भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

CIRCULAR

SEBI/HO/MIRSD/POD-1/P/CIR/2023/193 **December 27, 2023**

To
All Recognized Stock Exchanges
All Recognized Depositories
All Mutual Funds
All Asset Management Companies (AMCs)
All Trustee Companies/ Board of Trustees of Mutual Funds
Stock Brokers (Trading Members) through Recognized Stock Exchanges
Depository Participants through Depositories
All Registered Registrars to an Issue and Share Transfer Agents (RTAs)
All Listed Companies through Recognized Stock Exchanges
Association of Mutual Funds in India (AMFI)

Dear Sir / Madam,

Subject: Extension of timelines for providing 'choice of nomination' in eligible demat accounts and mutual fund folios

1. SEBI, vide circular nos. SEBI/HO/MIRSD/POD-1/CIR/2023/158 dated September 26, 2023 and SEBI/HO/IMD/IMD-I POD1/P/CIR/2023/160 dated September 27, 2023, extended the last date for submission of 'choice of nomination' for demat accounts and mutual fund folios respectively to December 31, 2023.

2. Based on representations received from the market participants, for ease of compliance and investor convenience, it has been decided to extend the last date for submission of 'choice of nomination' for demat accounts and mutual fund folios to **June 30, 2024.**

3. Depository Participants, AMCs and RTAs shall encourage the demat account holders/ mutual fund unit holders to fulfil the requirement for nomination/opting out of nomination by sending a communication on fortnightly basis by way of emails and SMS to all such demat account holders/ mutual fund unit holders who are not in compliance with the requirement of nomination. The communication shall provide guidance to provide nomination or opting out of nomination.

4. Stock Exchanges, Depositories, AMCs, RTAs and Listed Companies are further advised to:
    a) take necessary steps to implement the provisions of this circular, including making necessary amendment to the relevant bye-laws / business rules / regulations / operational instructions, as the case may be;
    b) bring the provisions of this circular to the notice of their respective constituents and also disseminate this circular on their websites;
    c) communicate to SEBI, the status of the implementation of the provisions of this circular; and
    d) monitor the compliance of this circular.

5. All other provisions related to requirement of Nomination as provided in SEBI Master Circular No. SEBI/HO/IMD/IMD-PoD-1/P/CIR/2023/74 dated May 19, 2023 for Mutual Funds and SEBI Master Circular No. SEBI/HO/MRD/MRD-PoD-2/P/CIR/2023/166 dated October 06, 2023 for Depositories shall remain unchanged.

6. This circular is issued in exercise of powers conferred by Section 11(1) of the Securities and Exchange Board of India Act, 1992, read with Section 19 of the Depositories Act, 1996 and Regulation 77 of SEBI (Mutual Funds) Regulations, 1996, to protect the interests of investors in securities and to promote the development of, and to regulate the securities market.

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

Yours faithfully,

Srishti Ambokar
Deputy General Manager
Market Intermediaries Regulation and Supervision Department
Tel. No. 022-2644 9354
Email id – srishtijc@sebi.gov.in

भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

MASTER CIRCULAR

SEBI/HO/MRD/MRD-PoD-2/P/CIR/2023/166 **October 06, 2023**

To,

All Depositories

Dear Sir / Madam,

Subject: Master Circular for Depositories

1. Securities and Exchange Board of India (SEBI), from time to time, has been issuing various circulars/directions to Depositories. Further, a Master Circular in the form of a compilation of all the relevant circulars was also issued on this subject on February 05, 2021. In order to enable the users to have access to all the applicable circulars/directions pertaining to depositories at one place, the Master Circular for Depositories has been prepared.

2. This Master Circular shall come into force from the date of its issuance. This Master Circular covers the relevant circulars/communications pertaining to depositories issued by SEBI upto August 31, 2023. References to the Statutes/Regulations which now stand repealed have been suitably updated in the Master Circular. This Master Circular rescinds the circulars and communications listed in **Schedule-A**.

3. Notwithstanding such rescission:
   a) anything done or any action taken or purported to have been done or taken under the rescinded circulars, including registrations or approvals granted, fees collected, registration or approval suspended or cancelled, any inspection or investigation or enquiry or adjudication commenced or show-cause notice issued, prior to such rescission, shall be deemed to have been done or taken under the corresponding provisions of this Master Circular;
   b) any application made to SEBI under the rescinded circulars, prior to such rescission, and pending before it shall be deemed to have been made under the corresponding provisions of this Master Circular;
   c) the previous operation of the rescinded circulars or anything duly done or suffered thereunder, any right, privilege, obligation or liability acquired, accrued or incurred under the rescinded circulars, any penalty, incurred in respect of any violation committed against the rescinded circulars, or any investigation, legal proceeding or remedy in respect of any such right, privilege, obligation, liability,

penalty as aforesaid, shall remain unaffected as if the rescinded circulars have never been rescinded.

4. The Master Circular consists of four sections i.e. Beneficial Owner (BO) Accounts, Depository Participants (DP) Related, Issuer related and Depositories Related. Efforts have been made to include provisions of circulars/communications relevant to each sections. However, cross referencing of circulars/communications amongst the sections may exist. Users may refer other sections also for compliance to provisions applicable to them.

5. Words and expressions used but not defined in this Circular shall have the same meanings as may be defined in Securities Contracts (Regulation) Act, 1956 or the Securities and Exchange Board of India Act, 1992 or the Depositories Act, 1996 or Regulations made thereunder i.e. Securities Contracts (Regulation) (Stock Exchanges and Clearing Corporations) Regulations, 2018, SEBI (Depositories and Participants) Regulations, 2018, PIT Regulations, SEBI (Prohibition of Fraudulent and Unfair Trade Practices relating to Securities Market) Regulations, 2003, unless the context requires otherwise.

6. This Master Circular is 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.

7. This Master Circular is available on the SEBI website at https://www.sebi.gov.in/ under the category "Legal→Master Circulars".

Yours faithfully

Vishal Shukla
General Manager
Market Regulation Department
Email: vishals@sebi.gov.in
Phone 022-26449959

भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

Table of Contents

Section 1: Beneficial Owner (BO) Accounts

1.1 Opening of BO Account by non-body corporates

1.1.1 Proof of Identity (PoI)

1.1.1.1 Permanent Account Number (PAN) to be the sole identification number for all transactions in the securities market[1]

With effect from July 02, 2007, PAN is the sole identification number for all transactions in the securities market, irrespective of the amount of transaction. A copy of the PAN card with photograph may be accepted as Proof of Identity. In this regard, intermediaries shall:-

a. Put necessary systems in place so that the databases of the clients and their transactions are linked to the PAN details of the client.

b. Build necessary infrastructure to enable accessibility and query based on PAN thereby enabling retrieval of all the details of the clients.

c. Collect copies of PAN cards issued to the existing as well as new clients by the Income Tax Department and maintain the same in their record after verifying with the original.

d. Cross-check the aforesaid details collected from their clients with the details on the website of the Income Tax Department i.e. http://incometaxindiaefiling.gov.in/challan/enterpanforchallan.jsp[2].

1.1.1.2 PAN as the sole identification number for all transactions in the securities market[3]

1.1.1.2.1 It has been decided to discontinue with the requirement of Unique Identification Number (UIN) under the SEBI (Central Database of market Participants Regulations), 2003 (MAPIN regulations)/circulars.

1.1.1.3 List of documents admissible as Proof of Identity[4]

a. Unique Identification Number (UID) (Aadhaar)/ Passport/ Voter ID card/ Driving license.

b. PAN card with photograph.

c. Identity card/ document with applicant's Photo, issued by any of the following: Central/State Government and its Departments, Statutory/Regulatory Authorities, Public Sector Undertakings, Scheduled Commercial Banks, Public Financial Institutions, Colleges affiliated to

[1] Reference: SEBI Circular MRD/DoP/Cir-5/2007 dated April 27, 2007
[2] Income Tax Department since changed the link for verification to: https://incometaxindiaefiling.gov.in/e-Filing/Services/KnowYourPanLink.html
[3] Reference: SEBI Circular MRD/DoP/Cir-08/2007 dated June 25, 2007
[4] Reference: SEBI Circular MIRSD/SE/Cir-21/2011 dated October 05, 2011

Universities, Professional Bodies such as ICAI, ICWAI, ICSI, Bar Council etc., to their Members; and Credit cards/Debit cards issued by Banks.

d. e-KYC service launched by UIDAI shall also be accepted as a valid process for Know Your Client ("**KYC**") verification. The information containing the relevant client details and photograph made available from UIDAI as a result of e-KYC process shall be treated as a valid proof of Identity.[5]

e. With a view to bring about operational flexibility and in order to ease the PAN verification process, the intermediaries may verify the PAN of their clients online at the Income Tax website without insisting on the original PAN card, provided that the client has presented a document for Proof of Identity other than the PAN card.[6]

1.1.2 Proof of Address (PoA)[7]

1.1.2.1 List of documents admissible as Proof of Address:

(*Documents having an expiry date should be valid on the date of submission.)

a. Passport/ Voters Identity Card/ Ration Card/ Registered Lease or Sale Agreement of Residence/ Driving License/ Flat Maintenance bill/ Insurance Copy.

b. Utility bills like Telephone Bill (only land line), Electricity bill or Gas bill - Not more than 3 months old.

c. Bank Account Statement/Passbook -- Not more than 3 months old.

d. Self-declaration by High Court and Supreme Court judges, giving the new address in respect of their own accounts.

e. Proof of address issued by any of the following: Bank Managers of Scheduled Commercial Banks/Scheduled Co-Operative Bank/Multinational Foreign Banks/Gazetted Officer/Notary public/ elected representatives to the Legislative Assembly/Parliament/Documents issued by any Govt. or Statutory Authority.

f. Identity card/document with address, issued by any of the following: Central/State Government and its Departments, Statutory/Regulatory Authorities, Public Sector Undertakings, Scheduled Commercial Banks, Public Financial Institutions, Colleges affiliated to Universities and Professional Bodies such as ICAI, ICWAI, ICSI, Bar Council etc., to their Members.

g. For FPI: Power of Attorney given by FPI to the Custodians (which are duly notarized and/or apostiled or consularised) that gives the registered address should be taken.

---

[5] Reference: SEBI Circular SEBI/MIRSD/09/2013 dated October 08, 2013

[6] Reference: SEBI Circular SEBI/MIRSD/01/2013 dated January 04, 2013

[7] Reference: SEBI Circular MIRSD/SE/Cir-21/2011 dated October 05, 2011

h. The proof of address in the name of the spouse may be accepted.

i. Aadhaar Letter issued by UIDAI shall be admissible as Proof of Address in addition to Proof of Identity.[8]

j. e-KYC service launched by UIDAI shall also be accepted as a valid process for KYC verification. The information containing the relevant client details and photograph made available from UIDAI as a result of e-KYC process shall be treated as a valid proof of address.[9]

1.1.2.2 DP shall ensure that all documents pertaining to proof of identity and proof of address are collected from all the account holders.[10] Submission of the aforesaid documents is the minimum requirement for opening a BO Account. DPs must verify the copy of the aforementioned documents with the original before accepting the same as valid. While opening a BO Account, DPs shall exercise due diligence[11] while establishing the identity of the person to ensure the safety and integrity of the depository system.

1.1.3 <u>Clarification on voluntary adaptation of Aadhaar based e-KYC process[12]</u>

SEBI has enabled Aadhaar based e-KYC service offered by UIDAI for KYC verification. Intermediaries have sought clarifications from SEBI on certain operational aspects of the same. It is clarified that for accessing the details enabling client identification and authentication from UIDAI based on client authorisation, on voluntary basis, intermediaries who utilize the services of KYC Service Agencies (KSAs) would be registered as KYC User Agencies (KUA) with UIDAI.[13]

i. For entering into account based relationship, the client may provide the following information to the intermediary*:*

a) Name
b) Aadhaar number
c) Permanent Account Number (PAN)

ii. The above information can be provided by the client electronically including through any web enabled device.

iii. The intermediary shall perform verification of the client with UIDAI through biometric authentication (fingerprint or iris scanning). Mutual Funds can also perform verification of the client with UIDAI through One Time password (OTP) received on client's mobile number or on e-mail address registered with UIDAI

[8] Reference: SEBI Circular MIRSD/09/2012 dated August 13, 2012
[9] Reference: SEBI Circular SEBI/MIRSD/09/2013 dated October 08, 2013
[10] Reference: SEBI Circular MRD/DoP/Dep/Cir-29/2004 dated August 24, 2004
[11] Reference: SEBI Circular Point 5 of part II on 'Customer Due Diligence' of Master SEBI Circular no. ISD/AML/CIR-1/2008 dated December 19, 2008
[12] Reference: SEBI Circular SEBI/MIRSD/09/2013 dated October 08, 2013
[13] Reference: SEBI Circular CIR/MIRSD/29/2016 dated January 22, 2016

provided, the amount invested by the client does not exceed INR 50,000 per financial year per Mutual Fund and payment for the same is made through electronic transfer from the client's bank account registered with that Mutual Fund.

iv. PAN of such client is to be verified from the income tax website.

v. After due validation of Aadhaar number provided by the client, the intermediary (acting as KUA) shall receive the KYC information about the client from UIDAI through KSA.

vi. The information downloaded from UIDAI shall be considered as sufficient information for the purpose of KYC verification. The intermediary shall upload this KYC information on the KRA system in terms of Securities and Exchange Board of India {KYC (Know Your Client) Registration Agency} Regulations, 2011 ("**KRA Regulations**").

vii. In case material difference is observed either in the name (as observed in the PAN vis-a-vis Aadhaar) or photograph in Aadhaar is not clear, the intermediary shall carry out additional due diligence and maintain a record of the additional documents sought pursuant to such due diligence.

viii. The records of KYC information so received shall be maintained by the intermediary as per the SEBI Act, Regulations and various circulars issued thereunder.

1.1.4 *Common and simplified norms for processing investor's service requests by RTAs and norms for furnishing PAN, KYC details and Nomination* [14]

Kindly refer para titled 'Common and Simplified Norms for processing investor's service request by RTAs and norms for furnishing PAN, KYC details and Nomination' of SEBI Circular SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2023/70 dated May 17, 2023 (Master Circular for Registrars to an Issue and Share Transfer Agents)

1.1.5 *SARAL Account Opening Form for resident individuals*[15]

1.1.5.1 It is gathered that a majority of new investors in the securities market begin with participation in the cash segment without obtaining various other facilities such as internet trading, margin trading, derivative trading and use of power of attorney. The account opening process can be simplified for such individual investors. With a view to encourage their participation, it is, therefore, decided that such individual investors can open a trading account and demat account by filling up a simplified Account Opening Form ('**AOF**') termed as 'SARAL AOF' given at **Annexure 1**.

1.1.5.2 This form will be separately available with the intermediaries and can also be downloaded from the Exchanges' and Depositories' website. The investors who open account through SARAL AOF will also have the option to obtain other

[14] Reference: SEBI Circular SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2023/37 dated March 16, 2023

[15] Reference: SEBI Circular MIRSD/1/2015 dated March 04, 2015

facilities, whenever they require, on furnishing of additional information as per prescribed regulations/circulars.

1.1.5.3 The standard set of documents viz. Rights and Obligations document, Uniform Risk Disclosure Document and Guidance Note and documentary proof related to identity and address as specified under **Para 2.14**, **Para 1.1.1** **and** **Para 1.1.2** shall continue to remain applicable. It is further clarified that the provisions laid down under the PMLA, Prevention of Money Laundering ("**PML**") Rules 2005, SEBI Master Circular on Guidelines on Anti-Money Laundering (AML) Standards and Combating the Financing of Terrorism (CFT) /Obligations of Securities Market Intermediaries under the Prevention of Money Laundering Act, 2002 and Rules framed there under dated February 03, 2023 shall also continue to remain applicable for set of individual investors mentioned in **Para 1.1.5.1** above.

1.1.5.4 For these set of individual investors, it has been decided to simplify the requirement of submission of 'proof of address'. The matter has been examined in the light of amendment to the PML Rules, 2005 and accordingly, the requirement of submission of 'proof of address' is as follows:

1.1.5.4.1 Henceforth, individual investor may submit only one documentary proof of address (either residence/correspondence or permanent) while opening a trading account and / or demat account or while undergoing updation.

1.1.5.4.2 In case the proof of address furnished by the said investor is not the address where the investor is currently residing, the intermediary may take a declaration of the residence/correspondence address on which all correspondence will be made by the intermediary with the investor. No proof is required to be submitted for such correspondence/residence address. In the event of change in this address due to relocation or any other reason, investor may intimate the new address for correspondence to the intermediary within two weeks of such a change. The residence/ correspondence address and any such change thereof may be verified by the intermediary through 'positive confirmation' such as

(i) acknowledgment of receipt Welcome Kit/ dispatch of contract notes / any periodical statement, etc.
(ii) telephonic conversation;
(iii) visits, etc.

1.1.6 Uniform Know Your Client (KYC) Requirements for the Securities Markets [16]

[16] Reference: SEBI Circular MIRSD/SE/Cir-21/2011 dated October 05, 2011

1.1.6.1 In case of stock brokers (and also for the stock brokers who are depository participants), the account opening process for investors has been simplified vide **Para 2.14**, KYC form capturing the basic details about the client has been prescribed as Part I of the account opening form and additional information specific to dealing in the stock exchange(s) are obtained in Part II of the form.

1.1.6.2 With a view to bring about uniformity in securities markets, it has also been decided that the same KYC form and supporting documents shall also be used by all captioned SEBI registered intermediaries. The KYC form as given in **Annexure 2** shall be filled by an investor at the account opening stage while dealing with any of the above intermediaries. Additional details specific to the area of activity of the intermediary being obtained now but not covered in the KYC form shall also be obtained from the investors in Part II of the account opening form.

1.1.6.3 The additional information (Part II) shall be prescribed by depositories for their depository participants and by Association of Mutual Funds in India ("**AMFI**") for all mutual funds. The portfolio managers, venture capital funds, and collective investment schemes shall capture the additional information specific to their area of activities, as considered appropriate by them. The intermediaries shall also continue to abide by circulars issued by SEBI from time to time for prevention of money laundering.

1.1.7 Acceptance of third party address as correspondence address[17]

1.1.7.1 SEBI has no objection to a BO authorizing the capture of an address of a third party as a correspondence address, provided that the DP ensures that all prescribed KYC norms are fulfilled for the third party also. The DP shall obtain proof of identity and proof of address for the third party. The DP shall also ensure that customer due diligence norms as specified in Rule 9 of PML Rules, 2005 are complied with in respect of the third party.

1.1.7.2 The depository participant should further ensure that the statement of transactions and holding are sent to the BO's permanent address at least once in a year.

1.1.7.3 However, the above provision shall not apply in case of PMS (Portfolio Management Services) clients.

1.2 Exemptions from and clarifications relating to mandatory requirement of PAN

1.2.1 Mandatory requirement of Permanent Account Number (PAN)[18]

The demat accounts for which PAN details have not been verified are "suspended for debit" until the same is verified with the DP. With effect from August 16, 2010 such PAN non-compliant demat accounts were also "suspended for credit" other than the credits arising out of automatic corporate actions. It was clarified that other credits

[17] Reference: SEBI Circular CIR/MRD/DP/37/2010 dated December 14, 2010
[18] Reference: SEBI Circular MRD/DP/22/2010dated July 29, 2010

including credits from IPO/FPO/Rights issue, off-market transactions or any secondary market transactions would not be allowed into such accounts.

1.2.2 Central and State Government and officials appointed by Courts[19]

PAN card may not be insisted upon in case of transactions undertaken on behalf of Central Government and/or State Government and where transactions are conducted by officials appointed by Courts e.g. Official liquidator, Court receiver etc.[20]

However DPs, before implementing the above exemption, shall verify the veracity of the claim of the organizations by collecting sufficient documentary evidence in support of their claim for such an exemption.

1.2.3 Investors in Sikkim[21]

Investors residing in the state of Sikkim are exempted from the mandatory requirement of furnishing PAN card details for their demat accounts.[22] DPs shall verify the veracity of the claim of the investors that they are residents of Sikkim, by collecting sufficient documentary evidence in support of their address.

1.2.4 UN entities and multilateral agencies exempt from paying taxes/ filing tax returns in India[23]

UN entities/ multilateral agencies exempt from paying taxes/filing tax returns in India are also exempt from the mandatory requirement of submitting their PAN card details, subject to the DPs collecting documentary evidence in support of such claims.

1.2.5 FPIs/Institutional Clients[24]

Custodians shall verify the PAN card details of institutional clients with the original PAN card and provide duly certified copies of such verified PAN details to the brokers. This requirement is applicable in respect of institutional clients, namely, FPIs, MFs, VCFs, FVCIs, Scheduled Commercial Banks, Multilateral and Bilateral Development Financial Institutions, State Industrial Development Corporations, Insurance Companies registered with IRDA and Public Financial Institution as defined under section 2(72) of the Companies Act, 2013.

1.2.6 HUF, Association of Persons (AoP), Partnership Firm, unregistered Trust, Registered Trust, Corporate Bodies, minors, etc.[15]

---

[19] Reference: SEBI Circular MRD/DoP/Cir-20/2008 dated June 30, 2008

[20] Reference: Rule 114C (1)(c) of Income Tax Rules

[21] Reference: SEBI Circular MRD/DoP/Dep/Cir-09/06 dated July 20, 2006

[22] Reference: Hon'ble High Court of Sikkim judgment dated March 31, 2006

[23] Reference: SEBI Circular MRD/DoP/Dep/Cir-09/06 dated July 20, 2006

[24] Reference: SEBI Circular MRD/DoP/Dep/SE/Cir-13/06 dated September 26, 2006

The BO account shall be in the name of natural persons, PAN card details of the respective HUF, AoP, Partnership Firm, Unregistered Trust, etc. shall be obtained. The PAN number of Registered Trust, Corporate Bodies and minors shall be obtained when accounts are opened in their respective names.

1.2.7 **Difference in maiden name and current name of investors.**[15]

DPs can collect the PAN card proof as submitted by the account holder subject to the DPs verifying the veracity of the claim of such investors by collecting sufficient documentary evidence in support of the identity of the investors.[25]

1.2.8 **NRI/PIOs**[26]

Citizens of India residing outside India, foreign citizens and other persons (like companies/ trusts/ firms) having no office of their own in India may obtain PAN card based on the copy of their passport as ID proof and a copy of passport/ bank account in the country of residence as address proof, based on the Directorate of Income Tax (Systems) guidelines.[27]

1.3 ***Simplification of demat account opening process***[28]

1.3.1 SEBI has taken a number of steps in the recent past to simplify the account opening and KYC process in the securities markets. In continuation of the efforts in the same direction, it has now been decided in consultation with both the depositories and associations of stock brokers and DPs to further simplify and rationalize the demat account opening process.

1.3.2 The existing Beneficial Owner-Depository Participant Agreements shall be replaced with a common document "Rights and Obligations of the Beneficial Owner and Depository Participant" (**Annexure 3**) . The document annexed herewith shall be mandatory and binding on all the existing and new clients and DPs. This will harmonize the account opening process for trading as well as demat account. This will also rationalize the number of signatures by the investor, which he is required to affix at present on a number of pages.

1.3.3 The DP shall provide a copy of Rights and Obligations Document to the BO and shall take an acknowledgement of the same. They shall ensure that any clause in any voluntary document neither dilutes the responsibility of the depository participant nor it shall be in conflict with any of the clauses in this document, rules, bye-laws, regulations, notices, guidelines and circulars issued by SEBI and the depositories from time to time. Any such clause introduced in the existing as well as new documents shall stand null and void.

---

[25] Reference: SEBI Circular MRD/DoP/Dep/Cir-29/2004 dated August 24, 2004

[26] Reference: SEBI Circular MRD/DoP/Dep/SE/Cir-17/06 dated October 27, 2006

[27] Reference: Income Tax (Systems) PAN SEBI Circular No. 4 dated October 11, 2006

[28] Reference: SEBI Circular SEBI/MIRSD/ 12/2013 dated December 04, 2013

1.3.4 In consultation with market participants, with a view to simplify the account opening kit, SEBI has decided that DP shall make available this document "Rights and Obligations of the Beneficial Owner and Depository Participant" to the clients, either in electronic or physical form, depending upon the preference of the client as part of account opening kit. In case the documents are made available in electronic form, DP shall maintain the logs of the same. It is also reiterated that Depositories/DP shall continue to make the aforesaid document available on their website and keep the clients informed about the same.[29]

1.4 Guidelines for online closure of demat accounts[30]

1.4.1 Depositories are advised to issue guidelines under **Para 1.4.4** to their participants and make available the facility for online closure of demat accounts from August 01, 2021.

1.4.2 Depositories shall inform clients regarding the availability of facility for online closure of demat accounts through emails, SMS, weekly / fortnightly / monthly newsletters etc.

1.4.3 Depositories shall also advise their participants to inform their clients regarding the availability of facility for online closure of demat accounts through emails, SMS, weekly / fortnightly / monthly newsletters etc. The procedure for online closure of demat accounts shall be prescribed in such communications.

1.4.4 **Guidelines for online closure of demat accounts**

1.4.4.1 Client shall be entitled to close the demat account through online mode without mandatorily giving any reasons to the DP. Clients shall not be restricted from requesting, through online mode or offline mode, for the closure of demat account maintained with the DP, subject to the compliance requirements as stipulated by SEBI / Depository from time to time.

1.4.4.2 Online closure of demat accounts shall be made available for the clients who have opened their accounts offline or online, by the DPs that provide various Depository related services in online mode. Those DPs which do not provide any services online and do not open accounts online may not be required to offer online closure of demat accounts.

1.4.4.3 Account closure for account with balance shall be done only through web portal / app of DP through secured access by way of client specific user ID and password (in case of internet clients) and the request send through emails, SMS, other messaging apps, etc. shall not be entertained by the DP. As the KYC process requires e-sign post which demat accounts can be opened by the DP, for online closure of accounts with balance also, client shall be required to e-sign the

[29] Reference: SEBI Circular CIR/MIRSD/64/2016 dated July 12, 2016
[30] Reference: SEBI MIRSD email dated July 15, 2021

form (using Aadhaar based online electronic signature service) to be verified by the DP in accordance with guidelines as stipulated by SEBI / Depositories from time to time.

1.4.4.4 In case of clients having demat accounts with nil balances can be closed by the DPs on the basis of emails received from the registered email ID of the demat account holder.

1.4.4.5 Once the application for closure of demat account is received, the DP shall intimate to the client on registered email id and / or mobile number (on both if available) about the receipt of closure request. A confirmation regarding the request made shall be sought from the client by way of OTP sent on the email id and / or mobile number updated in its source account (to be closed account).

1.4.4.6 The request for demat account closure shall include target account details (in case of request for closure of demat account having security balances is made) where the client intends to shift the securities.

1.4.4.7 Client would have to upload the scan / photograph of his / her signature alongwith Client Master Report (CMR) of the target account digitally signed by official of the target DP (CMR applicable in case of account having security balances). Filled Account Closure form alongwith uploaded ink-signature of the client and CMR as uploaded, would be displayed in one single file to the client, subsequent to which, client shall then be required to e-sign the form (using Aadhaar based online electronic signature service) alongwith the documents and submit the same for further processing. The requirement of obtaining a CMR will be exempted if the DP is able to verify the target demat account details (i.e. sole holder's name and PAN should match perfectly) directly from the Depository electronically.

1.4.4.8 If the DP authorises the request received, the account will get closed in the Depository system. If the DP rejects the client requests received, the DP shall inform the reason for such rejection to the client.

1.4.4.9 In case the target account of the client specified in the account closure form is not its own account i.e. not the same PAN both in source and target accounts, as per the extant requirements, it will be necessary for the client to submit an off-market transfer instruction delivery instruction slip for execution of such transfers along with the requirement of entering OTP as provided by the Depository.

1.4.4.10 After the closure of demat account by the DP, the same shall be intimated to the client through electronic mode enclosing the CMR & Transaction cum Holding Statement of the closed account.

1.4.4.11 DP shall maintain and store system logs of the closure instructions and e-signed electronic requests (uneditable) received in electronic form in a secured manner and the same shall be subject to 100% internal audit.

1.4.4.12 Notwithstanding any such closure of demat account, all rights, liabilities and obligations of the parties arising out of or in respect of transactions entered into prior to the closure of demat account shall continue to subsist and vest in / be binding on the respective parties or his / its respective heirs, executors, administrators, legal representatives or successors, as the case may be.

1.4.4.13 The above process shall be applicable in case of individual client accounts with single holder (without pledge/freeze/pending demat requests balances) and the closure requests accepted through above mechanism shall be considered as a valid client request and DPs / Depository shall not be held liable for acting on such requests.

1.4.4.14 Depositories shall put in place a complaint redressal mechanism for dealing with complaints related to online closure of demat accounts.

1.5 Guidelines on Identification of Beneficial Ownership[31]

1.5.1 The beneficial owner has been defined as the natural person or persons who ultimately own, control or influence a client and/or persons on whose behalf a transaction is being conducted, and includes a person who exercises ultimate effective control over a legal person or arrangement.

1.5.2 SEBI has prescribed uniform KYC requirements for the securities markets. Also, the KRA Regulations have been notified and guidelines have been issued under these regulations from time to time.

1.5.3 Further, the PML Rules, 2005 also require that every banking company, financial institution and intermediary, as the case may be, shall identify the beneficial owner and take all reasonable steps to verify his identity. The Government of India in consultation with the regulators has now specified a uniform approach to be followed towards determination of beneficial ownership. Accordingly, the intermediaries shall comply with the following guidelines.

A. For clients other than individuals or trusts:

1.5.4 Where the client is a person other than an individual or trust, viz., company, partnership or unincorporated association/body of individuals, the intermediary shall identify the beneficial owners of the client and take reasonable measures to verify the identity of such persons, through the following information:

a. The identity of the natural person, who, whether acting alone or together, or through one or more juridical person, exercises control through ownership or who ultimately has a controlling ownership interest.

Explanation: Controlling ownership interest means ownership of/entitlement to:

[31] Reference: SEBI Circular CIR/MIRSD/2/2013 dated January 24, 2013

i. more than 10%[32] of shares or capital or profits of the juridical person, where the juridical person is a company;

ii. more than 15% of the capital or profits of the juridical person, where the juridical person is a partnership; or

iii. more than 15% of the property or capital or profits of the juridical person, where the juridical person is an unincorporated association or body of individuals.

b. In cases where there exists doubt under **Para 1.5.4 (a)** above as to whether the person with the controlling ownership interest is the beneficial owner or where no natural person exerts control through ownership interests, the identity of the natural person exercising control over the juridical person through other means.

Explanation: Control through other means can be exercised through voting rights, agreement, arrangements or in any other manner.

c. Where no natural person is identified under **Para 1.5.4 (a)** or **Para 1.5.4 (b)** above, the identity of the relevant natural person who holds the position of senior managing official.

B. For client which is a trust:

1.5.5 Where the client is a trust, the intermediary shall identify the beneficial owners of the client and take reasonable measures to verify the identity of such persons, through the identity of the settler of the trust, the trustee, the protector, the beneficiaries with 10%[33] or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

C. Exemption in case of listed companies:

1.5.6 Where the client or the owner of the controlling interest is a company listed on a stock exchange, or is a majority-owned subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.

D. Applicability for foreign investors:

1.5.7 Intermediaries dealing with foreign investors' viz., Foreign Portfolio Investors, Sub Accounts and Qualified Foreign Investors, may be guided by the clarifications issued vide SEBI circular CIR/MIRSD/11/2012 dated September 5, 2012, for the purpose of identification of beneficial ownership of the client.

---

[32] Reference: Ministry of Finance (Department of Revenue) Notification No. S.O. 1074(E) dated March 07, 2023

[33] Reference: Ministry of Finance (Department of Revenue) Notification No. S.O. 1074(E) dated March 07, 2023

1.6 Opening of demat account in case of HUF[34]

It is noted that as per law, in case of HUF, shares can be held in the name of Existing Karta on behalf of HUF. Therefore, HUF demat accounts can be opened in the name of Existing Karta but not in the name of Deceased Karta and HUF entity.

After examining the issues regarding difference in opening of HUF demat account and procedure adopted in the event of death of Karta of HUF, it has been decided that opening of HUF demat account and procedure adopted in the event of death of Karta of HUF shall be as per the following guidelines[35]:

1.6.1 **Opening of HUF Demat Account**

a) The Demat account shall be opened in the name of HUF entity as the name of entity appears on the PAN Card. The PAN details of both the HUF entity and Karta of HUF shall be submitted to the DP.

1.6.2 **Death of Karta**

a) In the event of death of Karta of HUF, the name of the deceased Karta in the BO account shall be replaced by the new Karta of the HUF who in such a case shall be eldest coparcener in the HUF or a coparcener who is appointed as Karta by an agreement reached amongst all the coparceners of the HUF[36].

b) The new Karta shall submit the new list of members, a notarized copy of death certificate of the deceased Karta and a no objection from the surviving members of the HUF for him/her to act as Karta of the HUF.

c) In the event of death of Karta of HUF, the existing BO account need not to be closed and the same account may continue. The death of Karta shall not mean that the securities lying in the BO account of the HUF is deemed to have divided among coparceners as if the partition has taken place.

1.6.3 **Partition of HUF**

a) A total or partial partition shall be recognized only if a claim to that effect is made by one or more coparceners.

b) An intimation of a total or partial partition shall be accompanied by a signed letter mentioning the names of the members and their confirmation of a partition having taken place.

c) In case of partial partition of the HUF, if desired by one or more coparceners, the new Karta shall transfer shares to the said coparceners who seek partition

---

[34] Reference: SEBI Letter SEBI/HO/MRD/DP/OW/2016/25739/1 & 25740/1 dated September 14, 2016 and SEBI Letter MRD/DSA1/OW/4946/2018 and 4947/2018 dated February 14, 2018

[35] Reference: SEBI Letter SEBI/HO/MRD/DP/OW/2016/25739/1 & 25740/1 dated September 14, 2016

[36] Reference: SEBI Circular SEBI/HO/MRD/MRD-POD-2/P/CIR/2022/114 dated August 26, 2022

and the BO account of the HUF shall continue. The account of such coparceners shall be treated as their individual accounts.

d) In case of full partition of the HUF, the shares shall be divided amongst all the coparceners in the manner specified by the applicant subject to fulfilment of **Para 1.6.3 (c)** above and the HUF account shall cease to exist.

1.7 Operation of minor's demat account[37]

Under The Hindu Minority and Guardianship Act, 1956, permission of Court is required in the case of transfer by a natural guardian of immovable property of a minor. However, shares are not immovable properly. Section 2(7) of Sale of Goods Act, 1930 includes shares within the definition of "goods". Neither the Indian Contract Act, 1872 nor the Sale of Goods Act, 1930 provide for transfer by sale or otherwise by guardian /natural guardian of goods/movable property in the name of minor to the effect that permission of court is required in the matter of such transfer. In the case of accounts of minor in banks also, the guardian is entitled to open, operate and even close the account also. The DP account can, therefore, be operated by a natural guardian without any order from the court though the same is neither expressly permitted nor prohibited.

1.8 Facility for a Basic Services Demat Account (BSDA)[38]

1.8.1 All depository participants (DPs) shall make available a "Basic Services Demat Account" (BSDA) with limited services as per terms specified herein.

1.8.2 **Eligibility**: Individuals shall be eligible to opt for BSDA subject to the following conditions-

- ***i.*** All the individuals who have or propose to have only one demat account where they are the sole or first holder.
- ***ii.*** Individuals having any other demat account/s where they are not the first holder shall be eligible for BSDA in respect of the single demat account where they are sole or first holder.
- ***iii.*** The individual shall have only one BSDA in his/her name across all depositories.
- ***iv.*** Value of securities held in the demat account shall not exceed Rupees Two Lakhs at any point of time.

1.8.3 **Option to open BSDA**: The DP shall give option:

- ***i.*** To open BSDA to all eligible individuals who open a demat account;
- ***ii.*** To all the existing eligible individuals to convert their demat account into BSDA on the date of the next billing cycle based on value of holding of securities in the account as on the last day of previous billing cycle.

[37] Reference: SEBI Letter SEBI SMDRP/NSDL/4615 /2000 dated March 13, 2000
[38] Reference: SEBI Circular CIR/MRD/DP/22/2012 dated August 27, 2012

iii. In order to facilitate the eligible individuals to avail the benefits of BSDA, DPs are advised to convert all such eligible demat accounts into BSDA unless such Beneficial Owners (BOs) specifically opt to continue to avail the facility of a regular demat account.

1.8.4 **Charges**:

To further boost participation in Debt Market and based on representation received from market participants, the structure of charges for debt securities as defined in Securities and Exchange Board of India (Issue and Listing of Non-Convertible Securities) Regulations, 2021 is given below:

i. The charge structure may be on a slab basis as indicated below[39]:

a. No Annual Maintenance Charges (AMC) shall be levied if the value of holdings of debt securities is up to Rs. 1 lakh and a maximum AMC of Rs. 100 shall be levied if the value of holdings of debt securities is between Rs. 1,00,001 and Rs.2,00,000.

No AMC shall be levied if the value of holdings other than debt securities is below Rs. 50,000 and a maximum AMC of Rs. 100 shall be levied if the value of holdings other than debt securities is between Rs.50,001 and Rs.2,00,000.

ii. The value of holding shall be determined by the DPs on the basis of the daily closing price or NAV of the securities or units of mutual funds, as the case may be. Where such price is not available the last traded price may be taken into account and for unlisted securities other than units of mutual funds, face value may be taken in to account. The value of suspended securities may not be considered for the purpose of determining eligibility of demat account as BSDA.

iii. If the value of holding in such BSDA exceeds the prescribed criteria at any date, the DPs may levy charges as applicable to regular accounts (non BSDA) from that date onwards.

iv. The DPs shall assess the eligibility of the BOs at the end of the current billing cycle and convert eligible demat accounts into BSDA.

1.8.5 **Services for Basic Services Demat Accounts**:

i. Transaction statements:

a. Transaction statements shall be sent to the BO at the end of each quarter. If there are no transactions in any quarter, no transaction statement may be sent for that quarter.

b. If there are no transactions and no security balance in an account, then no further transaction statement needs to be provided.

[39] Reference: SEBI Circular MRD/DoP2DSA2/CIR/P/2019/51 dated April 10, 2019

c. Transaction statement shall be required to be provided for the quarter in which the account became a zero balance account.

ii. Holding Statement[40]:

a. DP shall send atleast one annual physical statement of holding to the stated address of the BO in respect of accounts with no transaction and nil balance even after the account has remained in such state for one year. The DP shall inform the BO that the dispatch of the physical statement may be discontinued if the account continues to remain zero balance even after one year.

b. One annual statement of holding shall be sent in respect of remaining accounts in physical or electronic form as opted for by the BO.

iii. Charges for statements: Electronic statements shall be provided free of cost. In case of physical statements, the DP shall provide at least two statements free of cost during the billing cycle. Additional physical statement may be charged at a fee not exceeding Rs.25/- per statement.

iv. All BOs opting for the facility of BSDA, shall register their mobile number for availing the SMS alert facility for debit transactions.

v. At least Two Delivery Instruction Slips (DIS) shall be issued at the time of account opening.

vi. All other conditions as applicable to regular demat accounts, other than the ones mentioned in this circular shall continue to apply to basic services demat account.

1.8.6 **Rationalisation of services with respect to regular accounts.**

In partial modification of the earlier directions, the following rationalisation measures shall be available for regular demat accounts:

i. Accounts with zero balance and nil transactions during the year[41]: DP shall send atleast one annual physical statement of holding to the stated address of the BO in respect of accounts with no transaction and nil balance even after the account has remained in such state for one year. The DP shall inform the BO that if no Annual Maintenance Charge (AMC) is received by the DP, the dispatch of the physical statement may be discontinued for the account which continues to remain zero balance even after one year.

ii. Accounts which become zero balance during the year: For such accounts, no transaction statement may be sent for the duration when the balance remains nil. However, an annual statement of holding shall be sent to the BO.

[40] Reference: SEBI Circular CIR/MRD/DP/21/2014 dated July 01, 2014
[41] Reference: SEBI Circular CIR/MRD/DP/21/2014 dated July 01, 2014

iii. Accounts with credit balance: For accounts with credit balance but no transactions during the year, half yearly statement of holding for the year shall be sent to the BO.

