भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

Consultation Paper

APPLICABILITY OF IT & CYBER SECURITY FRAMEWORK OF MIIs TO THEIR SUBSIDIARIES

SEPTEMBER 11, 2026

Objective

1. The objective of this consultation paper is to seek feedback with regard to the proposal of applicability of IT and Cyber Security framework of Market Infrastructure Institutions (MIIs) to their subsidiaries.

Background

2. With an aim to maintain uninterrupted securities market operations, SEBI, *from time to time*, has prescribed IT framework to Market Infrastructure Institutions (MIIs).

3. Further, with an increased reliance on digital ecosystem, threat of cyber-attacks has also increased. Attackers are using advanced technologies to exploit security gaps and gain unauthorized access to organizational data. In order to strengthen the cybersecurity posture of SEBI-regulated entities, ensuring they can anticipate, withstand, contain, and recover from cyber incidents, SEBI has also prescribed Cybersecurity and Cyber Resilience Framework (CSCRF).

4. The IT and Cyber Security framework together mandates strict, technology risk management, *inter-alia*, to its MIIs to protect market data, ensure operational continuity and prevent cyber-attacks.

Growth of Subsidiaries of MIIs and Need for Regulatory Clarity

5. As MIIs witness growth in the scale and complexity of their operations and undertake technology-driven and market-related activities, there could be a case for MIIs to take services of their subsidiaries to carry out certain activities. Such subsidiaries may be required to operate in close coordination with the parent MII and may utilize shared technology infrastructure, applications, market data or other critical IT resources. *(Note: Subsidiaries is as defined under Section 2(87) of Companies Act, 2013).*
6. While MIIs may be governed by and operating in compliance with SEBI's IT and cyber security framework, the applicability and regulatory jurisdiction of these IT and Cyber framework are not explicitly defined over their subsidiaries.
7. Providing greater clarity on the applicability of the IT and Cyber framework to subsidiaries of MIIs would help ensure that IT systems and activities performed through such subsidiaries are appropriately covered under the regulatory framework, thereby strengthening regulatory oversight and promoting consistent implementation.

Deliberation in SEBI's Technical Advisory Committee (TAC)

8. The aforesaid concern was deliberated in SEBI's Technical Advisory Committee (TAC) in its meeting held on December 09, 2025.

Proposal

9. As MIIs continue to diversify their business models through subsidiaries, extending the applicability of the framework would ensure that the regulatory framework remains aligned with the evolving market structure. With this objective, following is proposed:

9.1. Applicability of IT and Cyber framework

9.1.1. Subsidiaries covered by MII's IT and Cyber Security Framework

The IT and Cyber Security framework applicable to the parent MII shall also apply to the subsidiary where the subsidiary:

9.1.1.1. **is doing activity which directly contributes to domain pertaining to that MII. In other words, subsidiary is carrying out an activity which the MII is supposed to do or**

9.1.1.2. **is handling the data which the MII is supposed to handle or**

9.1.1.3. **is sharing the infrastructure with MII.**

Such subsidiaries shall comply with all the applicable requirements relating to cyber security, system audits, incident reporting, BCP-DR and technology governance, etc.

9.1.2. Subsidiaries exempted from complying with MII's IT and Cyber Security Framework

9.1.2.1. The IT and Cyber Security framework applicable to the parent MII shall not be applicable to the subsidiary where the subsidiary does not meet any of the aforesaid three criteria.

Illustrations on clarifications of applicability of IT and Cyber Security framework to MII's subsidiaries (Not Exhaustive) is provided in Annexure-A.

9.1.3. Exemption in the Interest of proportionality-

9.1.3.1. In case an MII is of the view that IT / Cyber framework may not

be extended to its subsidiary viz. meeting only condition (9.1.1.3) i.e. sharing of IT infrastructure with MII, it is proposed that MIIs may seek exemption from SEBI w.r.t not extending IT / Cyber framework to that subsidiary. Such proposal shall include details of compensatory controls put in place / proposed to be put in place by MIIs to ensure cyber and IT resilience of MIIs is not affected by such proposal along with views of SCOT and Board of the MII."

Public comments

10. Public Comments are solicited on the aforesaid proposals. The comments / suggestions along with rationale should be submitted not later than **October 2, 2026** through the online web-based form which can be accessed using the following link:

https://www.sebi.gov.in/sebiweb/publiccommentv2/PublicCommentAction.do?doPublicComments=yes

11. In case of any technical issue in submitting your comment(s) through the web based public comments form, you may email your comment(s) to following-

    a) **Shri Darshil Bhatt, Deputy General Manager** (darshilb@sebi.gov.in) and;

    b) **Shri Abhijeet Srivastava, Assistant General Manager** (abhijeets@sebi.gov.in)

While sending the email, kindly mention the subject as "**Applicability of IT and Cyber Security Framework of MIIs to their Subsidiaries**".

***

Annexure-A

Illustrations on clarifications of applicability of IT and Cyber Security framework to MII's subsidiaries (Not Exhaustive)

Sr. No.	*Scenario*	*Illustrative Example*	*Applicable / Not Applicable*	*Reason*
1.	***Technology subsidiary developing and maintaining the trading platform of a Stock Exchange***	*A subsidiary develops, operates and maintains the trading engine used by the parent Stock Exchange*	***Applicable***	*The subsidiary directly contributes to the regulated function of the MII and manages critical IT systems.*
2.	***Subsidiary providing cybersecurity services for the parent MII***	*A subsidiary operates the SOC, SIEM, vulnerability management and incident response for the parent MII.*	***Applicable***	*It manages critical cyber security functions affecting the MII.*
3.	***Shared Data Centre / Cloud subsidiary***	*A subsidiary hosts production servers, databases or disaster recovery infrastructure used by the parent MII.*	***Applicable***	*It shares critical infrastructure supporting regulated operations.*
4.	***Technology subsidiary handling MII data***	*A subsidiary provides analytics, surveillance or AI services using trading, settlement or investor data of the parent MII.*	***Applicable***	*It handles data that the MII is responsible for protecting.*
5.	***Common IT Services subsidiary***	*A subsidiary manages Active Directory, Identity & Access Management, email or network services for the parent MII.*	***Applicable***	*It provides shared technology services essential for secure operations.*
6.	***Shared Helpdesk / Infrastructure Management subsidiary***	*A subsidiary administers production servers, databases or storage used by the parent MII.*	***Applicable***	*It has privileged access to critical systems and infrastructure.*
7.	***Education or Training subsidiary***	*A subsidiary conducts investor awareness programmes or certification courses without accessing MII systems or data.*	***Not Applicable***	*Activities are unrelated to regulated market infrastructure operations.*
8.	***Real Estate / Facility Management subsidiary***	*A subsidiary manages office premises, administration or facility services.*	***Not Applicable***	*It does not process MII data or operate MII systems.*
9.	***Independent Financial Services subsidiary***	*A subsidiary undertakes an unrelated financial business regulated under a separate SEBI or RBI framework with independent IT infrastructure.*	***Not Applicable***	*It has independent operations and its own applicable regulatory framework.*
10.	***HR / Payroll Services subsidiary***	*A subsidiary maintains HR and payroll systems for employees without access to trading, clearing, settlement or depository systems.*	***Not Applicable***	*It neither supports regulated functions nor handles critical MII systems or data.*