भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

CIRCULAR

SEBI/HO/MIRSD/DoP/P/CIR/2022/74 **May 30, 2022**

To,

All KYC Registration Agencies

Dear Sir/ Madam,

Subject: - Modification in Cyber Security and Cyber resilience framework of KYC Registration Agencies (KRAs)

1. SEBI vide circular SEBI/HO/MIRSD/DOP/CIR/P/2019/111 dated October 15, 2019 prescribed framework for Cyber Security and Cyber Resilience for KYC Registration Agencies.

2. In partial modification to Annexure A of SEBI circular dated October 15, 2019, the paragraph-11, 40, 41 and 42 shall be read as under:

   11. KRAs shall identify and classify critical assets based on their sensitivity and criticality for business operations, services and data management. The critical assets shall include business critical systems, internet facing applications /systems, systems that contain sensitive data, sensitive personal data, sensitive financial data, Personally Identifiable Information (PII) data, etc. All the ancillary systems used for accessing/communicating with critical systems either for operations or maintenance shall also be classified as critical system. The Board of the KRAs shall approve the list of critical systems.

       To this end, KRAs shall maintain up-to-date inventory of its hardware and systems, software and information assets (internal and external), details of its network resources, connections to its network and data flows.

   40. KRAs shall carry out periodic vulnerability assessment and penetration tests (VAPT) which inter-alia include critical assets and infrastructure components like Servers, Networking systems, Security devices, load balancers, other IT systems pertaining to the activities done as KRAs etc., in order to detect security vulnerabilities in the IT environment and in-depth

evaluation of the security posture of the system through simulations of actual attacks on its systems and networks.

KRAs shall conduct VAPT at least once in a financial year. However, for the KRAs, whose systems have been identified as "protected system" by NCIIPC under the Information Technology (IT) Act, 2000, VAPT shall be conducted at least twice in a financial year. Further, all KRAs are required to engage only CERT-In empaneled organizations for conducting VAPT. The final report on said VAPT shall be submitted to SEBI after approval from Technology Committee of respective KRAs, within one month of completion of VAPT activity.

41. Any gaps/vulnerabilities detected shall be remedied on immediate basis and compliance of closure of findings identified during VAPT shall be submitted to SEBI within 3 months post the submission of final VAPT report.

42. In addition, KRAs shall perform vulnerability scanning and conduct penetration testing prior to the commissioning of a new system which is a critical system or part of an existing critical system.

3. Further, the KRAs are mandated to conduct comprehensive cyber audit at least twice a financial year. All KRAs shall submit a declaration from the MD/ CEO certifying compliance by the KRAs with all SEBI Circulars and advisories related to Cyber security from time to time, along with the cyber audit report.

4. KRAs shall take necessary steps to put in place systems for implementation of the circular.

5. All KRAs are directed to communicate the status of the implementation of the provisions of this circular to SEBI within 10 days from the date of this Circular.

6. The provisions of the Circular shall come into force with immediate effect.

7. This circular is being issued in exercise of powers conferred under Section 11 (1) of the Securities and Exchange Board of India Act, 1992 to protect the interests of investors in securities and to promote the development of, and to regulate the securities market.

8. The circular is issued with the approval of the competent authority.

9. This circular is available on SEBI website at www.sebi.gov.in under the categories “Legal Framework” and “Circulars”.

Yours faithfully,

Sapna Sinha
Deputy General Manager
Market Intermediaries Regulation and Supervision Department
Tel. no.:022 2644 9748
email id: sapnas@sebi.gov.in