1.9 Change of Name in the Beneficial Owner (BO) Account[42]

1.9.1 In order to simplify the procedure of change of name in individual Beneficial Owner's (BO) account, it has been decided that an individual BO may be allowed to change his/ her name, subject to the submission of following documents at the time of change of name of the individual in the BO account.

i. In case of change in name on account of marriage following documents shall be submitted:
Marriage Certificate or copy of Passport showing husband's name or publication of name change in official gazette.

ii. In case of change in name on account of reasons other than marriage Publication of name change in official gazette.

In case of change of name of an individual residing in the State of Karnataka and Punjab, for reasons other than marriage, the same may be allowed for the individual in the BO account subject to the submission of following documents[43]:

a) Request letter for change of name;

b) Sworn affidavit executed before the Notary Public/ Magistrate of First Class/ Executive Magistrate mentioning the reason for change of name and his complete address;

c) Paper publication in one local newspaper and one national newspaper; and

d) KYC in changed name

iii. In case of change in father's name:
Publication of name change in official gazette.

1.9.2 The Depository Participants (DPs) shall collect the self-attested copies of above documents and maintain the same in their records after verifying with the original document.

1.10 Fees/Charges to be paid by BO

1.10.1 **Account opening, custody and credit of securities**[44]

i. No investor shall pay any charge towards opening of a Beneficial Owner (BO) Account except for statutory charges as applicable;

ii. No investor shall pay any charge for credit of securities into his/her BO account; and

iii. No custody charge shall be levied on any investor who is opening a BO account.

---

[42] Reference: SEBI Circular CIR/MRD/DP/27/2012 dated November 01, 2012
[43] Reference: SEBI Circular CIR/MRD/DP/158/2018 dated December 27, 2018
[44] Reference: SEBI Circular MRD/DoP /SE/Dep/Cir-4/2005 dated January 28, 2005

1.10.2 Account Closure[45]

No Account closure charges shall be levied on BO on the closure of any account.

1.10.3 Inter Depository Transfer[46]

Inter-depository transfer of shares does not attract Stamp duty and it does not require compliance with section 56 of the Companies Act, 2013.

1.10.4 Transfer of a BO Account[47]

No charges shall be levied by a depository on any DP and by a DP on any BO when the BO transfers all the securities lying in his account to another branch of the same DP or to another DP under the same depository or another depository, provided the BO Account(s) at transferee DP and at transferor DP are one and the same, i.e. identical in all respects. In case the BO Account at transferor DP is a joint account, the BO Account at transferee DP should also be a joint account in the same sequence of ownership.

1.10.5 Account Maintenance Charges collected upfront on annual/ half yearly basis on demat accounts[48]

i. In the event of closing of the demat account or shifting of the demat account from one DP to another, the AMC collected upfront on annual/half yearly basis by the DP, shall be refunded by the DP to the BO for the balance of the quarter/s. For instance, in case annual AMC has been paid by the BO and if the BO closes/shifts his account in the first quarter, he shall be refunded the amount of the balance 3 quarters i.e. 3/4th of the AMC. Likewise, if a BO closes/shifts his account in the third quarter, he shall be refunded the amount for the balance one quarter i.e. 1/4th of the AMC.

ii. For the purpose of the above requirement the year shall begin from the date of opening of the account in quarterly rests.

iii. The above requirements shall be applicable to all existing and new accounts held with DPs which collect annual/half yearly upfront AMC. It is clarified that the above requirements shall not be applicable to those DPs who collect quarterly/ monthly AMC.

1.10.6 Dissemination of tariff/charge structure of DPs on the website of depositories [49]

i. DPs shall submit to their depository the tariff/charge structure every year, latest by 30th April, and also inform the depository the changes in their tariff/charge

[45] Reference: SEBI Circular D&CC/FITTC/CIR - 12/2002 dated October 30, 2002
[46] Reference: SEBI Circular SMDRP/Policy/Cir-29/99 dated August 23, 1999
[47] Reference: SEBI Circular MRD/DoP/Dep/Cir-22 /05 dated November 9, 2005
[48] Reference: SEBI Circular MRD/DP/20/2010 dated July 1, 2010
[49] Reference: SEBI Circular MRD/Dep/Cir- 20/06 dated December 11, 2006

structure as and when they are effected with a view to enabling the BOs to have a comparative analysis of the tariff/charge structure of various DPs.

ii. For this purpose depositories shall put in place necessary systems and procedures including formats, periodicity, etc. for collection of necessary data from the DPs and dissemination of the same on their website which would enable the investors to have a comparative analysis of the tariff/charge structure of various DPs.

1.11 Framework for automated deactivation of trading and demat accounts in cases of inadequate KYCs[50]

1.11.1 SEBI has, vide various circulars issued from time to time, mandated that addresses form a critical part of the KYC procedures. Thus, every address recorded for the purpose of compliance with KYC procedure has to be accurate. An intermediary has to update the address from time to time. However, it has been observed that in some cases accurate/updated addresses of clients are not maintained. This is borne out of the fact that when SEBI issues any notices, etc. during the course of any enforcement proceedings on such addresses, the same remain unserved.

1.11.2 To ensure that the client furnishes accurate/updated details of address and to ensure that KYC details are correct, the following framework involving stock exchanges (except Commodity Derivatives Exchanges) and depositories (hereinafter collectively referred to as "the MIIs") is proposed

1.11.2.1 Where SEBI instructs MIIs to serve any Show Cause Notice ("SCN") or order issued by SEBI, the MIIs shall arrange to physically deliver the same to the entity. The MIIs shall forward the signed acknowledgement of its receipt by the concerned addressee or its authorized representative to SEBI within a period of 30 working days from the date of receipt of such instructions from SEBI. If **none** of the MIIs are –

a. able to deliver the SCN or order, as the case may be, at any of the addresses mentioned in the KYC records linked to any trading/demat account of the entity; and

b. obtain a signed acknowledgement of its receipt from the entity or its authorized representative,

then all MIIs shall deactivate all trading and demat accounts i.e. implement a restraint/freeze on debit and credit *(except for corporate actions)* of all trading and demat accounts of the entity based on the entity's Permanent Account Number (PAN), within 5 working days from the last unsuccessful delivery report. MIIs shall send an email/SMS to the entity before deactivation. It is clarified that if one of the MIIs is able to deliver the SCN or order, as the case

[50] Reference: SEBI Circular SEBI/HO/EFD1/EFD1_DRA4/P/CIR/2022/104 dated July 29, 2022

may be, to the entity and obtain signed acknowledgement, then none of the accounts of the entity shall be deactivated. However, the MIIs, through their registered intermediaries, shall ensure that the KYC records linked to all accounts held by the entity, are updated, accurate and confirm the new KYC details to the concerned KYC Registration Agency (KRA).

1.11.2.2 Pending pay-in and pay-out obligations and open positions may be permitted to be settled, squared off or closed out, as the case may be, while enforcing the deactivation of trading/demat accounts of such entities.

1.11.2.3 MIIs shall ensure that they communicate the details of the deactivation along with reasons thereof to the respective registered intermediary. They shall also ensure that the reasons for the deactivation are displayed in a clear and unambiguous manner, when the entity attempts to transact using his trading/demat account.

1.11.2.4 Subject to the above, the MIIs shall ensure that the deactivated accounts are not used for dealing in securities market in any manner whatsoever.

1.11.2.5 The concerned entity may place a request to the registered intermediaries with which the entity holds a trading/demat account, seeking re-activation of trading/demat accounts along with –

a. the correct proof of address; and,
b. signed acknowledgement of receipt of the SCN or order, as the case may be, issued by SEBI referred to in **Para 1.11.2.1.**

1.11.2.6 The registered intermediary shall update the KYC records as per the extant norms and forward the copy of the signed acknowledgement of receipt of the SCN or order, as the case may be, to the concerned MII for re-activation of the trading/demat account.

1.11.2.7 The concerned MII shall re-activate all trading accounts/demat accounts of the entity after ensuring that –

a. the entity has provided a signed acknowledgement of receipt of the SCN / order passed by SEBI; and,
b. confirmation is received from the registered intermediary that the KYC records are compliant with the extant norms.

The concerned MII shall also inform the above to all other MIIs for reactivation of trading/ demat accounts. The signed acknowledgement shall be forwarded by the registered intermediary to the MII within 2 working days from the date of its receipt from the entity and the MII shall in turn forward it to SEBI within 2 working days of its receipt.

1.11.2.8 The process of reactivating the accounts by the MIIs shall not exceed more than 5 working days after receipt of request from the entity along with all the documents mentioned in **Para 1.11.2.5.**

1.11.2.9 The framework would also apply to joint accounts. However, before deactivating the joint accounts, MIIs shall endeavor to contact the entity through the co-holders for delivery of SCN / order simultaneously by following the same process outlined above.

1.11.2.10 The MIIs may deviate from the above provisions in appropriate cases, where the compliance with the framework is hampered due to factors beyond the control of the entity. In such cases, the MIIs shall record the reasons for deviating from the mandate of the framework and communicate the same to SEBI within 2 working days of such deviation.

1.11.2.11 MIIs shall have a mechanism for exchange of information and coordination amongst themselves for the purpose of implementing the framework described above. MIIs shall submit a consolidated report indicating status of requests forwarded by SEBI, on a monthly basis.

1.11.2.12 MIIs shall advise their registered intermediaries to ensure updation of KYC records at regular intervals as per the extant norms. This framework shall be in addition to and not in derogation of any Circular issued by SEBI or the MIIs with respect to KYC requirements or Unique Client Code norms.

1.11.2.13 An Illustration covering different scenarios is as follows:

Illustration:

Scenarios: Delivery failure, deactivation of accounts and reactivation of accounts.

SEBI advises the exchanges and depositories to serve the SCN on August 01, 2022. For the sake of simplicity, it is assumed that the entity has accounts with BSE, NSE, NSDL and CDSL with each account having different addresses* and that all calendar days are working days. The following table depicts the course of action that would be taken by the MIIs depending on the circumstances.

Action	BSE	NSE	NSDL	CDSL
Physical delivery of SCN	BSE makes multiple attempts on different addresses from August 1, 2022 to August 25, 2022 and the delivery at all locations becomes unsuccessful.	NSE attempts the service on August 15, 2022 and the delivery becomes unsuccessful.	NSDL attempts the service on August 16, 2022 and the delivery becomes unsuccessful.	CDSL attempts the service on August 16, 2022 and the delivery becomes unsuccessful.

Sharing of information on delivery status	The details of unsuccessful delivery shall be shared with all the other MIIs on August 25, 2022.	The details of unsuccessful delivery shall be shared with all the other MIIs on August 15, 2022.	The details of unsuccessful delivery shall be shared with all the other MIIs on August 16, 2022.	The details of unsuccessful delivery shall be shared with all the other MIIs on August 16, 2022.
Implementing freeze on debit and credit of trading/demat accounts (within 5 working days from the last unsuccessful delivery report)	Freeze shall be implemented by MIIs by August 30, 2022 as the last date of unsuccessful delivery is August 25, 2022. Before deactivation of the accounts, the MIIs shall once again reach out to the entity through email/SMS. Pursuant to the implementation of freeze, the reasons for the same shall be informed to the concerned intermediary and also displayed to the entity when an attempt is made to transact through his trading/demat account.			
Submission of updated KYC by the entity	The entity submits updated KYC and the signed acknowledgement to the registered intermediary of BSE through which it is registered, on October 01, 2022. The intermediary shall intimate the same to BSE immediately. The registered intermediary shall also confirm	NA	NA	NA

	the updated KYC details to the concerned KRA.			
Action	**BSE**	**NSE**	**NSDL**	**CDSL**
Re-activation of demat and trading accounts (within 5 working days from the date of request by the entity)	BSE shall re-activate the accounts and inform all the other MIIs within October 06, 2022 as the date of submission of request by the entity was October 01, 2022.	All the demat and trading accounts shall be re-activated within October 06, 2022.		
Forwarding of signed acknowledgement to MII within 2 working days from date of receipt by the intermediary	Signed acknowledgement shall be forwarded to BSE by the registered intermediary within October 03, 2022 as the date of receipt of signed acknowledgement by the intermediary was October 01, 2022.	NA	NA	NA
Forwarding of signed acknowledgement to SEBI within 2 working days from the date of receipt by MII	In case the signed acknowledgment is received by BSE on October 10, 2022, the same shall be forwarded to SEBI within October 12, 2022.	NA	NA	NA

*-In cases where the same address is available across the MIIs, the MIIs shall co-ordinate among themselves and share the information to avoid duplication of efforts.

1.12 *Safeguards to address the concerns of the investors on transfer of securities in dematerialized mode*[51]

Following safeguards shall be put in place to address the concerns of the investors arising out of transfer of securities from the BO Accounts:

1.12.1 The depositories shall give more emphasis on investor education particularly with regard to careful preservation of Delivery Instruction Slip ("**DIS**") by the BOs. The Depositories may advise the BOs not to leave "blank or signed" DIS with the DPs or any other person/entity.

1.12.2 The DPs shall not accept pre-signed DIS with blank columns from the BO(s).

1.12.3 If the DIS booklet is lost / stolen / not traceable by the BO, then the BO shall immediately intimate the DP in writing about the loss. On receipt of such intimation, the DP shall cancel the unused DIS of the said booklet.

1.12.4 The DPs shall not issue more than 10 loose DIS to one accountholder in a financial year (April to March). The loose DIS can be issued only if the BO(s) come in person and sign the loose DIS in the presence of an authorised DP official.

1.12.5 The DP shall also ensure that a new DIS booklet is issued only on the strength of the DIS instruction request slip (contained in the previous booklet) duly complete in all respects, unless the request for fresh booklet is due to loss, etc., as referred to in **Para 1.12.3** above

1.12.6 The DPs shall put in place appropriate checks and balances with regard to verification of signatures of the BOs while processing the DIS.

1.12.7 The DPs shall cross check with the BOs under exceptional circumstances before acting upon the DIS.

1.12.8 The DPs shall mandatorily verify with a BO before acting upon the DIS, in case of an account which remained inactive i.e., where no debit transaction had taken place for a continuous period of 6 months, whenever all the International Securities Identification Number (ISIN) balances in that account (irrespective of the number of ISINs) are transferred at a time. However, in case of active accounts, such verification may be mandatory only if the BO account has 5 or more ISINs and all such ISIN balances are transferred at a time. The authorized official of the DP verifying such transactions with the BO, shall record the details of the process, date, time, etc., of the verification on the instruction slip under his signature.

1.13 *Delivery Instruction Slip (DIS) Issuance and Processing*[52]

[51] Reference: SEBI Circular SEBI/MRD/Dep/Cir-03/2007 dated February 13, 2007 and SEBI Circular SEBI/MRD/Dep/Cir-03/2008 dated February 28, 2008

[52] Reference: SEBI Circular SEBI/MRD/DOP/01/2014 dated January 07, 2014

Standardization of DIS

i. Depositories shall ensure that the DIS is standardized across all DPs in terms of:
   a) Serial Numbering of DIS so as to enable system level checks by the depositories.
   b) Layout and size of DIS so as to facilitate scanning and easy retrievability of records

ii. The DIS must bear a pre-printed serial number, DP ID, and a pre-printed/pre stamped Beneficial Owner (BO) ID. The depositories shall prescribe a standard method of serial numbering and ensure that serial numbers issued by a DP are unique within the DP-ID.

iii. DPs shall ensure that
   a) same DIS shall not be used for giving both market and off-market instructions
   b) a single DIS shall not be used for transactions with multiple execution dates.

Monitoring of DIS

iv. Upon issuance of DIS booklets or loose slips to BO, the DPs shall make available immediately the following details of the DIS to the depository system electronically:
   a) the DIS serial number
   b) BO ID
   c) date of issuance, and
   d) any other relevant details as decided by the depository

v. At the time of execution of DIS, DPs shall enter the serial number of DIS in the depository system for validation. The depositories shall make provisions in their systems to facilitate the same.

vi. In respect of all the transfer instructions on a DIS, Depositories shall validate the serial number of DIS and shall ensure that no instructions accompanied by a used DIS or unissued DIS are processed.

Scanning of DIS

vii. DPs shall scan every DIS executed during a day along with all Annexures/ Computer printouts, if any, by the end of the next working day in the manner specified by the depository.

viii. The depositories shall ensure that their DPs have adequate infrastructure, systems and processes to implement scanning, storage and transfer of the scanned DIS in the manner specified by the depositories.

ix. The depositories shall ensure that the systems set up by the DPs maintain proper records of all scanned DIS images including audit trails for changes made, if any and put in place adequate checks and procedures to prevent unauthorized changes to scanned DIS.

x. Depositories shall utilize the archived scanned images for off-site inspection.

xi. Above provisions shall not be applicable for the instructions received from the clients by the DPs electronically in a manner approved by the Depository.

xii. Once a new DIS booklet is issued to a BO as per above provisions, old DIS issued to such a BO shall not be accepted by the DP. A period of one month may be given for receipt of DIS by the BOs. The DPs may accept old DIS during this transit period.[53] All the measures listed above under the head 'Monitoring of DIS' shall be made applicable to the DIS issued as per the provisions of this circular.

❖ **Acceptance of Delivery Instructions through Online Portal of Depository Participants[54]:**

While accepting delivery instructions through online portal of Depository Participants, Depositories need to ensure that investors' authentication is being carried-out by them, through Password/TPIN, along-with OTP, both generated at Depositories end, for each transaction.

❖ **Acceptance of Delivery Instruction through Online Portal of Intermediaries[55]**

1. Towards safeguarding the interest of the investors and market eco-system, it is decided that in case Depositories intend to permit acceptance of Delivery Instruction through Online Portal of intermediaries, they need to ensure that risk entailed by introducing such system are curtailed. Towards this end, Depositories need to incorporate necessary risk containment measures, including the following:

a) **e-DIS facility**: The facility of e-DIS has to be true to its label and should: -

i. Necessarily capture all details that are otherwise being captured in physical DIS, including settlement number and actual quantity to be transferred in case of on-market transfers.

ii. be an instruction towards actual transfer of securities to meet obligation for a single settlement number/date.

b) **Pre-trade authorization/ mandate**: If Depositories wish to continue providing the facility of enabling receipt of pre-trade mandate from client, Depositories should ensure the following:

i. The mandate should be received from client authorizing the concerned intermediary to transfer specific securities for meeting on-market settlement obligation only.

ii. Such mandate should necessarily pertain to a single settlement number/settlement date.

[53] Reference: SEBI Circular CIR/MRD/DP/22/2014 dated July 04, 2014
[54] Reference: SEBI Letter MRD2/DDAP/OW/P/2020/19443/1 dated November 13, 2020
[55] Reference: SEBI Letter SEBI/HO/MRD2/DDAP/OW/P/2021/1632/1 dated January 20, 2021

iii. Client shall be required to authorize each mandate valid for a single settlement number / settlement date, by way of OTP and PIN/password, both generated at Depositories end.

iv. Prior to executing actual transfer of securities based on details provided by intermediary, Depositories need to match and confirm the same with mandate provided by client as well as client-wise net delivery obligation arising from the trades executed on exchanges, as provided by Clearing Corporation to Depositories for each settlement date.

v. Securities transferred on the basis of mandate provided by client should be credited only to client's trading member pool account.

vi. Intermediary providing this facility have enabled its client to revoke / cancel the mandate provided by them.

vii. Depositories shall take necessary steps to safeguard themselves from any liability arising under Section 16 of Depositories Act, 1996, for losses, if any, to the beneficiary owner on account of providing this facility.

In addition, within the specified timeline, Depositories need to communicate to Stock Brokers/DPs providing this facility to ensure that mandate provided by client adheres to requirement specified in **Annexure 4**.

c) Depository shall ensure they have taken all risk containment measures while permitting intermediaries to provide e-DIS facility and pre-trade authorization/mandate, including cyber-security related measures.

d) Depository shall make necessary amendments to its bye-laws/business rules/operating instruction of Depositories for implementation of above directions.

e) Further, the requirement for Depositories to carry-out authentication based on Password/TPIN, along-with OTP, both generated at Depositories end for each transaction/ e-DIS transfer instruction/pre-trade mandate, shall continue to apply.

2. Implementation:

a. No new intermediary shall be permitted to provide e-DIS / mandate facility, until Depositories ensure necessary checks and balances are in place, including implementation of above directions.

b. Further, for existing Intermediaries to continue providing e-DIS/mandate facility, Depositories need to ensure that necessary checks and balances are in place, including implementation of the above directions

3. Depositories are further advised to place before their respective Boards the measures taken by the Depository towards incorporating the directions as stated above. Further, a compliance report, along-with comments of the board of

Depository, with regard to implementation of abovementioned SEBI directions shall be submitted to SEBI.

1.14 Nomination for Eligible Trading and Demat Accounts[56]

1.14.1 Section 72 of Companies Act, 2013 provides for nomination by a holder of securities.

1.14.2 Investors opening new demat account(s) on or after October 01, 2021, shall have the choice of providing nomination or opting out nomination, as follows;

a. The format for nomination form is given in **Annexure 5**

b. Opt out of nomination through 'Declaration Form', as provided in **Annexure 6**

These forms at Annexure 5 or 6, would also be applicable for any subsequent change/withdrawal of nomination.

1.14.3 In this regard, DPs shall activate new Demat accounts from October 01, 2021, only upon receipt of above formats.

1.14.4 The nomination and Declaration form shall be signed under wet signature of the account holder(s) and witness shall not be required. However, if the account holder(s) affixes thumb impression (instead of wet signature), then witness signature shall be required in the forms.

1.14.5 The on-line nomination and Declaration form may also be signed using e-Sign facility and in that case witness will not be required.

1.14.6 DPs shall ensure that adequate systems are in place including for providing for eSign facility and also take all necessary steps to maintain confidentiality and safety of client records.

1.14.7 Further, all existing eligible demat account holders shall provide choice of nomination as per the option given in **Para 1.14.2** above, on or before September 30, 2023[57], failing which the trading accounts shall be frozen for trading and demat account shall be frozen for debits.

1.14.8 DPs shall encourage their clients to update 'choice of nomination' by sending a communication on fortnightly basis by way of emails and SMS to all such demat accounts wherein the 'choice of nomination' is not captured. The communication shall provide guidance through which the client can provide his/her 'choice of nomination'.

1.14.9 On the basis of representations received from various stakeholders, it has been decided that[58]:

---

[56] Reference: SEBI Circular SEBI/HO/MIRSD/RTAMB/CIR/P/2021/601 dated July 23, 2021

[57] Reference: SEBI Circular SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2023/42 dated March 27, 2023

[58] Reference: SEBI Circular SEBI/HO/MIRSD/MIRSD_RTAMB/P/CIR/2022/23 dated February 24, 2022

a. Requirement mentioned at **Para 1.14.2** read with **Para 1.14.7** w.r.t. re-submission of nomination details shall be optional for the existing investors who have already provided the nomination details prior to July 23, 2021

b. existing investors who have not submitted nomination details and intend to submit their nomination or opt out of nomination (not to nominate any one) may also be allowed to do so by way of two factor authentication (2FA) login on the internet trading platform for Depository Participants providing such services.

1.15 Transmission of shares[59]

The depositories may permit upto three nominees with respect to a demat account.

1.16 Simplification of procedure and standardization of formats of documents for transmission of securities[60]

1.16.1 SEBI has reviewed the process being followed by the Registrars to an Issue and Share Transfer Agents (**"RTAs"**) and the Depositories/ Issuer companies for effecting transmission of securities.

1.16.2 As an on-going measure to enhance ease of dealing in securities markets and with a view to make the transmission process more efficient and investor friendly, the procedure for transmission of securities has been further simplified vide the Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) (Fourth Amendment) Regulations, 2022 **("LODR Amendment Regulations**") Gazette Notification no. SEBI/LAD-NRO/GN/2022/80 dated April 25th, 2022).

1.16.3 The LODR Amendment Regulations has inter alia enhanced the monetary limits for simplified documentation for transmission of securities, allowed 'Legal Heirship Certificate or equivalent certificate' as one of the acceptable documents for transmission and provided clarification regarding acceptability of Will as one of the valid documents for transmission of securities. Pursuant to the notification of the LODR Amendment Regulations, the formats of various documents which are required to be furnished for the processing of transmission of securities are being specified hereunder.

1.16.4 For ease of reference, a ready reckoner listing out the documents required for transmission of securities, in case of demise of the sole holder, is provided below:

Documents Required For Transmission Of Securities

[59] Reference: SEBI Letter MRD//DP/OW/23881/2015 dated August 24, 2015 regarding multiple nominations in demat accounts

[60] Reference: SEBI Circular SEBI/HO/MIRSD/MIRSD_RTAMB/P/CIR/2022/65 dated May 18, 2022

Sr. No.	Documents required for transmission	Sole holder deceased& nomination registered	Sole holder deceased & nomination not registered
1.	Transmission Request Form	Annexure 7	Annexure 7
2.	Original death certificate or Copy of death certificate attested by a notary public/gazette officer or copy of the death certificate attested by the nominee(s)/claimant(s)/legal heir(s), subject to verification with original by the RTA/Listed Issuer	✓	✓
3.	Self-attested copy of Permanent Account Number Card of the nominee(s)/claimant(s)/legal heir(s) issued by the Income Tax Department	✓	✓
4.	Copy of Birth Certificate (in case the nominee/claimant/legal heir is a minor)	✓	✓
5.	KYC* of the Claimant Guardian (in case of nominee /claimant being a minor / of unsound mind). *If not KYC compliant	✓	✓
6.	Original security certificate(s)	✓	✓
7.	Notarized affidavit from all legal heir(s) made on non-judicial stamp paper of appropriate value on identity and claim of ownership, as per the format provided in Annexure 8	**NA**	✓
8.	In case the legal heir(s)/claimant(s) are named in the Succession Certificate or Probate of Will or Will or Letter of Administration or Legal Heirship Certificate (or its equivalent certificate), instead of the document mentioned in point 7 above, an Affidavit from such legal heir(s)/claimant(s), duly Notarised and as per the format provided in Annexure 8, shall be sufficient.	**NA**	✓

9.	Copy of any of the following documents: (a) Succession certificate; or (b) Probate of Will; or (c) Will, along with a notarized indemnity bond from the legal heir(s)/claimant(s) to whom the securities are transmitted, as per the format specified provided in **Annexure 9**; or (d) Letter of Administration; or (e) Court Decree; or (f) Legal Heirship Certificate or its equivalent, along with i. a notarized indemnity bond from the legal heir (s)/claimant(s) to whom the securities are transmitted, as per the format specified provided in **Annexure 9**; and ii. No Objection from all the non-claimants, duly attested by a notary public or by a gazetted officer as per the format provided in **Annexure 10**. The document should be Attested by the legal heir(s)/claimant(s) subject to verification with the original or duly attested by a notary public or by a Gazetted officer.	**NA**	✓ ✓
10.	For cases where the value of securities is up to rupees five lakhs per listed entity as on the date of submission of complete documentation in case of securities held in physical mode and up to rupees fifteen lakhs per beneficial owner in case of securities held in dematerialized mode, instead of and where the documents mentioned in point 9 above are not available, the following documents may be submitted; (i) no objection certificate from all legal heirs(s), as per the format provided in **Annexure 10**, or copy of family settlement	NA	✓

	deed executed by all the legal heirs, duly attested by a notary public or by a gazetted officer; and (ii) notarized indemnity bond made on non-judicial stamp paper of appropriate value, indemnifying the Share Transfer Agent/listed entity, in as per the format provided in **Annexure 9**.		

The Operational Guidelines for processing investor's service request for the purpose of transmission of securities is provided as follows:

a. The RTA/Issuer Companies shall use the format for:

(i) Transmission Request Form ("TRF") – (**Annexure 7**)**,**

(ii) Affidavit made on non-judicial stamp paper, to the effect of identification and claim of legal ownership to the securities ("Affidavit") – (**Annexure 8**)**,**

(iii) Indemnity Bond made on appropriate non-judicial stamp paper of appropriate value("Indemnity Bond") – **Annexure 9**)**,** and

(iv) No objection certificate from all legal heirs who do not object to such transmission ("NOC") – (**Annexure 10**)**.**

b. After verifying and processing the request, the RTA / Issuer Companies shall intimate the claimant(s) about its execution as may be applicable, by way of issuing a Letter of Confirmation (Format at **Annexure 11**).

c. The RTA shall retain the physical securities as per the existing procedure and deface the certificate with a stamp "Letter of Confirmation Issued" on the face / reverse of the certificate, subsequent to processing of service request

d. The Letter of Confirmation shall, inter-alia, contain details of folio and demat account number (if available) of the claimant(s).

e. The Letter of Confirmation shall be sent by the RTA / Issuer Companies through Registered / Speed Post to the claimant(s) and a digitally signed copy of the Letter of Confirmation shall be sent by the RTA/Issuer Companies to the claimant(s) through e-mail.

f. Within 120 days of issue of the Letter of Confirmation, the claimant(s) shall submit the demat request, along with the original Letter of Confirmation or the digitally signed copy of the Letter of Confirmation, to the Depository Participant ("DP").

g. DP shall generate the demat request on the basis of the Letter of Confirmation and forward the same to the Issuer Company / RTA for processing the demat request.

h. In case of the securities which are required to be locked in, the RTA while approving / confirming the demat request, shall incorporate / intimate the Depository about the lock-in and its period.

i. The RTA / Issuer Companies shall issue a reminder after the end of 45 days and 90 days from the date of issuance of the Letter of Confirmation, informing the claimant(s) to submit the demat request as above, in case no such request has been received by the RTA / Issuer Company.

In case of non-receipt of demat request from the claimant(s) within 120 days of the date of issue of the Letter of Confirmation, the securities shall be credited to Suspense Escrow Demat Account of the Issuer Company.

1.16.5 The format of the form to be filed by nominee/claimant/legal heir while requesting transmission of securities is provided under **Annexure 7**

1.16.6 The revised documentation requirements in case of transmission of securities are specified below:

1.16.6.1 Where the securities are held in a single name with a nomination, nominee shall be informed about the procedure to be followed for the claim on the receipt of the intimation of death of the security holder.

1.16.6.2 Where the securities are held in single name with a nomination, the following documents shall be submitted:

(a) duly signed transmission request form by the nominee;

(b) original death certificate or copy of death certificate attested by the nominee subject to verification with the original or copy of death certificate duly attested by a notary public or by a gazetted officer;

(c) self-attested copy of the Permanent Account Number card of the nominee, issued by the Income Tax Department.

1.16.6.3 where the securities are held in single name without nomination, the following documents shall be submitted:

(a) duly signed transmission request form by the legal heir(s)/claimant(s);

(b) original death certificate or copy of death certificate attested by the legal heir(s)/claimant(s) subject to verification with the original or copy of death certificate duly attested by a notary public or by a gazetted officer;

(c) self-attested copy of the PAN card of the legal heir(s)/claimant(s), issued by the Income Tax Department;

(d) a notarized affidavit, in the format provided in **Annexure 8** from all legal heir(s) made on non-judicial stamp paper of appropriate value,

to the effect of identification and claim of legal ownership to the securities.

However, in case the legal heir(s)/claimant(s) are named in any of the documents for transmission of securities as mentioned in S. No. 8 of Para 1.16.4, an affidavit from such legal heir(s)/claimant(s) alone shall be sufficient;

(e) a copy of other requisite documents for transmission of securities as may be applicable as per Para 1.16.4, attested by the legal heir(s)/claimant(s) subject to verification with the original or duly attested by a notary public or by a gazetted officer:

1.16.6.4 In cases where a copy of Will is submitted as may be applicable in terms of Indian Succession Act, 1925 (39 of 1925) the same shall be accompanied with a notarized indemnity bond from the claimant (appropriate beneficiary of the Will) to whom the securities are transmitted, in the format provided in **Annexure 9**.

1.16.6.5 In cases where a copy of Legal Heirship Certificate or its equivalent certificate issued by a competent Government Authority is submitted, the same shall be accompanied with:

i. a notarized indemnity bond from the legal heir(s) /claimant(s) to whom the securities are transmitted, in the format provided in **Annexure 9**.

ii. No Objection from all non-claimants (remaining legal heirs), stating that they have relinquished their rights to the claim for transmission of securities, duly attested by a notary public or by a gazetted officer, in the format provided in **Annexure 10**.

1.16.6.6 For value of securities up to rupees five lakhs per listed entity in case of securities held in physical mode, and up to rupees fifteen lakhs per beneficial owner in case of securities held in dematerialized mode, as on date of application by the claimant, and where the documents mentioned in S. No. 9 of Para 1.16.4, are not available, the legal heir(s) /claimant(s) may submit the following documents:

i. a notarized indemnity bond made on non-judicial stamp paper of appropriate value in the format provided in **Annexure 9**, indemnifying the Share Transfer Agent/ listed entity;

ii. no objection certificate from all legal heir(s) stating that they do not object to such transmission in the format provided in **Annexure 10** or copy of family settlement deed executed by all the legal heirs, duly attested by a notary public or by a gazetted officer; and

The listed entity may, at its discretion, enhance the value of securities from the threshold limit of rupees five lakhs, in case of securities held in physical mode.

1.16.7 For transmission of securities to the surviving joint holder(s), RTAs shall comply with clause 23 of Table F in Schedule 1 read with Section 56(2)& 56(4)(c) of the Companies Act, 2013, and transmit securities in favour of surviving Joint holder(s), in the event of demise of one or more joint holder(s), provided that there is nothing contrary in the Articles of Association of the company.

1.16.8 The common norms stipulated in **Para 1.1.4** shall be applicable for transmission service requests.

1.16.9 In case the securities were held by the deceased holder in a single name and in physical mode, then after verifying and processing the documents submitted for transmission of securities, the RTAs/ Issuer companies shall intimate the claimant(s) about its execution as may be applicable, within 30 days of the receipt of such request, by way of issuing a Letter of Confirmation in the format provided in **Annexure 11**.

1.17 Mode of Operation and Transmission of Securities in Joint Demat Accounts[61]

1.17.1 In order to streamline the process of operation and make the transmission of securities more efficient and investor friendly in demat accounts with joint holding, it has been decided to incorporate the following changes:

Mode of Operation

i. The account holders having joint accounts may opt for any of the following modes of operation of the account by submitting a specific instruction at the time of demat account opening or at a later date duly signed by all account holders:

- ***a.*** 'Jointly'
- ***b.*** 'Anyone of the holders or survivor(s)'

ii. The mode of operation mentioned at **Para 1.17.1 (i)** (a) and (b) above may be used only for the following transactions:

- ***a.*** Transfer of securities including Inter-Depository Transfer.
- ***b.*** Pledge / hypothecation / margin pledge / margin re-pledge (creation, closure and invocation, and confirmation thereof, as applicable).
- ***c.*** Freeze/unfreeze account and/or the ISIN and/or specific number of securities

However, for all other transactions at joint account level, the mode of operation shall be as mentioned at **Para 1.17.1 (i)** (a) above.

iii. All existing joint account holders may also opt for one of the modes of operation mentioned at **Para 1.17.1 (i)**.

iv. Where the account holders have opted for operation by any one holder, the instructions above should be duly signed by any one of the holders of the joint

[61] Reference: SEBI Letter MRD2/DDAP/OW/P/2021/8568/1 dated April 09, 2021

account.

v. With regard to all transactions undertaken in the client demat account, signature of one of the client account holders as per the mandate of operation given by the joint account holders shall discharge the Participant in full vis-à-vis all account holders.

vi. Each client account holder in the demat account is jointly and severally liable towards the Participant for all the commitments entered into by himself/herself or by any other client account holder or authorized representative (within the limits of power).

vii. Any account holder may opt out from the facility as mentioned at **Para 1.17.1 (i)** by giving signed written request to the Participant and upon receipt of such a request by Participant, the Participant shall change the mode of operation to 'jointly'.

viii. In case of a joint account, all communications shall be sent to the first holder and shall be deemed to have been duly sent to all client account holders. Participant shall give an option to all joint account holders that communication will be sent to all joint account holders in electronic mode, if desired by account holders.

ix. This arrangement of mode of operation shall not expire on the death of one of the client holders, if the surviving account holders choose the option to continue with the same account by deletion of deceased's name. The surviving members have to inform the Participant about the death of account holder with requisite document within one year. If the surviving account holder(s) fails to report the death of deceased joint holder within one year of the date of demise, a new demat account shall be opened by the surviving account holder(s) to execute transmission as per the existing procedure. Depository shall retain an audit trail in the system to record the deletion of the client holders due to death.

x. In the event of the death of any of the joint holders, the liability of the Participant shall be discharged provided the Participant:

a. Exercises due care and caution in establishing the identity of the survivor(s) and the fact of death of the joint demat account holder, through appropriate documentary evidence;

b. Reasonably satisfies itself that there is no order from any competent court brought to its notice restraining the transmission of the deceased's securities; and

c. Makes it clear to the survivor(s) that he/she would be receiving the securities of the deceased as a trustee of the legal heirs of the deceased demat account holder.

1.18 Execution of Power of Attorney (PoA) by the Client in favour of the Stock Broker/ Stock

Broker and Depository Participant[62]

Kindly refer para titled 'Execution of Power of Attorney (PoA) by the Client in favour of the Stock Broker/ Stock Broker and Depository Participant' of SEBI Circular SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2023/71 dated May 17, 2023 (Master circular for Stock Brokers)

1.19 ***Execution of 'Demat Debit and Pledge Instruction' (DDPI) for transfer of securities towards deliveries/ settlement obligations and pledging/ re-pledging of securities***[63]

Kindly refer para titled 'Execution of Demat Debit and Pledge Instruction (DDPI) for transfer of securities towards deliveries / settlement obligations and pledging / re-pledging of securities' of SEBI Circular SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2023/71 dated May 17, 2023 (Master circular for Stock Brokers)

1.20 ***SMS alerts for demat accounts operated by Power of Attorney***[64]

Subscription to SMS Alert facility for depository accounts operated through Power of Attorney (POA) would be mandatory except in case of accounts held by non-individuals, foreign nationals, and NRIs.

1.21 ***Exemption from sending quarterly statements of transactions by depository participants (DPs) to clients in respect of demat accounts with no transactions and no security balances***[65]

1.21.1 SEBI has provided exemption to DPs from sending quarterly transaction statements to the clients in respect of demat accounts with no transactions and no security balances subject to the following conditions:

1.21.1.1 Client is informed in advance that it will not be receiving Transaction Statements for such accounts till there are any transactions or security holdings in the demat account.

1.21.1.2 KYC and PAN requirement in respect of all such depository accounts are complied.

1.21.1.3 No Annual Maintenance Charges are levied for such an account.

1.21.1.4 Information which is required to be disseminated by Participants by way of a note in the Transaction Statements will be required to be communicated to such

---

[62] Reference: SEBI Circular CIR/MRD/DMS/13/2010 dated April 23, 2010, CIR/MRD/DMS/28/2010 dated August 31, 2010 and SEBI/HO/MIRSD/DOP/CIR/P/2020/158 dated August 27, 2020

[63] Reference: SEBI Circular SEBI/HO/MIRSD/DoP/P/CIR/2022/44 dated April 04, 2022 and SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2022/137 dated October 06, 2022

[64] Reference: SEBI Letter SEBI/MRD/DEP/VM/169784 /09 dated July 15, 2009

[65] Reference: SEBI Letter MRD/CDSL/VM/155773/2009 dated February 27, 2009, MRD/DoP/NSDL/VM/168994 /2009 dated July 07, 2009 and MRD/CDSL/VM/168989 /2009 dated July 07, 2009

Clients separately.

1.21.1.5 The Internal Auditor of the Participant shall comment in its internal audit report on compliance of the aforesaid requirements.

1.21.2 Further, depository may like to consider whether, DPs should send a consolidated Transaction Statements for the entire financial year in case of the BOs to whom quarterly Transaction Statements are not sent.

1.22 Discontinuation of sending transaction statements by depository participants to clients[66]

SEBI has allowed discontinuation of sending transaction statements by depository participants to clients subject to the following conditions:

1.22.1 Transaction statements were returned undelivered on three consecutive occasions.

1.22.2 The DP maintains proof that the transaction statements were returned undelivered.

1.22.3 The transaction statements were returned undelivered for the reasons which clearly establish that the client no longer resides at the given address (i.e. party shifted, etc.) and not for other reasons (i.e. residence/office closed, address incorrect, address incomplete, etc.).

