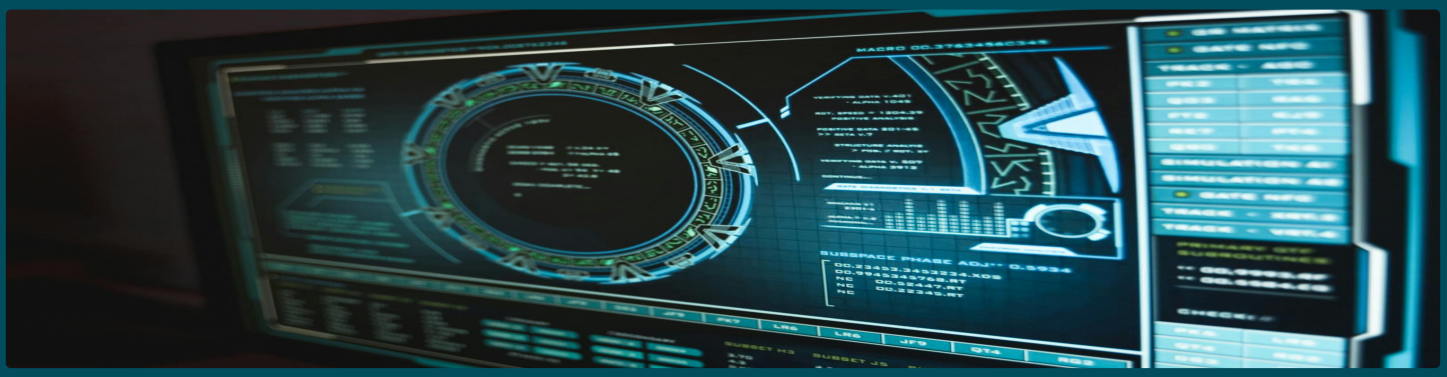
INDIALAW



CIVIL

SEBI’s Strategic Framework: Ensuring Cybersecurity and Resilience and Business Continuity in India’s Financial Sector

AUTHOR Rahul Sundaram

PUBLISHED 3 January 2025

Introduction: Pioneering Cybersecurity Resilience

The Securities and Exchange Board of India (SEBI) initially issued the **Cybersecurity and Cyber Resilience Framework (CSCRF)** for Regulated Entities (REs) on **August 20, 2024**, through circular SEBI/HO/ITD-1/ITD_CSC_EXT/P/CIR/2024/113. This framework was designed to address the rapidly evolving cyber threat landscape and technological advancements. Its goal was to ensure that SEBI-regulated entities maintain strong cybersecurity postures, implement resilience measures, and effectively respond to and recover from cyber threats.

Recognizing the need for further clarity and adjustments, SEBI issued an additional circular on **December 31, 2024** (SEBI/HO/ITD-1/ITD_CSC_EXT/P/CIR/2024/184), to address queries and feedback from REs, providing key clarifications and adjustments to the framework.

Table of contents

Background: Foundations of Cyber Resilience

The CSCRF was developed to strengthen the cybersecurity and resilience standards for regulated entities in the securities market. The framework builds upon foundational guidelines issued in 2015 for Market Infrastructure Institutions (MIIs) and subsequent extensions to other REs. Over the years, SEBI has issued several advisories to promote best practices in cybersecurity.

Key Objectives of the CSCRF:

1. Strengthening measures to mitigate cyber risks and ensuring strong cyber resilience.
2. Aligning with global cybersecurity standards, such as ISO 27001, NIST, and BIS guidelines.
3. Establishing uniformity in cybersecurity compliance across REs.

The CSCRF supersedes earlier circulars and consolidates prior guidance into a unified approach.

Objective: Strengthening Cybersecurity Frameworks

The primary goals of the CSCRF include:

1. Mitigating risks from evolving cyber threats.
2. Strengthening cybersecurity frameworks for operational resilience.
3. Enhancing reporting formats for consistent and structured compliance.

This ensures that all REs, regardless of size or scope, achieve adequate cybersecurity standards and are prepared for cyber incidents.

Approach: A Two-Pronged Strategy

The CSCRF is structured around two core approaches:

1. **Cybersecurity:** Focuses on governance, operational controls, and incident response mechanisms.

2. **Cyber Resilience:** Built upon five key goals:
    - **Anticipate:** Proactively preparing for potential threats.
    - **Withstand:** Maintaining operational continuity during attacks.
    - **Contain:** Isolating and neutralizing threats effectively.
    - **Recover:** Restoring normalcy post-incident.
    - **Evolve:** Continuously improving and adapting to new threats.

Implementation: A Roadmap for Compliance

The CSCRF outlines a phased and graded approach for REs based on their size and scope:

1. **Categorization of REs:** Divided into five categories (e.g., MIIs, Qualified REs, Mid-size REs).
2. **Compliance Reporting:** Standardized formats introduced for consistent compliance reporting.
3. **Guidance and Standards:** REs must adhere to specific cybersecurity functions:
    - **Governance:** Establishing risk management frameworks, roles, and oversight policies.
    - **Identify:** Classifying assets and analysing threats and vulnerabilities.
    - **Protect:** Implementing network segmentation, data encryption, and secure development practices.
    - **Detect:** Using Security Operations Centers (SOCs) for monitoring.
    - **Respond and Recover:** Developing incident response plans and recovery protocols.
    - **Evolve:** Incorporating adaptive controls and strategies.

Additionally, MIIs and Qualified REs are required to conduct regular **Cyber Capability Index (CCI)** assessments.

Key Standards and Guidelines: Best Practices in Cybersecurity

The CSCRF emphasizes:

- Implementation of internationally recognized standards, such as ISO 27001.
- Regular assessments, including Vulnerability Assessment and Penetration Testing (VAPT).
- Security-focused development practices, such as the Secure Software Development Lifecycle.

Compliance mechanisms include audits, SOC effectiveness evaluations, and structured incident reporting.

Clarifications: Updates in the December 31, 2024 Circular

SEBI's recent circular addresses key clarifications and adjustments:

1. **Regulatory Forbearance:**
    - Compliance with the CSCRF remains effective from **January 1, 2025**, but a grace period extends regulatory forbearance until **March 31, 2025**.
    - During this period, REs that demonstrate meaningful progress in implementing the framework will not face regulatory action. SEBI will evaluate their efforts before considering any penalties.
2. **Extension of Compliance Dates:**
    - **KYC Registration Agencies (KRAs):** Compliance deadline extended to **April 1, 2025**.
    - **Depository Participants (DPs):** Compliance deadline also extended to **April 1, 2025**.
3. **Data Localisation Guidelines:**
    - The implementation of Data Localisation standards (PR.DS.S2) has been deferred for further consultation. These provisions are on hold until SEBI provides additional guidance.

Effective Date and Legal Basis: Ensuring Robust Governance

- The December 31, 2024, circular is effective immediately, providing clarity on compliance timelines and regulatory measures.

- Issued under **Section 11(1) of the SEBI Act, 1992**, the circular aims to protect investors, promote market development, and regulate the securities market.

Conclusion: Paving the Way for Cybersecurity Excellence

SEBI's Cybersecurity and Cyber Resilience Framework reflects its commitment to securing the securities market against evolving cyber threats. By emphasizing strong compliance mechanisms, adaptive strategies, and international standards, SEBI ensures that all regulated entities are well-prepared to navigate today's digital environment. The clarifications and adjustments in the recent circular demonstrate SEBI's responsiveness to industry feedback, encouraging a collaborative and resilient approach to cybersecurity. Together, these measures set a solid foundation for safeguarding the integrity and stability of India's financial markets.

For further details write to contact@indialaw.in