भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

CIRCULAR

SEBI/HO/IMD/IMD-I/DOF2/P/CIR/2022/81 **June 9, 2022**

To,

All Mutual Funds/

All Asset Management Companies (AMCs)/

All Trustee Companies/ Boards of Trustees of Mutual Funds/

Association of Mutual Funds in India (AMFI)

Dear Sir/ Madam,

Subject: - Modification in Cyber Security and Cyber Resilience Framework of Mutual Funds/ Asset Management Companies (AMCs)

1. SEBI vide Circular No.SEBI/HO/IMD/DF2/CIR/P/2019/12 dated January 10, 2019 (hereafter referred as "the circular") prescribed framework for Cyber Security and Cyber Resilience for Mutual Funds / Asset Management Companies (AMCs).

2. In partial modification to Annexure 1 of SEBI circular dated January 10, 2019:

   i. To have uniformity for identifying and classifying critical assets, across the industry, paragraph 11 on section "Identify" of the circular shall be read as under:

   "11. Mutual Funds/ AMCs 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 assets. The Board of the AMCs and Trustees shall approve the list of critical assets.

   To this end, Mutual Funds/ AMCs 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."

ii. Based on the recommendation of IT-Projects Advisory Committee (IT-PAC) of SEBI and also to adopt "audit the auditor approach" for conducting the Vulnerability Assessment and Penetration Testing (VAPT) of the intermediaries, paragraphs 40, 41 & 42 on section "Vulnerability Assessment and Penetration Testing (VAPT)" of the circular shall be read as under:

"40. Mutual Funds/ AMCs shall carry out periodic VAPT, inter-alia, including critical assets and infrastructure components like servers, networking systems, security devices, load balancers, other IT systems pertaining to the activities done as a role of Mutual Funds/ AMCs, 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.

Mutual Funds/ AMCs shall conduct VAPT at least once in a financial year. However, for the Mutual Funds/ AMCs, whose systems have been identified as "protected system" by National Critical Information Infrastructure Protection Centre (NCIIPC) under the Information Technology (IT) Act, 2000, VAPT shall be conducted at least twice in a financial year.

Further, all Mutual Funds/ AMCs shall engage only Indian Computer Emergency Response Team (CERT-In) empanelled organizations for conducting VAPT. The final report on said VAPT shall be submitted to SEBI after approval from Technology Committee of respective Mutual Funds/ AMCs, within 1 month of completion of VAPT activity.

41. Any gaps or 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, Mutual Funds/ AMCs 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."

iii. For receipt of quarterly reports containing information on cyber-attacks and threats experienced by Mutual Funds/ AMCs in a time bound manner, paragraph 51 on section "Sharing of information" of the circular shall be read as under:

"51. All cyber-attacks, threats, cyber-incidents, and breaches experienced by Mutual Funds/ AMCs shall be reported to SEBI within 6 hours of noticing/ detecting such incidents or being brought to their notice about such

incidents. The incident shall also be reported to CERT-In in accordance with the guidelines/ directions issued by CERT-In from time to time. Additionally, the Mutual Funds/ AMCs, whose systems have been identified as "protected system" by NCIIPC, shall also report the incident to NCIIPC. The quarterly reports containing information on cyber-attacks, threats, cyber-incidents, and breaches experienced by Mutual Funds/ AMCs and measures taken to mitigate vulnerabilities, threats and attacks including information on bugs/ vulnerabilities/ threats that may be useful for other Mutual Funds/ AMCs shall be submitted to SEBI within 15 days from the quarter ended June, September, December and March of every year.

iv. The above information/ reports shall be shared through the dedicated e-mail ids: vapt_reports@sebi.gov.in and cybersecurity_amc@sebi.gov.in

3. Further, the Mutual Funds/ AMCs are mandated to conduct comprehensive cyber audit at least 2 times in a financial year. Along with the cyber audit reports, henceforth, all Mutual Funds/ AMCs are directed to submit a declaration from the Managing Director (MD)/ Chief Executive Officer (CEO) certifying compliance by the Mutual Funds/ AMCs with all SEBI Circulars and advisories related to cyber security from time to time.

4. Mutual Funds/ AMCs are required to take necessary steps to put in place systems for implementation of the circular, including modification of internal policies, if any.

5. Applicability: The provisions of this Circular shall come into force with effect from July 15, 2022.

6. This circular is issued in exercise of the powers conferred under Section 11 (1) of the Securities and Exchange Board of India Act 1992, read with the provision of Regulation 77 of SEBI (Mutual Funds) Regulation, 1996 to protect the interests of investors in securities and to promote the development of, and to regulate the securities market.

Yours faithfully,

Hruda Ranjan Sahoo
Deputy General Manager
Tel no.: 022-26449586
Email: hrsahoo@sebi.gov.in