1.22.4 The DP informs such clients through alternative means (such as outbound call, SMS or email) that their transaction statements are returned undelivered and they need to communicate the proper (new) address.

1.22.5 The DP ensures that on receipt of request for address modification from the client as per the stipulated procedure, the dispatch of transaction statements is immediately started. Further, the DP ensures that transaction statements that were not delivered and dispatched due to discontinuation are also dispatched immediately without any additional cost to the clients.

1.23 Exemption to Depository Participants (DPs) from providing hard copies of transaction statements to BOs[67]

DPs are permitted to provide transaction statements and other documents to the BOs under Digital signature, as governed under the Information Technology Act, 2000, subject to the DP entering into a legally enforceable arrangement with the BO for the said purpose. While such practice in the aforesaid manner shall be deemed to be in compliance of the provisions of the Regulation 60 of Securities and Exchange Board of India (Depositories & Participants) Regulations, 2018 ("**DP Regulations**"); if the BO is still desirous of receiving statements in hard copy, DPs shall be duty bound to provide the same.

1.24 Consolidated Account Statement (CAS) for all securities assets[68]

[66] Reference: SEBI Letter MRD/NSDL/VM/158886 /2009 dated March 30, 2009
[67] Reference: SEBI Circular MRD/DoP/Dep/Cir-27/2004 dated August 16, 2004
[68] Reference: SEBI Circular CIR/MRD/DP/31/2014 dated November 12, 2014

1.24.1 It has been decided to enable a single consolidated view of all the investments of an investor in Mutual Funds (MF) and securities held in demat form with the Depositories.

1.24.2 The Depositories and the Asset Management Companies (AMCs)/ MF-RTAs shall put in place systems to facilitate generation and dispatch of single Consolidated Account Statements (CAS) for investors having MF investments and holding demat accounts. AMCs/ RTAs shall share the requisite information with the Depositories on monthly basis to enable generation of CAS.

1.24.3 Consolidation of account statement shall be done on the basis of PAN. In case of multiple holding, it shall be PAN of the first holder and pattern of holding. Based on the PANs provided by the AMCs/MF-RTAs, the Depositories shall match their PAN database to determine the common PANs and allocate the PANs among themselves for the purpose of sending CAS. For PANs which are common between depositories and AMCs, the Depositories shall send the CAS. In other cases (i.e. PANs with no demat account and only MF units holding), the AMCs/ MF-RTAs shall continue to send the CAS to their unit holders as is being done presently in compliance with the Regulation 36(4) of the Securities and Exchange Board of India (Mutual Funds) Regulations, 1996 ("**Mutual Fund Regulations**").

1.24.4 In case investors have multiple accounts across the two depositories, the depository having the demat account which has been opened earlier shall be the default depository which will consolidate details across depositories and MF investments and dispatch the CAS to the investor. However, option shall be given to the demat account holder by the default depository to choose the depository through which the investor wishes to receive the CAS.

1.24.5 The CAS shall be generated on a monthly basis. The AMCs /MF-RTAs shall provide the data with respect to the common PANs to the depositories within three days from the month end. The depositories shall then consolidate and dispatch the CAS within ten days from the month end.

1.24.6 Where statements are presently being dispatched by email either by the Mutual Funds or by the Depositories, CAS shall be sent through email. However, where an investor does not wish to receive CAS through email, option shall be given to the investor to receive the CAS in physical form at the address registered in the Depository system.

1.24.7 A proper grievance redressal mechanism shall be put in place by the depositories and the AMCs/MF-RTAs which shall also be communicated to the investors through CAS. AMCs/MF-RTAs would be accountable for the authenticity of the information provided through CAS in respect of MF investments and timely sharing of such information with Depositories. The Depositories would be responsible for the timely dispatch of CAS to the investors serviced by them and

the demat account information.

1.24.8 The depositories and the AMCs/ MF-RTAs shall ensure data integrity and confidentiality in respect of the shared information. The depositories shall utilise the shared data only for the purpose of providing CAS and shall not share the same with their DPs. Where Depositories are required to share such information with unregulated entities like third party printers, the depositories shall enter into necessary data confidentiality agreements with them.

1.24.9 The CAS shall be implemented from the month of March 2015 with respect to the transactions carried out during the month of February 2015.

1.24.10 If an investor does not wish to receive CAS, an option shall be given to the investor to indicate negative consent. Depositories shall accordingly inform investors in their statements from the month of January 2015 about the facility of CAS and give them information on how to opt out of the facility if they do not wish to avail it.

1.24.11 Where such an option is exercised, the concerned depository shall inform the AMC/MF-RTA accordingly and the data with respect to the said investor shall not be shared by the AMC/MF-RTA with the depository.

1.24.12 If there is any transaction in any of the demat accounts of the investor or in any of his mutual fund folios, then CAS shall be sent to that investor on monthly basis. In case there is no transaction in any of the mutual fund folios and demat accounts then CAS with holding details shall be sent to the investor on half yearly basis. However, in case of demat accounts with nil balance and no transactions in securities and in mutual fund folios, the requirement to send physical statement shall be applicable as specified under **Para 1.8.5** and **Para 1.8.6**.

1.24.13 Further, the holding statement dispatched by the DPs to their BOs with respect to the dormant demat accounts with balances shall also be dispatched half-yearly.

1.24.14 The dispatch of CAS by the depositories to BOs would constitute compliance by the Depository Participants with requirement under Regulation 60 of DP Regulations, to provide statements of account to the BOs as also compliance by the MFs with the requirement under Regulation 36(4) of the Mutual Funds Regulations.

1.25 Generation and Dispatch of Consolidated Account Statement[69]

1.25.1 It is noted that depositories are providing CAS to all investors having a demat account and mutual fund holdings in statement of account (SOA) form only. Further, in scenarios where investor is having mutual fund holdings in demat form or having only demat account with no mutual fund holdings, no consolidation is happening across depositories and depositories are providing separate holding statements for

[69] Reference: SEBI Letter SEBI/HO/MRD/SEC-2/P/OW/2023/00001730411 dated April 28, 2023

themselves.

1.25.2 In this regard, it is felt that extending the requirement of generation and dispatch of CAS to abovementioned scenarios will truly enable a single consolidated view of all the investments of investor in mutual fund and securities held in demat form with the depositories.

1.25.3 In view of the above, depositories are advised to coordinate with each other so as to provide for generation and dispatch of CAS for the above mentioned scenarios.

1.25.4 Further, all the other provisions and modalities with regards to generation and dispatch of CAS will remain the same as prescribed in **Para 1.24** above.

1.26 Redressal of investor grievances through SEBI Complaints Redress System (SCORES) platform[70] & Procedure for filing and redressal of investor grievances using SCORES[71]

Kindly refer SEBI Circular SEBI/HO/OIAE/IGRD/P/CIR/202 dated November 07, 2022 (Master Circular on the redressal of investor grievances through the SEBI Complaints Redress System (SCORES) platform)

1.27 Framework for the process of accreditation of investors for the purpose of Innovators Growth Platform[72]

Kindly refer para titled 'Framework for the process of recognition of investors for the purpose of Innovators Growth Platform' of SEBI Circular SEBI/HO/CFD/PoD-2/P/CIR/2023/00094 dated June 21, 2023 (Master Circular for Issue of Capital and Disclosure Requirements)

1.28 Common Application Form for Foreign Portfolio Investors[73]

Kindly refer para titled 'Guidance for Processing of FPI applications by DDPs' of SEBI Circular SEBI/HO/AFD-2/CIR/P/2022/175 dated December 19, 2022 (Master Circular for Foreign Portfolio Investors, Designated Depository Participants and Eligible Foreign Investors)

[70] Reference: SEBI Circular CIR/OIAE/1/2014 dated December 18, 2014
[71] Reference: SEBI Circular SEBI/HO/OIAE/IGRD/CIR/P/2018/58 dated March 26, 2018
[72] Reference: SEBI Circular SEBI/HO/CFD/DIL2/CIR/P/2019/67 dated May 22, 2019
[73] Reference: SEBI Circular IMD/FPI&C/CIR/P/2020/022 dated February 04, 2020

Section 2: Depository Participants Related

2.1 *Online Registration Mechanism for Securities Market Intermediaries*[74]

Kindly refer para titled 'Online Registration Mechanism for Securities Market Intermediaries' of SEBI Circular SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2023/71 dated May 17, 2023 (Master circular for Stock Brokers)

2.2 *Supervision of branches of DPs*[75]

2.2.1 To ensure compliance with Regulation 63 of the DP Regulations, and Clause 19 of the Code of Conduct for Participants contained in the Third Schedule to the DP Regulations the DP shall ensure that it has satisfactory internal control procedure in place, inclusive of their branch offices. DPs are therefore required in terms of these provisions to put in place appropriate mechanisms to ensure that their branches are carrying on the operations in compliance with the applicable regulations, bye-laws, etc. DPs are also required to put in place suitable internal control systems to ensure that all branches exercise due diligence in opening accounts, complying with KYC requirements, in ensuring systems safety in complying with client instructions, manner of uploading client instructions, in verifying signatures and maintaining client records, etc. DPs shall also ensure that the branches are suitably integrated.

2.2.2 Depositories shall examine the adequacy of the above mechanisms during their inspections of DPs. The Depositories shall also carry out surprise inspections/ checks of the DP branches apart from the regular inspection of the DPs. Depositories shall also put in place appropriate mechanisms for monitoring opening of branches by DPs.

2.3 *Incentivisation to Depositories Participants (DPs)*[76]

2.3.1 In order to compensate the DPs towards the cost of opening and maintaining Basic Services Demat Accounts (BSDA), the depositories shall pay an incentive of Rs. 100/- for every new BSDA opened by their participants in other than the top 15 cities. The name of the top 15 cities is given in following table:

Top 15 Cities

Sr. No.	Name of the City
1.	MUMBAI
2.	DELHI
3.	AHMEDABAD

[74] Reference: SEBI Circular SEBI/HO/MIRSD/MIRSD1/CIR/P/2017/38 dated May 02, 2017
[75] Reference: SEBI Circular MIRSD/DPS-III/Cir-9/07 dated July 3, 2007
[76] Reference: SEBI Circular CIR/MRD/DP/18/2015 dated December 09, 2015

4.	BANGALORE
5.	CHENNAI
6.	PUNE
7.	KOLKATA
8.	THANE
9.	HYDERABAD
10.	SURAT
11.	JAIPUR
12.	VADODARA
13.	SECUNDARABAD
14.	RAJKOT
15.	INDORE

2.3.2 The incentive shall be provided at the end of the financial year only with respect to the new BSDA opened during the financial year and which displayed at least one credit in the account during the Financial Year.

2.3.3 Further to the above, in order to incentivize the DPs to promote holdings in the BSDA, the depositories may pay an amount of Rs. 2 per folio per ISIN to the respective depository participant (DP), in respect of the ISIN positions held in Basic Service Demat Accounts (BSDA). This incentive may be provided with respect to all the BSDA in the depository system.

2.3.4 The reimbursement to DPs shall be made on an annual basis at the end of the financial year. The depositories shall set aside 20% of the incremental revenue received from the Issuers to manage the aforementioned incentive schemes. Any surplus after reimbursement of DPs may be utilized by the depositories to incentivize the DPs for promoting financial inclusion, encouraging investors to hold Mutual Fund Units in demat account and familiarizing the investors on the OFS mechanism, etc.

2.3.5 The incentive scheme may be reviewed after a period of two years.

2.4 Guidelines on Outsourcing of Activities by Intermediaries[77]

2.4.1 SEBI Regulations for various intermediaries require that they shall render at all times high standards of service and exercise due diligence and ensure proper care in their operations.

2.4.2 It has been observed that often the intermediaries resort to outsourcing with a view to reduce costs, and at times, for strategic reasons.

[77] Reference: SEBI Circular CIR/MIRSD/24/2011 dated December 15, 2011

2.4.3 Outsourcing may be defined as the use of one or more than one third party – either within or outside the group - by a registered intermediary to perform the activities associated with services which the intermediary offers.

2.4.4 **Principles for Outsourcing**

The risks associated with outsourcing may be operational risk, reputational risk, legal risk, country risk, strategic risk, exit-strategy risk, counter party risk, concentration and systemic risk. In order to address the concerns arising from the outsourcing of activities by intermediaries based on the principles advocated by the IOSCO and the experience of Indian markets, SEBI had prepared a concept paper on outsourcing of activities related to services offered by intermediaries.

Based on the feedback received on the discussion paper and also discussion held with various intermediaries, stock exchanges and depositories, the principles for outsourcing by intermediaries have been framed. The principles for outsourcing are given below at **Para 2.4.7 to Para 2.4.14.** These principles shall be followed by all intermediaries registered with SEBI.

2.4.5 **Activities that shall not be Outsourced**

The intermediaries desirous of outsourcing their activities shall not, however, outsource their core business activities and compliance functions. A few examples of core business activities may be – execution of orders and monitoring of trading activities of clients in case of stock brokers; dematerialisation of securities in case of depository participants; investment related activities in case of Mutual Funds and Portfolio Managers. Regarding Know Your Client (KYC) requirements, the intermediaries shall comply with the provisions of KRA Regulations and Guidelines issued thereunder from time to time.

2.4.6 **Other Obligations**

i. **Reporting To Financial Intelligence Unit (FIU)** - The intermediaries shall be responsible for reporting of any suspicious transactions / reports to FIU or any other competent authority in respect of activities carried out by the third parties.

ii. **Need for Self-Assessment of existing Outsourcing Arrangements –** In view of the changing business activities and complexities of various financial products, intermediaries shall conduct a self-assessment of their existing outsourcing arrangements within a time bound plan* and bring them in line with the requirements of the guidelines/principles

**not later than six months from the date of issuance of original circular i.e. December 15, 2011*

PRINCIPLES FOR OUTSOURCING FOR INTERMEDIARIES

2.4.7 An intermediary seeking to outsource activities shall have in place a comprehensive policy to guide the assessment of whether and how those activities can be appropriately outsourced. The Board / partners (as the case may be)

{hereinafter referred to as the "the Board"} of the intermediary shall have the responsibility for the outsourcing policy and related overall responsibility for activities undertaken under that policy.

2.4.7.1 The policy shall cover activities or the nature of activities that can be outsourced, the authorities who can approve outsourcing of such activities, and the selection of third party to whom it can be outsourced. For example, an activity shall not be outsourced if it would impair the supervisory authority's right to assess, or its ability to supervise the business of the intermediary. The policy shall be based on an evaluation of risk concentrations, limits on the acceptable overall level of outsourced activities, risks arising from outsourcing multiple activities to the same entity, etc.

2.4.7.2 The Board shall mandate a regular review of outsourcing policy for such activities in the wake of changing business environment. It shall also have overall responsibility for ensuring that all ongoing outsourcing decisions taken by the intermediary and the activities undertaken by the third-party, are in keeping with its outsourcing policy.

2.4.8 The intermediary shall establish a comprehensive outsourcing risk management programme to address the outsourced activities and the relationship with the third party.

2.4.8.1 An intermediary shall make an assessment of outsourcing risk which depends on several factors, including the scope and materiality of the outsourced activity, etc. The factors that could help in considering materiality in a risk management programme include-

2.4.8.1.1 The impact of failure of a third party to adequately perform the activity on the financial, reputational and operational performance of the intermediary and on the investors / clients;

2.4.8.1.2 Ability of the intermediary to cope up with the work, in case of non-performance or failure by a third party by having suitable back-up arrangements;

2.4.8.1.3 Regulatory status of the third party, including its fitness and probity status;

2.4.8.1.4 Situations involving conflict of interest between the intermediary and the third party and the measures put in place by the intermediary to address such potential conflicts, etc.

2.4.8.2 While there shall not be any prohibition on a group entity / associate of the intermediary to act as the third party, systems shall be put in place to have an arm's length distance between the intermediary and the third party in terms of infrastructure, manpower, decision-making, record keeping, etc. for avoidance of potential conflict of interests. Necessary disclosures in this regard shall be made as part of the contractual agreement. It shall be kept in mind that the risk

management practices expected to be adopted by an intermediary while outsourcing to a related party or an associate would be identical to those followed while outsourcing to an unrelated party.

2.4.8.3 The records relating to all activities outsourced shall be preserved centrally so that the same is readily accessible for review by the Board of the intermediary and / or its senior management, as and when needed. Such records shall be regularly updated and may also form part of the corporate governance review by the management of the intermediary.

2.4.8.4 Regular reviews by internal or external auditors of the outsourcing policies, risk management system and requirements of the regulator shall be mandated by the Board wherever felt necessary. The intermediary shall review the financial and operational capabilities of the third party in order to assess its ability to continue to meet its outsourcing obligations.

2.4.9 The intermediary shall ensure that outsourcing arrangements neither diminish its ability to fulfil its obligations to customers and regulators, nor impede effective supervision by the regulators.

2.4.9.1 The intermediary shall be fully liable and accountable for the activities that are being outsourced to the same extent as if the service were provided in-house.

2.4.9.2 Outsourcing arrangements shall not affect the rights of an investor or client against the intermediary in any manner. The intermediary shall be liable to the investors for the loss incurred by them due to the failure of the third party and also be responsible for redressal of the grievances received from investors arising out of activities rendered by the third party.

2.4.9.3 The facilities / premises / data that are involved in carrying out the outsourced activity by the service provider shall be deemed to be those of the registered intermediary. The intermediary itself and Regulator or the persons authorized by it shall have the right to access the same at any point of time.

2.4.9.4 Outsourcing arrangements shall not impair the ability of SEBI/SRO or auditors to exercise its regulatory responsibilities such as supervision/inspection of the intermediary.

2.4.10 The intermediary shall conduct appropriate due diligence in selecting the third party and in monitoring of its performance.

2.4.10.1 It is important that the intermediary exercises due care, skill, and diligence in the selection of the third party to ensure that the third party has the ability and capacity to undertake the provision of the service effectively.

2.4.10.2 The due diligence undertaken by an intermediary shall include assessment of:

2.4.10.2.1 third party's resources and capabilities, including financial soundness, to perform the outsourcing work within the timelines fixed;

2.4.10.2.2 compatibility of the practices and systems of the third party with the intermediary's requirements and objectives;

2.4.10.2.3 market feedback of the prospective third party's business reputation and track record of their services rendered in the past;

2.4.10.2.4 level of concentration of the outsourced arrangements with a single third party; and

2.4.10.2.5 the environment of the foreign country where the third party is located.

2.4.11 Outsourcing relationships shall be governed by written contracts / agreements / terms and conditions (as deemed appropriate) {hereinafter referred to as "contract"} that clearly describe all material aspects of the outsourcing arrangement, including the rights, responsibilities and expectations of the parties to the contract, client confidentiality issues, termination procedures, etc.

2.4.11.1 Outsourcing arrangements shall be governed by a clearly defined and legally binding written contract between the intermediary and each of the third parties, the nature and detail of which shall be appropriate to the materiality of the outsourced activity in relation to the ongoing business of the intermediary.

2.4.11.2 Care shall be taken to ensure that the outsourcing contract:

2.4.11.2.1 clearly defines what activities are going to be outsourced, including appropriate service and performance levels;

2.4.11.2.2 provides for mutual rights, obligations and responsibilities of the intermediary and the third party, including indemnity by the parties;

2.4.11.2.3 provides for the liability of the third party to the intermediary for unsatisfactory performance/other breach of the contract

2.4.11.2.4 provides for the continuous monitoring and assessment by the intermediary of the third party so that any necessary corrective measures can be taken up immediately, i.e., the contract shall enable the intermediary to retain an appropriate level of control over the outsourcing and the right to intervene with appropriate measures to meet legal and regulatory obligations;

2.4.11.2.5 includes, where necessary, conditions of sub-contracting by the third-party, i.e. the contract shall enable intermediary to maintain a similar control over the risks when a third party outsources to further third parties as in the original direct outsourcing;

2.4.11.2.6 has unambiguous confidentiality clauses to ensure protection of proprietary and customer data during the tenure of the contract and also after the expiry of the contract;

2.4.11.2.7 specifies the responsibilities of the third party with respect to the IT security and contingency plans, insurance cover, business continuity and disaster recovery plans, force majeure clause, etc.;

2.4.11.2.8 provides for preservation of the documents and data by third party ;

2.4.11.2.9 provides for the mechanisms to resolve disputes arising from implementation of the outsourcing contract;

2.4.11.2.10 provides for termination of the contract, termination rights, transfer of information and exit strategies;

2.4.11.2.11 addresses additional issues arising from country risks and potential obstacles in exercising oversight and management of the arrangements when intermediary outsources its activities to foreign third party. For example, the contract shall include choice-of-law provisions and agreement covenants and jurisdictional covenants that provide for adjudication of disputes between the parties under the laws of a specific jurisdiction;

2.4.11.2.12 neither prevents nor impedes the intermediary from meeting its respective regulatory obligations, nor the regulator from exercising its regulatory powers; and

2.4.11.2.13 provides for the intermediary and /or the regulator or the persons authorized by it to have the ability to inspect, access all books, records and information relevant to the outsourced activity with the third party.

2.4.12 The intermediary and its third parties shall establish and maintain contingency plans, including a plan for disaster recovery and periodic testing of backup facilities.

2.4.12.1 Specific contingency plans shall be separately developed for each outsourcing arrangement, as is done in individual business lines.

2.4.12.2 An intermediary shall take appropriate steps to assess and address the potential consequence of a business disruption or other problems at the third party level. Notably, it shall consider contingency plans at the third party; co-ordination of contingency plans at both the intermediary and the third party; and contingency plans of the intermediary in the event of non-performance by the third party.

2.4.12.3 To ensure business continuity, robust information technology security is a necessity. A breakdown in the IT capacity may impair the ability of the intermediary to fulfil its obligations to other market participants/clients/regulators and could undermine the privacy interests of its customers, harm the intermediary's reputation, and may ultimately impact on its overall operational risk profile. Intermediaries shall, therefore, seek to ensure that third party maintains appropriate IT security and robust disaster recovery capabilities.

2.4.12.4 Periodic tests of the critical security procedures and systems and review of the backup facilities shall be undertaken by the intermediary to confirm the adequacy of the third party's systems.

2.4.13 The intermediary shall take appropriate steps to require that third parties protect confidential information of both the intermediary and its customers from intentional or inadvertent disclosure to unauthorised persons.

2.4.13.1 An intermediary that engages in outsourcing is expected to take appropriate steps to protect its proprietary and confidential customer information and ensure that it is not misused or misappropriated.

2.4.13.2 The intermediary shall prevail upon the third party to ensure that the employees of the third party have limited access to the data handled and only on a "need to know" basis and the third party shall have adequate checks and balances to ensure the same.

2.4.13.3 In cases where the third party is providing similar services to multiple entities, the intermediary shall ensure that adequate care is taken by the third party to build safeguards for data security and confidentiality.

2.4.14 Potential risks posed where the outsourced activities of multiple intermediaries are concentrated with a limited number of third parties.

2.4.14.1 In instances, where the third party acts as an outsourcing agent for multiple intermediaries, it is the duty of the third party and the intermediary to ensure that strong safeguards are put in place so that there is no co-mingling of information /documents, records and assets.

2.5 *Implementation of the Multilateral Competent Authority Agreement and Foreign Account Tax Compliance Act*[78]

Kindly refer para titled 'Implementation of the Multilateral Competent Authority Agreement and Foreign Account Tax Compliance Act' of SEBI Circular SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2023/71 dated May 17, 2023 (Master circular for Stock Brokers)

2.6 *Interest and Dividend information reporting in case of Custodial Accounts Rule 114G(1)(e) of the Income Tax Rules, 1962*[79]

2.6.1 In terms of Rule 114G(1)(e)(i) of Income Tax Rules, 1962 issued under Section 285BA of Income Tax Act, 1961 following information is required to be reported by reporting financial institution in the case of reportable custodial account: -

(i) the total gross amount of interest, the total gross amount of dividends, and the total gross amount of other income generated with respect to the assets held in the account, in each case paid or credited to the account (or with respect to the account) during the calendar year;

[78] Reference: SEBI Circular CIR/MIRSD/2/2015 dated August 26, 2015

[79] Reference: SEBI Circular CIR/HO/MIRSD/MIRSD2/CIR/P/2017/59 dated June 15, 2017

2.6.2 In respect of the above it has been decided in consultation with Central Board of Direct Taxes, Department of Revenue, Ministry of Finance that:-

2.6.2.1 Depositories shall provide additional field in the depository system to the RTAs whereby the RTAs can incorporate the details of corporate action viz. dividend/interest in rupee terms per unit of the security at the time of setting up of corporate action. Depositories shall make available such information to DPs to enable them to do necessary reporting.

2.6.2.2 The reporting with respect to dividend/interest is to be done by DPs on 'entitlement' basis and not on the basis of actual payment received by the demat account holder.

2.6.2.3 If a demat account is identified as a 'reportable account' during a calendar year by the DP, the reporting under Rule 114G (1) (e) is to be done for the dividend /interest entitlements during the entire calendar year i.e. including the period of the calendar year before identification of such account as a 'reportable account' by the DP.

2.7 *Printing of Grievances Redressal Mechanism on Delivery Instruction Form Book* [80]

To promote investor awareness regarding mechanism for redressing investor grievances, the information placed below shall be printed on the inside back cover of the Delivery Instruction Form (DIF) Book issued by all Depository Participants.

In case you have grievances against a listed company or intermediary registered with SEBI, you should first approach the concerned company or intermediary against whom you have grievance. If you are not satisfied with their response, you may approach SEBI or other regulatory bodies. You can approach SEBI for following type of grievances.	
Listed Companies • Refund / Allotment/ Bonus/ Dividend/ Rights/ Redemption/ Interest • Prelisting offer documents (shares) • Prelisting offer documents (debentures and bonds) • Delisting of Securities • Buyback of Securities • Takeover and Restructuring	**Brokers and stock exchanges** • Stock Brokers • Sub brokers • Portfolio managers • Stock exchanges

[80] Reference: SEBI Circular CIR/MRD/DP/DA/25/2012 dated September 21, 2012

• Corporate Governance and Listing conditions	
Registrar and Transfer Agents	**Other entities** Collective Investment Schemes Debenture Trustees Merchant Bankers Bankers to Issue Credit Rating Agencies Custodian of Securities Foreign Institutional Investors Underwriters Venture Capital Funds KYC Registration Agency(KRA) Alternative Investment Fund
Mutual Funds	
Depository and Depository Participants	
Information to SEBI: • Price Manipulation • Insider trading	

You can file your complaints online at **http://scores.gov.in** or alternately send your complaints to Office of Investor Assistance and Education of SEBI at Mumbai or Regional Offices at the following addresses:

Address of SEBI Offices

- Office of Investor Assistance and Education, SEBI Bhavan, Plot No.C4-A, 'G' Block, Bandra Kurla Complex, Bandra (E), Mumbai 400 051 Tel: 022-26449188 / 26449199 (http://scores.gov.in)
- SEBI, Northern Regional Office, 5th Floor, Bank of Baroda Building, 16, Sansad Marg, New Delhi -110001 Tel: 011-23724001-05 (sebinro@sebi.gov.in)
- SEBI, Eastern Regional Office, L&T Chambers, 3rd Floor, 16, Camac Street, Kolkata - 700 016 Tel: 033-23023000. (sebiero@sebi.gov.in)
- SEBI, Southern Regional Office, 7th Floor, Overseas Towers, 756-L, Anna Salai Chennai 600 0102 Tel: 044-24674000/ 24674150 (sebisro@sebi.gov.in)
- SEBI, Ahmedabad Regional Office, Unit No: 002, Ground Floor, SAKAR I, Near Gandhigram Railway Station, Opp. Nehru Bridge Ashram Road, Ahmedabad - 380 009 Tel : 079-26583633-35 (sebiaro@sebi.gov.in)

For more information visit our website - http://scores.gov.in

2.8 Operationalisation of Central KYC Records Registry (CKYCR)[81]

2.8.1 Government of India has authorized the central Registry of Securitization and Asset Reconstruction and Security interest of India (CERSAI), setup under sub-section (1) of Section 20 of Securitisation and Reconstruction of Financial Assets and Enforcement of Security Interest Act, 2002, to act as, and to perform the functions of, the Central KYC Records Registry under the PML Rules 2005, including receiving, storing, safeguarding and retrieving the KYC records in digital form of a client.

2.8.2 As per the 2015 amendment to Prevention of Money Laundering (Maintenance of Records) Rules, 2005, every reporting entity shall capture the KYC information for sharing with the Central KYC Records Registry in the manner mentioned in the Rules, as per the KYC template for "individuals" finalised by CERSAI.

2.8.3 Accordingly, the KYC template finalised by CERSAI (as and when amended by CERSAI) shall be used by the registered intermediaries as Part I of Account Opening Form (AOF) for individuals. The Revised KYC template for "individuals"[82] and the "Central KYC Registry Operating Guidelines 2016" for uploading KYC records on CKYCR as finalised by CERSAI is available for reference and necessary action.

2.8.4 In this regard, it is clarified that the requirement for Permanent Account Number (PAN) would continue to be mandatory for completing the KYC process.

2.9 Rollout of Legal Entity Template[83]

2.9.1 CKYCR, in its communication no. CKYC/2020/11 dated January 04, 2021 has specified that since CKYCR is fully operational for individual clients, it has been decided to extend CKYCR to Legal Entities (LE) as well. Accordingly, Registered Intermediaries (RIs) shall upload the KYC records of LE accounts opened on or after April 01, 2021 on to CKYCR in terms of Rule 9 (1A) of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005. The LE Template and the Annexure thereof are attached below:

2.9.1.1 LE Template

2.9.1.2 Annexure to LE Template

2.9.2 The LE template is made available by CERSAI in the CKYCR test environment (https://testbed.ckycindia.in/ckyc/index.php) enabling RIs to develop necessary infrastructure.

2.9.3 RIs shall ensure that in case of LE accounts opened prior to April 1, 2021, the KYC records are uploaded on to CKYCR when the updated KYC information is

[81] Reference: SEBI Circular CIR/MIRSD/ 66/2016 dated July 21, 2016
[82] Reference: Central KYC Registry Circular CKYC/2020/01 dated January 10, 2020
[83] Reference: SEBI Circular SEBI/HO/MIRSD/DOP/CIR/P/2021/31 dated March 10, 2021

obtained/received from the client. RIs shall ensure that during such receipt of updated information, the clients' KYC details are migrated to current Client Due Diligence (CDD) standards.

2.9.4 Further, to ensure that all existing KYC records of individual clients are incrementally uploaded on to CKYCR, RIs shall upload the KYC records pertaining to accounts of individuals opened prior to August 01, 2016, as and when updated KYC information is obtained/received from the client.

2.9.5 Where a client, for the purpose of establishing an account based relationship, submits a KYC Identifier to a RI, with an explicit consent to download records from CKYCR, then such RI shall retrieve the KYC records online from CKYCR using the KYC Identifier and the client shall not be required to submit the same KYC records or information or any other additional identification documents or details, unless there is a change in the information of the client as existing in the records of CKYCR.

2.9.6 Once KYC Identifier is generated by CKYCR, the RIs shall ensure that the same is communicated to the individual/legal entity.

2.9.7 The above provisions are not applicable to Foreign Portfolio Investors (FPIs).

2.10 e-KYC Authentication facility under section 11A of the Prevention of Money Laundering Act, 2002 by Entities in the securities market for Resident Investors[84] and Entities permitted to undertake e-KYC Aadhaar Authentication service of UIDAI in Securities Market[85]

2.10.1 SEBI simplified the account opening process for investors vide **Para 2.14.** Further, SEBI vide **Para 1.1.6** issued guidelines for uniform KYC requirements for investors while opening accounts with any intermediary in the securities market.

2.10.2 SEBI vide **Para 1.1.2.1** clarified that the Aadhaar Letter issued by UIDAI shall be admissible as Proof of Address in addition to its being recognized as Proof of Identity.

2.10.3 Subsequently, vide **Para 1.1.1.3 (d)** **and** **Para 1.1.2.1 (j)**, it is clarified that it was decided to accept e-KYC service launched by UIDAI also, as a valid process for KYC verification. The information containing relevant client details and photograph made available from UIDAI as a result of e-KYC process shall be treated as sufficient Proof of identity and Address of the client. Also vide **Para 1.1.3**, it is clarified that the usage of Aadhaar card as issued by the UIDAI is voluntary.

[84] Reference: SEBI Circular SEBI/HO/MIRSD/DOP/CIR/P/2019/123 dated November 05, 2019
[85] Reference: SEBI Circular SEBI/HO/MIRSD/DOP/CIR/P/2020/80 dated May 12, 2020

2.10.4 Hon'ble Supreme Court, in its judgement dated September 26, 2018, had struck down Section 57 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 ("**Aadhaar Act**") as "unconstitutional" which means that no company or private entity can seek Aadhaar identification from clients or investors.

2.10.5 The Aadhaar and Other Laws (Amendment) Ordinance, 2019 was promulgated on March 02, 2019 through which a new Section 11A was inserted in chapter IV of the PMLA. The Aadhaar and Other Laws (Amendment) Act, 2019 was notified in the Gazette of India on July 24, 2019.

2.10.6 The Department of Revenue (DoR), Ministry of Finance issued a circular dated May 09, 2019 on procedure for processing of applications under section 11A of the PMLA), for use of Aadhaar authentication services by entities other than the Banking companies. In terms of the said circular, if the Central Government is satisfied with the recommendations of the Regulator and UIDAI and reporting entity complies with such standards of privacy and security under the Aadhaar Act, and it is necessary and expedient to do so, it may by notification, permit such entity to carry out authentication of the Aadhaar number of clients using e-KYC authentication facility.

2.10.7 The said circular also inter-alia specified that, applications by the concerned entities under Section 11A of the PMLA for use of Aadhaar authentication services shall be filed before the Regulator, who after scrutiny shall forward the applications to UIDAI along with its recommendation. UIDAI shall scrutinize the applications received and send its recommendation to the Department of Revenue for notification under Section 11A of the PMLA. The Central Government, if satisfied with the recommendations of the Regulator and the UIDAI that the applicant fulfils all conditions under Section 11A, may by notification permit such applicant to perform authentication under clause (a) of sub-section (1) of Section 11A. At any point, after issue of such notification, based on a report of the appropriate Regulator or UIDAI or otherwise, if it is found that the reporting entity no longer fulfils the requirements for performing authentication under clause (a) of sub-section (1) of section 11A, the Central Government may withdraw the notification after giving an opportunity to the reporting entity.

2.10.8 Accordingly, entities in the securities market, as may be notified by the Central Government, shall be allowed to undertake Aadhaar Authentication under section 11A of the PMLA. SEBI Registered intermediaries for reasons such as online on-boarding of clients, customer convenience, increased efficiency and reduced time for client on- boarding would prefer to use Aadhaar based e-KYC facility to complete the KYC of the client.

Government of India, DoR, vide Gazette Notification No. G.S.R. 261(E) dated April 22, 2020 has notified nine reporting entities as per the recommendation by UIDAI and SEBI to undertake Aadhaar authentication service of the UIDAI under section 11A of the PMLA. In view of the same, the following entities shall undertake Aadhaar Authentication service of UIDAI subject to compliance of the conditions as laid down in this regard:

a. Bombay Stock Exchange Limited
b. National Securities Depository Limited
c. Central Depository Services (India) Limited
d. CDSL Ventures Limited
e. NSDL Database Management Limited
f. NSE Data and Analytics Limited
g. CAMS Investor Services Private Limited
h. Computer Age Management Services Private Limited
i. National Stock Exchange of India Limited[86]

Note

a. Department of Revenue-Ministry of Finance, Government of India, vide Gazette Notification No. S.O. 3187(E) dated July 13, 2022 has notified 155 reporting entities as sub-KUA to use Aadhaar authentication services of UIDAI under section 11A of the Prevention of Money-laundering Act, 2002. A copy of the same is enclosed here. (Reporting entities as sub-KUA to use Aadhaar authentication services of UIDAI)[87]
The KUAs shall facilitate the onboarding of these entities as sub-KUAs to provide the services of Aadhaar authentication with respect to KYC.

b. Department of Revenue-Ministry of Finance, Government of India, vide Gazette Notification No. S.O. 446 (E) dated January 30, 2023 has notified another 39 reporting entities to use Aadhaar authentication services of UIDAI under section 11A of the Prevention of Money-laundering Act, 2002. A copy of the notification is attached here: Notification[88]

2.10.9 These entities shall get registered with UIDAI as KYC user agency ("KUA") and shall allow SEBI registered intermediaries / mutual fund distributors to undertake Aadhaar Authentication of their clients for the purpose of KYC through them.

2.10.10 The SEBI registered intermediaries/mutual fund distributors, who want to undertake Aadhaar authentication services through KUAs, shall enter into an

[86] Reference: SEBI Circular SEBI/HO/MIRSD/DOP/CIR/P/2020/167 dated September 08, 2020
[87] Reference: SEBI Circular SEBI/HO/MIRSD/SEC-5/P/CIR/2022/99 dated July 20, 2022
[88] Reference: SEBI Circular SEBI/HO/MIRSD/SEC-5/P/CIR/2023/0026 dated February 08, 2023

agreement with any one KUA and get themselves registered with UIDAI as sub-KUAs. The agreement in this regard shall be as may be prescribed by UIDAI.

2.10.11 Upon notification by the Central Government / registration with UIDAI, the KUAs and sub-KUAs shall adopt the following process for Aadhaar e-KYC of investors (resident) in the securities market and as may be prescribed by UIDAI from time to time.

2.10.11.1 **<u>Online Portal based Investor (Resident) e-KYC Process (Aadhaar as an OVD)</u>**

2.10.11.1.1 Investor visits portal of KUA or the SEBI registered intermediary which is also a Sub-KUA to open account/invest through intermediary.

2.10.11.1.2 For Aadhaar e-KYC, investor is redirected to KUA portal. Investor enters the Aadhaar Number or Virtual Id and provides consent on KUA portal. Adequate controls shall be in place to ensure that Aadhaar Number is not stored anywhere by the Sub-KUA or KUA.

2.10.11.1.3 Investor will receive OTP in mobile number registered with Aadhaar. Investor enters the OTP sent by UIDAI on KUA portal for Aadhaar e-KYC.

2.10.11.1.4 KUA will receive the e-KYC details from UIDAI upon successful Aadhaar authentication which will be further forwarded to Sub-KUA in encrypted format (using KUAs own encryption key) and will be displayed to the investor on portal. Sharing of e-KYC data by the KUA with Sub-KUA may be allowed under Regulation 16(2) of Aadhaar (Authentication) Regulation, 2016. Sub-KUA shall clearly specify the name of the KUA and Sub- KUA, and details of sharing of data among KUA and Sub-KUA while capturing investor consent.

2.10.11.1.5 Investor will fill the additional detail as required under KYC format.

2.10.11.1.6 SEBI registered Intermediary will upload additional KYC details to the KUA.

2.10.11.2 **<u>Assisted Investor (Resident) e-KYC process (Aadhaar as an OVD)</u>**

2.10.11.2.1 Investor approaches any of the SEBI Registered Entity/ Sub-KUAs i.e. Mutual Fund Distributors or appointed persons for e-KYC through Aadhaar.

2.10.11.2.2 SEBI registered entities (Sub-KUAs) will perform e-KYC using registered / Whitelisted devices with KUAs.

2.10.11.2.3 KUA will ensure that all devices and device operators of Sub-KUA are registered / whitelisted devices with KUA.

2.10.11.2.4 Investor will enter Aadhaar No. or Virtual Id and provides consent on the registered device.

2.10.11.2.5 Investor provides biometric on the registered device.

2.10.11.2.6 SEBI registered intermediary (Sub-KUA) fetches the e-KYC details through the KUA from UIDAI which will be displayed to the investor on the registered device.

2.10.11.2.7 Investor will also provide the additional detail as required.

2.10.12 The KUA/ sub-KUA while performing the Aadhaar authentication shall also comply with the following:

2.10.12.1 For sharing of e-KYC data with Sub-KUA under Regulation 16(2) of Aadhaar (Authentication) Regulations, 2016, KUA shall obtain special permission from UIDAI by submitting an application in this regard. Such permissible sharing of e- KYC details by KUA can be allowed with their associated Sub-KUAs only.

