CDSL/OPS/RTA/POLCY/2022/111 **May 31, 2022**

MODIFICATION IN CYBER SECURITY AND CYBER RESILIENCE FRAMEWORK OF QUALIFIED REGISTRARS TO AN ISSUE AND SHARE TRANSFER AGENTS ("QRTAS")

Issuers/RTAs are advised to refer to SEBI Circular no. SEBI/HO/MIRSD/MIRSD_RTAMB/P/CIR/2022/73 dated May 27, 2022 regarding **Modification in Cyber Security and Cyber resilience framework of Qualified Registrars to an Issue and Share Transfer Agents ("QRTAs")** [**refer Annexure**].

Issuers/RTAs are advised to take note of the same and ensure compliance.

Queries regarding this communiqué may be addressed to **CDSL – Helpdesk:** on telephone numbers (022) 2305-8624, 2305-8639, 2305-8642, 2305-8663, 2305-8640, 2300-2041 or 2300-2033. Emails may be sent to: helpdesk@cdslindia.com.

sd/-

Nilesh Shah
Asst. Vice President - Operations

भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

CIRCULAR

SEBI/HO/MIRSD/MIRSD_RTAMB/P/CIR/2022/73 May 27, 2022

To,

Registered Registrar to an Issue and Share Transfer Agents

Dear Sir/ Madam,

Subject: - Modification in Cyber Security and Cyber resilience framework of Qualified Registrars to an Issue and Share Transfer Agents ("QRTAs")

1. SEBI vide circular SEBI/HO/MIRSD/CIR/P/2017/100 dated September 08, 2017 prescribed framework for Cyber Security and Cyber Resilience for Qualified Registrars to an Issue and Share Transfer Agents ("QRTAs")

2. In partial modification to Annexure A of SEBI circular dated September 08, 2017, the paragraph-11, 40, 41 and 42 shall be read as under:

   11. *QRTAs shall identify and classify critical assets based on their sensitivity and criticality for business operations, services and data management. The critical assets should 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 should also be classified as critical system. The Board of the QRTAs shall approve the list of critical systems.*

   To this end, QRTAs should 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. *QRTAs 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 etc. pertaining to the activities done as a QRTAs 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.*

    QRTAs shall conduct VAPT at least once in a financial year. However, for the QRTAs, 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 QRTAs 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 QRTAs, within 1 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, QRTAs 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 QRTAs are mandated to conduct comprehensive cyber audit at least twice in a financial year. All QRTAs shall submit a declaration from the MD/ CEO certifying compliance by the QRTAs with all SEBI Circulars and advisories related to Cyber security from time to time, along with the Cyber audit reports.

4. QRTAs are required to take necessary steps to put in place systems for implementation of the circular.

5. All QRTAs 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,

Aradhana Verma
Deputy General Manager
Market Intermediaries Regulation and Supervision Department
Tel. No. 022-2644 9633
Email id - aradhanad@sebi.gov.in