



Department: Inspection	Segment: All
Circular No: MSE/INSP/19958/2026	Date: October 21, 2026

Subject: Advisory on Common Cyber Security Non-Compliances Observed During Cyber Revalidation Audit and CSK Monitoring

To All Trading Members,

The Securities and Exchange Board of India (SEBI), in coordination with the Stock Exchanges, recently conducted a special purpose cyber revalidation audit to assess the comprehensiveness of Cyber Security and Cyber Resilience Audit conducted by stock brokers and the effectiveness of monitoring of stock brokers' systems through the CERT-In Cyber Swachhta Kendra (CSK) platform.

Based on the observations emanating from the revalidation audit and monitoring undertaken through the CSK platform, certain common cyber security non-compliances have been observed across members' systems. Such observations indicate gaps in understanding and implementation of applicable cyber security and cyber resilience requirements. The sharing of common observations to members is expected to enhance awareness, bridging the gap between requirements and interpretation, and thereby ensuring better compliance.

The details of the commonly observed non-compliances are enclosed as **Annexure – A** to this advisory.

All Trading Members are advised to take note of the above and put in place necessary systems, controls & procedures to strengthen their cyber security posture and adhere to the compliance with all applicable SEBI and Exchange circulars relating to Cyber Security and Cyber Resilience Framework (CSCRF).

In case of any query kindly contact Inspection Department on (022) 6112 9000, Extn. 9038, 9039, 9040, 9041, 9042 and 9127 or mail on 'compliancemsx@mse.co.in' or 'inspectionmsx@mse.co.in'.

For and on behalf of
Metropolitan Stock Exchange of India Limited

Anshu Bharti
Assistant Vice President

Annexure A

Commonly Observed Non-compliances

A. Governance and Policy related issues

1. There was a lack of clear classification & categorization of critical assets in line with the Cyber Security and Cyber Resilience Framework (CSCRF) especially the policy document for categorizing assets as 'critical'. As a result, auditors found that all assets which are critical in nature have not been included in the critical assets inventory.
2. Greater level of granularity is required in the asset inventory of critical assets for the auditors to carry out audits as per the CSCRF framework. It was found that the asset inventory does not contain the details such as end of life of the product, end of support for the product and date of installation etc.
3. The gaps were found in the cyber security internal policy document of stock brokers. It was observed during the audits that the cyber security policy documents does not contain details of exceptions and deviations allowed from the policy framework. The policy document is expected to be comprehensive one.
4. The exceptions carved out in the policy documents are critical in evaluating the compliance with the stipulated internal policy of the stock brokers. Further, in cases where exceptions and deviation have been specified, there is lack of differentiation between the two. Hence more emphasis is required while framing the policy document from coverage, exceptions and deviations perspective etc.
5. It was found during the audit that the role, level and the grade of the CISO is not positioned at a level equivalent to CTO/CIO. Such approach/practices may affect the independence w.r.t governance of the cyber security framework in the organization.
6. Auditors observed a gap between the implementation of RTO and RPO timelines and those specified in the CSCRF. As a result, RTO/RPO timelines were not standardized as per CSCRF requirements.

B. Security system related issues

1. It was observed during the audit that there was a lack of centralized access matrix for application, infrastructure tools and SAAS tools to review (by auditors) all access granted across the organization. Such practices severely limit visibility at centralized level, increases the risk of unauthorized access, and lengthen the audit process.
2. Auditors found that the interpretation of multi-factor authentication differs across the stock brokers. Further, it was also found that multi-factor authentication has not been fully implemented in certain internal applications. As a result, non-compliances have been observed by auditors. In addition, it was observed that login passwords are stored in browser making them easily accessible.