2.10.12.2 KUA shall not share UIDAI digitally signed e-KYC data with other KUAs. However, KUAs may share data after digitally signing it using their own signature for internal working of the system.

2.10.12.3 e-KYC data received as response upon successful Aadhaar authentication from UIDAI will be stored by KUA and Sub-KUA in the manner prescribed by Aadhaar Act/Regulations and circulars issued by UIDAI time to time.

2.10.12.4 KUA/Sub-KUA shall not store Aadhaar number in their database under any circumstances. It shall be ensured that Aadhaar number is captured only using UIDAI`s Aadhaar Number Capture Services (ANCS).

2.10.12.5 The KUA shall maintain auditable logs of all such transactions where e-KYC data has been shared with sub-KUA, for a period specified by the Authority.

2.10.12.6 It shall be ensured that full Aadhaar number is not stored and displayed anywhere in the system and wherever required only last 4 digits of Aadhaar number may be displayed.

2.10.12.7 As per Regulation 14(i) of the Aadhaar (Authentication) Regulation, 2016, requesting entity shall implement exception-handling mechanisms and backup identity authentication mechanism to ensure seamless provision of authentication services to Aadhaar number holders.

2.10.12.8 UIDAI may conduct audit of all KUAs and Sub KUAs as per the Aadhaar Act, Aadhaar Regulations, AUA/KUA Agreement, Guidelines, circulars etc. issued by UIDAI from time to time.

2.10.12.9 Monitoring of irregular transactions - KUAs shall develop appropriate monitoring mechanism to record irregular transactions and their reporting to UIDAI.

2.10.12.10 Investor Grievance Handling Mechanism - Investor may approach KUA for their grievance redressal. KUA will ensure that the grievance is redressed

within the timeframe as prescribed by UIDAI. KUA will also submit report on grievance redressal to UIDAI as per timelines prescribed by UIDAI.

2.10.13 **Onboarding process of KUA/Sub-KUA by UIDAI**:

2.10.13.1 As provided in the DoR circular dated May 09, 2019, SEBI after scrutiny of the application forms of KUAs shall forward the applications along with its recommendation to UIDAI.

2.10.13.2 For appointment of SEBI registered intermediary / MF distributors as Sub-KUAs, KUA will send list of proposed Sub-KUAs to SEBI and SEBI would forward the list of recommended Sub-KUAs to UIDAI for onboarding. An agreement will be signed between KUA and Sub-KUA, as prescribed by UIDAI. Sub-KUA shall also comply with the Aadhaar Act, Regulations, circulars, Guidelines etc. issued by UIDAI from time to time.

2.10.13.3 Each sub-KUA shall be assigned a separate Sub-KUA code by UIDAI.

2.10.14 The KUA/sub-KUA shall be guided by the above for use of Aadhaar authentication services of UIDAI for e-KYC.

2.10.15 For non-compliances if any observed on the part of the reporting entities (KUAs/ Sub- KUAs), SEBI may take necessary action under the applicable laws and also bring the same to the notice of DoR / FIU for further necessary action, if any. Reporting entity (KUAs/Sub-KUAs) shall also adhere to the continuing compliances and standards of privacy and security prescribed by UIDAI to carry out Aadhaar Authentication Services under section 11A of PMLA. Based on a report from SEBI / UIDAI or otherwise, if it is found that the reporting entity no longer fulfils the requirements for performing authentication under clause (a) of section 11A(1) of PMLA, the Central Government may withdraw the notification after giving an opportunity to the reporting entity.

2.11 The Securities and Exchange Board of India (KYC Registration Agency) Regulations, 2011[89]

SEBI has formulated the KRA Regulations, which have been notified vide notification No. LAD-NRO/GN/2011-12/29/36772 dated December 2, 2011. The KRA Regulations cover the registration of KRAs, functions and responsibilities of the KRAs and intermediaries, code of conduct, data security, etc. A copy of the same is attached below:

Enclosure: Copy of KRA Regulations

[89] Reference: SEBI Circular MIRSD/Cir-23/2011 dated December 02, 2011

2.12 *Guidelines in pursuance of the SEBI KYC Registration Agency (KRA) Regulations, 2011 and for In-Person Verification (IPV)*[90]

With a view to implement the KRA Regulations effectively, the following guidelines are being issued:

2.12.1 Guidelines for Intermediaries:

2.12.1.1 After doing the initial KYC of the new clients, the intermediary shall forthwith upload the KYC information with proper authentication on the system of the KRA, furnish the scanned images of the KYC documents to the KRA, and retain the physical KYC documents.[91]

2.12.1.2 In case a client's KYC documents sent by the intermediary to KRA are not complete, the KRA shall inform the same to the intermediary who shall forward the required information / documents promptly to KRA.

2.12.1.3 For existing clients, the KYC data may be uploaded by the intermediary provided they are in conformity with details sought in the uniform KYC form specified under **Para 1.1.6**. While uploading these clients' data the intermediary shall ensure that there is no duplication of data in the KRA system.

2.12.1.4 The intermediary shall carry out KYC when the client chooses to trade/invest /deal through it.

2.12.1.5 The intermediaries shall maintain electronic records of KYCs of clients and keeping physical records would not be necessary.

2.12.1.6 The intermediary shall promptly provide KYC related information to KRA, as and when required.

2.12.1.7 The intermediary shall have adequate internal controls to ensure the security/authenticity of data uploaded by it.

2.12.2 Guidelines for KRAs:

2.12.2.1 KRA system shall provide KYC information in data and image form to the intermediary.

2.12.2.2 KRA shall send a letter to the client within 10 working days of the receipt of the initial/updated KYC documents from intermediary, confirming the details thereof and maintain the proof of dispatch.

2.12.2.3 KRA(s) shall develop systems, in co-ordination with each other, to prevent duplication of entry of KYC details of a client and to ensure uniformity in formats of uploading / modification / downloading of KYC data by the intermediary.

---

[90] Reference: SEBI Circular MIRSD/Cir- 26 /2011 dated December 23, 2011

[91] Reference: KYC Registration Agency (Amendment) Regulations, 2013 vide Notification No. LAD-NRO/GN/2012-13/35/6998 dated March 22, 2013

2.12.2.4 KRA shall maintain an audit trail of the upload / modifications / downloads made in the KYC data, by the intermediary in its system.

2.12.2.5 KRA shall ensure that a comprehensive audit of its systems, controls, procedures, safeguards and security of information and documents is carried out annually by an independent auditor. The Audit Report along with the steps taken to rectify the deficiencies, if any, shall be placed before its Board of Directors. Thereafter, the KRA shall send the Action Taken Report to SEBI within 3 months.

2.12.2.6 KRA systems shall clearly indicate the status of clients falling under PAN exempt categories viz. investors residing in the state of Sikkim, UN entities / multilateral agencies exempt from paying taxes / filing tax returns in India.

2.12.2.7 A client can start trading / investing/ dealing with the intermediary and its group / subsidiary / holding company as soon as the initial KYC is done and other necessary information is obtained while the remaining process of KRA is in progress.

2.12.3 **In-Person Verification (IPV):**

With regard to the requirement of in-person' verification (IPV), SEBI has issued guidelines to the stock brokers and DPs. However, in line with the uniformity brought out in the KYC procedure across intermediaries, the IPV requirements for all the intermediaries have now been streamlined and harmonized, as follows:

2.12.3.1 It shall be mandatory for all the intermediaries addressed under this section to carry out IPV of their clients.

2.12.3.2 The intermediary shall ensure that the details like name of the person doing IPV, his designation, organization with his signatures and date are recorded on the KYC form at the time of IPV.

2.12.3.3 The IPV carried out by one SEBI registered intermediary can be relied upon by another intermediary.

2.12.3.4 In case of Stock brokers, their sub-brokers or Authorised Persons (appointed by the stock brokers after getting approval from the concerned Stock Exchanges in terms of Section 32.2 of SEBI Circular SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2023/71 dated May 17, 2023) can perform the IPV.

2.12.3.5 In case of Mutual Funds, their Asset Management Companies (AMCs) and the distributors who comply with the certification process of National Institute of Securities Market (NISM) or Association of Mutual Funds (AMFI) and have undergone the process of 'Know Your Distributor (KYD)', can perform the IPV. However, in case of applications received by the mutual funds directly from the clients (i.e. not through any distributor), they may also rely upon the IPV performed by the scheduled commercial banks.

Note:[92]

a. IPV/ VIPV would not be required when the KYC of the investor is completed using the Aadhaar authentication / verification of UIDAI.

b. IPV/ VIPV shall not be required by the RI when the KYC form has been submitted online, documents have been provided through digilocker or any other source which could be verified online.

2.13 Clarification on Know Your Client (KYC) Process and Use of Technology for KYC[93]

2.13.1 Know Your Customer (KYC) and Customer Due Diligence (CDD) policies as part of KYC are the foundation of an effective Anti-Money Laundering process. The KYC process requires every SEBI registered intermediary (hereinafter referred to as 'RI') to collect and verify the Proof of Identity (PoI) and Proof of Address (PoA) from the investor.

2.13.2 The provisions as laid down under the PMLA, Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, SEBI Master Circular on Guidelines on Anti-Money Laundering (AML) Standards and Combating the Financing of Terrorism (CFT) /Obligations of Securities Market Intermediaries under the Prevention of Money Laundering Act, 2002 and Rules framed there under dated February 03, 2023 and relevant KYC / AML circulars issued from time to time shall continue to remain applicable. Further, the SEBI registered intermediary shall continue to ensure to obtain the express consent of the investor before undertaking online KYC.

2.13.3 SEBI, has issued various circulars to simplify, harmonize the process of KYC by investors / RI. Constant technology evolution has taken place in the market and innovative platforms are being created to allow investors to complete KYC process online. SEBI held discussions with various market participants and based on their feedback and with a view to allow ease of doing business in the securities market, it is decided to make use of following technological innovations which can facilitate online KYC:

2.13.3.1 eSign service is an online electronic signature service that can facilitate an Aadhaar holder to forward the document after digitally signing the same provided the eSign signature framework is operated under the provisions of Second schedule of the Information Technology Act, 2000 and guidelines issued by the controller.

2.13.3.2 In terms of Rule 2 (1) (cb) of PML Rules 2005, "equivalent e-document" means an electronic equivalent of a document, issued by the issuing authority of such document with its valid digital signature, including documents issued to the Digital Locker account of the investor as per Rule 9 of the Information

[92] Reference: SEBI Circular SEBI/HO/MIRSD/DOP/CIR/P/2020/73 dated April 24, 2020
[93] Reference: SEBI Circular SEBI/HO/MIRSD/DOP/CIR/P/2020/73 dated April 24, 2020

Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016.

2.13.3.3 Section 5 of the Information Technology Act, 2000 recognizes electronic signatures (which includes digital signature) and states that where any law provides that information or any other matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person then such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of a digital signature affixed in such manner as prescribed by the Central Government. Therefore, the eSign mechanism of Aadhaar shall be accepted in lieu of wet signature on the documents provided by the investor. Even the cropped signature affixed on the online KYC form under eSign shall also be accepted as valid signature.

2.13.4 In order to enable the Online KYC process for establishing account based relationship with the RI, Investor's KYC can be completed through online / App based KYC, in-person verification through video, online submission of Officially Valid Document (OVD) / other documents under eSign, in the following manner:

2.13.4.1 The investor visits the website/App/digital platform of the RI and fills up the online KYC form and submits requisite documents online.

2.13.4.2 The name, photograph, address, mobile number, email ID, Bank details of the investor shall be captured online and OVD / PAN / signed cancelled cheque shall be provided as a photo / scan of the original under eSign and the same shall be verified as under:

2.13.4.2.1 Mobile and email is verified through One Time Password (OTP) or other verifiable mechanism. The mobile number/s of investor accepted as part of KYC should preferably be the one seeded with Aadhaar. (the RI shall ensure to meet the requirements of the mobile number and email as detailed under Section 33 'SMS and E-mail alerts to investors by Stock Exchanges' of SEBI Circular SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2023/71 dated May 17, 2023)

2.13.4.2.2 Aadhaar is verified through UIDAIs authentication / verification mechanism. Further, in terms of Rule 9 (16) of the PML Rules 2005, every RI shall, where the investor submits his Aadhaar number, ensure that such investor to redact or blackout his Aadhaar number through appropriate means where the authentication of Aadhaar number is not required under sub-rule (15). RI shall not store/ save the Aadhaar number of investor in their system. e-KYC through Aadhaar Authentication service of UIDAI or offline verification through Aadhaar QR Code/ XML file can be undertaken, provided the XML file or Aadhaar Secure QR Code generation date is not older than 3 days from

the date of carrying out KYC. The usage of Aadhaar is optional and purely on a voluntary basis by the investor.

2.13.4.2.3 PAN is verified online using the Income Tax Database.

2.13.4.2.4 Bank account details are verified by Penny Drop mechanism or any other mechanism using API of the Bank. (Explanation: based on bank details in the copy of the cancelled cheque provided by the investor, the money is deposited into the bank account of the investors to fetch the bank account details and name.) The name and bank details as obtained shall be verified with the information provided by investor.

2.13.4.2.5 Any OVD other than Aadhaar shall be submitted through Digilocker/under eSign mechanism.

2.13.4.3 In terms of Rule 2 (d) of PML Rules 2005, "Officially Valid Documents" means the following:

2.13.4.3.1 the passport,

2.13.4.3.2 the driving licence,

2.13.4.3.3 proof of possession of Aadhaar number,

2.13.4.3.4 the Voter's Identity Card issued by Election Commission of India,

2.13.4.3.5 job card issued by NREGA duly signed by an officer of the State Government and

2.13.4.3.6 the letter issued by the National Population Register containing details of name, address, or any other document as notified by the Central Government in consultation with the Regulator.

2.13.4.4 Further, Rule 9(18) of PML Rules 2005 states that in case OVD furnished by the investor does not contain updated address, the document as prescribed therein in the above stated Rule shall be deemed to be the OVD for the limited purpose of proof of address.

2.13.4.5 PML Rules 2005 allows an investor to submit other OVD instead of PAN, however, the requirement of mandatory submission of PAN by the investors for transaction in the securities market shall continue to apply.

2.13.4.6 Once all the information as required as per the online KYC form is filled up by the investor, KYC process could be completed as under:

2.13.4.6.1 The investor would take a print out of the completed KYC form and after affixing their wet signature, send the scanned copy / photograph of the same to the RI under eSign, or

2.13.4.6.2 Affix online the cropped signature on the filled KYC form and submit the same to the RI under eSign.

2.13.4.7 The RI shall forward the KYC completion intimation letter through registered post/ speed post or courier, to the address of the investor in cases where the investor has given address other than as given in the OVD. In such cases of

return of the intimation letter for wrong / incorrect address, addressee not available etc., no transactions shall be allowed in such account and intimation shall also sent to the Stock Exchange and Depository.

2.13.4.8 The original seen and verified requirement for OVD would be met where the investor provides the OVD in the following manner:

2.13.4.8.1 As a clear photograph or scanned copy of the original OVD, through the eSign mechanism, or;

2.13.4.8.2 As digitally signed document of the OVD, issued to the DigiLocker by the issuing authority.

2.13.4.9 SEBI has harmonized the IPV requirements for the intermediaries. In order to ease the IPV process for KYC, the said SEBI circular pertaining to IPV stands modified as under:

2.13.4.9.1 IPV/ VIPV would not be required when the KYC of the investor is completed using the Aadhaar authentication / verification of UIDAI.

2.13.4.9.2 IPV / VIPV shall not be required by the RI when the KYC form has been submitted online, documents have been provided through digilocker or any other source which could be verified online.

2.13.5 **Features for online KYC App of the RI** - SEBI registered intermediary may implement their own Application (App) for undertaking online KYC of investors. The App shall facilitate taking photograph, scanning, acceptance of OVD through Digilocker, video capturing in live environment, usage of the App only by authorized person of the RI. The App shall also have features of random action initiation for investor response to establish that the interactions not pre-recorded, time stamping, geo-location tagging to ensure physical location in India etc is also implemented. RI shall ensure that the process is a seamless, real-time, secured, end-to-end encrypted audio-visual interaction with the customer and the quality of the communication is adequate to allow identification of the customer beyond doubt. RI shall carry out the liveliness check in order to guard against spoofing and such other fraudulent manipulations. The RI shall before rolling out and periodically, carry out software and security audit and validation of their App. The RI may have additional safety and security features other than as prescribed above.

2.13.6 **Feature for Video in Person Verification (VIPV) for Individuals –** To enable ease of completing IPV of an investor, intermediary may undertake the VIPV of an individual investor through their App. The following process shall be adopted in this regard:

2.13.6.1 Intermediary through their authorised official, specifically trained for this purpose, may undertake live VIPV of an individual customer, after obtaining his/her informed consent. The activity log along with the credentials of the person performing the VIPV shall be stored for easy retrieval.

2.13.6.2 The VIPV shall be in a live environment.

2.13.6.3 The VIPV shall be clear and still, the investor in the video shall be easily recognisable and shall not be covering their face in any manner.

2.13.6.4 The VIPV process shall include random question and response from the investor including displaying the OVD, KYC form and signature or could also be confirmed by an OTP.

2.13.6.5 The RI shall ensure that photograph of the customer downloaded through the Aadhaar authentication / verification process matches with the investor in the VIPV.

2.13.6.6 The VIPV shall be digitally saved in a safe, secure and tamper-proof, easily retrievable manner and shall bear date and time stamping.

2.13.6.7 The RI may have additional safety and security features other than as prescribed above.

2.14 Simplification and Rationalization of Trading Account Opening Process [94]

Kindly refer para titled 'Simplification and Rationalization of Trading Account Opening Process' of SEBI Circular SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2023/71 dated May 17, 2023 (Master circular for Stock Brokers)

2.15 Recording of Non Disposal Undertaking (NDU) in the Depository System[95]

Securities and Exchange Board of India (Substantial Acquisition of Shares and Takeovers) Regulations, 2011 ("**SAST Regulations**"), requires promoters of a company to disclose details of their encumbered shares including NDUs by promoters which are covered under the scope of disclosures of 'Encumbrances'.

It has been observed that some shareholders, primarily promoters, enter into non-disposal agreements/non-disposal undertaking (NDU) for borrowing funds from various lenders. NDUs are typically undertakings given by a shareholder not to transfer or otherwise alienate the securities and are in the nature of negative lien given in favour of another party, usually a lender.

In order to enable the shareholders to record the NDUs in the depository system, it has been decided to permit the depositories to offer a system for capturing and recording the NDUs

In this regard, the depositories are advised the following:

2.15.1 Depositories shall develop a separate module/ transaction type in their system for recording NDUs.

2.15.2 Both parties to the NDU shall have a demat account with the same depository and be KYC compliant.

[94] Reference: SEBI Circular CIR/MIRSD/16/2011 dated August 22, 2011
[95] Reference: SEBI Circular CIR/MRD/DP/56/2017 dated June14, 2017

2.15.3 Pursuant to entering the NDU, the Beneficial Owner (BO) along with the other party shall make an application through the participant (where the BO holds his securities) to the depository, for the purpose of recording the NDU transaction.

2.15.4 The application shall necessarily include details of BO ID, PAN, email-id, signature(s), name of the entity in whose favor such NDU is entered and the quantity of securities. Such entity in whose favor NDU is entered shall also authorize the participant of the BO holding the shares, to access the signatures as recorded in that entity's demat account.

2.15.5 The participant after being satisfied that the securities are available for NDU shall record the NDU and freeze for debit the requisite quantity of securities under NDU in the depository system.

2.15.6 The depositories shall make suitable provisions for capturing the details of BO ID and PAN of the entity in whose favor such NDU is entered by the participant. The depositories shall also make available to the said participant, the details of authorized signatories as recorded in the demat account of the entity in whose favor such NDU is entered.

2.15.7 On creation of freeze in the depository system, the depository/ participant of the BO holding shares, shall inform both parties of the NDU regarding creation of freeze under NDU.

2.15.8 The depositories shall make suitable provisions for capturing the details of company/ promoters if they are part of the NDU.

2.15.9 In case if the participant does not create the NDU, it shall intimate the same to the parties of the NDU along with the reasons thereof.

2.15.10 Once the freeze for debits is created under the NDU for a particular quantity of shares, the depository shall not facilitate or effect any transfer, pledge, hypothecation, lending, rematerialisation or in any manner alienate or otherwise allow dealing in the shares held under NDU till receipt of instructions from both parties for the cancellation of NDU.

2.15.11 The entry of NDU made as per **Para 2.15.5** above may be cancelled by the depository/participant of the BO through unfreeze of specified quantity if parties to the NDU jointly make such application to the depository through the participant of the BO.

2.15.12 On unfreeze of shares upon termination/cancellation of NDU, the depository shall inform both parties of the NDU in the form and manner agreed upon at the time of creating the freeze. The unfreeze shall be effected in the depository system after a cooling period of 2 clear business days but no later than 4 clear business days.

2.15.13 The freeze and unfreeze instructions executed by the Participant for recording NDUs will be subject to 100% concurrent audit.

2.15.14 The DPs shall not facilitate or be a party to any NDU outside the depository system as outlined herein.

2.16 Recording of all types of Encumbrances in Depository system[96]

2.16.1 The SAST Regulations requires promoters of a company to disclose details of their encumbered shares. Apart from pledge, hypothecation and non-disposal undertakings(NDUs), there is no framework to capture the details of other types of encumbrances in the depository system.

2.16.2 In this regard, Depositories shall put in place a system for capturing and recording all types of encumbrances, which are specified under Regulation 28(3) of the SAST Regulations, as amended from time to time. Towards this end, Depositories shall follow processes and other norms similar to that stipulated for the purpose of capturing and recording NDUs in Depository system. This is apart from pledge and hypothecation, whose processes and specific norms are separately provided in DP Regulations and circulars issued thereon. Further:

2.16.2.1 All types of encumbrances as defined under Regulation 28(3) of SAST Regulations shall necessarily be recorded in the depository system.[97]

2.16.2.2 The depositories shall capture details of the ultimate lender along with name of the trustee acting on behalf of such ultimate lender such as banks, NBFCs, etc. In case of issuance of debentures, name of the debenture issuer shall be captured in the depository system.

2.16.2.3 The depositories shall now capture the reasons for encumbrances in the depository system.

2.16.3 The freeze and unfreeze instructions executed by the Participant for recording all encumbrances will be subject to 100% concurrent audit.

2.16.4 The Depository Participant shall not facilitate or be party to any type of encumbrance outside the Depository system as outlined herein.

2.17 Cyber Security & Cyber Resilience framework for Depository Participant[98]

2.17.1 Rapid technological developments in securities market have highlighted the need for maintaining robust cyber security and cyber resilience framework to protect the integrity of data and guard against breaches of privacy.

2.17.2 Since depository participants perform significant functions in providing services to holders of securities, it is desirable that these entities have robust cyber security and

[96] Reference: SEBI Circular SEBI/HO/MRD2/DDAP/CIR/P/2020/137 dated July 24, 2020
[97] Reference: SEBI Circular SEBI/HO/CFD/DCR-3/P/CIR/2022/27 dated March 07, 2022
[98] Reference: SEBI Circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018

cyber resilience framework in order to provide essential facilities and perform systemically critical functions relating to securities market.

2.17.3 Accordingly, a framework on cyber security and cyber resilience has been designed which is specified below. The framework would be required to be complied by all Depository Participants registered with SEBI.

2.17.4 Further, the Depository Participants are mandated to conduct comprehensive cyber audit at least once in a financial year. All Depository Participants shall submit with Depository a declaration from the MD/ CEO/ Partners/ Proprietors certifying compliance by the Depository Participants with all SEBI Circulars and advisories related to Cyber security from time to time, along with the Cyber audit report[99]

2.17.5 The framework on cyber security and cyber resilience is as follows:

2.17.5.1 Cyber-attacks and threats attempt to compromise the Confidentiality, Integrity and Availability (CIA) of the computer systems, networks and databases (Confidentiality refers to limiting access of systems and information to authorized users, Integrity is the assurance that the information is reliable and accurate, and Availability refers to guarantee of reliable access to the systems and information by authorized users). Cyber security framework includes measures, tools and processes that are intended to prevent cyber-attacks and improve cyber resilience. Cyber Resilience is an organization's ability to prepare and respond to a cyber-attack and to continue operation during, and recover from, a cyber-attack.

Governance

2.17.5.2 As part of the operational risk management framework to manage risk to systems, networks and databases from cyber-attacks and threats, Depository Participants should formulate a comprehensive Cyber Security and Cyber Resilience policy document encompassing the framework mentioned hereunder. In case of deviations from the suggested framework, reasons for such deviations, technical or otherwise, should be provided in the policy document.

The policy document should be approved by the Board / Partners / Proprietor of the Depository Participants. The policy document should be reviewed by the aforementioned group at least annually with the view to strengthen and improve its Cyber Security and Cyber Resilience framework.

2.17.5.3 The Cyber Security Policy should include the following process to identify, assess, and manage Cyber Security risk associated with processes, information, networks and systems:

a. 'Identify' critical IT assets and risks associated with such assets.
b. 'Protect' assets by deploying suitable controls, tools and measures.

[99] Reference: SEBI Circular SEBI/HO/MIRSD/TPD/P/CIR/2022/80 dated June 07, 2022

c. 'Detect' incidents, anomalies and attacks through appropriate monitoring tools/processes.
d. 'Respond' by taking immediate steps after identification of the incident, anomaly or attack.
e. 'Recover' from incident through incident management and other appropriate recovery mechanisms.

2.17.5.4 The Cyber Security Policy of Depository Participants should consider the principles prescribed by National Critical Information Infrastructure Protection Centre (NCIIPC) of National Technical Research Organization (NTRO), Government of India (titled 'Guidelines for Protection of National Critical Information Infrastructure') and subsequent revisions, if any, from time to time.

2.17.5.5 Depository Participants may refer to best practices from international standards like ISO27001, COBIT5,etc., or their subsequent revisions, if any, from time to time.

2.17.5.6 Depository Participants should designate a senior official or management personnel (henceforth, referred to as the "Designated Officer") whose function would be to assess, identify, and reduce security and Cyber Security risks, respond to incidents, establish appropriate standards and controls, and direct the establishment and implementation of processes and procedures as per the Cyber Security Policy.

2.17.5.7 The Board/Partners/Proprietor of the Depository Participants shall constitute an Technology Committee[100] comprising experts. This Technology Committee should on a half yearly basis review the implementation of the Cyber Security and Cyber Resilience policy approved by their Board/Partners/Proprietor, and such review should include review of their current IT and Cyber Security and Cyber Resilience capabilities, set goals for a target level of Cyber Resilience, and establish plans to improve and strengthen Cyber Security and Cyber Resilience. The review shall be placed before the Board/Partners/Proprietor of the Depository Participants for appropriate action.

2.17.5.8 Depository Participants should establish a reporting procedure to facilitate communication of unusual activities and events to the Designated Officer in a timely manner.

2.17.5.9 The Designated officer and the technology committee of the Depository Participants should periodically review instances of cyber-attacks, if any, domestically and globally, and take steps to strengthen Cyber Security and cyber resilience framework.

[100] Reference: SEBI Circular CIR/HO/MIRSD/DOS2/CIR/PB/2019/038 dated March 15, 2019 - in Para 7, the words "Internal Technology Committee" stands replaced as "Technology Committee".

2.17.5.10 Depository Participants should define responsibilities of its employees, outsourced staff, and employees of vendors, members or participants and other entities, who may have privileged access or use systems / networks of Depository Participants towards ensuring the goal of Cyber Security.

Identification

2.17.5.11 Depository Participants 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/Partners/Proprietor of the Depository Participants shall approve the list of critical systems.[101]

To this end, Depository Participants 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.

2.17.5.12 Depository Participants should accordingly identify cyber risks (threats and vulnerabilities) that it may face, along with the likelihood of such threats and impact on the business and thereby, deploy controls commensurate to the criticality.

Protection

Access controls

2.17.5.13 No person by virtue of rank or position should have any intrinsic right to access confidential data, applications, system resources or facilities.

2.17.5.14 Any access to Depository Participants systems, applications, networks, databases, etc., should be for a defined purpose and for a defined period. Depository Participants should grant access to IT systems, applications, databases and networks on a need-to-use basis and based on the principle of least privilege. Such access should be for the period when the access is required and should be authorized using strong authentication mechanisms.

2.17.5.15 Depository Participants should implement an access policy which addresses strong password controls for users' access to systems, applications, networks and databases. Illustrative examples for this are given under **Annexure 14**

2.17.5.16 All critical systems of the Depository Participant accessible over the internet should have two-factor security (such as VPNs, Firewall controls etc.)

[101] Reference: SEBI Circular SEBI/HO/MIRSD/TPD/P/CIR/2022/80 dated June 07, 2022

2.17.5.17 Depository Participants should ensure that records of user access to critical systems, wherever possible, are uniquely identified and logged for audit and review purposes. Such logs should be maintained and stored in a secure location for a time period not less than two (2) years.

2.17.5.18 Depository Participants should deploy controls and security measures to supervise staff with elevated system access entitlements (such as admin or privileged users) to Depository Participant's critical systems. Such controls and measures should inter-alia include restricting the number of privileged users, periodic review of privileged users' activities, disallow privileged users from accessing systems logs in which their activities are being captured, strong controls over remote access by privileged users, etc.

2.17.5.19 Employees and outsourced staff such as employees of vendors or service providers, who may be given authorized access to the Depository Participants critical systems, networks and other computer resources, should be subject to stringent supervision, monitoring and access restrictions.

2.17.5.20 Depository Participants should formulate an Internet access policy to monitor and regulate the use of internet and internet based services such as social media sites, cloud-based internet storage sites, etc. within the Depository Participant's critical IT infrastructure.

2.17.5.21 User Management must address deactivation of access of privileges of users who are leaving the organization or whose access privileges have been withdrawn.

Physical Security

2.17.5.22 Physical access to the critical systems should be restricted to minimum and only to authorized officials. Physical access of outsourced staff/visitors should be properly supervised by ensuring at the minimum that outsourced staff/visitors are accompanied at all times by authorized employees.

2.17.5.23 Physical access to the critical systems should be revoked immediately if the same is no longer required.

2.17.5.24 Depository Participants should ensure that the perimeter of the critical equipment room, if any, are physically secured and monitored by employing physical, human and procedural controls such as the use of security guards, CCTVs, card access systems, mantraps, bollards, etc. where appropriate.

Network Security Management

2.17.5.25 Depository Participants should establish baseline standards to facilitate consistent application of security configurations to operating systems, databases, network devices and enterprise mobile devices within their IT environment. The LAN and wireless networks should be secured within the Depository Participants' premises with proper access controls.

2.17.5.26 For algorithmic trading facilities, adequate measures should be taken to isolate and secure the perimeter and connectivity to the servers running algorithmic trading applications.

2.17.5.27 Depository Participants should install network security devices, such as firewalls, proxy servers, intrusion detection and prevention systems (IDS) to protect their IT infrastructure which is exposed to the internet, from security exposures originating from internal and external sources.

2.17.5.28 Adequate controls must be deployed to address virus / malware / ransomware attacks. These controls may include host / network / application based IDS systems, customized kernels for Linux, anti-virus and anti-malware software etc.

Data security

2.17.5.29 Critical data must be identified and encrypted in motion and at rest by using strong encryption methods. Illustrative measures in this regard are given under **Annexure 12** & **Annexure 13**.

2.17.5.30 Depository Participants should implement measures to prevent unauthorized access or copying or transmission of data / information held in contractual or fiduciary capacity. It should be ensured that confidentiality of information is not compromised during the process of exchanging and transferring information with external parties. Illustrative measures to ensure security during transportation of data over the internet are given under **Annexure 13**

2.17.5.31 The information security policy should also cover use of devices such as mobile phones, faxes, photocopiers, scanners, etc., within their critical IT infrastructure, that can be used for capturing and transmission of sensitive data. For instance, defining access policies for personnel, and network connectivity for such devices etc.

2.17.5.32 Depository Participants should allow only authorized data storage devices within their IT infrastructure through appropriate validation processes.

Hardening of Hardware and Software

2.17.5.33 Depository Participants should only deploy hardened hardware / software, including replacing default passwords with strong passwords and disabling or removing services identified as unnecessary for the functioning of the system.

2.17.5.34 Open ports on networks and systems which are not in use or that can be potentially used for exploitation of data should be blocked and measures taken to secure them.

Application Security in Customer Facing Applications

2.17.5.35 Application security for Customer facing applications offered over the Internet such as IBTs (Internet Based Trading applications), portals containing sensitive or private information and Back office applications (repository of financial and

personal information offered by Brokers to Customers) are paramount as they carry significant attack surfaces by virtue of being available publicly over the Internet for mass use. An illustrative list of measures for ensuring security in such applications is provided under **Annexure 14**.

Certification of off-the-shelf products

2.17.5.36 Depository Participants should ensure that off the shelf products being used for core business functionality (such as Back office applications) should bear Indian Common criteria certification of Evaluation Assurance Level 4. The Common criteria certification in India is being provided by (STQC) Standardisation Testing and Quality Certification (Ministry of Electronics and Information Technology). Custom developed / in-house software and components need not obtain the certification, but have to undergo intensive regression testing, configuration testing etc. The scope of tests should include business logic and security controls.

Patch management

2.17.5.37 Depository Participants should establish and ensure that the patch management procedures include the identification, categorization and prioritization of patches and updates. An implementation timeframe for each category of patches should be established to apply them in a timely manner.

2.17.5.38 Depository Participants should perform rigorous testing of security patches and updates, where possible, before deployment into the production environment so as to ensure that the application of patches do not impact other systems.

Disposal of data, systems and storage devices

2.17.5.39 Depository Participants should frame suitable policy for disposal of storage media and systems. The critical data / Information on such devices and systems should be removed by using methods such as crypto shredding / degauss / Physical destruction as applicable.

2.17.5.40 Depository Participants should formulate a data-disposal and data- retention policy to identify the value and lifetime of various parcels of data.

Vulnerability Assessment and Penetration Testing (VAPT)

2.17.5.41 Depository Participants should regularly conduct vulnerability assessment to detect security vulnerabilities in their IT environments exposed to the internet.[102]

2.17.5.42 Depository Participants with systems publicly available over the internet should also carry out penetration tests, at-least once a year, in order to conduct an in-

[102] Reference: SEBI Circular SEBI/HO/MIRSD/TPD/P/CIR/2022/80 dated June 07, 2022

depth evaluation of the security posture of the system through simulations of actual attacks on its systems and networks that are exposed to the internet.[103] In addition, Depository Participants should perform vulnerability scanning and conduct penetration testing prior to the commissioning of a new system that is accessible over the internet.

2.17.5.43 In case of vulnerabilities discovered in off-the-shelf products (used for core business) or applications provided by exchange empanelled vendors, Depository Participants should report them to the vendors and the exchanges in a timely manner.

2.17.5.44 Remedial actions should be immediately taken to address gaps that are identified during vulnerability assessment and penetration testing.[104]

Monitoring and Detection

2.17.5.45 Depository Participants should establish appropriate security monitoring systems and processes to facilitate continuous monitoring of security events / alerts and timely detection of unauthorised or malicious activities, unauthorised changes, unauthorised access and unauthorised copying or transmission of data / information held in contractual or fiduciary capacity, by internal and external parties. The security logs of systems, applications and network devices exposed to the internet should also be monitored for anomalies.

2.17.5.46 Further, to ensure high resilience, high availability and timely detection of attacks on systems and networks exposed to the internet, Depository Participants should implement suitable mechanisms to monitor capacity utilization of its critical systems and networks that are exposed to the internet, for example, controls such as firewalls to monitor bandwidth usage.

Response and Recovery

2.17.5.47 Alerts generated from monitoring and detection systems should be suitably investigated in order to determine activities that are to be performed to prevent expansion of such incident of cyber-attack or breach, mitigate its effect and eradicate the incident.

2.17.5.48 The response and recovery plan of the Depository Participants should have plans for the timely restoration of systems affected by incidents of cyber-attacks or breaches, for instance, offering alternate services or systems to Customers. Depository Participants should have the same Recovery Time Objective (RTO) and Recovery Point Objective (RPO) as specified by SEBI for Market Infrastructure Institutions under **Para 4.31** as amended from time to time

[103] Reference: SEBI Circular SEBI/HO/MIRSD/TPD/P/CIR/2022/80 dated June 07, 2022
[104] Reference: SEBI Circular SEBI/HO/MIRSD/TPD/P/CIR/2022/80 dated June 07, 2022

2.17.5.49 The response plan should define responsibilities and actions to be performed by its employees and support / outsourced staff in the event of cyber-attacks or breach of Cyber Security mechanism.

2.17.5.50 Any incident of loss or destruction of data or systems should be thoroughly analyzed and lessons learned from such incidents should be incorporated to strengthen the security mechanism and improve recovery planning and processes.

2.17.5.51 Depository Participants should also conduct suitable periodic drills to test the adequacy and effectiveness of the aforementioned response and recovery plan.

Sharing of Information

2.17.5.52 [105]All Cyber-attacks, threats, cyber-incidents and breaches experienced by Depositories Participants shall be reported to Depositories & SEBI within 6 hours of noticing/detecting such incidents or being brought to notice about such incidents. This information shall be shared to SEBI through the dedicated e-mail id: sbdp-cyberincidents@sebi.gov.in.

The incident shall also be reported to Indian Computer Emergency Response team (CERT-In) in accordance with the guidelines / directions issued by CERT-In from time to time. Additionally, the Depository Participants, whose systems have been identified as "Protected system" by National Critical Information Infrastructure Protection Centre (NCIIPC) shall also report the incident to NCIIPC.

The quarterly reports containing information on cyber-attacks, threats, cyber-incidents and breaches experienced by Depository Participants and measures taken to mitigate vulnerabilities, threats and attacks including information on bugs / vulnerabilities, threats that may be useful for other Depository Participants/ Depositories and SEBI, shall be submitted to Depositories within 15 days from the quarter ended June, September, December and March of every year.

The following guidelines are for timelines & submission of report/information[106]:

i. The format for submitting the reports is attached below.
ii. The mode of submission of such reports by the depository participants may be prescribed by Depositories.

[105] Reference: SEBI Circular SEBI/HO/MIRSD/TPD/P/CIR/2022/93 dated June 30, 2022
[106] Reference: SEBI Circular SEBI/HO/MIRSD/DOP/CIR/P/2019/109 dated October 15, 2019

भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

Format

Incident Reporting Form			
1.Letter/ Report Subject-			
Name of the Member / Depository Participant - Name of the Stock Exchange/ Depository- Member ID/DPID-			
2. Reporting Periodicity Year-			
☐ Quarter1 (Apr-Jun) ☐ Quarter2 (Jul-Sep)		☐ Quarter3 (Oct-Dec) ☐ Quarter4(Jan-Mar)	
3. Designated Officer (Reporting Officer details) -			
Name:		Organization:	Title:
Phone / Fax No:		Mobile:	Email:
Address:			
Cyber-attack/ breach observed in Quarter: (If yes, please fill **Annexure I**) (If no, please submit the NIL report)			
Date & Time	Brief information on the Cyber-attack/ breached observed		

Annexure I				
1. Physical location of affected computer /network and name of ISP-				
2. Date and time incident occurred -				
Date:		Time:		
3. Information of affected system-				
IP Address:	Computer /Host Name:	Operating System (incl. Ver. / release No.):	Last Patched/ Updated:	Hardware Vendor/ Model:
4. Type of incident -				

• Phishing • Network scanning/Probing Break- in/Root Compromise • Virus/Malicious Code • Website Defacement • System Misuse	• Spam • Bot/Botnet • Email Spoofing • Denial of Service (DoS) • Distributed Denial of Service (DDoS) • User Account • Compromise	• Website Intrusion • Social • Engineering • Technical • Vulnerability • IP Spoofing • Ransomware • Other

5. Description of incident-

6. Unusual behaviour/symptoms(Tick the symptoms)-

• System crashes • New user accounts/ Accounting discrepancies • Failed or successful social engineering attempts • Unexplained, poor system performance • Unaccounted for changes in the DNS tables, router rules, or firewall rules • Unexplained elevation or use of privileges Operation of a program or sniffer device to capture network traffic; • An indicated last time of usage of a user account that does not correspond to the actual last time of usage for that user • A system alarm or similar indication from an intrusion detection tool • Altered home pages, which are usually the intentional target for visibility, or other pages on the Webserver	• Anomalies • Suspicious probes • Suspicious browsing New files • Changes in file lengths or dates • Attempts to write to system • Data modification or deletion • Denial of service • Door knob rattling • Unusual time of usage • Unusual usage patterns • Unusual log file entries • Presence of new setuid or setgid files Changes in system directories and files • Presence of cracking utilities • Activity during non-working hours or holidays • Other (Please specify)

7. Details of unusual behavior/symptoms -

8. Has this problem been experienced earlier? If yes, details-

9. Agencies notified-

Law Enforcement	Private Agency	Affected Product Vendor	Other___

10. IP Address of apparent or suspected source-

Source IP address:	Other information available:

11. How many host(s)are affected-

1 to 10	10 to 100	More than 100

12. Details of actions taken for mitigation and any preventive measure applied-

Training and Education

2.17.5.53 Depository Participants should work on building Cyber Security and basic system hygiene awareness of staff (with a focus on staff from non-technical disciplines).

