KHAITAN & CO
ADVOCATES
SINCE 1911

27 August 2024

Strengthening Cybersecurity and Resilience: An Overview of SEBI's New CSCRF Framework

INTRODUCTION

The Cybersecurity and Cyber Resilience Framework (CSCRF) is a comprehensive and standardized framework developed by the Securities and Exchange Board of India (SEBI) to provide standards and guidelines for strengthening cyber resilience and maintaining robust cybersecurity of SEBI regulated entities (REs). The CSCRF was released by SEBI on 20 August 2024.

The CSCRF applies to SEBI REs[1] and also further sub classifies the REs into the following categories based on their operational scale, number of clients, trade volume, and assets under management, and provides for specific compliance requirements for each category:

- Market Infrastructure Institutions (MIIs);
- Qualified REs;
- Mid-size REs;
- Small-size REs; and
- Self-certification REs.

For the six categories of REs where cybersecurity and cyber resilience circular already exists (for example for portfolio managers, mutual funds and stock brokers/depository participants), the CSCRF is required to be complied with by 1 January 2025, while for other REs the date is 1 April 2025.

Structure: The CSCRF framework is structured into four parts: (i) Objectives and Standards; (ii) Guidelines on how to achieve a particular outcome or meet certain objectives and implement respective standards; (iii) Compliance Formats for submission of CSCRF compliance reports; and (iv) Annexures and References containing guidelines to auditors, scenario-based cyber resilience testing, etc.

Cybersecurity Functions, Cyber Resilience Goals, and Compliance Requirements: The CSCRF is broadly based on two approaches: (1) cybersecurity functions; and (2) cyber resilience goals. The cybersecurity functions broadly covers: Governance, Identify, Detect, Protect, Respond, and Recover, while there are five cyber resilience goals: Anticipate, Withstand, Contain, Recover, and Evolve. The below table provides a snapshot of key compliance requirements for REs, as mapped with the approaches of cybersecurity functions and cyber resilience goals:

Cybersecurity Function	Cyber Resilience Goal	Compliance Requirements
Governance	Anticipate	**Cybersecurity Accountability**: REs are required to establish clear roles, responsibilities, and a comprehensive cybersecurity policy approved by the board/partners. **Risk Management**: MIIs, Qualified REs, and mid-size REs are required to maintain a continuous cyber risk management framework for identification, analysis, evaluation, prioritization etc of cyber risks. **Cyber Capability Index (CCI)**: MIIs are required to undergo third-party assessments of their cyber resilience using CCI on a half-yearly basis, while Qualified REs are

[1] The CSCRF is applicable to the following REs: (i) Alternative Investment Funds; (ii) Bankers to an Issue and Self-Certified Syndicate Banks; (iii) Clearing Corporations; (iv) Collective Investment Schemes; (v) Credit Rating Agencies; (vi) Custodians; (vii) Debenture Trustees; (viii) Depositories; (ix) Designated Depository Participants; (x) Depository Participants through Depositories; (xi) Investment Advisors / Research Analysts; (xii) KYC Registration Agencies; (xiii) Merchant Bankers; (xiv) Mutual Funds / Asset Management Companies; (xv) Portfolio Managers; (xvi) Registrar to an Issue and Share Transfer Agents; (xvii) Stock Brokers through Exchanges; (xviii) Stock Exchanges; and (xix) Venture Capital Funds.

