KHAITAN &CO ADVOCATES SINCE 1911

UPDATE

ERGO

Analysing developments impacting business

SEBI TIGHTENS CYBER SECURITY AND CYBER RESILIENCE FRAMEWORK OF MUTUAL FUNDS AND ASSET MANAGEMENT COMPANIES TO SAFEGUARD INVESTOR

29 June 2022

Introduction

On 10 January 2019 the Securities and Exchange Board of India (SEBI) had prescribed the framework for cyber security and cyber resilience for mutual funds / asset management companies vide Circular No. SEBI/HO/IMD/DF2/CIR/P/2019/12.

Subsequently, SEBI had outlined a modified cyber security and cyber resilience framework for stockbrokers and depository participants, market infrastructure institutions (stock exchanges, depository and clearing corporations) and KYC registration agencies (KRAs).

In continuation thereof, partially modifying Annexure 1 of the 10 January 2019 circular, SEBI has now issued a circular on "modification in cyber resilience and cyber security framework for mutual funds / asset management companies" (June 2022 Circular).

Applicability

The provisions of this June 2022 Circular shall come into effect from 15 July 2022 and will be applicable to the following entities:

- All Mutual Funds (MFs)
- All Asset Management Companies (AMCs)
- All trustee companies / boards of trustees of MFs
- the association of mutual funds of India (AMFI)

Our analysis and comments on this June 2022 Circular are outlined below.

Analysis

The crucial highlights and amendments introduced by the June 2022 Circular are as follows:

- *Identification, classification, and segregation of critical assets:*
  - MFs and AMCs need to identify and classify critical assets based upon their sensitivity and criticality for business operations, services, and data management.

- Such critical assets shall include business critical systems, internet applications, communication systems, or other systems containing sensitive data, sensitive personal data, sensitive financial data, personally identifiable information (PII) data etc.

- All ancillary systems which access or communicate with critical systems, whether for operational or maintenance purposes, are also to be designated as critical assets.

➢ *Key Obligations of the Board of MFs / AMCs:*

- Board of the AMCs and trustees must approve the list of critical assets.

- For this purpose, all MFs and AMCs are required to prepare an up-to-date inventory of their hardware and systems, details of their network resources, connections to its network, data flows, internal and external software, and information assets.

➢ *Stress Tests - Conducting Vulnerability Assessment and Penetration Testing (VAPT):*

- A periodic VAPT is to be conducted by the MFs and AMCs covering among others the critical assets and network infrastructure components including servers, security devices, and other IT systems to detect security vulnerabilities in the IT environment and for in-depth security assessment of the of the system through simulations of real attacks on its systems and networks.

  - VAPT shall be conducted at least once in each financial year, unless their systems have been identified as "protected systems" (by National Critical Information Infrastructure Protection Centre (NCIIPC)), in which case VAPT shall be conducted at least twice in a financial year.

  - VAPT Vendor: Can hire only an Indian Computer Emergency Response Team (CERT-In) empanelled organisation for conducting the VAPT assessment.

  - Within 1 (one) month of completion of VAPT, the final report shall be submitted to SEBI, after securing approval from the technology committee of respective MFs / AMCs.

- On an immediate basis, the identified deviations or vulnerabilities shall be corrected and within 3 (three) months from the submission of final VAPT report and the compliance towards closure of findings shall be submitted to SEBI.

- Additionally, before installing a new system or updating an existing critical system, the MFs / AMCs are required to conduct a vulnerability scanning and perform penetration testing.

➢ *Time bound reporting:*

- The MFs / AMCs shall within 6 (six) hours of detecting such any cyber-incidents, attack, or breach, report the same to SEBI.

- The incident shall also be reported to CERT-In as per the periodic guidelines and directions issued.

- Moreover, the MFs / AMCs, whose systems have been identified as "protected system" by NCIIPC, shall also report the incident to NCIIPC.

- The MFs / AMCs shall submit, quarterly reports to SEBI within 15 (fifteen) days from the end of each quarter, detailing the cyber-attacks, threats, incidents, and breaches, the steps taken to mitigate and overcome the underlying vulnerabilities including information on the related bugs, so that other AMCs can use such information to embrace the precautionary measures and thereby preclude any further incidents.

- The MFs / AMCs shall submit all the cyber security information and related VAPT reports on the dedicated email ids: vapt_reports@sebi.gov.in and cybersecurity_amc@sebi.gov.in

➢ *Cyber audit:*

- At least 2 (two) times in a financial year, the MFs / AMCs are mandated to conduct a comprehensive cyber audit.

- All MFs / AMCs are required to submit a declaration from the managing director (MD) / chief executive officer (CEO) certifying their compliance with all periodic SEBI Circulars and advisories related to cyber security (in addition to the cyber audit reports).

➢ *Systems and implementation policies:*

MFs / AMCs shall take all necessary measures to initiate systems for implementation and modify internal policies, to comply with this cyber security framework circular.

Comments

In the pursuit of establishing a robust and enduring cybersecurity arrangement, seeking to protect our digital lives, we have witnessed the proliferation of the cyber related regulatory and legislative compliances.

In the same vein, SEBI has under this June 2022 Circular, outlined additional safeguards to preserve the critical assets, prevent any cyber threat, and in case of any security breach, has also prescribed the operational measures which the MFs and AMCs are required to implement, aimed at protecting the interests of the investors.

Though these regulations considerably escalate the business risk due to non-compliance, as well as the enhanced costs and efforts of operational implementation, they serve as a confidence building measure for the customers, since strengthening the MFs and AMCs cyber security framework, provides an added protection for their mutual fund investments, preventing them from falling prey to any form of cyber incidents.

- *Achint Kaur (Counsel)*

For any queries please contact: editors@khaitanco.com