2.17.5.54 Depository Participants should conduct periodic training programs to enhance knowledge of IT / Cyber Security Policy and standards among the employees incorporating up-to-date Cyber Security threat alerts. Where possible, this should be extended to outsourced staff, vendors etc.

2.17.5.55 The training programs should be reviewed and updated to ensure that the contents of the program remain current and relevant.

Systems managed by vendors

2.17.5.56 Where the systems (IBT, Back office and other Customer facing applications, IT infrastructure, etc.) of a Depository Participants are managed by vendors and the Depository Participants may not be able to implement some of the aforementioned guidelines directly, the Depository Participants should instruct the vendors to adhere to the applicable guidelines in the Cyber Security and Cyber Resilience policy and obtain the necessary self-certifications from them to ensure compliance with the policy guidelines.

Systems managed by MIIs

2.17.5.57 Where applications are offered to customers over the internet by MIIs (Market Infrastructure Institutions), for e.g.: NSE's NOW, BSE's BEST etc., the responsibility of ensuring Cyber Resilience on those applications reside with the MIIs and not with the Depository Participant. The Depository Participant is exempted from applying the aforementioned guidelines to such systems offered by MIIs such as NOW, BEST, etc.

Periodic Audit[107]

2.17.5.58 The Depository Participants shall arrange to have their systems audited on an annual basis to check compliance with the above areas and shall submit the report to Depositories along with the comments of the Board / Partners / Proprietor of Depository Participant within three months of the end of the financial year.

The auditors qualified in following certifications can audit the systems of depository participants to check the compliance of Cyber Security and Cyber Resilience provisions:

a. CERT-IN empanelled auditor, an independent DISA (ICAI) Qualification, CISA (Certified Information System Auditor) from

[107] Reference: SEBI Circular SEBI/HO/MIRSD/DOP/CIR/P/2019/109 dated October 15, 2019

ISACA, CISM (Certified Information Securities Manager) from ISACA, CISSP (Certified Information Systems Security Professional) from International Information Systems Security Certification Consortium (commonly known as (ISC)2).

2.18 Standard Operating Procedure (SOP) for handling cyber security incidents of intermediaries and Categorisation of Intermediaries[108]

The following Standard Operating Procedure (SOP) needs to be complied with by DPs:

2.18.1 DPs to have their own cyber security incident handling process document, SOP in place.

2.18.2 DPs to examine the incident and classify the incident High / Medium / Low as per their cyber security incident handling document. Decide Action / Response for the incident based on severity.

2.18.3 Report incident to Indian Computer Emergency Response Team (CERT-In).

2.18.4 DPs to provide the reference details of the reported incident to the respective depository and SEBI. They also need to provide details regarding whether CERT-In team is in touch with the DP for any assistance. If not reported to CERT-In, they should submit the reasons for the same to the depository and SEBI. DPs to communicate with CERT-In / MHA / Cybercrime police for further assistance.

2.18.5 DPs to submit details whether they have registered complaint with law enforcement agencies such as Police or cyber security cell. If yes, details need to be provided to MIIs and SEBI. If not, reason for not registering complaint should also be provided to MIIs and SEBI.

In addition to the above, the depositories are also requested to categorise their participants into three categories as per the details tabulated below:

Category of Intermediaries	Type of Intermediaries	Frequency of Penetration Testing to be conducted by SEBI	Frequency of PT to be conducted through MIIs	Parameters that may be considered
Set-A (High Impact)	Depository Participants	Will be conducted on yearly basis.	-	Top DPs in terms of number of demat accounts. The list shall also include intermediaries having significant online

[108] Reference: SEBI MIRSD email dated April 16, 2021

				presence like: Zerodha, ICICI direct, Upstox, HDFC securities, Kotak securities, Sharekhan, etc.erodha, ICICI direct, Upstox, HDFC securities, Kotak securities, Sharekhan, etc. The list is to be reviewed on yearly basis and the revised list shall be submitted to SEBI in first week of April. The parameters listed above are indicative and Depositories may include any other relevant parameter(s) to categorise their participants under Set A. For categorising participants under Set A, depositories may arrive at a suitable percentage for parameters identified.
Set-B (Medium Impact)	Depository Participants	-	For DPs coming under the purview of Depositories , risk based audit / PT will be conducted by Depositories once in a year.	For categorising members / participants under Set B, depositories may arrive at a suitable percentage for parameters identified. The list is to be reviewed on yearly basis and the revised list shall be submitted to SEBI in first week of April. Depositories to define and communicate risk based policy / approach for conducting audit / PT for their intermediaries to Division of Supervision of Market Intermediaries Regulation and Supervision Department (DoS-MIRSD) and Chief Information Security Officer (CISO) of SEBI.

				The audit / PT report of Set B intermediaries shall be submitted by Depositories to DoS-MIRSD.
Set-C (Low Impact)	Depository Participants other than that in Set-A and Set-B. The revised list shall be submitted to SEBI in first week of April.	-	For DPs coming under the purview of Depositories, risk based audit / PT will be conducted by Depositories once in 2 years.	Depository to define and communicate risk based policy / approach for conducting audit / PT for their intermediaries to DoS-MIRSD and CISO SEBI. The audit / PT report of Set C DPs shall be submitted by Depositories to DoS-MIRSD.

Depositories shall communicate the above to their participants and inform SEBI. The details as per **Para 2.18.4** and **Para 2.18.5** above, shall be submitted to Division Chiefs (in-charge of divisions at the time of submission) of DOS-MIRSD and CISO of SEBI.

The list of depository participants, categorised as Set A, Set B, Set C, shall be sent to Division Chiefs (in-charge of divisions at the time of submission) of DoS-MIRSD and CISO of SEBI, along with the criteria decided by depositories to categorise participants. The revised list every year (in first week of April) shall also be submitted to Division Chiefs (in-charge of divisions at the time of submission) of DoS-MIRSD and CISO of SEBI.

2.19 CERT-In Advisory "Preventing Data Breaches / Data Leaks"[109]

In view of the rising incidents of data breaches / data leaks, CERT-In has issued an Advisory Dated January 20, 2021 w.r.t. "Preventing Data Breaches / Data Leaks", wherein following relevant aspects have been detailed:

2.19.1 Common causes of data breach / data leak,

2.19.2 Best practices to prevent data breaches,

2.19.3 Steps to be taken when organisation/entity is affected by a data breach/data leak,

2.19.4 Best practices for individual users to safeguard against data breaches

[109] Reference: SEBI MIRSD email dated March 02, 2022

All Depositories are hereby advised to issue this advisory to their participants to prevent data breaches / data leaks in future.

All Depositories are also advised to instruct their participants to continue to adhere to cyber security guidelines/advisories issued by SEBI in the past and follow best industry practices and comply with other guidelines issued by CERT-In and NCIIPC from time to time.

2.20 Reporting for Artificial Intelligence (AI) and Machine Learning (ML) applications and systems offered and used by market intermediaries[110]

Background

2.20.1 There is increasing usage of AI (Artificial Intelligence) and ML (Machine Learning) as product offerings by market intermediaries and participants (e.g..: "robo advisors") in investor and consumer facing products. SEBI is conducting a survey and creating an inventory of the AI / ML landscape in the Indian financial markets to gain an in-depth understanding of the adoption of such technologies in the markets and to ensure preparedness for any AI / ML policies that may arise in the future.

2.20.2 As most AI / ML systems are black boxes and their behaviour cannot be easily quantified, it is imperative to ensure that any advertised financial benefit owing to these technologies in investor facing financial products offered by intermediaries should not constitute to misrepresentation.

Scope definition

2.20.3 Any set of applications/software/programs/executable/systems (computer systems) –cumulatively called application and systems,

2.20.3.1 that are offered to investors (individuals and institutions) by market intermediaries to facilitate investing and trading,

or

2.20.3.2 to disseminate investments strategies and advice,

or

2.20.3.3 to carry out compliance operations / activities,

where AI / ML is portrayed as a part of the public product offering or under usage for compliance or management purposes, is included in the scope of this section. Here, "AI" / "ML" refers to the terms "Artificial Intelligence" and" Machine Learning" used as a part of the product offerings. In order to make the scope of this section inclusive of various AI and ML technologies in use, the scope also covers Fin-Tech and Reg-Tech initiatives undertaken by market participants that involves AI and ML

[110] Reference: SEBI Circular SEBI/HO/MIRSD/DOS2/CIR/P/2019/10 dated January 04, 2019

2.20.4 Technologies that are considered to be categorized as AI and ML technologies in the scope of this section, are explained below:

Systems deemed to be based on AI and ML technology

Applications and Systems belonging but not limited to following categories or a combination of these:

2.20.4.1 Natural Language Processing (NLP), sentiment analysis or text mining systems that gather intelligence from unstructured data –In this case, Voice to text, text to intelligence systems in any natural language will be considered in scope. Eg: robo chat bots, big data intelligence gathering systems.

2.20.4.2 Neural Networks or a modified form of it –In this case, any systems that uses a number of nodes (physical or software simulated nodes) mimicking natural neural networks of any scale, so as to carry out learning from previous firing of the nodes will be considered in scope. Eg: Recurrent Neural networks and Deep Learning Neural Networks

2.20.4.3 Machine learning through supervised, unsupervised learning or a combination of both. In this case, any application or systems that carry out knowledge representation to form a knowledge base of domain, by learning and creating its outputs with real world input data and deciding future outputs based upon the knowledge base. Eg: System based on Decision tree, random forest, K mean, Markov decision process, Gradient boosting Algorithms.

2.20.4.4 A system that uses statistical heuristics method instead of procedural algorithms or the system/application applies clustering or categorization algorithms to categorize data without a predefined set of categories

2.20.4.5 A system that uses a feedback mechanism to improve its parameters and bases it subsequent execution steps on these parameters.

2.20.4.6 A system that does knowledge representation and maintains a knowledge base

Regulatory requirements

2.20.5 All registered Depository Participants offering or using applications or systems as defined in **Para 2.20.4**, should participate in the reporting process by completing the AI/ML reporting form (See **Annexure 15**).

2.20.6 With effect from quarter ending March 2019, registered Depository Participants using AI/ML based application or system as defined in **Para 2.20.4**, are required to fill in the form (**Annexure 15**) and make submissions on quarterly basis within 15 calendar days of the expiry of the quarter.

2.20.7 Depositories have to consolidate and compile a report, on AI/ML applications and systems reported by registered Depository Participants in

the reporting format (**Annexure 16)** on quarterly basis. The said report (**Annexure 16**) shall be submitted in soft copy only at AI_DEP@sebi.gov.in (for Depositories) to SEBI within 30 calendar days of the expiry of the quarter, starting from quarter ending March 2019.

2.21 Flashing a link to SCOREs on the dashboard of Demat Accounts[111]

2.21.1 A study was conducted under aegis of Quality Council of India (QCI) to understand some of the root causes of grievances / complaints on securities market related issues lodged on Centralised Public Grievance Redressal and Monitoring System (CPGRAMS) portal and the measures suggested to address the issues included providing a link to SCORES portal within Demat/Trading Account Dashboard of the Clients/ investors to make it easier to lodge grievances.

2.21.2 The suggestion has been examined and it has been decided to implement the same. Accordingly, depositories are advised to issue necessary directions to depository participants to ensure that the Demat Account Dashboard of clients/investors provides a link to SCORES portal.

2.22 Displaying of information regarding SEBI Complaint Redress System (SCORES) in the website[112]

2.22.1 SEBI has commenced processing of complaints through SCORES since June, 2011.

2.22.2 With a view to make the complaint redressal mechanism through SCORES more efficient, all Depository Participants are directed to display the following information on their websites:

Filing complaints on SCORES – Easy & quick

a. Register on SCORES portal

b. Mandatory details for filing complaints on SCORES:

- ***i.*** Name, PAN, Address, Mobile Number, Email ID

c. Benefits:

- ***i.*** Effective communication
- ***ii.*** Speedy redressal of the grievances

2.22.3 Further, all the Depository Participants to include procedure for filing of complaints on SCORES and benefits for the same in the welcome kit to be given to the investors at the time of their registration with them.

2.22.4 The Depositories are advised to bring the contents to the notice of Depository Participants for necessary action.

---

[111] Reference: SEBI Letter MIRSD2/DB/AEA/OW/2018/7292 dated March 07, 2018

[112] Reference: SEBI Letter SEBI/MIRSD/16742/2019 dated July 03, 2019

2.23 ***Block Mechanism in demat account of clients undertaking sale transactions***[113]

Kindly refer para titled 'Block Mechanism in demat account of clients undertaking sale transactions' of SEBI Circular SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2023/71 dated May 17, 2023 (Master circular for Stock Brokers)

2.24 ***Validation of Instructions for Pay-In of Securities from Client demat account to Trading Member (TM) Pool Account against obligations received from the Clearing Corporations***[114]

Kindly refer para titled 'Validation of Instructions for Pay-In of Securities from Client demat account to Trading Member (TM) Pool Account against obligations received from the Clearing Corporations' of SEBI Circular SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2023/71 dated May 17, 2023 (Master circular for Stock Brokers)

2.25 ***MONITORING AND PERIODICAL REPORTING OF THE COMPLIANCE WITH THE REQUIREMENTS PERTAINING TO 'SECURITY AND COVENANT MONITORING' SYSTEM HOSTED BY DEPOSITORIES***[115]

2.25.1 Depositories shall ensure periodic monitoring regarding compliance with the requirements of various provisions pertaining to 'Security & Covenant Monitoring System' issued by SEBI from time to time, including circular SEBI/HO/DDHS-PoD1/P/CIR/2023/109 dated March 31, 2023, and shall also bring to the notice of SEBI, any instances of noncompliance, on a quarterly basis, not later than one month from the end of the quarter, in the format specified as under:

ISIN	Stakeholders involved & their status of compliance	Reference to the provision of the relevant circulars pertaining to non-compliance	Reasons/ remarks for such non-compliance	Date of compliance / expected date of compliance
	<Name of the Issuer>			
	<Name of the Debenture Trustee>			
	<Name of the Credit Rating Agency>			

[113] Reference: SEBI Circular SEBI/HO/MIRSD/DOP/P/CIR/2021/595 dated July 16, 2021, SEBI Circular SEBI/HO/MIRSD/DoP/P/CIR/2022/109 dated August 18, 2022 & SEBI Circular SEBI/HO/MIRSD/DoP/P/CIR/2022/143 dated October 27, 2022

[114] Reference: SEBI Circular SEBI/HO/MIRSD/DoP/P/CIR/2022/119 dated September 19, 2022

[115] Reference: SEBI Circular SEBI/HO/DDHS/RACPOD1/CIR/P/2023/0002 dated January 05, 2023

2.26 *MAINTENANCE of a website by depository participants* [116]

2.26.1 Considering the advancement in technology and need to provide better services to the investors, all DPs are mandated to maintain a designated website.

2.26.2 Such website shall mandatorily display the following information, in addition to all such information, which have been mandated by SEBI/depositories from time to time.

2.26.2.1 Basic details of the DP such as registration number, registered address of Head Office and branches, if any.

2.26.2.2 Names and contact details such as email ids etc. of all key managerial personnel (KMPs) including compliance officer.

2.26.2.3 Step-by-step procedures for opening an account, filing a complaint on a designated email id, and finding out the status of the complaint, etc.

2.26.2.4 Details of Authorized Persons.

2.26.3 Any modification in the URL to the website of a DP shall be reported to the depositories within 3 days of such change.

2.27 *Advisory for SEBI Regulated Entities (REs) regarding Cybersecurity best practices*[117]

2.27.1 An efficient and effective response to and recovery from a cyber-incident by REs are essential to limit any related financial stability risks. For ensuring the same, Financial Computer Security Incident Response Team (CSIRT-Fin) has provided important recommendations in its report sent to SEBI. The applicable recommendations, in the form of an advisory, are provided under **Para 2.27.4**

2.27.2 This advisory should be read in conjunction with the applicable SEBI circulars (including but not limited to Cybersecurity and Cyber Resilience framework, Annual System Audit framework, etc.) and subsequent updates issued by SEBI from time to time.

2.27.3 The compliance of the advisory shall be provided by the REs along with their cybersecurity audit report (conducted as per the applicable SEBI Cybersecurity and Cyber Resilience framework). The compliance shall be submitted as per the existing reporting mechanism and frequency of the respective cybersecurity audit.

2.27.4 In view of the increasing cybersecurity threat to the securities market, SEBI Regulated Entities (REs) are advised to implement the following practices as recommended by CSIRT-Fin:

2.27.4.1 **Roles and Responsibilities of Chief Information Security Officer (CISO)/ Designated Officer:**

---

[116] Reference: SEBI Circular SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2023/30 dated February 15, 2023

[117] Reference: SEBI Circular SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/032 dated February 22, 2023

REs are advised to define roles and responsibilities of Chief Information Security Officer (CISO) and other senior personnel. Reporting and compliance requirements shall be clearly specified in the security policy.

2.27.4.2 **Measures against Phishing attacks/ websites:**

2.27.4.2.1 The REs need to proactively monitor the cyberspace to identify phishing websites w.r.t. to REs domain and report the same to CSIRT-Fin/CERT-In for taking appropriate action.

2.27.4.2.2 Majority of the infections are primarily introduced via phishing emails, malicious adverts on websites, and third-party apps and programs. Hence, thoughtfully designed security awareness campaigns that stress the avoidance of clicking on links and attachments in email, can establish an essential pillar of defense. Additionally, the advisories issued by CERT-In/ CSIRT-Fin may be referred for assistance in conducting exercises for public awareness.

2.27.4.3 **Patch Management and Vulnerability Assessment and Penetration Testing (VAPT):**

2.27.4.3.1 All operating systems and applications should be updated with the latest patches on a regular basis. As an interim measure for zero-day vulnerabilities and where patches are not available, virtual patching can be considered for protecting systems and networks. This measure hinders cybercriminals from gaining access to any system through vulnerabilities in end-of-support and end-of-life applications and software. Patches should be sourced only from the authorized sites of the OEM.

2.27.4.3.2 Security audit / Vulnerability Assessment and Penetration Testing (VAPT) of the application should be conducted at regular basis and in accordance with the Cyber Security and Cyber Resilience circulars of SEBI issued from time to time.

The observation/ gaps of VAPT/Security Audit should be resolved as per the timelines prescribed by SEBI.

2.27.4.4 **Measures for Data Protection and Data breach:**

2.27.4.4.1 REs are advised to prepare detailed incident response plan.

2.27.4.4.2 Enforce effective data protection, backup, and recovery measures.

2.27.4.4.3 Encryption of the data at rest should be implemented to prevent the attacker from accessing the unencrypted data.

2.27.4.4.4 Identify and classify sensitive and Personally Identifiable Information (PII) data and apply measures for encrypting such data in transit and at rest.

2.27.4.4.5 Deploy data leakage prevention (DLP) solutions / processes.

2.27.4.5 **Log retention:**

Strong log retention policy should be implemented as per extant SEBI regulations and required by CERT-In and IT Act 2000. REs are advised to audit that all logs are being collected. Monitoring of all logs of events and incidents to identify unusual patterns and behaviours should be done.

2.27.4.6 **Password Policy/ Authentication Mechanisms:**

2.27.4.6.1 Strong password policy should be implemented. The policy should include a clause of periodic review of accounts of ex-employees Passwords should not be reused across multiple accounts or list of passwords should not be stored on the system.

2.27.4.6.2 Enable multi factor authentication (MFA) for all users that connect using online/internet facility and also particularly for virtual private networks, webmail and accounts that access critical systems.

2.27.4.6.3 Maker and Checker framework should be implemented in strict manner and MFA should be enabled for all user accounts, especially for user accounts accessing critical applications.

2.27.4.7 **Privilege Management:**

2.27.4.7.1 Maker-Checker framework should be implemented for modifying the user's right in internal applications.

2.27.4.7.2 For mitigating the insider threat problem, 'least privilege' approach to provide security for both on-and off-premises resources (i.e., zero-trust models) should be implemented. Zero Trust is rooted in the principle of "trust nothing, verify everything." This security model requires strict identity verification for each and every resource and device attempting to get access to any information on a private network, regardless of where they are situated, within or outside of a network perimeter.

2.27.4.8 **Cybersecurity Controls:**

2.27.4.8.1 Deploy web and email filters on the network. Configure these devices to scan for known bad domains, sources, and addresses, block these before receiving and downloading messages. Scan all emails, attachments, and downloads both on the host and at the mail gateway with a reputable antivirus solution.

2.27.4.8.2 Block the malicious domains/IPs after diligently verifying them without impacting the operations. CSIRT-Fin/CERT-In advisories which are published periodically should be referred for latest malicious domains/IPs, C&C DNS and links.

2.27.4.8.3 Restrict execution of "powershell" and "wscript" in enterprise environment, if not required. Ensure installation and use of the latest version of PowerShell, with enhanced logging enabled, script block

logging and transcription enabled. Send the associated logs to a centralized log repository for monitoring and analysis.

2.27.4.8.4 Utilize host based firewall to prevent Remote Procedure Call (RPC) and Server Message Block (SMB) communication among endpoints whenever possible. This limits lateral movement as well as other attack activities.

2.27.4.8.5 Practice of whitelisting of ports based on business usage at Firewall level should be implemented rather than blacklisting of certain ports. Traffic on all other ports which have not been whitelisted should be blocked by default.

2.27.4.9 **Security of Cloud Services:**

2.27.4.9.1 Check public accessibility of all cloud instances in use. Make sure that no server/bucket is inadvertently leaking data due to inappropriate configurations.

2.27.4.9.2 Ensure proper security of cloud access tokens. The tokens should not be exposed publicly in website source code, any configuration files etc.

2.27.4.9.3 Implement appropriate security measures for testing, staging and backup environments hosted on cloud. Ensure that production environment is kept properly segregated from these. Disable/remove older or testing environments if their usage is no longer required.

2.27.4.9.4 Consider employing hybrid data security tools that focus on operating in a shared responsibility model for cloud-based environments.

2.27.4.10 **Implementation of CERT-In/ CSIRT-Fin Advisories:**

The advisories issued by CERT-In should be implemented in letter and spirit by the regulated entities. Additionally, the advisories should be implemented promptly as and when received.

2.27.4.11 **Concentration Risk on Outsourced Agencies:**

2.27.4.11.1 It has been observed that single third party vendors are providing services to multiple REs, which creates concentration risk. Here, such third parties though being small non-financial organizations, if any cyber-attack, happens at such organizations, the same could have systemic implication due to high concentration risk.

2.27.4.11.2 Thus, there is a need for identification of such organizations and prescribing specific cyber security controls, including audit of their systems and protocols from independent auditors, to mitigate such concentration risk.

2.27.4.11.3 Further, REs also need to take into account this concentration risk while outsourcing multiple critical services to the same vendor.

2.27.4.12 **Audit and ISO Certification:**

2.27.4.12.1 SEBI's instructions on external audit of REs by independent auditors empaneled by CERT-In should be complied with in letter and spirit.

2.27.4.12.2 The REs are also advised to go for ISO certification as the same provides a reasonable assurance on the preparedness of the RE with respect to cybersecurity.

2.27.4.12.3 Due diligence with respect to audit process and tools used for such audit needs to be undertaken to ensure competence and effectiveness of audits.

2.28 Combating Financing Of Terrorism (CFT) under Unlawful Activities (Prevention) Act, 1967 – Directions to Stock Exchanges, Depositories and all Registered Intermediaries

Kindly refer SEBI Circular SEBI/HO/MIRSD/MIRSD-SEC-5/P/CIR/2023/022 dated February 03, 2023 (Guidelines on Anti-Money Laundering (AML) Standards and Combating the Financing of Terrorism (CFT) /Obligations of Securities Market Intermediaries under the Prevention of Money Laundering Act, 2002 and Rules framed thereunder)

2.29 Framework for Adoption of Cloud Services by SEBI Regulated Entities (REs)[118]

Kindly refer SEBI Circular SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/033 dated March 06, 2023 in respect of Adoption Of Cloud Services By SEBI Regulated Entities for necessary compliance in respect of Depository Participants.

2.30 Cyber Security Operations Center for SEBI registered intermediaries[119]

2.30.1 Recognizing the need for a robust Cyber Security and Cyber Resilience framework at Market Infrastructure Institutions (MIIs), i.e. Stock Exchanges, Clearing Corporations and Depositories, SEBI under **Para 4.41**, has prescribed a detailed regulatory framework on cyber security and cyber resilience.

2.30.2 With the view to further strengthening cyber security in securities market the Cyber Security and Cyber Resilience framework has been extended to Depository Participants under vide **Para 2.17**

2.30.3 During the discussions held with the market participants, it was gathered that compliance with the cyber security guidelines may be onerous for smaller intermediaries because of the lack of knowledge in cyber security and also the cost factor involved in setting up own Security Operations Center (SOC). These intermediaries may utilize the services of Market SOC which is proposed to be set up by MIIs with the objective of providing cyber security solution to such intermediaries. The intermediaries' membership in Market SOC is non-mandatory.

2.30.4 The particulars of the Market SOC will be as follows:

[118] Reference: SEBI Circular SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/033 dated March 06, 2023
[119] Reference: SEBI Circular CIR/MRD/CSC/151/2018 dated December 14, 2018

2.30.4.1 The Market SOC shall be set up as a separate entity and MIIs shall have at least 51% stake in the new entity.

2.30.4.2 Intermediaries who do not have capability to set up a SOC on their own can opt for the Market SOC.

2.30.4.3 The Market SOC should be in accordance with **Para 2.17** and should ensure that participating intermediaries are in compliance to the said circular, should they opt for the market SOC. Market SOC would provide only the technology perspective for the abovementioned cyber security guidelines and the people & process perspectives of cyber security as mandated by the aforementioned circular would still be have to be managed by the intermediaries.

2.30.4.4 The Market SOC should be evolving continuously in order to be able to manage new security controls and guidelines that may issue by SEBI from time to time.

2.30.4.5 The Market SOC to ensure that intermediaries participating in their SOC should adhere to the minimum IT guidelines and security protocols all the time.

2.30.4.6 MII will carry out audit of their Market SOC activity annually and submit the report to SEBI.

2.30.4.7 The Market SOC will issue an audit report as prescribed under **Para 2.17**, to the participating intermediary.

2.30.4.8 If an intermediary is subscribed to Market SOC, audit report submitted by intermediary through the Market SOC would be deemed compliant.

2.30.4.9 Approval for the Market SOC which is to be set up as a separate entity would be in terms of Regulation 38 of Securities Contracts (Regulation) (Stock Exchanges and Clearing Corporations) Regulations, 2018.

SECTION 3: Issuer Related

3.1 Charges to be paid by Issuers [120]

3.1.1 Depositories may levy and collect the charges towards custody from the issuers, on the basis of average no. of folios (ISIN position) during the previous financial year, as per the details given below:

3.1.1.1 Issuers to pay @ Rs.11.00 (*) per folio (ISIN position) in the respective depositories, subject to a minimum as mentioned below:

Nominal value of admitted securities (Rs.)	*Annual Custodial Fee payable by an Issuer to each Depository (Rs.)(*)*
Upto 5 crore	9,000
Above 5 crore and upto 10 crore	22,500
Above 10 crore and upto 20 crore	45,000
Above 20 crore	75,000

**** Plus service tax as applicable***

3.1.2 The average no. of folios (ISIN positions) for an Issuer may be arrived at by dividing the total number of folios for the entire financial year by the total number of working days in the said financial year.

3.1.3 Temporary ISIN shall not be considered for the purpose of computing the annual issuer charges.

If the issuer fails to make the payment, Depositories may charge penal interest subject to a maximum of 12% per annum

3.2 Activation of ISIN in case of IPO and additional issue of shares/ securities

3.2.1 Depositories shall activate the ISINs only on the date of commencement of trading on the stock exchanges in case of IPOs for both the equity and debt securities.[121]

3.2.2 Further, in order to curtail the transfer of additional issue of shares/ securities including by way of further public offerings, rights issue, preferential allotment, bonus issue etc of the listed company, prior to receipt of final listing / trading approval, the depositories shall devise a mechanism so that such new securities

[120] Reference: SEBI Circular SEBI/MRD/SE/DEP/Cir-4/2005 dated January 28, 2005, SEBI Circular MRD/DoP/SE/Dep/Cir-2/2009 dated February 10, 2009, SEBI Circular CIR/MRD/DP/05/2011 dated April 27, 2011 and SEBI Circular CIR/MRD/DP/18/2015 dated December 09, 2015

[121] Reference: SEBI Circular SEBI/MRD/DEP/Cir-2/06 dated January 19, 2006 and SEBI Circular CIR/MRD/DP/ 21 /2012 dated August 02, 2012 and DDHS email dated February 20, 2020

created shall be frozen till the time final listing/ trading permission is granted by the exchange.[122]

3.2.3 In order to achieve the above, the Depositories are advised to allot such additional shares/securities under a new temporary ISIN which shall be kept frozen. Upon receipt of the final listing/ trading permission from the exchange for such additional shares/ securities, the shares/securities credited in the new temporary ISIN shall be debited and the same would get credited in the pre existing ISIN for the said security. Thereafter, the additional securities shall be available for trading.

3.2.4 The stock exchanges are advised to provide the details to the depositories whenever final listing / trading permission is given to securities. Further, in case of issuance of equity shares by a company, listed on multiple stock exchanges, the concerned stock exchanges shall synchronize their effective dates of listing / trading approvals and intimate the same to depositories in advance.

3.2.5 In similar lines, depositories are advised to follow similar process as provided above even in case of units of REITs/InvITs as securities of a listed company.

3.3 Streamlining the Process of Rights Issue[123]

Kindly refer para titled 'Streamlining the process of Rights Issue' of SEBI Circular SEBI/HO/CFD/PoD-2/P/CIR/2023/00094 dated June 21, 2023 (Master Circular for Issue of Capital and Disclosure Requirements)

3.4 Registrar and Share Transfer Agent

3.4.1 Appointment of a single agency for share registry work[124]

All work related to share registry pertaining in terms of both physical and electronic shares shall be maintained at a single point i.e. either in-house by the company or by a SEBI registered Registrar and Transfer Agent.

3.4.2 Inter-Depository transfers[125]

In case of inter-Depository transfers of securities, the Registrars shall communicate the confirmation of such transfers within two hours, failing which such transfers shall be deemed to have been confirmed. The Registrars shall not reject inter-Depository transfers except where

i. A Depository does not have adequate balance of securities in its account or

ii. there is mismatch of transfer requests from the Depositories.

3.4.3 Common Registrars and Share Transfer agents[126]

[122] Reference: SEBI Circular CIR/MRD/DP/24/2012 dated September 11, 2012
[123] Reference: SEBI Circular SEBI/HO/CFD/DIL2/CIR/P/2020/13 dated January 22, 2020
[124] Reference: SEBI Circular D&CC/FITTC/Cir-15/2002 dated December 27, 2002
[125] Reference: SEBI Circular SMDRP/Policy/Cir-28/99 dated August 23, 1999
[126] Reference: SEBI Circular SMDRP/Policy/Cir-28/99 dated August 23, 1999

Every company shall appoint the same Registrars and Share Transfer agents for both the depositories.

3.4.4 Dematerialisation requests[127]

3.4.4.1 Registrars and Share Transfer agents shall accept partial dematerialisation requests and will not reject or return the entire dematerialization request where only a part of the request had to be rejected. In cases where a DP has already sent information about dematerialisation electronically to a Registrar but physical shares have not yet been delivered, the Registrar shall accept the demat request and carry out dematerialization on an indemnity given by the DP and proof of dispatch of document given by DP.

3.4.4.2 The above provision shall be applicable to all the securities like scrips, bonds, debentures, debenture stock or other marketable securities eligible to be held in dematerialised form in a depository as defined in Regulation 42 of the DP Regulations.

3.5 *American Depository Receipts (ADRs)/Global Depository Receipts (GDRs)*

3.5.1 Delivery of underlying shares of GDRs/ADRs in dematerialised form[128]

Underlying shares of GDRs/ADRs shall be compulsorily delivered in dematerialised form. Pursuant to RBI directions in this regard, a non-resident holder of ADRs/GDRs issued by a company registered in India, on surrender of such ADRs/GDRs, can acquire the underlying shares when such shares are released by the Indian Custodian of the ADR/GDR issue. Further, the company whose shares are so released, or a Depository shall enter in the register or books, wherein such securities are registered or inscribed, an address outside India of the non-resident holder of shares.

3.5.2 Tracking of underlying shares of GDRs/ADRs[129]

To ensure easy tracking of the underlying shares released on conversion of the "depositories receipts" all such shares shall be credited to a separate Depository Receipts (DRs) account of the respective investor. In this regard, Depositories shall ensure that the following information is provided to the domestic custodian holding the underlying shares on a regular basis:

i. Total number of shares at the beginning of the month
ii. Number of shares transferred into the account (credited) during the month
iii. Number of shares transferred out of the account (debited) during the month.
iv. Balance at the end of the month.

---

[127] Reference: SEBI Letter D&CC/ 1099 / 2002 dated November 01, 2002
[128] Reference: SEBI Circular SMDRP/Policy/Cir-9/99 dated May 6, 1999
[129] Reference: SEBI Circular D&CC/FITTC/Cir-09/2002 dated July 4, 2002 and SEBI Circular D&CC/FITTC/Cir-10/2002 dated September 25, 2002

This service can be availed of only by foreign investors other than the OCBs.

3.6 Framework for issue of Depository Receipts (DRs)[130]

3.6.1 Reference is drawn to Section 41 of the Companies Act, 2013, Companies (Issue of Global Depository Receipts) Rules, 2014 ('GDR Rules'), the Depository Receipts Scheme, 2014 ('DR Scheme'), Reserve Bank of India ('RBI') notification dated December 15, 2014, Central Government notification dated September 18, 2019 and Central Government notification dated October 07, 2019.

3.6.2 Only 'a company incorporated in India and listed on a Recognized Stock Exchange in India' ('Listed Company') may issue Permissible Securities or their holders may transfer Permissible Securities, for the purpose of issue of DR, subject to compliance with the following requirements:

Eligibility

3.6.2.1 Listed Company is in compliance with the requirements prescribed under LODR Regulations and any amendments thereof.

3.6.2.2 Listed company shall be eligible to issue Permissible Securities, for the purpose of issue of DRs, if:

3.6.2.2.1 the Listed Company, any of its promoters, promoter group or directors or selling shareholders are not debarred from accessing the capital market by SEBI;

3.6.2.2.2 any of the promoters or directors of the Listed Company is a promoter or director of any other company which is not debarred from accessing the capital market by SEBI;

3.6.2.2.3 the listed company or any of its promoters or directors is not a wilful defaulter;

3.6.2.2.4 any of its promoters or directors is not a fugitive economic offender.

3.6.2.3 Existing holders shall be eligible to transfer Permissible Securities, for the purpose of issue of DRs, if:

3.6.2.3.1 the Listed Company or the holder transferring Permissible Securities are not debarred from accessing the capital market by SEBI;

3.6.2.3.2 the Listed Company or the holder transferring Permissible Securities is not a wilful defaulter;

3.6.2.3.3 the holder transferring Permissible Securities or any of the promoters or directors of the Listed Company are not a fugitive economic offender.

Explanation 1: The restrictions at **Para 3.6.2.2** and **Para 3.6.2.3** above shall not apply to the persons or entities mentioned therein, who were debarred in the

[130] Reference: SEBI Circular SEBI/HO/MRD/DOP1/CIR/P/2019/106 dated October 10, 2019, and SEBI Circular SEBI/HO/MRD/DCAP/CIR/P/2020/190 dated October 01, 2020

past by SEBI and the period of debarment is already over as on the date of filing of the document as referred at **Para 3.6.2.13**

Explanation 2: DR means a foreign currency denominated instrument, listed on an international exchange, issued by a foreign depository in a permissible jurisdiction on the back of permissible securities issued or transferred to a domestic custodian and includes 'global depository receipt' as defined in section 2(44) of the Companies Act, 2013.

Explanation 3: 'Foreign Depository' means a person which:

a) is not prohibited from acquiring permissible securities;
b) is regulated in any of the Permissible Jurisdiction as defined here; and
c) has legal capacity to issue DRs in the Permissible Jurisdiction where issue of DRs is proposed.

Explanation 4: 'transfer of permissible securities by existing holders' means deposit of existing Permissible Securities of the Listed Company with a Domestic Custodian, for the purpose of issue of DRs, pursuant to formal agreement(s) among the Listed Company and the Foreign Depository. For this purpose, the Listed Company may also enter into arrangement(s) with, Indian Depository, Domestic Custodian and existing Permissible Securities holder(s), as may be necessary.

3.6.2.4 For the purpose of an initial issue and listing of DRs, pursuant to 'transfer by existing holders', the Listed Company shall provide an opportunity to its equity shareholders to tender their shares for participation in such listing of DRs.

3.6.2.5 Subsequent issue and listing of DRs, pursuant to 'transfer by existing shareholders' may take place subject to the limits approved pursuant to a special resolution in terms of GDR Rules.

3.6.2.6 A company proposing to make a public offer and list on a Recognized Stock Exchange, and also simultaneously proposing to issue Permissible Securities or transfer Permissible Securities of existing holders, for the purpose of issue of DRs and listing such DRs on an International Exchange, may seek in-principle and final approval from Recognized Stock Exchange as well as International Exchange. However, such issue or transfer of Permissible Securities for the purpose of issue of DRs shall be subsequent to, the receipt of trading approval from the Recognized Stock Exchange for the public offer.

Permissible Jurisdictions and International Exchanges

3.6.2.7 Listed Company shall be permitted to issue Permissible Securities or transfer Permissible Securities of existing holders, for the purpose of issue of DRs, only

in Permissible Jurisdictions and said DRs shall be listed on any of the specified International Exchange(s) of the Permissible Jurisdiction.

Explanation 1: 'Permissible Jurisdiction' shall mean jurisdictions as may be notified by the Central Government from time to time, pursuant to notification no. G.S.R. 669(E) dated September 18, 2019 in respect of sub-rule 1 of rule 9 of Prevention of Money-Laundering (Maintenance of Records) Rules, 2005.

Explanation 2: 'International Exchange(s)' shall mean exchange(s) as may be notified by SEBI from time to time**.**

Note[131]: The Central Government vide notification dated November 28, 2019, notified the list of Permissible Jurisdictions in pursuance of notification dated September 18, 2019. Accordingly, a list of Permissible Jurisdictions and International Exchange(s) is placed below:

List of Permissible Jurisdictions and International Exchanges

1. United States of America - NASDAQ, NYSE
2. Japan - Tokyo Stock Exchange
3. South Korea - Korea Exchange Inc.
4. United Kingdom excluding British Overseas Territories- London Stock Exchange
5. France - Euronext Paris
6. Germany - Frankfurt Stock Exchange
7. Canada - Toronto Stock Exchange
8. International Financial Services Centre in India - India International Exchange, NSE International Exchange

3.6.2.8 Listing of DRs on specified International Exchange shall meet the highest applicable level / standards for such listing by foreign issuers.

