providers, need for software BOM prior to procurement to enable security checks and adequate manpower</td></tr>
<tr><td colspan="4">STAGE II – PROTECT</td></tr>
<tr><td>Access Control - Identity management, authentication</td><td>Follow - Principle of least privilege & zero trust model, MFA for critical systems, user logs storage for 2 years and prescribed by CERT_IN, SEBI, strong authentication, authorization, data-disposal/ retention policy, strong monitoring of physical access to critical system and access restriction to outsourced staff.</td><td colspan="2">Stringent policies for critical functions with stronger supervision</td></tr>
</table>

Awareness and Training	Cybersecurity and basic system hygiene awareness, update cybersecurity threat alerts		
Data Security	Data and storage device security through encryption methods, DLP solutions, backup, and recovery measures, blocking administrative rights on end-user workstations. Security for customer facing applications and certified off-the shelf products STQC etc.	Stringent policies for critical functions with stronger supervision and use of confidential computing for sensitive personal data	
Information Protection Process and procedures	-Secure software development lifecycle from development, testing, production release, undertakings from OEMs -Securing cloud services through access tokens and checks on public accessibility -Monitoring third party service providers and cyber audit certifications from service providers -Onboard CERT-in empaneled auditors for 3 years with 2 year cooling period		MII primarily responsible for applications and not REs who are users of the data ISO 27001 certificate for PD, DR, NDR sites Compliance with CIS critical security controls
Maintenance	Hardening of hardware and software and strong patch management systems		
Protective technology and resilience	Effective API security, endpoint security for threat detections, usage of active directory servers and restricted use of removable media	Prepare SoPs for open-source application security and emerging tech security concerns	
STAGE III – DETECT			
Security continuous monitoring	Monitoring systems for unauthorized/ malicious activities, deploy SOC services and VAPT deployment	Reporting	24*7*365 cybersecurity operation center
Detection Process	Functional efficacy of SOC through outlined parameters and quantitative method	Deploy BAS, Decoy and vulnerability management solutions and half yearly red-teaming exercise	
STAGE IV – RESPOND			
Response Planning	Formulate Cyber crises management plan, incident reporting management and its SoPs		SoP for cybersecurity incident response and recovery

Communication	-Cyber threat intelligence data to be shared with SEBI CISO Reporting incidents to SEBI (within 6 hours), CERT-in and NCIIPC, if applicable. -Quarterly reporting to SEBI of threats identified	Press release for cyber-attacks of high impact including mitigation mechanism and operation resumption status
Analysis and Improvement	Suitable mechanism for data collection, analysis of incidence, evidence preparation and root cause analysis should be done. Bi-annual review & updation of response plan to address future incidents	
STAGE V – RECOVERY		
Recovery Planning	Devise strong recovery plan – In line with Recovery Time Objective (RTO) and Recovery Point Objective (RPO), declare incident as disaster in case of disruption of critical systems within 30 mins to enable RTO action in 2 hours as recommended by IOSCO and periodic drills	
Communication	Plan discussed in oversight SCOT of stock exchanges, clearing corporations and IT committee for internal and external communication a) (e.g., coordinating centres, Internet Service Providers, victims, other CSIRTs, and 3P service providers).	

The circular captures details regarding compliance for the REs through:

1. **ISO certification and VAPT report in prescribed format –** The VAPT report of REs as identified by National Critical Information Infrastructure Protection Centre would be bi-annual and other would be annual and to commence at the beginning of the year. There are timelines prescribed for submission, closure of findings and revalidations.
2. **Cyber Audit** for compliance with this framework to be undertaken bi-annually for MIIs and specified REs and annual for others

The reports/ certificates are required to be submitted by stockbrokers and Depository Participants to Stock Exchange and Depositories respectively while others required to submit to SEBI.

Key Takeaways:

The consultation paper tries to address cybersecurity risks and promote cyber resilience among the REs (Regulated Entities) by aligning requirements across various categories of REs and bringing integrated framework for all RE using graded approach and integrating internationally acknowledged standards, national level cyber security agencies. SEBI has welcomed inputs from stakeholders to ensure the framework adequately addresses the dynamic cybersecurity requirements of the securities market and all entities under its oversight.

Deloitte.