Cybersecurity Function	Cyber Resilience Goal	Compliance Requirements
		required to perform self-assessments of the same annually. **Third-Party Accountability**: REs are responsible for all aspects of third-party services obtained by them, such as those pertaining to data security, and to ensure compliance with all applicable laws when engaging third parties.
Identify	Anticipate	**Critical Systems Identification**: REs are required to identify and classify critical systems, and conduct periodic risk assessments that include scenario-based testing.
Protect	Anticipate	**Access Restriction**: REs are required to design and implement network segmentation techniques to restrict access to the sensitive information, hosts, and services. **Audits and VAPT**: Periodic audits by an Indian Computer Emergency Response Team (CERT-In) empanelled IS auditing organization and Vulnerability Assessment and Penetration Testing (VAPT) are required to be conducted. **ISO 27001 Certification**: MIIs and Qualified REs are required to obtain the ISO 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements certification.
Detect	Anticipate	**SOC Implementation**: REs are required to establish appropriate security mechanisms through Security Operations Centre (SOC) for continuous monitoring of security events and timely detection of anomalous activities. **Setting up of Market SOCs**: Bombay Stock Exchange and National Stock Exchange are required to setup a market SOC by 1 January 2025. Small-size REs and self-certification REs are required to be onboarded on the market SOC.

Cybersecurity Function	Cyber Resilience Goal	Compliance Requirements
Respond	Withstand & Contain	**Incident Management**: All cybersecurity incidents are required to be reported in a timely manner through SEBI's incident reporting portal. Further REs are required to establish a comprehensive incident response plan, and an updated cyber crisis management plan. In case of an incident, root cause analysis (RCA) is required be conducted. In cases where the RCA is not conclusive, a forensic analysis is required to be undertaken. **Incident Reporting**: Any cybersecurity incident as specified under the directions of the CERT-In is required to be notified to SEBI, CERT-In, and the National Critical Information Infrastructure Protection Centre (as applicable) within the prescribed timelines. **Initiatives of the CERT-In:** MIIs and Qualified REs are required to get onboarded to Cyber Swachhta Kendra and participate in other CERT-In initiatives as may be applicable.
Recover	Recover	**Recovery Plan**: A comprehensive response and recovery plan (CRRP) is required to be documented by REs. Actions taken during recovery process is required to be informed to all the relevant internal and external stakeholders as set out in the CRRP as well as to executive and management teams.
Adapt	Evolve	**Adapting and Evolving**: MIIs and Qualified REs are required to continuously adapt and evolve to counter new cybersecurity threats and challenges. Further, Mid-size and Small-size REs are required to periodically evaluate their cyber resilience posture.

Data Localisation: REs are required to keep the regulatory data (ie data related to core and critical activities of the RE, as well as any supporting/ ancillary data impacting core and critical activities, including communication between investors and REs through applications and data that is deemed necessary or sensitive by the RE/ SEBI/ Central or State Government), available and easily accessible in legible and usable form, within India. Further, IT and cybersecurity data (ie data including but not limited to logs and metadata related to IT systems and their operations not containing any regulatory data and sensitive data such as internal network architecture, vulnerability details, details of admin/ privileged users of REs, password hashes, system configuration, etc.) is required to be made available to SEBI/ CERT-In/ any other government agency whenever required within a reasonable time, not exceeding 48 hours from the time of request.

CONCLUSION: The CSCRF provides a comprehensive and structured approach to enhancing cybersecurity and resilience across SEBI-regulated entities. By categorizing REs and setting clear goals, the framework ensures that cybersecurity measures are both robust and adaptable. With its forward-looking approach, including provisions for emerging technologies like quantum computing, the CSCRF is designed to protect the integrity of the securities market well into the future. Compliance with this framework will be crucial for REs to safeguard their operations and maintain trust in the evolving digital landscape.

- *Supratim Chakraborty (Partner); Sumantra Bose (Counsel) & Himeli Chatterjee (Associate)*

For any queries please contact: editors@khaitanco.com

AMBITION STATEMENT

“Our ambition is to be a respectable law firm providing efficient and courteous service, to act with fairness, integrity and diligence, to be socially responsible and to enjoy life. We should put greater emphasis on working in consonance with our aforesaid values than on maximizing earnings. Earn we should but with dignity and pleasure.”

Khaitan & Co is a premier full-service Indian law firm with 25+ practice areas, over 1,000 lawyers, including 200+ partners. To know more about us, please visit www.khaitanco.com