Explanation: Examples of DR listing programs that would qualify for the aforesaid criteria:

Issuer-sponsored Level III ADR programs listed on Nasdaq or the NYSE, DRs listed on the Main Board of the Hong Kong Stock Exchange, Global Depositary Receipts admitted to the Standard Segment of the Official List of the FCA and to trading on the London Stock Exchange.

Obligations of Listed Company

3.6.2.9 Listed Company shall ensure compliance with extant laws relating to issuance of DRs, including, requirements prescribed here, the Companies Act, 2013, the Foreign Exchange Management Act, 1999 ('FEMA'), Prevention of Money-Laundering Act, 2002, and rules and regulations made thereunder. For this

[131] Reference: SEBI Circular SEBI/HO/MRD2/DCAP/CIR/P/2019/146 dated November 28, 2019

purpose, Listed Company may also enter into necessary arrangements with Custodian, Indian Depository and Foreign Depository.

3.6.2.10 Listed Company shall ensure that DRs are issued only with Permissible Securities as the underlying.

Explanation: 'Permissible Securities' shall mean equity shares and debt securities, which are in dematerialized form and rank *pari passu* with the securities issued and listed on a Recognized Stock Exchange.

3.6.2.11 Listed Company shall ensure that the aggregate of Permissible Securities which may be issued or transferred for the purpose of issue of DRs, along with Permissible Securities already held by persons resident outside India, shall not exceed the limit on foreign holding of such Permissible Securities under the applicable regulations of FEMA:

Provided that within the above limit, the maximum of aggregate of Permissible Securities which may be issued by the Listed Company or transferred by the existing holders, for the purpose of issue of DRs, shall be such that the Listed Company is able to ensure compliance with the minimum public shareholding requirement, after excluding the Permissible Securities held by the depository for the purpose of issue of DRs.

3.6.2.12 Listed Company shall ensure that the agreement entered with the Foreign Depository, for the purpose of issue of DRs, provides that the Permissible holder, including its Beneficial Owner(s), shall ensure compliance with holding limits prescribed under **Para 3.6.2.19**

A. The onus of identification of NRIs holders, who are issued DRs in terms employee benefit scheme, would lie with the listed company. The listed company shall provide the information of such NRI DR holders to the designated depository for the purpose of monitoring of limits[132]

3.6.2.13 Listed Company shall, through an intermediary, file with SEBI and the Recognized Stock Exchange(s), a copy of the initial document, by whatever name called, for initial issue of DRs issued on the back of Permissible Securities.

3.6.2.13.1 SEBI shall endeavor to forward its comments, if any, to the Recognized Stock Exchange(s) within a period of 7 working days from the receipt of the document and in the event of no comments being issued by SEBI within such period, it shall be deemed that SEBI does not have comments to offer.

3.6.2.13.2 Recognized Stock Exchange(s) shall take into consideration the comments of SEBI while granting in-principle approval to the Listed Company and decide on the approval within 15 working days of receipt of application and required documents.

[132] Reference: SEBI Circular SEBI/HO/MRD2/DCAP/CIR/P/2020/243 dated December 18, 2020

Further, final document for such initial issue shall be filed with Recognized Stock Exchange(s) and SEBI for record purpose.

3.6.2.14 Listed Company shall ensure that any public disclosures made by the Listed Company on International Exchange(s) in compliance with the requirements of the Permissible Jurisdiction where the DRs are listed or of the International Exchange(s), are also filed with the Recognized Stock Exchange as soon as reasonably possible but not later than twenty-four hours from the date of filing.

Permissible holder [133]

3.6.2.15 Permissible holder means a holder of DR, including its Beneficial Owner(s), satisfying the following conditions:

a. who is not a person resident in India;

b. who is not a Non-Resident Indian (NRI)

Provided that the restriction under this Clause shall not apply in case of issue of DRs to NRIs, pursuant to share based employee benefit schemes which are implemented by a company in terms of SEBI (Share Based Employee Benefits) Regulations 2014;

Provided further that the restriction under this Clause shall also not apply in case of issue of DRs by the company to NRIs pursuant to a bonus issue or a rights issue;

Explanation 1: For the purpose of this Circular, 'Beneficial Owner' shall have the same meaning as provided in proviso to sub-rule 1 of rule 9 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005, as amended by the Central Government vide notification no.G.S.R.669(E) dated September 18, 2019.

Explanation 2: The Permissible holder, including its Beneficial Owner(s), shall be responsible for ensuring compliance with this requirement.

Explanation 3: Except as permitted under the provisos above, NRIs shall neither subscribe to any further issue of DRs nor make any further acquisition of DRs (including of DRs issued prior to October 10, 2019).

Voting rights

3.6.2.16 Listed Company shall ensure that the agreement entered between the holder of DRs, the Listed Company and the Depository provides that the voting rights on Permissible Securities, if any, shall be exercised by the DR holder through the Foreign Depository pursuant to voting instruction only from such DR holder.

[133] Reference: SEBI Circular SEBI/HO/MRD2/DCAP/CIR/P/2020/243 dated December 18, 2020

Pricing

3.6.2.17 In case of a simultaneous listing of, Permissible Securities on Recognised Stock Exchange(s) pursuant to a public offer / preferential allotment / qualified institutions placement under ICDR Regulations, and DRs on the International Exchange, the price of issue or transfer of Permissible Securities, for the purpose of issue of DRs by Foreign Depository, shall not be less than the price for the public offer / preferential allotment / qualified institutions placement to domestic investors under the applicable laws.

3.6.2.18 Where Permissible Securities are issued by a Listed Company or 'transferred by the existing holders', for the purpose of issue of DRs by the Foreign Depository, the same shall be issued at a price, not less than the price applicable to a corresponding mode of issue of such Permissible Securities to domestic investors under the applicable laws.

Obligations of Indian Depository, Foreign Depository and Domestic Custodian

3.6.2.19 Indian Depositories, in consultation with each other, shall develop a system to ensure that aggregate holding of DR holders along with their holding, if any, through offshore derivative instruments and holding as a Foreign Portfolio Investor belonging to same investor group shall not exceed the limit on foreign holding under the FEMA and applicable SEBI Regulations. For this purpose, Indian Depositories shall have necessary arrangement with the Domestic Custodian and / or Foreign Depository.

Explanation- For the purposes of above para, the term 'investor group' shall have the meaning as prescribed to such term in the Securities and Exchange Board of India (Foreign Portfolio Investors) Regulations, 2019 or amendments thereof.

The Broad operational guidelines for the above purpose are given under **3.6.3.19.1 to 3.6.3.19.6**.

Indian Depositories, in consultation with each other and market participants, may prescribe the formats and other details, as may be necessary to operationalize the same.

Broad Operational Guidelines

3.6.2.19.1 Listed Company shall appoint one of the Indian Depository as the Designated Depository for the purpose of monitoring of limits in respect of Depository Receipts.

3.6.2.19.2 The Designated Depository in co-ordination with Domestic Custodian, other Depository and Foreign Depository (if required) shall compute, monitor and disseminate the Depository Receipts (DRs) information as prescribed in the framework. The said information shall be disseminated on website of both the Indian Depositories. For this purpose, the

Designated Depository shall act as a Lead Depository and the other depository shall act as a Feed Depository.

3.6.2.19.3 Domestic Custodian shall:

3.6.2.19.3.1 Provide one-time details of DRs in the format and manner as may be prescribed by the Indian Depositories.

3.6.2.19.3.2 Provide the requisite information as may be prescribed by Designated Depository for the purpose of computation of information in respect of Depository Receipts as and when requested.

3.6.2.19.3.3 Ensure that the underlying permissible securities, pertaining to a listed company, against which DRs are issued in the Permissible Jurisdiction, are held in a demat account, under a separate Type & Sub-Type as prescribed by the Indian Depositories for the purpose of issue of DRs.

3.6.2.19.3.4 Provide certificate / declaration / information, to the Designated Depository in the prescribed format upon termination/cancellation of DR program. For this, the issuer or Foreign Depository shall be required to report such termination / cancellation to the Domestic Custodian.

3.6.2.19.4 **Procedure for the purpose of monitoring of limits**

3.6.2.19.4.1 The Designated Depository shall forward the list of such companies (ISINs) for which it will be monitoring the DR issuance to Feed Depository. For any addition or deletion of ISINs, the Designated Depository shall communicate to the Feed Depository regarding the same through Incremental information sent on a periodic basis.

3.6.2.19.4.2 Feed Depository shall provide the ISIN wise demat holdings of investors tagged with separate sub-type to the Designated Depository on a daily basis.

3.6.2.19.4.3 The Designated Depository shall ascertain the details of holdings pertaining to Foreign Depository lying under demat account(s) tagged under such separate Type & Sub-Type as well as other investors with 'DR' sub type held at both depositories and consolidate such holdings to arrive at the outstanding Permissible Securities against which the DRs are outstanding.

3.6.2.19.4.4 Calculation of headroom i.e. 'the limit up to which Permissible Securities can be converted to DRs', may be undertaken in the following manner:

	Particulars
(A)	Number of DRs originally issued including corporate action

(B)	Outstanding Permissible Securities against which the DRs are outstanding
(C)	Re-issuance approval granted by Domestic Custodian (unutilized) at End of Day
Headroom = A – (B + C)	**the limit up to which Permissible Securities can be converted to DRs**

3.6.2.19.4.5 The Indian Depositories shall exchange with each other their respective list of companies, for dissemination of DR headroom related information, which shall be consolidated by both depositories and thereafter published on their respective websites.

3.6.2.19.5 **Re-issuance mechanism**

3.6.2.19.5.1 For the purpose of re-issuance of permissible securities, a Foreign Investor shall request SEBI registered Broker with requisite quantity of securities (based on available headroom) required for re-issuance of depository receipts which shall be forwarded to the Domestic Custodian.

3.6.2.19.5.2 Based on last available headroom disseminated by Designated Depository, the Domestic Custodian shall grant approval (T- day where T is date of approval granted by Domestic Custodian) to such request received from SEBI registered Broker for re-issuance purpose which shall be valid for a period of 3 trading days (T+3) from the date of approval of request granted by Domestic Custodian.

3.6.2.19.5.3 The Domestic Custodian shall report such request approvals along with requisite quantity granted to Designated Depository on same day (i.e. T day) and based on which the Designated Depository shall block the quantity for the purpose of calculation of Headroom.

3.6.2.19.5.4 The Domestic Custodian shall report the status of utilisation of such approved request to the Designated Depository upon receipt of securities in the demat account of Foreign Depository for the purpose of calculation of Headroom. The domestic custodian shall report the final utilisation status of such approved request with respect to receipt of securities on D+1 basis (where D is a date of credit of security in the Foreign Depository's account) before such time as may be prescribed by Designated Depository. In case of non-receipt of securities within the specified timeline, Custodian shall unblock the requisite quantity of approval granted and report the same to Designated Depository.

3.6.2.19.6 **Monitoring of Investor group limits**

3.6.2.19.6.1 FPI shall report the details of all such FPIs forming part of the same investor group as well as Offshore Derivative Instruments (ODI) subscribers and/or DR holders having common ownership, directly or indirectly, of more than fifty percent or on the basis of common control, to its Designated Depository Participant (DDP). The investor group may appoint one such FPI to act as a Nodal entity for reporting the aforesaid grouping information to its DDP in the format enclosed at **Annexure 17**. Further, such Nodal FPI shall report the investment holding in the underlying Indian security as held by ODI subscriber and / or as DR holder, including securities held in the Depository Receipt account upon conversion ('DR conversion' account), to its Domestic Custodian on a monthly basis (by the 10th of every month) in the format enclosed at **Annexure 18**. Similarly, the FPIs who do not belong to the same investor group shall report such investment holding details in the underlying Indian security as ODI subscriber and / or as DR holder, including securities held in the 'DR conversion' account, to its Custodian in the aforesaid format on a monthly basis (by 10th of the month).

3.6.2.19.6.2 The DDP shall report FPI grouping information as reported by Nodal FPI to such Indian Depository (by 17th of the month) where FPI group demat accounts are held in the manner and format as specified by such Indian Depository. Similarly, the Custodian of Nodal entity (who also happen to be the DDP) shall report the investment holdings in the underlying Indian security as held by the ODI subscriber and / or DR holder in respect of the aforesaid FPI group on monthly basis to such Indian Depository (by 17th of the month) where FPI group demat accounts are held in the manner and format as specified by such Indian Depository.

3.6.2.19.6.3 The Depository which monitors the FPI group limits shall club the investment pertaining to DR holding, ODI holding and FPI holding of same investor group and monitor the investment limits as applicable to FPI group in a Listed Indian company on a monthly basis. However, in respect of FPIs which do not belong to the same investor group, responsibility of monitoring the investment limits of FPI shall be with the respective DDP / Custodian. The Custodian of such FPIs not forming part of investor group shall club the investment as held by FPIs as well as investment as held by such FPI in the capacity of ODI subscriber and / or DR holder and monitor the investment limits as applicable to single FPI. In case where the

investment holding breaches the prescribed limits, the Indian Depository / Custodian, as the case may be, shall advise the concerned investor / investor group, to divest the excess holding within 5 trading days similar to requirement prescribed under SEBI Circular dated November 05, 2019 on 'Operational Guidelines for FPIs & DDPs under SEBI (Foreign Portfolio Investors), Regulations 2019 and for Eligible Foreign Investors.

3.6.2.20 Domestic Custodian shall maintain records in respect of, and report to, Indian depositories all transactions in the nature of issue and cancellation of depository receipts, for the purpose of monitoring limits.

3.6.2.21 Indian Depositories shall coordinate among themselves and with Domestic Custodian to disseminate:

(a) the outstanding Permissible Securities against which the DRs are outstanding; and,

(b) the limit up to which Permissible Securities can be converted to DRs.

3.6.2.22 The Foreign Depository shall not issue or pre-release the DRs unless the Domestic Custodian has confirmed the receipt of underlying Permissible Securities.

3.6.3 Words and expressions used and not defined here but defined in the DR Scheme, Securities Contracts (Regulation) Act, 1956 or the Securities and Exchange Board of India Act, 1992 or the Depositories Act, 1996 or the Companies Act, 2013 or the Reserve Bank of India Act, 1934 or the Foreign Exchange Management Act, 1999 or Prevention of Money-Laundering Act, 2002, and rules and regulations made thereunder shall have the meanings respectively assigned to them, as the case may be, in those Acts, unless the context requires otherwise.

Power to remove difficulties

3.6.4 In case of any difficulties in the application or interpretation or to relax strict enforcement of the aforesaid requirements, the Board may issue clarifications through guidance notes or circulars after receipt of request from the issuer.

3.6.5 The above provisions shall be applicable only to DR issuance by a Listed Company after the effective date i.e. October 10, 2019.

3.7 Redemption of Indian Depository Receipts (IDRs) into Underlying Equity Shares[134]

Kindly refer para titled 'Disclosure norms for Indian Depository Receipts' of SEBI Circular SEBI/HO/CFD/PoD2/CIR/P/2023/120 dated July 11, 2023 (Master circular for compliance with the provisions of the Securities and Exchange Board of India

[134] Reference: SEBI Circular CIR/CFD/DIL/10/2012 dated August 28, 2012 & SEBI Circular CIR/CFD/DIL/6/2013 dated March 01, 2013

(Listing Obligations and Disclosure Requirements) Regulations, 2015 by listed entities)

3.8 Electronic Clearing System (ECS) facility

3.8.1 Use of ECS for refund in public/rights issues.[135]

For locations where facility of refund through ECS is available details of applicants shall be taken directly from the database of the depositories in respect of issues made completely in dematerialised form. Accordingly, DPs shall maintain and update on real time basis the MICR (Magnetic Ink Character Recognition) code of Bank branch of BOs and other bank details of the applicants in the database of depositories. This is to ensure that the refunds through ECS are made in a smooth manner and that there are no failed/wrong credits.

3.8.2 Updation of bank accounts details, MICR code and IFSC of bank branches by Depository Participants (DPs)[136]

3.8.2.1 It has been informed by RBI that they have been receiving complaints from managers to the issues that the funds routed through the electronic mode are getting returned by destination banks because of incorrect or old account numbers provided by beneficiary account holders.

3.8.2.2 RBI has stated that Investors will have to ensure through their DPs that bank account particulars are updated in master record periodically, to ensure that their refunds, dividend payments etc. reach the correct account, without loss of time. RBI has also suggested incorporation of Indian Financial System Code (IFSC) of customer's bank branches apart from 9 digit MICR code; since IFSC of bank's branches is used for remittance through National Electronic Funds Transfer (NEFT).

3.8.2.3 It is advised that necessary action be taken in this matter to ensure that correct account particulars of investors are available in the database of depositories.

3.9 Withdrawal by issuers from the depository[137]

3.9.1 As regards voluntary withdrawal by issuers from the depository, it is informed that listed companies may not be allowed to withdraw from the depository system unless they delist their securities from the stock exchanges.

3.9.2 As regards companies under liquidation are concerned, it is informed that deactivation of the ISIN may be only done in cases where companies have been liquidated. In other cases, where companies are being liquidated, deactivation of

---

[135] Reference: SEBI Circular SEBI/MRD/DEP/Cir-3/06 dated February 21, 2006 & SEBI Circular SEBI/CFD/DIL/DIP/29/2008/01/02 dated February 1, 2008

[136] Reference: SEBI Letter MRD/DEP/PP/123624 /2008 dated April 23, 2008

[137] Reference: SEBI Letter MRD/DoP/NSDL/VM/ 162378 /2009 dated May 06, 2009

ISIN resulting in total freezing may not be desirable as it will disallow investors to hold shares in dematerialized form

3.10 ***Further issue of shares under Section 43 of Companies Act and the Companies (Share Capital and Debentures) Rules, 2014***[138]

In all cases of shares issued by companies under Section 43(a) (ii) of Companies Act 2013 and the Companies (Share Capital and Debentures) Rules, 2014, separate ISIN may be allotted to differentiate such shares from ordinary shares.

3.11 ***Redressal of investor grievances through SCORES platform***[139]

Kindly refer SEBI Circular SEBI/HO/OIAE/IGRD/P/CIR/202 dated November 07, 2022 in respect of Master Circular on the redressal of investor grievances through the SEBI Complaints Redress System (SCORES) platform.

3.12 ***Streamlining issuance of SCORES Authentication for SEBI registered intermediaries***[140]

Kindly refer para titled 'SCORES Authentication for intermediaries and MIIs' of SEBI Circular SEBI/HO/OIAE/IGRD/P/CIR/202 dated November 07, 2022 (Master Circular on the redressal of investor grievances through the SEBI Complaints Redress System (SCORES) platform)

3.13 ***Clarification on applicability of regulation 40(1) of SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 to open offers, buybacks and delisting of securities of listed entities***[141]

Kindly refer para titled 'Tendering by shareholders holding securities in physical form' of SEBI Circular SEBI/HO/CFD/PoD-1/P/CIR/2023/31 dated February 16, 2023 (Master Circular for Substantial Acquisition of Shares and Takeovers)

3.14 ***Streamlining the Process for Acquisition of Shares pursuant to Tender-Offers made for Takeovers, Buy Back and Delisting of Securities***[142]

Kindly refer para titled 'Procedure for tendering of shares and settlement through stock exchange' of SEBI Circular SEBI/HO/CFD/PoD-1/P/CIR/2023/31 dated February 16, 2023 (Master Circular for Substantial Acquisition of Shares and Takeovers)

3.15 ***Non-compliance with the Minimum Public Shareholding (MPS) requirements***[143]

---

[138] Reference: SEBI Letter MRD/DoP/MC/141442 /2008 dated October 17, 2008
[139] Reference: SEBI Circular CIR/OIAE/1/2014 dated December 18, 2014
[140] Reference: SEBI Circular SEBI/HO/OIAE/IGRD/CIR/P/2019/86 dated August 02, 2019
[141] Reference: SEBI Circular SEBI/HO/CFD/CMD1/CIR/P/2020/144 dated July 31, 2020
[142] Reference: SEBI Circular CFD/DCR2/CIR/P/2016/131 dated December 09, 2016
[143] Reference: SEBI Circular CFD/CMD/CIR/P/2017/115 dated October 10, 2017

Kindly refer para titled 'Non-compliance with the Minimum Public Shareholding requirements' of SEBI Circular SEBI/HO/CFD/PoD2/CIR/P/2023/120 dated July 11, 2023 (Master circular for compliance with the provisions of the Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015 by listed entities)

3.16 Non-compliance with certain provisions of the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 and the Standard Operating Procedure for suspension and revocation of trading of specified securities[144]

Kindly refer para titled 'Non-compliance with certain provisions of the LODR Regulations and the Standard Operating Procedure for suspension and revocation of trading of specified securities' of SEBI Circular SEBI/HO/CFD/PoD2/CIR/P/2023/120 dated July 11, 2023 (Master Circular for compliance with the provisions of the Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015 by listed entities)

3.17 Investor grievances redressal mechanism – Handling of SCORES complaints by stock exchanges and Standard Operating Procedure for non-redressal of grievances by listed companies[145]

Kindly refer para titled 'Handling of complaints by stock exchanges against certain listed companies', 'Action for failure to redress investor complaints by such listed companies' & 'Action after redressal of investor grievance by such listed companies' of SEBI Circular SEBI/HO/OIAE/IGRD/P/CIR/202 dated November 07, 2022 (Master Circular on the redressal of investor grievances through the SEBI Complaints Redress System (SCORES) platform)

3.18 Automation of Continual Disclosures under Regulation 7(2) of SEBI (Prohibition of Insider Trading) Regulations, 2015 - System driven disclosures[146]

Kindly refer para titled 'Automation of Continual Disclosures under Regulation 7(2) of SEBI (Prohibition of Insider Trading) Regulations, 2015 -System driven disclosures' of SEBI Circular SEBI/HO/ISD/ISD-PoD-2/P/CIR/2023/039 dated March 23, 2023 (Master Circular on Surveillance of Securities Market)

3.19 A Trading Window closure period under Clause 4 of Schedule B read with Regulation 9 of SEBI (Prohibition of Insider Trading) Regulations, 2015 ("PIT Regulations") –

[144] Reference: SEBI Circular SEBI/HO/CFD/CMD/CIR/P/2020/12 dated January 22, 2020
[145] Reference: SEBI Circular SEBI/HO/OIAE/IGRD/CIR/P/2020/152 dated August 13, 2020
[146] Reference: SEBI Circular SEBI/HO/ISD/ISD/CIR/P/2020/168 dated September 09, 2020 & SEBI Circular SEBI/HO/ISD/ISD/CIR/P/2021/578 dated June 16, 2021

Framework for restricting trading by Designated Persons ("DPs") by freezing PAN at security level[147]

Kindly refer para titled 'Trading Window closure period under Clause 4 of Schedule B read with Regulation 9 of PIT Regulations-Framework for restricting trading by Designated Persons ("DPs") by freezing Permanent Account Number (PAN) at security level' of SEBI Circular SEBI/HO/ISD/ISD-PoD-2/P/CIR/2023/039 dated March 23, 2023 (Master Circular on Surveillance of Securities Market)

3.20 Reconciliation of Share Capital Audit[148]

3.20.1 All the issuer companies shall subject themselves to a reconciliation of share capital audit to be undertaken by a qualified Chartered Accountant or a Company Secretary, for the purposes of reconciliation of the total admitted capital with both the depositories and the total issued and listed capital. The audit shall cover the following aspects and certify among others:

3.20.1.1 That the total of the shares held in NSDL, CDSL and in the physical form tally with the issued / paid-up capital.

3.20.1.2 That the Register of Members (RoM) is updated.

3.20.1.3 That the dematerialisation requests have been confirmed within 21 days and state the shares pending confirmation for more than 21 days from the date of requests and reasons for delay.

3.20.1.4 The details of changes in share capital (due to rights, bonus, preferential issue, IPO, buyback, capital reduction, amalgamation, de-merger etc) during the quarter and certify in case of listed companies whether in-principle approval for listing from all stock exchanges was obtained in respect of all further issues.

3.20.2 The issuer companies shall submit the audit report on a quarterly basis within 30 days of the end of each quarter to the stock exchange/s where they are listed. Any difference observed in the admitted, issued and listed capital shall be immediately brought to the notice of SEBI and both the Depositories by the stock exchanges. This report shall also be placed before the Board of Directors of the issuer company.

3.20.3 Any non-compliance by the issuer company shall be viewed seriously and suitable action shall be initiated under the Depositories Act, 1996 against the issuer company and its Directors.

3.21 Streamlining the Process of Public Issue of Equity Shares and convertibles[149]

3.21.1 Kindly refer SEBI Circular SEBI/HO/CFD/PoD-2/P/CIR/2023/00094 dated June 21, 2023 (Master Circular for Issue of Capital and Disclosure Requirements)

---

[147] Reference: SEBI Circular SEBI/HO/ISD/ISD-SEC-4/P/CIR/2022/107 dated August 05, 2022

[148] Reference: SEBI Circular D&CC/FITTC/CIR – 16/2002 dated December 31, 2002 and SEBI Circular CIR/MRD/DP/30/2010 dated September 06, 2010)

[149] Reference: SEBI Circular SEBI/HO/CFD/DIL2/CIR/P/2018/138 dated November 01, 2018

3.21.2 Further the role of depositories in respect to the Process of Public Issue of Equity Shares and convertibles is as follows:

3.21.2.1 **Validation by Depositories**

3.21.2.1.1 The details of investor viz. PAN, DP ID / Client ID, entered in the Stock Exchange platform at the time of bidding, shall be validated by the Stock Exchange/s with the Depositories on real time basis.

3.21.2.1.2 Stock Exchanges and Depositories shall put in place necessary infrastructure for this purpose.

SECTION-4: Depositories Related

4.1 *Online Registration Mechanism and Filing system for Depositories*[150]

4.1.1 In order to ease the process of application for recognition / renewal, reporting and other filings in terms of Securities and Exchange Board of India (Depositories and Participants) Regulations, 2018 and other circulars issued from time to time, SEBI has introduced a digital platform for online filings related to Depositories.

4.1.2 All applicants desirous of seeking registration as a Depository in terms of Regulation 3 of the Securities and Exchange Board of India (Depositories and Participants) Regulations, 2018, shall now submit their applications online, through SEBI Intermediary Portal at https://siportal.sebi.gov.in.

4.1.3 The applicants would be required to upload scanned copy of relevant documents such as any declaration or undertaking or notarised copy of documents as may be prescribed in Securities and Exchange Board of India (Depositories and Participants) Regulations 2018, and keep hard copy of the same to be furnished to SEBI whenever required.

4.1.4 Further, all other filings including Annual Financial Statements and Returns, Monthly Development Report, Rules, Bye-laws, etc.,shall also be submitted online.

4.1.5 The aforesaid online registration and filing system for Depositories is operational. Recognised Depositories are advised to note the same for immediate compliance.

4.1.6 Link for SEBI Intermediary Portal is also available on SEBI website – www.sebi.gov.in. In case of any queries and clarifications, users may refer to the manual provided in the portal or contact the SEBI Portal helpline on 022-26449364 or may write at portalhelp@sebi.gov.in.

4.2 *Activity schedule for depositories for T+2 rolling Settlement*[151]**-** *As on date, the activity schedule for settlement is as per SEBI circular* SEBI Circular SEBI/HO/MRD2/DCAP/P/CIR/2021/628 dated September 07, 2021 (i.e. T+1) . *The activity schedule for T+2 settlement is mentioned under* ***Para 4.83***.

4.3 *Introduction of T+1 rolling settlement on an optional basis* [152]

4.3.1 SEBI, vide circular no. SMD/POLICY/Cir - /03 dated February 6, 2003, shortened the settlement cycle from T+3 rolling settlement to T+2 w.e.f. April 01, 2003.

4.3.2 SEBI has been receiving request from various stakeholders to further shorten the settlement cycle. Based on discussions with Market Infrastructure Institutions (Stock Exchanges, Clearing Corporations and Depositories), it has been decided to provide flexibility to Stock Exchanges to offer either T+1 or T+2 settlement cycle.

---

[150] Reference: SEBI Circular SEBI/HO/MRD/DSA/CIR/P/2018/1 dated January 29, 2018

[151] Reference: SEBI Circular DCC/FITTC/Cir-19/2003 dated March 4, 2003 and SEBI Circular MRD/DoP/SE/Dep/Cir-18/2005 dated September 2, 2005

[152] Reference: SEBI Circular SEBI/HO/MRD2/DCAP/P/CIR/2021/628 dated September 07, 2021

4.3.3 Accordingly, a Stock Exchange may choose to offer T+1 settlement cycle on any of the scrips, after giving an advance notice of at least one month, regarding change in the settlement cycle, to all stakeholders, including the public at large, and also disseminating the same on its website.

4.3.4 After opting for T+1 settlement cycle for a scrip, the Stock Exchange shall have to mandatorily continue with the same for a minimum period of 6 months. Thereafter, in case, the Stock Exchange intends to switch back to T+2 settlement cycle, it shall do so by giving 1-month advance notice to the market.

4.3.5 Any subsequent switch (from T+1 to T+2 or vice versa) shall be subject to minimum period and notice period as mentioned in **Para 4.3.4** above.

4.3.6 There shall be no netting between T+1 and T+2 settlements.

4.3.7 The settlement option for security shall be applicable to all types of transactions in the security on that Stock Exchange. For example, if a security is placed under T+1 settlement on a Stock Exchange, the regular market deals as well as block deals will follow the T+1 settlement cycle on that Stock Exchange.

4.3.8 The provisions of this circular shall come into force with effect from January 01, 2022.

4.4 Settlement of transactions in case of holidays[153]

4.4.1 Due to lack of uniformity of holidays and force majeure conditions which necessitate sudden closure of one or more Stock Exchanges and banks in a particular state, result in situations where multiple settlements have to be completed by the Stock Exchanges on the working day immediately following the day(s) of the closure of the banks. Accordingly, the Stock Exchanges/Depositories are advised to follow the guidelines and adhere to the time line.

4.4.1.1 The Stock Exchanges shall clear and settle the trades on a sequential basis i.e., the pay-in and the pay-out of the first settlement shall be completed before the commencement of the pay-in and pay-out of the subsequent settlement/s.

4.4.1.2 The cash/securities pay out from the first settlement shall be made available to the member for meeting his pay-in obligations for the subsequent settlement/s.

4.4.1.3 Further, in-order to meet his pay-in obligations for the subsequent settlement, the member may need to move securities from one depository to another. The Depositories shall, therefore, facilitate the inter-depository transfers within one hour and before pay-in for the subsequent settlement begins.

4.4.1.4 The Stock Exchanges/Depositories shall follow a strict time schedule to ensure that the settlements are completed on the same day.

4.4.1.5 The Clearing Corporation/Clearing House of the Stock Exchanges shall execute Auto DO facility for all the settlements together, so as to make the funds and the

[153] Reference: SEBI Circular SEBI/MRD/Policy/AT/Cir- 19/2004 dated April 21, 2004

securities available with the member on the same day for all the settlements, thereby enabling the availability of the funds/securities at the client level by the end of the same day.

4.5 Deadline time for accepting non pay-in related instructions[154]

4.5.1 The depositories are advised that any overrun of the time specified for 'spot delivery contract' in the SCRA would result in the contract becoming illegal under section 16 of the SCRA (unless it is put through the stock exchange). The Rights and Obligations of the BO and DP cannot add anything to or subtract anything from this position. However, it should be the responsibility of the DP to ensure that the client's contract is not rendered illegal on account of delayed execution of the delivery instruction.

4.5.2 Keeping the hardships to change all the existing Rights and Obligations of the BO and DP to enforce the above into consideration, it is advised that suitable bye laws can be made under section 26(2)(e) and (d) of Depositories Act, 1996 for imposing such obligation on the DPs. Therefore, it is advised to amend/insert bye laws which should expressly provide that the DPs shall execute the non pay-in related instructions on the same day or on the next day of the instruction. Further, pending such amendment, suitable instructions may be issued to DPs to adhere to such time limit.

4.5.3 The above clause may be suitably incorporated in the Rights and Obligations of the BO and DP while opening new accounts.

4.6 Approval of amendments to Bye Laws/Rules of Stock Exchanges and Depositories[155]

4.6.1 Depositories and exchanges shall submit the following information while seeking SEBI approval for amendment to Bye Laws/ Rules/ Regulations and amendments thereto:

4.6.1.1 The objective/purpose of amendments.

4.6.1.2 Whether the amendment is consequential to any directive/circulars/ guidelines from SEBI/ Government and the details thereof.

4.6.1.3 Whether such amendments necessitate any consequential amendments to any other Bye Laws/ Rules/ Regulations.

4.6.1.4 The proceedings of the Governing Board or Governing Council, as the case may be, wherein these proposed amendments were approved by the Exchanges/ Depositories.

4.6.1.5 If documents other than Bye Laws/ Rules/ Regulations are sent for approval, the justification and need for forwarding the same to SEBI, indicating whether it forms a part of any Bye Law/ Rule/ Regulation.

[154] Reference: SEBI Letter MRD/VSS/ARR/ 12255/2004 dated June 10, 2004

[155] Reference: SEBI Circular LGL/Cir-2/2003 dated February 19, 2003

4.6.2 Further, all Exchanges shall ensure that requests for dispensation of the requirement of pre-publication shall be accompanied with proper justification and indicate how the public interest or interest of trade shall be served by such dispensation of pre-publication.

4.7 Periodical Report – Grant of prior approval to Depository Participants[156]

4.7.1 The Depositories shall submit a periodical report to SEBI regarding the following changes, as per the format (**Annexure 19**) and in accordance with the guidelines given below:

4.7.1.1 Amalgamation, demerger, consolidation or any other kind of corporate restructuring falling within the scope of Chapter XV of the Companies Act, 2013 or the corresponding provision of any other law for the time being in force;

4.7.1.2 Change in Director, including managing director/ whole-time director;

4.7.1.3 Change in shareholding not resulting in change in control;

4.7.1.4 Any other purpose as may be considered appropriate by the Depositories.

If there is no change during the relevant quarter, it shall be indicated in the report.

4.7.2 **Guidelines to fill up the Annexure and sending the same to SEBI**

4.7.2.1 A separate annexure shall be submitted for each "Type of change" as specified in the format.

4.7.2.2 The report shall be signed by an authorized representative of the Depository and the same shall be stamped.

4.7.2.3 The Depositories shall furnish the report to SEBI by 7th day of month following the end of each quarter, starting with report for the quarter ending June 2011.

4.7.2.4 The report shall be submitted by e-mail at dp@sebi.gov.in. A hard copy of the report shall also be submitted to SEBI.

4.8 Preservation of Records[157]

4.8.1 Depositories and Depository Participants (DPs) are required to preserve the records and documents for a minimum period of 8 years.

4.8.2 Depositories and DPs shall preserve respective original forms of documents either in physical form or an electronic record, copies of which have been taken by CBI, Police or any other enforcement agency during the course of their investigation till the trial is completed.

4.9 Participation as Financial Information Providers in Account Aggregator framework[158]

---

[156] Reference: SEBI Circular CIR/MIRSD/9/2011 dated June 17, 2011

[157] Reference: SEBI Circular: MRD/DoP/DEP/Cir 20/2009 dated December 9, 2009 and SEBI/HO/MRD2/DDAP/CIR/P/2020/153 dated August 18, 2020

[158] Reference: SEBI Circular SEBI/HO/MRD/DCAP/P/CIR/2022/110 dated August 19, 2022

4.9.1 An Account Aggregator (AA), is a Reserve Bank of India (RBI) regulated Non-Banking Finance Company (NBFC) that facilitates retrieval or collection of financial information, pertaining to a customer, from Financial Information Providers ("FIP") on the basis of explicit consent of the customer. The financial information shared through the Account Aggregator is not stored by the AA and it shall not be the property of the AA. This information is not to be used in any other manner except for the purpose of providing it to the customer or consented Financial Information User (FIU). Thus, Account Aggregator facilitates consolidation, organization, presentation of the financial information to the customer or FIU based on the explicit consent of the customer.

4.9.2 RBI has issued Non-Banking Financial Company –Account Aggregator Master Directions DNBR.PD.009/03.10.119/2016-17 dated September 02, 2016 for compliance by every Non-Banking Financial Company (NBFC-Account Aggregator) undertaking the business of AA.

4.9.3 Out of the list of entities mentioned as Financial Information Providers (FIPs) under the Clause 3 (xi) of the Master Directions, the Asset Management Companies (AMCs) through their Registrar and Transfer Agents (RTAs) and the Depositories are inter-alia specified as Financial Information Providers (FIPs) for the purpose of sharing of information. Thus, hereinafter the Depositories and AMCs (through their RTAs) are referred as FIPs in the securities markets.

4.9.4 The FIPs in the securities market will provide the "Financial Information", as specified in Clause 3(ix) of the RBI Master Directions, to the customers and FIUs who furnish the consent artefact (electronic consent as defined in RBI Master Guidelines) through any of the Account Aggregators registered with RBI. Further, FIPs in securities market shall enter into a contractual framework with the AAs, and the same shall distinctly specify the following:

a. Rights and obligations of each party

b. Modalities of Dispute Resolution mechanism

4.9.5 The FIPs in the securities markets shall share the "Financial Information" pertaining to securities markets, through the AA only on receipt of a valid consent artefact from the customer through the Account Aggregator. The consent architecture is detailed under Clause 6 of the RBI Master Directions. Further, the FIPs in the securities markets shall also verify, through appropriate means, the following in the consent artefact:

a. validity of consent

b. specified dates and usage; and

c. the credentials of the AA

4.9.6 Upon due verification of the consent artefact, the FIPs in the securities markets shall digitally sign the financial information and securely transmit the same to the AA in accordance with the terms contained in the consent artefact.

4.9.7 All responses of the FIPs in the securities markets shall be in real time.

4.9.8 To enable these data flows, the FIPs in the securities markets shall:

a. implement interfaces that will allow an AA to submit consent artefacts, and authenticate each other, and would enable secure flow of financial information to the AA;

b. adopt means to verify the consent including digital signatures, if any, contained in the consent artefact;

c. implement means to digitally sign the financial information that is shared by them about the customers;

d. maintain a log of all information sharing requests and the actions performed by them pursuant to such requests.

4.9.9 The FIPs in the securities markets are expected to adopt the technical specifications published by ReBIT, as updated from time to time and adopt required Information Technology (IT) framework and interfaces to ensure secure data flows to AA. The technology should also be scalable to cover any other AA as may be specified by Reserve Bank of India in future.

4.9.10 There shall be adequate safeguards built in IT systems of FIPs in the securities markets to ensure that it is protected against unauthorized access, alteration, destruction, disclosure or dissemination of records and data.

4.9.11 The FIPs in the securities markets shall also abide by the code of conduct as specified in the SEBI regulations applicable to them, including redressal of grievances of the customers.

4.9.12 The FIPs in the securities markets shall continue to comply with all the regulatory provisions under the SEBI Act, 1992, Depositories Act, 1996 and the regulations framed thereunder.

4.9.13 The provisions of this circular shall come into force with effect from August 19, 2022.

4.9.14 The participation of depositories as FIPs in the AA ecosystem shall not impact the existing mechanism as per circular CIR/MRD/DP31/2014 dated November 12, 2014 of issuances of Consolidated Account Statement to the investors by depositories or AMCs/MF-RTAs providing consolidated information of the mutual fund investments and holdings of investors in demat accounts.

4.9.15 The Financial Information Providers (FIPs) in securities market must disclose prominently on their websites the names of the Account Aggregators through which the FIP shares the information about assets held with respect to securities markets with the customers and Financial Information Users (FIUs).

4.10 ***Facilitating transaction in Mutual Fund schemes through the Stock Exchange Infrastructure***[159]

Kindly refer para titled 'Facilitating transactions in Mutual Fund schemes through the Stock Exchange infrastructure' of SEBI Circular SEBI/HO/IMD/IMD-PoD-1/P/CIR/2023/74 dated May 19, 2023 (Master Circular for Mutual Funds)

4.11 ***Discontinuation of usage of pool accounts for transactions in units of Mutual Funds on the Stock Exchange Platforms***[160]

Kindly refer para titled 'Discontinuation of usage of pool accounts for transactions in units of Mutual Funds on the Stock Exchange Platforms' of SEBI Circular SEBI/HO/IMD/IMD-PoD-1/P/CIR/2023/74 dated May 19, 2023 (Master Circular for Mutual Funds)

4.12 ***RTA inter-operable Platform for enhancing investors' experience in Mutual Fund transactions / service requests*** [161]

Kindly refer para titled 'RTA inter-operable Platform for enhancing investors' experience in Mutual Fund transactions/service requests' of SEBI Circular SEBI/HO/IMD/IMD-PoD-1/P/CIR/2023/74 dated May 19, 2023 (Master Circular for Mutual Funds)

4.13 ***Pledge of Shares through depository system***[162]

4.13.1 Section 12 of the Depositories Act, 1996 and Regulation 79 of the Securities and Exchange Board of India (Depositories and Participants) Regulations, 2018 ("**DP Regulations**") along with the relevant Bye Laws of the Depositories clearly enumerate the manner of creating pledge. It is felt that there is a need to communicate to the BOs that any procedure followed other than as specified under the aforesaid provisions of law shall not be treated as pledge.

4.13.2 In order to clarify the same, the depositories are advised to issue a communiqué to the DPs advising them to inform BOs about the procedure for pledging of shares held in demat form as enumerated in the relevant sections of the Depositories Act, 1996 and DP Regulations. Depositories may also advise DPs that an off-market transfer of shares leads to change in ownership and cannot be treated as pledge.

---

[159] Reference: SEBI Circular CIR/MRD/DSA/32/2013 dated October 04, 2013, SEBI Circular CIR/MRD/DSA/33/2014 dated December 09, 2014, SEBI Circular SEBI/HO/MRD/DSA/CIR/P/2016/113 dated October 19, 2016, SEBI Circular SEBI/HO/MRD1/DSAP/CIR/P/2020/29 dated February 26, 2020, SEBI Circular SEBI/IMD/CIR No. 11/183204/2009 dated November 13, 2009 and SEBI Circular CIR/IMD/DF/17/2010 dated November 09, 2010

[160] Reference: SEBI Circular SEBI/HO/IMD/IMD-IDOF5/P/CIR/2021/635 dated October 4, 2021

[161] Reference: SEBI Circular SEBI/HO/IMD/IMD-II DOF3/P/CIR/2021/604 dated July 26, 2021

[162] Reference: SEBI Letter MRD/DoP/MAS – OW/16723/2010 dated August 17, 2010

Further, this issue may also be taken up in the investor awareness programs wherein the manner of creation of pledge can be effectively communicated to the BOs directly.

4.14 Margin obligations to be given by way of Pledge/ Re-pledge in the Depository System[163]

Kindly refer para titled 'Margin obligation to be given by way of Pledge/ Re-pledge in the Depository System' of SEBI Circular SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2023/71 dated May 17, 2023 (Master circular for Stock Brokers)

For the purpose of Section 41.4 of the above-mentioned circular, Depositories shall provide a separate pledge type viz. 'margin pledge', for pledging client's securities as margin to the TM / CM.

4.15 Foreign investments in infrastructure companies in securities markets[164]

4.15.1 Pursuant to Government of India Policy, foreign investments in infrastructure companies in the securities markets, namely Stock Exchanges, Depositories and Clearing Corporations shall be as under:

4.15.1.1 Foreign investment shall be allowed in such companies with a separate FDI and FPI cap as per the prevailing policy of GoI;

4.15.1.2 FDI shall be allowed subject to specific prior approval (if any) as per the FDI policy of GoI;

4.15.1.3 FPI shall be allowed only through purchases in the secondary market;

Clarification[165] **-** In respect of exchanges that are not listed, FPIs purchase of shares of such exchanges can be through transactions outside of the exchange provided it is not an initial allotment. However, if the exchange is listed, transactions by FPIs should be done through the exchange.

4.15.1.4 FPI shall not seek and will not get representation on the Board of Directors;

4.15.1.5 Foreign investors, including persons acting in concert, may hold equity shares in a depository as per the limits specified under Regulation 21 (2) of the Securities and Exchange Board of India (Depositories and Participants) Regulation, 2018.

---

[163] Reference: SEBI Circular SEBI/HO/MIRSD/DOP/CIR/P/2020/28 dated February 25, 2020, SEBI/HO/MIRSD/DOP/CIR/P/2020/88 dated May 25, 2020, SEBI/HO/MIRSD/DOP/CIR/P/2020/90 dated May 29, 2020, SEBI/HO/MIRSD/DOP/CIR/P/2020/143 dated July 29, 2020 and SEBI/HO/MIRSD/DoP/P/CIR/2022/44 dated April 04, 2022

[164] Reference: SEBI Circular MRD/DSA/SE/Dep/Cust/Cir-23/06 dated December 22, 2006

[165] Reference: SEBI Circular MRD/DSA/SE/Dep/Cust/CIR-30/08 dated October 23, 2008

4.15.2 The aforesaid limits for foreign investment in respect of recognised Stock Exchanges shall be subject to 5% shareholding limit as prescribed under the Securities Contracts (Regulation) (Stock Exchanges And Clearing Corporations) Regulations, 2018.

4.16 Designated e-mail ID for regulatory communication with SEBI[166]

Depositories shall create a designated e-mail id for regulatory communication and inform it to SEBI. This e-mail id shall be exclusive and shall not be person-centric.

4.17 Designated e-mail ID for redressal of investor complaints[167]

4.17.1 Depositories and registered DPs shall designate an exclusive e-mail ID for the grievance redressal division/compliance officer exclusively for registering investor complaints.

4.17.2 The designated email ID and other relevant details shall be prominently displayed on the websites and in the various materials/pamphlets/advertisement campaigns initiated by the Depositories and DPs for creating investor awareness.

4.18 Redressal of complaints against Depositories through SEBI Complaints Redress System (SCORES)[168]

4.18.1 The complaints received by SEBI against Depositories shall be electronically sent through SCORES. Depositories are advised to view the pending complaints at http://scores.gov.in/admin and submit the Action Taken Report (ATR) along with supporting documents electronically in SCORES. Updation of action taken shall not be possible with physical ATRs. Hence, submission of physical ATR shall not be accepted for complaints lodged in SCORES.

4.18.2 The Depositories shall do the following:

4.18.2.1 Indicate a contact person in case of SCORES, who is an employee heading the complaint services division/cell/department. Contact detail (i.e. phone no., email id, postal address) of the said contact person be made widely available for e.g. on the websites of Depositories.

4.18.2.2 Address/redress the complaints within a period of 21 calendar days upon receipt of complaint and keep the Board informed about the number and the nature of redressal

4.18.2.3 Maintain a monthly record of the complaints which are not addressed/redressed within 21 calendar days from the date of receipt of the complaint/information, alongwith the reason for such pendency.

---

[166] Reference: SEBI Circular MIRSD/DPS- III/Cir-23/08 dated July 25, 2008

[167] Reference: SEBI Circular MRD/DoP/Dep/SE/Cir-22/06 dated December 18, 2006

[168] Reference: SEBI Circular CIR/MRD/ICC/16/2012 dated June 15, 2012

4.18.2.4 Upload/update the ATR on the SCORES. Failure to do so shall be considered as non-redressal of the complaint and the complaint shall be shown as pending.

4.19 Limitation period for filing an arbitration reference[169]

The provisions dealing with mediation, conciliation and arbitration have been superseded with the introduction of Online Dispute Resolution (ODR) Mechanism. Kindly refer SEBI Circular SEBI/HO/OIAE/OIAE_IAD-1/P/CIR/2023/145 dated July 31, 2023 (Master circular for Online Resolution of Disputes in the Indian Securities Market)

4.20 Disclosure of investor complaints and arbitration details on Depository website[170]

4.20.1 Depositories shall disclose the details of complaints lodged by Beneficiary Owners (BO's)/investors against Depository Participants (DPs) on their website. The aforesaid disclosure shall also include details pertaining to penal action against the DPs.

4.20.2 The format for the reports for the aforesaid disclosure consists of the following reports:

4.20.2.1 Report 1A: Complaints received against DPs during current year

4.20.2.2 Report 1B: Redressal of Complaints received against DPs during previous year

4.20.2.3 Report 1C: Redressal of Complaints received against DPs during current year

4.20.2.4 Report 2A[171]

4.20.2.5 Report 2B[172]

4.20.2.6 Report 3A: Penal Actions against DPs during previous year

4.20.2.7 Report 3B: Penal Actions against DPs during current year

4.20.2.8 Report 4A: Redressal of Complaints lodged by investors against Listed Companies during previous year

4.20.2.9 Report 4B: Redressal of Complaints lodged by investors against Listed Companies during current year

4.20.3 Depositories are accordingly advised to

---

[169] Reference: SEBI Circular CIR/MRD/DP/4/2011 dated April 7, 2011

[170] Reference: SEBI Circular SEBI/MRD/ OIAE/ Dep/ Cir- 4/2010 dated January 29, 2010

[171] Repealed by SEBI Circular SEBI/HO/OIAE/OIAE_IAD-1/P/CIR/2023/145 dated July 31, 2023 in respect of Master SEBI Circular for Online Resolution of Disputes in the Indian Securities Market.

[172] Repealed by SEBI Circular SEBI/HO/OIAE/OIAE_IAD-1/P/CIR/2023/145 dated July 31, 2023 in respect of Master SEBI Circular for Online Resolution of Disputes in the Indian Securities Market.

4.20.3.1 disclose details as per the aforesaid reports in their website on a continuous basis

4.20.3.2 update the aforesaid reports on a quarterly basis, except the Report 1A, which shall be updated on a weekly basis

The provisions dealing with mediation, conciliation and arbitration have been superseded with the introduction of Online Dispute Resolution (ODR) Mechanism. Kindly refer SEBI Circular SEBI/HO/OIAE/OIAE_IAD-1/P/CIR/2023/145 dated July 31, 2023 (Master circular for Online Resolution of Disputes in the Indian Securities Market)

भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

Report 1A: Complaints received against Depository Participants (DPs)# during current year: Updated on mmm dd yyyy (to be updated weekly) (In excel sheet)

Sl. No.	Details of Complaint					Status of Complaint				
	Date of Receipt	Name of Complainant	Type of Complaint*	SEBI Ref. No. (if applicable	Name of DP	Status**	Status Date##	Date of Filing Arbitration	Name of Arbitrator(s)	Date of Arbitration Award
1										
2										
3										
N										

including against its authorized persons, employees, etc.

Status date is the date of resolution/reference to arbitration/finding it non-actionable. If under process, it is the date of updation of this sheet. */** As per Table 1A below

Table 1A

Type	*Complaint Type
Type I	***Account Opening Related***
I a	Denial in opening an account
I b	Account opened in another name than as requested
I c	Non receipt of Account Opening Kit
I d	Delay in activation/ opening of account
I e	Non Receipt of copy of DP Client Agreement/Schedule A of Charges
Type II	***Demat/Remat Related***
II a	Delay in Dematerialisation request processing
II b	Delay in Rematerialisation request processing
II c	Delay in/ Non-Receipt of Original certificate after demat rejection
II d	Non Acceptance of demat/remat request
Type III	***Transaction Statement Related***
III a	Delay in/ Non-Receipt of Statements from DP
III b	Discrepancy in Transaction statement
Type IV	***Improper Service Related***
IV a	Insistence on Power of Attorney in its favour
IV b	Deactivation/ Freezing/ Suspension related
IV c	Defreezing related
IV d	Transmission Related

** Status	
Type	**Description**
I	**Non actionable**
I a	Complaint incomplete
I b	Outside the scope of Depository
I c	Pertains to non-responding company.
II	**Resolved**
III	**Under Process**
IV	**Referred to Arbitration**
V	**Forwarded to Company/RTA for appropriate action.**

IV e	Pledge Related
IV f	SMS Related
IV g	Non-updation of changes in account (address/ signatories/bank details/ PAN/ Nomination etc.)
Type V	***Charges Related***
V a	Wrong/ Excess Charges
V b	Charges paid but not credited
V c	Charges for Opening/closure of Account
Type VI	***Delivery Instruction Related(DIS)***
VI a	Non acceptance of DIS for transfer
VI b	Delay in/ non Execution of DIS
VI c	Delay in Issuance / Reissuance of DIS Booklet
Type VII	***Closure***
VII a	Non closure/ delay in closure of account
VII b	Closure of a/c without intimation by DP
Type VIII	***Manipulation/ Unauthorised Action***
VIII a	Unauthorised Transaction in account
VIII b	Manipulation
VIII c	Unauthorised changes in account (address/ signatories/bank details/PAN etc.)
Type IX	***Company/ RTA related***
IX a	Action – Cash

IX b	Action – Non–Cash
IX c	Initial Public Offer/ Follow-on Public Offer Related
Type X	***Others***

भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

Report 1B: Redressal of Complaints received against Depository Participants (DPs) during previous year: Updated on mmm dd yyyy (to be updated every quarter) (In excel sheet)

Sl. No.	Name of the DP	Status of DP (active/inactive/ in process of termination /withdrawal)	No. of BOs accounts at the beginning of the year	No. of Complaints received against the DP *	Of the Complaints received during previous year							
					No. of Complaints							
					Resolved through the Depository	Non actionable**	Arbitration Advised	Pending for redressal with Depository	No. of Arbitration filed by BOs	Decided by the Arbitrators	Decided by Arbitrators in favour of the BOs	Pending for Redressal with Arbitrators
1												
2												
3												
N												
Total												

*including against its authorized persons, employees, etc.

Non actionable means the complaint that are incomplete / outside the scope of Depository

(Arrange the DPs in descending number of complaints filed against them during the period)

भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

Report 1C: Redressal of Complaints received against Depository Participants (DPs) during current year: Updated on mmm dd yyyy (to be updated every quarter) (In excel sheet)

Sl. No.	Name of the DP	Status of DP (active/inactive/ in process of termination /withdrawal)	No. of BOs accounts at the beginning of the year	No. of Complaints received against the DP *	Of the Complaints received during previous year							
					No. of Complaints							
					Resolved through the Depository	Non actionable**	Arbitration Advised	Pending for redressal with Depository	No. of Arbitration filed by BOs	Decided by the Arbitrators	Decided by Arbitrators in favour of the BOs	Pending for Redressal with Arbitrators
1												
2												
3												
N												

*including against authorized persons, employees, etc.

Non actionable means the complaint that are incomplete / outside the scope of Depository

(Arrange the DPs in descending number of complaints filed against them during the period)

Report 2A: Details of Arbitration Proceedings (where BO is a party) during previous year - Repealed by SEBI Circular SEBI/HO/OIAE/OIAE_IAD-1/P/CIR/2023/145 dated July 31, 2023 in respect of Master circular for Online Resolution of Disputes in the Indian Securities Market.

Report 2B: Details of Arbitration Proceedings (where BO is a party) during current year - Repealed by SEBI Circular SEBI/HO/OIAE/OIAE_IAD-1/P/CIR/2023/145 dated July 31, 2023 in respect of Master circular for Online Resolution of Disputes in the Indian Securities Market.

भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

Report 3A: Penal Actions against Depository Participants (DPs) during previous year: Updated on mmm dd yyyy (to be updated every quarter) (in excel sheet)

Sl. No.	Name of DP	Registration No.	No. of Complaints received	Action against DP, its authorized person and employees together				
				No. of Penal Orders issued		Monetary Penalties levied (Rs. lakh)		No. of Arbitration Awards issued against DP
				For complaints	For others	For complaints	For others	
1								
2								
3								
N								

भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

Report 3B: Penal Actions against Depository Participants (DPs) during current year: Updated on mmm dd yyyy (to be updated every quarter) (in excel sheet)

Sl. No.	Name of DP	Registration No.	No. of Complaints received	Action against DP, its authorized person and employees together				
				No. of Penal Orders issued		Monetary Penalties levied (Rs. lakh)		No. of Arbitration Awards issued against DP
				For complaints	For others	For complaints	For others	
1								
2								
3								
N								

भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

Report 4A: Redressal of Complaints lodged by investors against Listed Companies during previous year: Updated on mmm dd yyyy (to be updated every quarter) (In excel format)

Sl. No.	Name of the Company	No. of Complaints			
		Received	Redressed through Depository	Non-Actionable*	Pending for Redressal with Depository
1					
2					
3					
N					
Total					

***Non actionable** means the **c**omplaint that are incomplete / outside the scope of Depository

(Arrange the companies in descending number of complaints filed against them during the period)

भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

Report 4B:Redressal of Complaints lodged by investors against Listed Companies during current year: Updated on mmm dd yyyy (to be updated every quarter) (In excel format)

Sl. No.	Name of the Company	No. of Complaints			
		Received	Redressed through Depository	Non-Actionable*	Pending for Redressal with Depository
1					
2					
3					
N					
Total					

***Non actionable** means the complaints that are incomplete / outside the scope of Depository

(Arrange the companies in descending number of complaints filed against them during the period)

4.21 *Disclosure of Complaints against the Depositories*[173]

4.21.1 In order to bring about transparency in the Investor Grievance Redressal Mechanism, it has been decided that all the Depositories shall disclose on their websites, the data on complaints received against them and redressal thereof, latest by 7th of succeeding month, as per the format enclosed at **Annexure 20**

4.21.2 These disclosure requirements are in addition to those already mandated by SEBI

4.22 *Disclosure of regulatory orders and arbitration awards on Depository website*[174]

The provisions dealing with mediation, conciliation and arbitration have been superseded with the introduction of Online Dispute Resolution (ODR) Mechanism. Kindly refer SEBI Circular SEBI/HO/OIAE/OIAE_IAD-1/P/CIR/2023/145 dated July 31, 2023 (Master circular for Online Resolution of Disputes in the Indian Securities Market)

4.23 *Disclosure of Investor Charter for Depositories and Depositor Participants*[175]

4.23.1 SEBI, vide e-mail dated November 18, 2021, has forwarded the Investor Charter for Depositories and Depository Participants (DPs) along with the information to be provided in the links of the charter (**Annexure 21**) and advised Depositories to disclose the same on their respective websites.

4.23.2 In this regard, Depositories are directed to advise DPs to bring the Investor Charter for Depositories and Depository Participants along with the information to be provided in the links of the charter, to the notice of their clients (existing as well as new clients) through disclosing the Investor Charter on their respective websites, making them available at prominent places in the office, provide a copy of Investor Charter as a part of account opening kit to the clients, through e-mails/ letters etc.

4.23.3 Additionally, in order to bring about transparency in the Investor Grievance Redressal Mechanism, it has been decided that all the DPs shall disclose on their respective websites, the data on complaints received against them or against issues dealt by them and redressal thereof, latest by 7th of succeeding month, as per the format enclosed at **Annexure 22** to this letter.

4.23.4 These disclosure requirements are in addition to those already mandated by SEBI.

4.24 *Guideline for websites of depositories*[176]

4.24.1 This is with reference to the policy of website management of depositories.

---

[173] Reference: SEBI Circular SEBI/HO/MRD1/MRD1_ICC1/P/CIR/2021/664 dated November 23, 2021

[174] Reference: SEBI Circular SEBI/MRD/ DP/ 19/2010 dated June 10, 2010

[175] Reference: SEBI Letter SEBI/HO/MIRSD/DOP/OW/P/2021/37347/1 dated December 15, 2021

[176] Reference: SEBI Letter MRD/DSA/OW/11447/2/2019 dated May 8, 2019

4.24.2 As a good practice, the guidelines issued by National Informatics Centre for Indian Government website, which is available at https://guidelines.india.gov.in/ may be adopted by depositories.

4.24.3 Depositories are advised to comply with the aforesaid guidelines for their website and mobile app.

4.25 ***Arbitration / Appellate Arbitration fees on the remanded back matter for fresh arbitration proceedings***[177]

The provisions dealing with mediation, conciliation and arbitration have been superseded with the introduction of Online Dispute Resolution (ODR) Mechanism.

Kindly refer SEBI Circular SEBI/HO/OIAE/OIAE_IAD-1/P/CIR/2023/145 dated July 31, 2023 (Master circular for Online Resolution of Disputes in the Indian Securities Market)

4.26 ***Establishment of connectivity by Clearing House/Clearing Corporation (CH/CC) with the Depository – Clarification***[178]

4.26.1 On examination of the provisions of Regulations 35(a) and 45 of the DP Regulations, it is advised that registration of a CC/CH of a stock exchange as a DP with SEBI is not mandatory and a pre-requisite for it to obtain connectivity with the depositories. However, if the CC/CH of a stock exchange desires to function as any other "Depository Participant", i.e. to open BO accounts for investors or clearing member account, registration as DP with SEBI is mandatory.

4.26.2 In view of the above, Depositories are advised to provide continuous electronic means of communication / connectivity to the CH/CC of the Exchanges without insisting for a mandatory registration as DP with SEBI with a condition that such entities would not be permitted to open BO accounts for investors or clearing member account.

4.27 ***Issue of Master Circular by Stock Exchanges, Clearing Corporations and Depositories***[179]

4.27.1 Stock Exchanges, Clearing Corporations and Depositories (hereinafter collectively referred to as 'Market Infrastructure Institutions (MIIs)') communicate with market participants including investors on a regular basis by way of circulars, directions, operating instructions, communiques or any other mode of communication

[177] Reference: SEBI Letter SEBI/MRD/ICC/OW/P/2018/27066/1 dated September 25, 2018
[178] Reference: SEBI Letter MRD/DoP/ Dep/82334 /2006 dated December 14, 2006
[179] Reference: SEBI Circular SEBI/HO/MRD/POD 3/CIR/P/2023/58 dated April 20, 2023

(hereinafter collectively referred to as 'guidelines') for necessary compliance. This has led to a plethora of guidelines by the MIIs on various subjects.

4.27.2 Due to the issuance of such guidelines of varied nature and based on the feedback received from the market participants, to ensure that all market participants, including investors, find all applicable provisions on a specific subject at a place, the MIIs shall ensure the following:

4.27.2.1 Issue the respective Master Circulars consolidating all guidelines issued and applicable as on March 31 of every year, segregated subject-wise.

4.27.2.2 Take due care to include only the relevant guidelines into the respective Master Circular while reviewing all the existing guidelines on a particular subject.

4.27.2.3 Such Master Circular shall not include the following:

4.76.1.1.1 Bye-laws, Rules and Regulations issued by MIIs.

4.76.1.1.2 Status of any compliance by the market participant

4.76.1.1.3 Actions taken against any entity.

4.27.2.4 Each Master Circular shall contain a list of all guidelines incorporated therein as well as a provision rescinding all such guidelines with effect from the date of implementation of the Master Circular. All such rescinded guidelines shall be archived on the respective websites of the MIIs.

4.27.2.5 The Master Circulars shall contain a savings clause as under:

"Notwithstanding such rescission,

a. *Anything done or any action taken or purported to have been done or contemplated under the rescinded guidelines before the commencement of this Master Circular shall be deemed to have been done or taken or commenced or contemplated under the corresponding provisions of the Master Circular or rescinded guidelines whichever is applicable.*

b. *The previous operation of the rescinded guidelines or anything duly done or suffered thereunder, any right, privilege, obligation or liability acquired, accrued or incurred under the rescinded guidelines, any penalty, incurred in respect of any violation committed against the rescinded guidelines, or any investigation, legal proceeding or remedy in respect of any such right, privilege, obligation, liability, penalty as aforesaid, shall remain unaffected as if the rescinded guidelines have never been rescinded."*

4.27.3 MIIs shall update the Master Circular incorporating all guidelines issued during the financial year, and issue the same on or before April 30 of each year.

4.28 *Principles of Financial Market Infrastructures (PFMIs)*[180]

4.28.1 To promote and sustain an efficient and robust global financial infrastructure, the Committee on Payments and Settlement Systems (CPSS) and the International Organization of Securities Commissions (IOSCO) published the *Principles for financial market infrastructures*[1] (PFMIs) on April 2012. They replace the three existing sets of international standards set out in the Core Principles for Systemically Important Payment Systems (CPSIPS); the Recommendations for Securities Settlement Systems (RSSS); and the Recommendations for Central Counterparties (RCCP). CPSS and IOSCO have strengthened and harmonised these three sets of standards by raising minimum requirements, providing more detailed guidance and broadening the scope of the standards to cover new risk-management areas and new types of FMIs.

4.28.2 The PFMIs comprise **24 principles** (**Annexure 23**) for Financial Market Infrastructure to provide for effective regulation, supervision and oversight of FMIs. They are designed to ensure that the infrastructure supporting global financial markets is robust and well placed to withstand financial shocks.

4.28.3 Full, timely and consistent implementation of the PFMIs is fundamental to ensuring the safety, soundness and efficiency of key FMIs and for supporting the resilience of the global financial system. In addition, the PFMIs play an important part in the G20's mandate that all standardized over-the-counter (OTC) derivatives should be centrally cleared. Global central clearing requirements reinforce the importance of strong safeguards and consistent oversight of derivatives CCPs in particular.

Financial Market Infrastructure (FMI)

4.28.4 The Principles apply to systematically important financial market infrastructures entities such as Central Counterparty (CCP), Central Securities Depository (CSD)/ Securities Settlement System (SSS), Payment and Settlement systems, and Trade Repository (TR) which are responsible for providing clearing, settlement and recording of monetary and other financial transactions. The principles are international standards set forth to –

- ***a.*** Enhance safety and efficiency in payment, clearing, settlement, and recording arrangements,
- ***b.*** Reduce systemic risk.
- ***c.*** Foster transparency and financial stability and
- ***d.*** Promote protection of participants and investors.

[180] Reference: SEBI Circular SEBI/MRD/DRMNP/26/2013 dated September 04, 2013

4.28.5 Financial Market Infrastructure (FMI) are critically important institutions responsible for providing clearing, settlement and recording of monetary and other financial transactions. The different categories of FMIs, as identified under PFMIs, are listed below –

4.28.5.1 *Payment Systems (PSS)*

A payment system is a set of instruments, procedures, and rules for the transfer of funds between or among participants. The system includes the participants and the entity operating the arrangement. Payment systems are typically based on an agreement between or among participants and the operator of the arrangement, and the transfer of funds is effected using an agreed-upon operational infrastructure.

4.28.5.2 *Central Securities Depositories (CSD)*

Central securities depository provides securities accounts, central safekeeping services, and asset services, which may include the administration of corporate actions and redemptions, and plays an important role in helping to ensure the integrity of securities issues (that is, ensure that securities are not accidentally or fraudulently created or destroyed or their details changed). A CSD can hold securities either in physical form (but immobilised) or in dematerialised form (that is, they exist only as electronic records). A CSD may maintain the definitive record of legal ownership for a security; in some cases, however, a separate securities registrar will serve this notary function.

4.28.5.3 *Securities Settlement Systems (SSS)*

A securities settlement system enables securities to be transferred and settled by book entry according to a set of predetermined multilateral rules. Such systems allow transfers of securities either free of payment or against payment. When transfer is against payment, many systems provide delivery versus payment (DvP), where delivery of the security occurs if and only if payment occurs. An SSS may be organised to provide additional securities clearing and settlement functions, such as the confirmation of trade and settlement instructions.

4.28.5.4 *Central Counterparties (CCP)*

A central counterparty interposes itself between counterparties to contracts traded in one or more financial markets, becoming the buyer to every seller and the seller to every buyer and thereby ensuring the performance of open contracts. A CCP becomes counterparty to trades with market participants through novation, an open-offer system, or through an analogous legally binding arrangement. CCPs have the potential to significantly reduce risks to participants through the multilateral netting of trades and by imposing more

effective risk controls on all participants. For example, CCPs typically require participants to provide collateral (in the form of initial margin and other financial resources) to cover current and potential future exposures. CCPs may also mutualise certain risks through devices such as default funds. As a result of their potential to reduce risks to participants, CCPs also can reduce systemic risk in the markets they serve.

4.28.5.5 *Trade Repositories (TR)*

A trade repository is an entity that maintains a centralised electronic record (database) of transaction data. TRs have emerged as a new type of FMI and have recently grown in importance, particularly in the OTC derivatives market. By centralising the collection, storage, and dissemination of data, a well-designed TR that operates with effective risk controls can serve an important role in enhancing the transparency of transaction information to relevant authorities and the public, promoting financial stability, and supporting the detection and prevention of market abuse. An important function of a TR is to provide information that supports risk reduction, operational efficiency and effectiveness, and cost savings for both individual entities and the market as a whole. Such entities may include the principals to a trade, their agents, CCPs, and other service providers offering complementary services, including central settlement of payment obligations, electronic novation and affirmation, portfolio compression and reconciliation, and collateral.

Adoption of Principles of Financial Market Infrastructures

4.28.6 All CPSS and IOSCO members are required to strive to adopt the PFMIs and implement them in their respective jurisdictions.

4.28.7 SEBI as a member of IOSCO is committed to the adoption and implementation of the new CPSS-IOSCO standards of PFMIs in its regulatory functions of oversight, supervision and governance of the key financial market infrastructures under its purview.

4.28.8 Depositories and Clearing Corporations regulated by SEBI are FMIs in terms of the criteria described above. These systemically important financial infrastructures provide essential facilities and perform systemically critical functions in the market and shall hence be required to comply with the principles of financial market infrastructures specified by CPSS-IOSCO as applicable to them. The list of SEBI regulated FMIs is as follows:

1. **Clearing Corporations**
   - ***a.*** Indian Clearing Corporation Ltd. (ICCL)
   - ***b.*** Metropolitan Clearing Corporation of India Ltd. (MCCIL)
   - ***c.*** National Securities Clearing Corporation Ltd. (NSCCL)

2. **Depositories**
   a. Central Depository Services Ltd. (CDSL)
   b. National Securities Depository Ltd (NSDL)

4.28.9 All FMIs in the securities market shall be monitored and assessed against the PFMIs on a periodic basis.

4.29 System and Network Audit of Market Infrastructure Institutions (MIIs)[181]

4.29.1 Based on discussions with Stock Exchanges, Clearing Corporations, Depositories (hereinafter referred as 'Market Infrastructure Institutions – MIIs), and recommendations of the Technical Advisory Committee (TAC) of SEBI, the existing System Audit Framework has been reviewed.

4.29.2 MIIs are required to conduct System and Network Audit as per the framework and Terms of Reference (TOR) laid under **Para 4.29.6** & **4.29.7** respectively.
MIIs are also required to maintain a list of all the relevant SEBI circulars/ directions/ advices, etc. pertaining to technology and compliance thereof, as per format enclosed as **Annexure 24** and the same shall be included under the scope of System and Network Audit.

4.29.3 MIIs are also required to submit information with regard to exceptional major Non-Compliances (NCs)/ minor NCs observed in the System and Network audit as per format enclosed as **Annexure 25** and are required to categorically highlight those observations/NCs/suggestions pointed out in the System and Network audit (current and previous) which remain open.

4.29.4 The Systems and Network audit Report including compliance with SEBI circulars/ guidelines and exceptional observation format along with compliance status of previous year observations shall be placed before the Governing Board of the MII and then the report along with the comments of the Management of the MII shall be communicated to SEBI within a month of completion of audit.

4.29.5 Further, along with the audit report, MIIs are required to submit a Joint declaration from the Managing Director(MD)/Chief Executive Officer(CEO) and Chief Technology Officer (CTO) certifying:

4.29.5.1 the security and integrity of their IT Systems.

4.29.5.2 correctness and completeness of data provided to the Auditor

4.29.5.3 entire network architecture, connectivity (including co-lo facility) and its linkage to the trading infrastructure are in conformity with SEBI's regulatory framework to provide fair equitable, transparent and non-discriminatory treatment to all the market participants

[181] Reference: SEBI Circular SEBI/HO/MRD1/MRD1_DTCS/P/CIR/2022/58 dated May 02, 2022

4.29.5.4 internal review of Critical Systems as defined under **Para 4.31** was carried out during the Audit period, including the Failure Modes and Effects Analysis (FMEA).

4.29.6 **Framework for System and Network Audit**

Audit Process

4.29.6.1 For the System and Network Audit, the following broad areas shall be considered in order to ensure that the audit is comprehensive and effective:

4.29.6.1.1 The Audit shall be conducted according to the Norms, Terms of Reference (TOR) and Guidelines issued by SEBI.

4.29.6.1.2 The Governing Board of the Market Infrastructure Institution (MII) shall appoint the Auditors based on the prescribed Auditor Selection Norms and TOR.

4.29.6.1.3 An Auditor can perform a maximum of 3 successive audits. However, such auditor shall be eligible for re-appointment after a cooling-off period of two years.

4.29.6.1.4 Further, during the cooling-off period, the incoming auditor may not include:

(i) Any firm that has common partner(s) with the outgoing audit firm; and

(ii) Any associate / affiliate firm(s) of the outgoing audit firm which are under the same network of audit firms wherein the term "same network" includes the firms operating or functioning, hitherto or in future, under the same brand name, trade name or common control.

4.29.6.1.5 The number of years an auditor has performed an audit prior to this circular shall also be considered in order to determine its eligibility in terms of **Para 4.29.6.1.3** above.

4.29.6.1.6 The scope of the Audit may be broadened by the Auditor to inter-alia incorporate any new developments that may arise due to issuance of circulars/ directions/ advice by SEBI from time to time.

4.29.6.1.7 The audit shall be conducted once in a financial year and period of audit shall be 12 months. However, for the MIIs, whose systems have been identified as “protected system” by National Critical Information Infrastructure Protection Centre (NCIIPC), the audit shall be conducted on a half yearly basis and audit period shall be of 6 months. Further, the audit shall be completed within 2 months from the end of the audit period.

4.29.6.1.8 In the Audit report, the Auditor shall include its comments on whether the areas covered in the Audit are in compliance with the

norms/directions/ advices issued by SEBI, internal policy of the MII, etc. Further, the audit report shall also include specific non-compliances (NCs), observations for minor deviations and suggestions for improvement. The audit report shall take previous audit reports into consideration and cover any open items therein. The auditor should indicate if a follow-on audit is required to review the status of NCs.

4.29.6.1.9 For each of the NCs/ observations and suggestions made by the Auditor, specific corrective action as deemed fit may be taken by the MII. The management of the MII shall provide its comments on the NCs, observations and suggestions made by the Auditor, corrective actions taken or proposed to be taken along with time-line for such corrective actions.

4.29.6.1.10 The Audit report along with the comments of management shall be placed before the Governing Board of the MII. The Audit report along with comments of the Governing Board shall be submitted to SEBI, within 1 month of completion of audit.

4.29.6.1.11 The follow-on audit should be completed within one month of the corrective actions taken by the MII. After the follow-on audit, the MII shall submit a report to SEBI within 1 month from the date of completion of the follow-on audit. The report shall include updated Issue-Log to indicate the corrective actions taken and specific comments of the Auditor on the NCs and the corrective actions.

4.29.6.1.12 In cases wherein follow-on audit is not required, the MII shall submit an Action Taken Report (ATR) to the Auditor. After verification of the ATR by the Auditor, the MII shall submit a report to SEBI within 1 month from the date of completion of verification by the Auditor. The report shall include updated Issue-Log to indicate the corrective actions taken and specific comments of the auditor on the ATR.

4.29.6.1.13 The overall timeline from the last date of the audit period till completion of final compliance by MII, including follow-on audit, if any, should not exceed one year/6 months(as applicable).In exceptional cases, if MII is of the view that compliance with certain observations may extend beyond said period, then the concerned MII shall seek specific approval from the Governing Board.

Auditor Selection Norms

4.29.6.2 MII shall ensure compliance with the following norms while appointing Auditor:

4.29.6.2.1 The Auditor must have minimum 3 years of demonstrable experience in IT audit of securities market participants e.g. stock exchanges, clearing corporations, depositories, intermediaries, etc. and/ or financial services sector i.e. banking, insurance, Fin-tech etc.

4.29.6.2.2 The team performing system and network audit must have experience in / direct access to experienced resources in the areas covered under TOR. It is recommended that resources deployed by the Auditor for the purpose of system and network audit shall have relevant industry recognized certifications e.g. CISA (Certified Information Systems Auditor) from ISACA, CISM (Certified Information Securities Manager) from ISACA, GSNA (GIAC Systems and Network Auditor), CISSP (Certified Information Systems Security Professional) from International Information Systems Security Certification Consortium, commonly known as (ISC).

4.29.6.2.3 The Auditor shall have experience in working on Network audit/IT audit/governance/IT service management frameworks and processes conforming to industry leading practices like CobiT/ ISO 27001 and beyond.

4.29.6.2.4 The Auditor should have the capability to undertake forensic audit and undertake such audit as part of system and network audit, if required.

4.29.6.2.5 The Auditor must not have any conflict of interest in conducting fair, objective and independent audit of the exchange / depository/ clearing corporation. It should not have been engaged over the last three years in any consulting engagement with any departments / units of the entity being audited.

4.29.6.2.6 The Auditor should not have any cases pending against it, which point to its incompetence and/or unsuitability to perform the audit task.

4.29.6.2.7 The proposed audit agency must be empanelled with CERT-In.

4.29.6.2.8 Any criteria, in addition to the aforesaid criteria, that the MII may deem fit for the purpose of selection of Auditor.

Audit Report Guidelines

4.29.6.3 The Audit report should cover each of the major areas mentioned in the TOR and compliance with SEBI circulars/directions/advices, etc. related to technology. The Auditor in the Audit Report shall give its views indicating the NCs to the standards or observations or suggestions. For each section, auditors should also provide qualitative inputs/suggestions about ways to improve the processes, based upon the best industry practices.

4.29.6.4 The auditor shall certify that entire network architecture, connectivity (including co-lo facility) and its linkage to the trading infrastructure are in conformity with SEBI's regulatory framework to provide fair equitable, transparent and non-discriminatory treatment to all the market participants.

4.29.6.5 The report should also include tabulated data to show NCs / observations for each of the major areas in the TOR.

4.29.6.6 The audit report to include point-wise compliance of areas prescribed in Terms of Reference (TOR) and areas emanating from relevant SEBI circulars/directions/advices along with any accompanying evidence.

4.29.6.7 Evidences should be specified in the audit report while reporting/ closing an issue.

4.29.6.8 A detailed report with regard to the system and network audit shall be submitted to SEBI. The report shall include an Executive Summary as per the following format:

Issue Log Column Heading	Description	Responsibility
Major Area	Comprehensive identification of major areas in compliance with various SEBI circulars / norms and internal policies of MII	Auditor/Auditee
Point wise Compliance	Point-wise list of areas/relevant clauses in TOR against which compliance is being audited (in tabular format).	Auditor
Description of Finding/ Observation	Describe the findings in sufficient detail, referencing any accompanying evidence (e.g. procedure manual, interview notes, reports etc.)	Auditor
Reference	Reference to the section in detailed report – where full background information about the findings are available	Auditor
Process/ Unit	Process or unit where the audit is conducted and the finding pertains to	Auditor
Category of Findings	Major/Minor Non-compliance, Observation, Suggestion etc.	Auditor

Audited By	Which Auditor covered the findings	Auditor
Root Cause Analysis	A detailed analysis on the cause of the Non-compliance	Auditee
Remediation	The action (to be) taken to correct the Non-compliance	Auditee
Target Completion Date for Remedial Action	The date by which remedial action must be/will be completed	Auditor/Auditee
Status	Status of finding on reporting date (open/close)	Auditor/Auditee
Verified By	Auditing personnel (upon verification that finding can be closed)	Auditor
Closing Date	Date when finding is verified and can be closed	Auditor

4.29.7 **<u>Terms of Reference (TOR) for System and Network audit Program</u>**

4.29.7.1 The scope of audit shall encompass all the IT resources including hardware, software, network, policies, procedures etc. of MIIs (Primary Data Centre (PDC), Disaster Recovery Site (DRS) and Near Site (NS))

4.29.7.2 **IT environment**

4.29.7.2.1 Organization details

a. Name

b. Address

c. IT team size (in house- employees)

d. IT team size (vendors)

4.29.7.2.2 IT and network set up and usage

a. PDC, DRS, NS and Regional/ Branch offices (location, owned/ outsourced)

b. Connectivity amongst PDC, NS and DRS

c. IT infrastructure / applications pertaining to the activities done as a MII.

d. System Architecture

e. Network architecture

f. Telecommunication network

4.29.7.3 **IT Governance**

4.29.7.3.1 Whether IT Governance framework exists to include the following:

a. IT organization structure including roles and responsibilities of key IT personnel;

b. IT governance processes including policy making, implementation and monitoring to ensure that the governance principles are followed;

4.29.7.3.2 IT policies and procedures

a. Whether the organization has a defined and documented IT policy? If yes, is it approved by the Governing Board (GB)?

b. Is the current System Architecture, including infrastructure, network and application components describing system linkages and dependencies, documented?

c. Whether defined and documented Standard Operating Procedures (SOPs) for the following processes are in place?

i. IT Assets Acquisition
ii. Access Management
iii. Change Management
iv. Backup and Recovery
v. Incident Management
vi. Problem Management
vii. Patch Management
viii. Data Centre Operations
ix. Operating Systems and Database Management
x. Network Management
xi. DRS Operations
xii. Data Retention and Disposal
xiii. Asset Inventory
xiv. IT asset refresh/replacement policy
xv. Database security
xvi. Interface Security
xvii. Application Security
xviii. Password Security
xix. Archived and backed up data security

4.29.7.3.3 Whether the above mentioned SOPs is reviewed at periodic intervals or upon the occurrence of any major event? In this regard, whether any organization policy has been formulated by the MII?

4.29.7.4 **Business Controls**

4.29.7.4.1 General Controls for Data Centre Facilities

a. Application Access – segregation of duties, database and application access etc. (Approved Policy clearly defining roles and responsibilities of the personnel handling business operations)

b. Maintenance Access – vendor engineers

c. Physical Access controls – permissions, logging, exception reporting & alerts

d. Environmental Controls – fire protection, AC monitoring, etc.

e. Fault Resolution Mechanism

f. Folder Sharing and Back Up Controls – safeguard of critical information on local desktops

g. Incidences of violations in the previous audit report and corrective action(s), if any, taken

h. Any other controls, as deemed fit, by the MII

4.29.7.4.2 Software change control

a. Whether pre-implementation review of application controls (including controls over change management) was undertaken?

b. Adherence to secure Software Development Life Cycle (SDLC) / Software Testing Life Cycle (STLC) standards/ methodologies

c. Whether post implementation review of application controls was undertaken?

d. Is the review of processes to ensure data integrity post implementation of new application or system followed by implementation team?

e. User awareness

f. Processing of new feature request

g. Fault reporting / tracking mechanism & process for resolutions

h. Testing of New releases / Bug-fixes – Testing process (automation level)

i. Version Control – History, Change Management process etc.

j. Development / Test/ Production environment – Segregation

k. New Release in Production – Promotion, Release note approvals

l. Production Issues / disruptions reported in the previous audit report, root cause analysis & corrective actions taken, if any

m. Software Development Stage

n. Software Design to ensure adequate system capacity to enable functioning in a degraded manner in the event of a crash.

o. Any other controls, as deemed fit, by the MII

4.29.7.4.3 Data Communication/ Network Controls

a. Network Administration – Redundancy, Monitoring, breakdown resolution etc.

b. WAN Management – Connectivity provisions for business continuity.

c. Encryption - Router based as well as during transmission

d. Connection Permissions – Restriction on need to have basis

e. Fallback Mechanism – Dial-up connections controls etc.

f. Hardware based Signing Process

g. Incidences of access violations observed in the previous report & corrective actions taken, if any

h. Any other controls, as deemed fit, by the MII

4.29.7.4.4 Security Controls

a. Secured e-mail with other entities such as SEBI, other partners

b. Email Archival Implementation

4.29.7.4.5 Access Policy and Controls

a. Defined and documented policies and procedures for managing access to applications and infrastructure –PDC, DRS, NS, branches (including network, operating systems and database) and approved by relevant authority

b. Review of access logs

c. Access rights and roles review procedures for all systems

d. Segregation of Duties (SOD) matrix describing key roles

e. Risk acceptance for violation of SOPs and alternate mechanism put in place

f. Privileged access to system and record of logs,

g. Periodic monitoring of access rights for privileged users

h. Authentication mechanisms used for access to systems including use of passwords, One Time Passwords (OTP), Single Sign on, etc.

i. Any other controls, as deemed fit, by the MII

4.29.7.4.6 Electronic Document Controls

4.29.7.4.7 General Access Controls

4.29.7.4.8 Performance Audit

a. Comparison of changes in transaction volumes since previous audit

b. Review of systems (hardware, software, network) performance over the period

c. Review of the current volumes against the last performance test and against the current system utilization

4.29.7.4.9 Business Continuity / Disaster Recovery Facilities

a. Business Continuity Planning (BCP) manual, including Business Impact Analysis (BIA), Risk Assessment and Disaster Recovery (DR) process, Roles and responsibilities of Incent Response Team (IRT) /Crisis Management Team (CMT), employees, support/outsourced staff.

b. Implementation of policies

c. Back-up procedures and recovery mechanism using back-ups.

d. Storage of Back-up (Remote site, DRS etc.)

e. Redundancy – Equipment, Network, Site etc.

f. DRS installation and Drills - Management statement on targeted resumption capability (in terms of time required & extent of loss of data)

g. Evidence of achieving the set targets during the DR drills in event of various disaster scenarios.

h. Debrief / review of any actual event when the DR/BCP was invoked during the year

i. User awareness and training

j. Is Recovery Time Objective (RTO) /Recovery Process Objective (RPO) during BIA documented?

k. Is annual review of BCP-DR or in case of major change in business/ infrastructure undertaken?

l. Is quarterly review regarding implementation of BCP policy done by Standing Committee of Technology (SCOT) of the MII?

m. Testing of BCP-DR plan through appropriate strategies including simulations, DR drills, system recovery, etc.

n. Is the recordkeeping of quarterly DR drills, live trading sessions from DRS being maintained?

o. Is BCP-DR policy document prepared and implemented in line with SEBI circular on BCP and DR of MII?

4.29.7.4.10 IT/Network Support & IT Asset Management

a. Utilization Monitoring – including report of prior year utilization

b. Capacity Planning – including projection of business volumes

c. Capacity and performance management process for the network/systems

d. IT (S/W, H/W & N/W) Assets, Licenses & maintenance contracts

e. Comprehensive review of Assets life cycle management (Acquisition, commissioning, deployment, monitoring, maintenance and de commissioning) and relevant records related to it.

f. Insurance

g. Disposal – Equipment, media, etc.

4.29.7.5 Entity Specific Software used for or in support of trading/clearing systems / peripheral systems and critical processes

4.29.7.6 **Human Resources Management**

4.29.7.6.1 Screening of Employee, Third party vendors / contractors

4.29.7.6.2 Onboarding

4.29.7.6.3 Off boarding

4.29.7.6.4 Consequence Management (Incident / Breach of policies)

4.29.7.6.5 Awareness and Trainings

4.29.7.6.6 Non-Disclosure Agreements (NDAs) and confidentiality agreement

4.29.7.7 **Network audit**

4.29.7.7.1 The audit shall cover entire network infrastructure which shall inter-alia includes physical verification and tracing of the connectivity paths, server configuration, physical checking wire to wire connectivity and configurations of computer networking devices etc.

4.29.7.7.2 The audit shall require tracing of the connectivity and network diagram based on the physical audit.

4.29.7.7.3 The audit shall cover the link, the path, device-level redundancy, no single-point failures, high availability, and fault tolerance aspects in the network.

4.29.7.7.4 The audit shall cover entire network that is used to connect members to the MIIs (POP, MPLS, VSAT, COLO, etc.)

4.29.7.7.5 The audit shall cover applications, internal networks, servers, etc. of the MIIs/offered by the MIIs to its members that are used for trading, risk management, clearing and settlement etc.

4.29.7.7.6 Network performance and design

4.29.7.7.7 Network Security implementation

4.29.7.7.8 Network health monitoring and alert system

4.29.7.7.9 Log management process

4.29.7.7.10 Service level definition for vendors/Service level management

4.29.7.7.11 Governance process for network service delivery by vendors

4.29.7.8 The results of all testing that was conducted before deployment of any IT system/application in production environment, shall be checked by auditor during system audit.

4.29.7.9 **IT Vendor Selection and Management**

4.29.7.9.1 Identification of eligible vendors

4.29.7.9.2 Dissemination process of Request for Proposal (RFP)

4.29.7.9.3 Definition of criteria of evaluation

4.29.7.9.4 Process of competitive analysis

4.29.7.9.5 Approach for selection

4.29.7.9.6 Escrow arrangement for keeping source code

4.29.7.10 **E-Mail system**

4.29.7.10.1 Existence of policy for the acceptable use of electronic mail

4.29.7.10.2 Regulations governing file transfer and exchange of messages with external parties

4.29.7.10.3 Rules based on which e-mail addresses are assigned

4.29.7.10.4 Storage, backup and retrieval

4.29.7.11 **Redressal of Technological Complaints**

4.29.7.11.1 Ageing analysis of technology complaints

4.29.7.11.2 Whether all complaints received are brought to their logical conclusion?

4.29.7.12 **Any other Item(s)**

4.29.7.12.1 Electronic Waste Disposal

4.29.7.12.2 Observation(s) based on previous Audit Report (s)

4.29.7.12.3 Any other specific area(s) that may be informed by SEBI.

4.30 ***Testing Framework for the Information Technology (IT) systems of the Market Infrastructure Institutions (MIIs)***[182]

4.30.1 MIIs (i.e. Stock Exchanges, Clearing Corporations and Depositories) are systemically important institutions as they, inter-alia, provide infrastructure necessary for the smooth and uninterrupted functioning of the securities market. Therefore, it is imperative to devise a comprehensive testing framework to manage the IT systems/applications of MIIs throughout their lifecycle, which can assist the MIIs in performing thorough risk assessment before deploying any IT systems in production/ live environment.

4.30.2 Based on the recommendations of the TAC, MIIs are hereby directed to ensure the following requirements while establishing the testing framework of their IT systems/applications:-

4.30.2.1 All MIIs should do extensive testing, validation and documentation whenever new systems/ applications or changes to existing systems/applications are introduced before the deployment in production/live environment.

4.30.2.2 A comprehensive methodology for system testing, functional testing, application security testing should be established and the same shall be

[182] Reference: SEBI Circular SEBI/HO/MRD/TPD/P/CIR/2023/65 dated May 05, 2023

approved by Standing Committee on Technology (SCOT) of respective MIIs. The scope of testing shall, inter-alia, cover business logic, system function, security controls and system performance under load and stress conditions. Any dependency on the existing systems shall be properly tested.

4.30.2.3 Testing should be carried out in a separate environment that replicates/mirrors the production environment in order to minimize any disruption.

4.30.2.4 All MIIs shall have the practice of traceability matrix to ensure that the test plan covers all intended functionality of the IT system and application.

4.30.2.5 All MIIs shall adopt the practice of using automated testing techniques to run the test cases automatically, which may increase the depth and scope of tests and ultimately help to improve the software quality.

4.30.2.6 All MIIs shall establish policy/procedures on the use of third party systems/applications/software codes to ensure these systems are subject to review and testing before they are integrated with the systems of the MIIs.

4.30.2.7 All MIIs shall ensure that core code components operate as intended and do not produce unintended consequences. Further, any new code shall not have any impact on the existing functionality. All MIIs shall also ensure that Application Programming Interface Testing is done so that the concerned application can interact with other applications without causing disruptions of any kind.

4.30.2.8 All MIIs should perform regression testing for changes (e.g. enhancement, rectification, etc.) to an existing IT system to validate that it continues to function properly after the changes have been implemented. After fixing the defects found during the testing, all MIIs shall perform regression testing again to ensure that other existing functionalities are not affected during fixing the defects. All MIIs shall explore to capture the automated test cases so that regression testing can be performed multiple times with much wider coverage test cases in a short time.

4.30.2.9 All MIIs may institute tools to measure test/code coverage to assess comprehensiveness of the test.

4.30.2.10 All Issues identified from testing, including system defects or software bugs, should be properly tracked and remediated immediately. Major issues that could have an adverse impact on the MII should be reported to their SCOT and addressed prior to deployment to the production environment.

4.30.2.11 All MIIs should ensure that the results of all testing, including results of User Acceptance Testing (UAT), that was conducted, are documented in the test report. The same shall be checked by the auditor during System and Network Audit.

4.30.2.12 All MIIs shall periodically conduct non-functional testing such as volume testing, resilience testing, scalability testing, performance testing, stress testing, application security testing, BCP testing, negative/destructive testing etc. for all IT systems/applications throughout their lifecycle (pre-implementation, post implementation, after changes).

4.30.2.13 All MIIs shall perform white box testing or structural testing, which shall inter-alia include analyzing data flow, control flow, information flow, coding practices, exception and error handling within the system.

4.31 Guidelines for Business Continuity Plan (BCP) and Disaster Recovery (DR)[183]

4.31.1 Upon examination and based on consultation with MIIs and TAC of SEBI, the modified framework for BCP and DR shall be as under:

4.31.1.1 Stock Exchanges, Clearing Corporations and Depositories (collectively referred as Market Infrastructure Institutions – MIIs) shall have in place BCP and DRS so as to maintain data and transaction integrity.

4.31.1.2 Apart from DRS, all MIIs including Depositories shall also have a Near Site (NS) to ensure zero data loss.

4.31.1.3 The DRS should preferably be set up in different seismic zones and in case due to certain reasons such as operational constraints, change of seismic zones, etc., minimum distance of 500 kilometer shall be ensured between PDC and DRS so that both DRS and PDC are not affected by the same disaster.

4.31.1.4 The manpower deployed at DRS/NS shall have the same expertise as available at PDC in terms of knowledge/ awareness of various technological and procedural systems and processes relating to all operations such that DRS/NS can function at short notice, independently. MIIs shall have sufficient number of trained staff at their DRS so as to have the capability of running live operations from DRS without involving staff of the PDC.

4.31.1.5 All MIIs shall constitute an Incident and Response team (IRT)/ Crisis Management Team (CMT), which shall be chaired by the Managing Director (MD) of the MII or by the Chief Technology Officer (CTO), in case of non-availability of MD. IRT/ CMT shall be responsible for the actual

[183] Reference: SEBI Circular SEBI/HO/MRD1/DTCS/CIR/P/2021/33 dated March 22, 2021

declaration of disaster, invoking the BCP and shifting of operations from PDC to DRS whenever required. Details of roles, responsibilities and actions to be performed by employees, IRT/ CMT and support/outsourced staff in the event of any Disaster shall be defined and documented by the MII as part of BCP-DR Policy Document.

4.31.1.6 The Technology Committee of the MIIs shall review the implementation of BCP-DR policy approved by the Governing board of the MII on a quarterly basis.

4.31.1.7 MIIs shall conduct periodic training programs to enhance the preparedness and awareness level among its employees and outsourced staff, vendors, etc. to perform as per BCP policy.

4.31.2 Configuration of DRS / NS with PDC

4.31.2.1 Hardware, system software, application environment, network and security devices and associated application environments of DRS / NS and PDC shall have one to one correspondence between them.

4.31.2.2 MIIs should develop systems that do not require configuration changes at the end of trading members/ clearing members/ depository participants for switchover from the PDC to DRS. Further, MIIs should test such switchover functionality by conducting unannounced live trading from its DRS for at least 1 day in every six months. Unannounced live trading from DRS of MIIs shall be done at a short notice of 45 minutes after 90 days from the date of this circular.

4.31.2.3 In the event of disruption of any one or more of the 'Critical Systems' (as defined below), the MII shall, within 30 minutes of the incident, declare that incident as 'Disaster' and take measures to restore operations including from DRS within 45 minutes of the declaration of 'Disaster'. Accordingly, the Recovery Time Objective(RTO)- the maximum time taken to restore operations of 'Critical Systems' from DRS after declaration of Disaster- shall be 45 minutes, to be implemented within 90 days from the date of the circular. 'Critical Systems' for an Exchange/ Clearing Corporation shall include Trading, Risk Management, Collateral Management, Clearing and Settlement and Index computation. 'Critical Systems' for a Depository shall include systems supporting settlement process and inter-depository transfer system.

4.31.2.4 MIIs to also ensure that the Recovery Point Objective (RPO) - the maximum tolerable period for which data might be lost due to a major incident- shall be 15 minutes.

4.31.2.5 Solution architecture of PDC and DRS / NS should ensure high

availability, fault tolerance, no single point of failure, zero data loss, and data and transaction integrity.

4.31.2.6 Any updates made at the PDC should be reflected at DRS/ NS immediately (before end of day) with head room flexibility without compromising any of the performance metrics.

4.31.2.7 Replication architecture, bandwidth and load consideration between the DRS / NS and PDC should be within stipulated RTO and ensure high availability, right sizing, and no single point of failure.

4.31.2.8 Replication between PDC and NS should be synchronous to ensure zero data loss whereas, the one between PDC and DRS and between NS and DRS may be asynchronous.

4.31.2.9 Adequate resources (with appropriate training and experience) should be available at all times to handle operations at PDC, NS or DRS, as the case may be, on a regular basis as well as during disasters.

4.31.3 DR Drills / Testing

4.31.3.1 DR drills should be conducted on a quarterly basis. In case of Exchanges and Clearing Corporations, these drills should be closer to real life scenario (trading days) with minimal notice to DRS staff involved.

4.31.3.2 During the drills, the staff based at PDC should not be involved in supporting operations in any manner.

4.31.3.3 The drill should include running all operations from DRS for at least 1 full trading day.

4.31.3.4 Before DR drills, the timing diagrams clearly identifying resources at both ends (DRS as well as PDC) should be in place.

4.31.3.5 The results and observations of these drills should be documented and placed before the Governing Board of Stock Exchanges /Clearing Corporations/ Depositories. Subsequently, the same along with the comments of the Governing Board should be forwarded to SEBI within a month of the DR drill.

4.31.3.6 The System Auditor while covering the BCP – DR as a part of mandated annual System Audit should check the preparedness of the MII to shift its operations from PDC to DRS unannounced and also comment on documented results and observations of DR drills.

4.31.3.7 'Live' trading sessions from DR site shall be scheduled for at least two consecutive days in every six months. Such live trading sessions from the DRS shall be organized on normal working days (i.e. not on weekends / trading holidays). The Stock Exchange/ Clearing Corporation/ Depository shall ensure that staff members working at DRS have the abilities and skills

to run live trading session independent of the PDC staff.

4.31.3.8 Stock Exchanges, Clearing Corporations and Depositories shall include a scenario of intraday shifting from PDC to DRS during the mock trading sessions in order to demonstrate its preparedness to meet RTO/RPO as stipulated above.

4.31.3.9 MII should undertake and document Root Cause Analysis (RCA) of their technical/ system related problems in order to identify the causes and to prevent reoccurrence of similar problems.

4.31.4 BCP - DR Policy Document

4.31.4.1 MIIs shall put in place a comprehensive BCP-DR policy document outlining the following:

i. Broad scenarios that would be defined as a Disaster for an MII (in addition to definition provided in **Para 4.31.2.3**).

ii. Standard Operating Procedure to be followed in the event of Disaster.

iii. Escalation hierarchy within the MII to handle the Disaster.

iv. Clear and comprehensive Communication Protocols and procedures for both internal and external communications from the time of incident till resumption of operations of the MII.

v. Documentation policy on record keeping pertaining to DR drills.

vi. Scenarios demonstrating the preparedness of MIIs to handle issues in Critical Systems that may arise as a result of Disaster.

vii. Preparedness of Depositories to handle any issue which may arise due to trading halts in Stock Exchanges.

viii. Framework to constantly monitor health and performance of Critical Systems in normal course of business.

4.31.4.2 The BCP-DR policy document of MII should be approved by Governing Board of the MIIs after being vetted by Technology Committee and thereafter communicated to SEBI. The BCP-DR policy document should be periodically reviewed at least once in six months and after every occurrence of disaster.

4.31.4.3 In case an MII desires to lease its premise at the DRS to other entities including to its subsidiaries or entities in which it has stake, the MII should ensure that such arrangements do not compromise confidentiality, integrity, availability, targeted performance and service levels of the MII's systems at the DRS. The right of first use of all the resources at DRS including network resources should be with the MII. Further, MII should deploy necessary access controls

to restrict access (including physical access) of such entities to its critical systems and networks.

4.31.5 Stock Exchanges, Clearing Corporations and Depositories should ensure that **Para** 4.31.3.6 and 4.31.4.1(v) mentioned above are also included in the scope of System Audit.

4.32 IT (Information Technology) Governance For Depositories[184]

4.32.1 SEBI constituted the Depository System Review Committee (DSRC) to undertake a comprehensive review of the Indian depository system. Based on the recommendations of DSRC, following guidelines are issued to strengthen the information Technology (IT) governance framework of depositories.

4.32.2 The Depositories shall formulate an IT strategy document and an Information Security policy which should be approved by the Board and reviewed annually.

4.32.3 The Depositories shall create an Office of Information Security and designate a senior official as Chief Information Security Officer (CISO) whose work would be to assess, identify and reduce information technology (IT) risks, respond to incidents, establish appropriate standards and controls, and direct the establishment and implementation of policies and procedures.

4.32.4 SEBI has laid down Guidelines for Business Continuity Plan (BCP) and Disaster Recovery (DR) for MIIs under Para 4.31. In addition to the requirements under Para 4.31, depositories shall designate a senior official as the head of BCP function.

4.33 Guidelines for inspection of Depository Participants (DPs) by Depositories[185]

4.33.1 Depository System Review Committee (DSRC) was constituted by SEBI to undertake a comprehensive review of the depository system of Indian Securities market.

4.33.2 As a first measure, DSRC has reviewed framework adopted by the depositories with regard to the inspection of depository participants (DPs). Considering the recommendations of the committee, it has been decided that depositories shall ensure the following while inspecting their DPs.

Inspection Areas and Sample Size

4.33.3 For conducting inspection of DPs, depositories shall inspect the following areas as mentioned below:

4.33.3.1 Depositories shall inspect the areas mentioned at Para 4.33.3.2 below during inspection of DPs with regards to any

4.33.3.1.1 Circulars / Guidelines issued by SEBI on the areas mentioned below

4.33.3.1.2 Guidelines / Operating Instructions / Directions from depositories on the

[184] Reference: SEBI Circular MRD/DMS/03/2014 dated January 21, 2014

[185] Reference: SEBI Circular SEBI/MRD/DMS/05/2014 dated February 07, 2014

areas mentioned below.

4.33.3.2 In case there are built in system checks at the depository that ensure compliance of any of the inspection areas/sub –areas with regard to **Para 4.33.3.1.1 and Para 4.33.3.1.2** above, the depository may decide on the including the same during the inspection of DPs

Inspection Areas

A. Account Opening / KYC Documents

- ***A.1.*** Account Opening forms
- ***A.2.*** KYC Documents
  - A.2.1. PAN Verification
  - A.2.2. In-person verification
  - A.2.3. Forwarding of Documents to KYC Registration Agency (KRA)
- ***A.3.*** Proof of Identity (POI)
- ***A.4.*** Proof of Address
- ***A.5.*** Correspondence Address
- ***A.6.*** Authorized Signatories
- ***A.7.*** Completeness / Validation of data entered into DPM with data provided in the Account Opening forms
- ***A.8.*** Minor BO / Joint / HUF accounts
- ***A.9.*** Account Activation
- ***A.10.*** PMS Accounts
- ***A.11.*** Nomination
- ***A.12.*** Any other area as may be specified by the depository

B. Basic Service Demat Account (BSDA)

- ***B.1.*** Procedures and Checks pertaining to BSDA
- ***B.2.*** Any other area as may be specified by the depository

C. Client Data Modification (CDM)

- ***C.1.*** Procedure for CDM
- ***C.2.*** Any other area as may be specified by the depository

D. Demat / Remat / Conversion /Reconversion request

- ***D.1.*** Procedure for receiving/processing requests pertaining to Demat / Remat / Conversion /Reconversion request
- ***D.2.*** Procedure for forwarding requests pertaining to Demat / Remat / Conversion /Reconversion request to RTA / issuer
- ***D.3.*** Arrangement for Safekeeping of Security / Share Certificates
- ***D.4.*** Tracking of demat requests

D.5. Rejection of above requests attributable to DPs

D.6. Checks pertaining to processing of Demat / Remat / Conversion / Reconversion request

D.7. Any other area as may be specified by the depository

E. Delivery Instruction Slip (DIS)

E.1. Issuance of DIS

E.2. Inventory Control of DIS

E.3. First Instruction Slip Booklet

E.4. Requisition Slip

E.5. Procedure for Loose DIS

E.6. Depository specific areas

E.7. Verification of DIS

E.8. Procedure for accepting DIS

E.9. Time Stamping and related Areas

E.10. Accepting DIS by Fax

E.11. Accepting DIS in form of Annexure

E.12. Completeness of DIS

E.13. Accepting DIS in electronic form

E.14. Procedure for Verification of DIS

E.15. Signature Verification

E.16. Corrections / Cancellations to DIS

E.17. Blocking of used / executed / lost / misplaced / Stolen DIS

E.18. Procedure for processing of DIS

E.19. Any other area as may be specified by the depository

F. Transaction

F.1. Checks pertaining to setting up / processing of transactions

F.2. Future dated transactions

F.3. Transfer of all ISINs of BO account having 5 or more ISINs

F.4. Any other area as may be specified by the depository

G. Transaction Statement (TS)

G.1. Validation of TS

G.2. Maintenance of records of TS

G.3. Issuance of TS to BOs

G.4. Any other area as may be specified by the depository

H. Compliance under Prevention of Money Laundering Act, 2002 (PMLA)

H.1. Compliance with PMLA Act, 2002 and SEBI Guidelines on areas such as Customer due diligence, suspicious transaction monitoring , reporting and record keeping

H.2. Appointment of Principal officer as required under PMLA Act,2002

H.3. Mechanism to deal with alerts provided by Depository

H.4. Suspicious Transactions reports to FIU

H.5. Any other area as may be specified by the depository

I. Maintenance of record and documents

I.1. Information regarding place(s) of record keeping

I.2. Outsourcing of record keeping activities

I.3. Any other area as may be specified by the depository

J. Service Centre Opening and closing/ modification of service centers

J.1. Procedure for Opening /Closureof Service centers

J.2. Details of Service centre on Depository website

J.3. Qualified persons at service centers

J.4. Any other area as may be specified by the depository

K. Information Technology areas

K.1. Hardware, Software and Network requirements / configurations

K.2. Logical and Physical restrictions / safeguards

K.3. IT Security

K.4. Procedure for alteration of parameters / configurations

K.5. Redundancy

K.6. Any other area as may be specified by the depository

L. Power of Attorney (POA)

L.1. Documents executed

L.2. Maintenance of POA Register

L.3. Clauses of POA

L.4. Registration of BO for SMS Alert facility for POA

L.5. Any other area as may be specified by the depository

M. Inter Depository Transfers (IDT)

M.1. Processing of IDT

M.2. Checks pertaining to IDT

M.3. Any other area as may be specified by the depository

N. Account Transfer

N.1. Procedure followed for account transfer

N.2. Checks pertaining to Account transfer

N.3. Waiver claimed for inter depository transfer

N.4. Any other area as may be specified by the depository

O. Transmission

O.1. Procedure followed for transmission

O.2. Checks pertaining to Transmission

O.3. Waiver Claimed for inter depository transfer

O.4. Any other area as may be specified by the depository

P. Pledge / Unpledge

P.1. Procedure followed for Pledge / Unpledge

P.2. Checks pertaining to Pledge / Unpledge

P.3. Any other area as may be specified by the depository

Q. Freeze / Unfreeze

Q.1. Freeze facility

Q.2. Procedure followed for Freeze

Q.3. Checks pertaining to freeze

Q.4. Any other area as may be specified by the depository

R. Miscellaneous areas

R.1. Investor Grievance

R.2. Forms for various activities

R.3. Execution of any supplementary agreement/ Letter of Confirmation

R.4. Submission of Internal Audit / Concurrent Audit / Net worth Certificate

R.5. Submission of Annual Financial Statement

R.6. Outsourcing of Activities

R.7. Closure / transfer of Balances

R.8. Submission of Information sought by Depositories specifically through Circulars / Letters.

R.9. Half Yearly Compliance

R.10. Any other area as may be specified by the depository

S. Status of compliance for deviations / observations noted in last inspection

T. Complaints

T.1. Account Opening

T.2. Demat / Remat

T.3. Transaction Statement

T.4. Improper Service

T.5. Charges

T.6. Delivery Instruction Related(DIS)

T.7. Closure

T.8. Manipulation / Unauthorized Action

T.9. Monthly report for client complaints

During inspection, depositories shall cover implementation of circulars / guidelines issued by SEBI and guidelines / operating instructions / directions by depositories in respect of these areas. In addition, Depositories may include such other areas as felt appropriate.

4.33.4 For the purpose of determining the size of sample, depositories shall be guided by 'Adaptive Sample Size determination methodology' as mentioned below:

***4.33.4.1* Sample Size for inspection area of 'Account Opening'**

- The sample selection for account opening shall cover all categories of clients such as individuals, HUF, Corporate, FPIs etc.
- Base sample size: 5% of Account Opening Forms (AOFs) or 150 AOFs whichever is higher, with a maximum cap of 1000 accounts.
- Final Sample Size: The final sample size shall also be dependent on past rating / categorization of DP. The following multipliers shall be used to determine the final sample size for the current inspection. In case the total number of instances / cases is less than the final sample size, then 100% of the samples shall be verified.

DP Rating / Categorization	Multiplier
High risk	3
Medium High risk	2
Medium risk	1.5
Low risk	1

- The selected sample shall maintain the proportion of new accounts opened in each category, except for Account Opening Forms (AOF) relating to FIPs where it shall be checked on a 100% basis.

***4.33.4.2* Sample Size for sinspection area relating to DIS**

- Base sample size: 10% of total DIS processed or 200 processed DIS whichever is higher, with a maximum cap of 1000 DIS.
- Final Sample Size: The sample size shall also be dependent on rating / categorization of DP. The following multipliers shall be used to determine the final sample size for the current inspection. In case the total number of instances / cases is less than the final sample size, then 100% of the samples shall be verified.

DP Rating / Categorization	Multiplier

High risk	3
Medium High risk	2
Medium risk	1.5
Low risk	1

- Out of total intra depository instructions to be verified, the percentage of on and off market instructions would be in the ratio of 1/3 and 2/3.
- DIS issuance sample size shall be 5% of the total samples verified for DIS.

4.33.4.3 **Sample Sizes for inspection areas of 'Demat / Remat request' and 'Pledge/Unpledge'**

- 5% of Demat / Remat request processed or 100 requests whichever is higher with a maximum cap of 500 such requests.
- 5% of Pledge / Unpledge request processed or 100 requests whichever is higher with a maximum cap of 500 such requests.

4.33.4.4 **Sample Size for inspection area of 'Client Data Modification', 'Miscellaneous areas' and 'Other depository specific requirements'**

- Base Sample Size
  - Address change = 50
    - Samples from Urban, Semi Urban and Rural Areas shall be equally represented if available.
  - Nomination Change= 25
  - Signature change = 100
  - Addition / Deletion / Modification of POA = 100
  - Freeze/ Unfreeze= 50
  - Bank Details Change= 100
  - PAN modification = 100
  - Account closure initiated by clients = 25
  - Closure initiated by DPs = 25
  - Demat rejection = 30
  - Transactions = 25
  - Change in e-mail Id = 25
  - Change in mobile number = 25
  - Change in SMS flag = 50
  - Change in standing instruction flag = 50
  - Transmission = 50% of total transmission cases
  - Previous compliance = 100% of total samples
  - Final sample size shall be arrived at after multiplying with the respective multiplier corresponding to the DP Risk rating / categorization as given below.

In case the total number of instances / cases is less than the final sample size, then 100% of the samples shall be verified.

DP Rating/ Categorisation	Multiplier
High risk	3
Medium High risk	2
Medium risk	1.5
Low risk	1

4.33.4.5 **Other Aspects**

- A uniform Base sample size of 100 shall be adopted in case of all other activities. In case the total number of samples is less than 100, then 100% of the samples shall be verified.

Categorization / Risk Rating of DPs

4.33.5 For the purpose of computing total risk score of DPs, depositories shall be guided by "DP Rating Model / Categorization" as mentioned below:

4.33.5.1 **Quantitative Score Calculation:** Specific weights shall be assigned to each area as decided by each depository. The Total Quantitative Score shall be the summation of all individual inspection scores.

Table: Indicative Table for calculation of Quantitative Score

S. No	Inspection Areas	Weight (A)	B = No of Instances divided by Sample size	Inspection Score IS = A*B
A.	**Inspection Area 1**			
A.1.	Inspection Sub Area A 1			
A.2.	Inspection Sub Area 2			
	Total Score for ***Inspection Area 1***			
B.	**Inspection Area 2**			
B.1.	Inspection Sub Area B 1			
B.2.	Inspection Sub Area B 2			
B.3.	Inspection Sub Area B 3			
	Total Score for ***Inspection Area 2***			

Depositories shall include all inspection areas and sub areas, as per Para 4.33.3 (List of Inspection Areas), in the above model to arrive at the Quantitative Score for a DP.

Table: Indicative Table for calculation of Quantitative Score for Complaints Received

S. No.	Type and Nature of Complaint	Weight (A)	(Number of Complaints redressed) / Number of Complaints received)	Inspection Score IS = A*B
T	**Complaints**			
T.1	Complaint Sub Area 1			
T.2	Complaint Sub Area 2			
	Total Score for ***Complaints***			

Quantitative Score = Σ (Scores of Inspection Areas including Total score for Complaints)

4.33.5.2 **Qualitative Score Calculation**: Specific weights shall be assigned to each area as decided by depository. The Total Qualitative Score shall be the summation of all area scores.

Sr. No	Qualitative Factors	Weight (A)	Point on the scale of 1 to 10. [10 being the Worst] (B)	Area score =(A) * (B)
1	Ownership and Governance			
2	IT security and Business Continuity			
3	Regulatory / procedural Compliance			
4	Automation of systems and processes for critical activities			
5	Quality of Management			
6	Financial Status / profitability of DPs			
7	Pending enquires / Penalties imposed by SEBI / Depositories on DP operations			
8	Complaints redressal			
9	Adverse findings of other activities (eg. Broking / custodian / banks etc)			
Total Qualitative Score = Σ (Area Scores)				

Following indicative factors shall be taken into account for arriving at above mentioned qualitative score:

(a) **Ownership and Governance**

1. Constitution of Board of DP – Number of promoter directors, Independent Directors etc.

2. Role of non-executive directors / Independent directors.

(b) **Quality of Management**

1. Experience, Fit and Proper and Qualification of Key Personnel.

2. Existence of Succession planning for top management especially in control functions.

3. Chinese walls between the activities in terms of manpower, resources etc.

4. Training and development of employees.

5. Adequacy of staff strength.

6. Compliance level of previous inspection observations/ directions of regulatory bodies

(c) **IT security and Business Continuity**

1. High Availability.

2. Appropriate Interconnected Architecture.

3. Appropriate Recovery Time Objective (RTO) and Recovery Point Objective (RPO) and near "Zero Data Loss".

4. Periodic drills that simulate the real life disaster scenarios on a regular basis.

5. Technological glitches in the past period and remedies taken.

6. Information security.

7. Upgradation of technology

(d) **Financial Status / profitability of DPs**

1. The net-worth of the DPs (whether reducing or increasing from previous years)

2. Net Profits of DPs operations.

(e) **Complaints redressal**

1. Complaint redressal system

2. Percentage of complaints pending and resolved.

(f) **Other adverse findings**

1. Actions taken by Stock exchange and SEBI / RBI with respect to other activities

2. Actions taken by other depository.

4.33.5.3 **Total Score = Qualitative Score + Quantitative Score**

4.33.6 Depositories should periodically undertake risk - impact analysis for each of the inspection areas, assign appropriate risk weightage, calculate risk scores for each DPs in the lines mentioned below.

a. Risk Weightage: Depositories shall assign risk weights for each of inspection areas after taking into consideration following factors:

1. Operational risks in each of the inspection areas.
2. Category of DPs (such as stock broker DPs, bank DP, etc.)
3. Size of Operation
4. Repetitive violations
5. IT Security and BCP
6. Complaints received and redressed

b. Quantitative Score Calculation: Depositories shall arrive at a Quantitative Risk Score for each inspection area by multiplying percentage of non-compliance to the sample size with the corresponding assigned risk weight.

c. Qualitative Score Calculation: Depositories shall arrive at a Qualitative Risk Score for each qualitative area by multiplying the score assigned by inspection team to DP with corresponding assigned risk weight.

d. Total DP Risk Score shall be the summation of quantitative and qualitative scores assigned to the DP.

e. Depositories shall suitably normalize the scales of the qualitative and quantitative scores in arriving at the Total DP risk score.

4.33.7 Depositories shall categorize their DPs as 'High Risk', 'Medium to High Risk', 'Medium Risk', and 'Low Risk' DPs based on the percentile of risk score.

DP Risk Rating / Categorization	Percentile of Risk Score
High	≥ 80
Medium-High	46-79
Medium	21-45
Low	≤ 20

4.33.8 After arriving at the risk rating / categorization as mentioned above, for subsequent inspections, depositories shall use the DP risk rating/ categorization to decide on the frequency of inspection of DPs

4.33.9 Apart from the above, depositories may undertake specific purpose inspections for DPs which score high in the specific inspection areas as **Para 4.33.3**

4.33.10 Depositories shall jointly inspect DPs which are registered with both depositories to have better control over DPs, avoid duplicity of manpower, time and cost and also to reduce the possibility of regulatory arbitrage, if any. Depositories shall share the risk rating / categorization of common DPs with each other. For the purpose of determining sample size and frequency of the joint inspection of such common DPs, the higher risk categorization assigned by any of the Depository shall prevail.

4.34 ***Dissemination of information on action taken against Depository Participants on the website of Depositories***[186]

4.34.1 The following directions have been approved by SEBI:

4.34.1.1 Wherever powers are conferred upon Depositories to take actions in case of default/non-compliance by DPs, the data of such actions/non-compliance should be made available in public domain by the depository

4.34.1.2 A link may be provided in the SEBI website leading to the Depository website as detailed in **Para 4.34.1.1** above.

4.34.2 Depositories are advised to make available on its website, the information pertaining to action taken against DP pursuant to joint inspection/suo-moto independent inspection carried out. For prospective cases, the same shall be uploaded within 10 days of concluding the matter.

4.35 ***Activity of Demat of warehouse receipts***[187]

The aforesaid activity is not in compliance with Regulation 42 of DP Regulations and therefore depositories cannot carry out this activity. Depositories are therefore advised to take suitable steps in this regard, either to hive-off or to discontinue the activity.

4.36 ***Voting rights in respect of securities held in pool account***[188]

The corporate benefits availed by the clearing member, clearing corporation and intermediaries shall be held in trust on behalf of beneficiary owners. Therefore, the clearing member, clearing corporation as well as the intermediaries cannot have voting rights in respect of securities held in the pool account.

4.37 ***e-Voting Facility Provided by Listed Entities***[189]

Kindly refer para titled 'e-voting facility provided by listed entities' of SEBI Circular SEBI/HO/CFD/PoD2/CIR/P/2023/120 dated July 11, 2023 (Master circular for compliance with the provisions of the Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015 by listed entities)

4.38 ***Risk Management Policy at the Depositories***[190]

4.38.1 The depositories are advised to establish a clear, comprehensive and well documented risk management framework which shall include the following:

---

[186] Reference: SEBI Letter SEBI/HO/MIRSD/DPIEA/OW/2021/10188/3 dated May 11, 2021

[187] Reference: SEBI Letter MRD/DP/SG-OW/202/2012 and MRD/DP/SG-OW/203/2012 dated January 4, 2012

[188] Reference: SEBI Letter SMDRP/NSDL/26563/2001 dated April 10, 2001

[189] Reference: SEBI Circular SEBI/HO/CFD/CMD/CIR/P/2020/242 dated December 09, 2020

[190] Reference: SEBI Circular CIR/MRD/DP/1/2015 dated January 12, 2015

4.38.1.1 an integrated and comprehensive view of risks to the depository including those emanating from participants, participants' clients and third parties to whom activities are outsourced etc.;

4.38.1.2 list out all relevant risks, including technological, legal, operational, custody and general business risks and the ways and means to address the same;

4.38.1.3 the systems, policies and procedures to identify, assess, monitor and manage the risks that arise in or are borne by the depository;

4.38.1.4 the depository's risk-tolerance policy;

4.38.1.5 responsibilities and accountability for risk decisions and decision making process in crises and emergencies.

4.38.2 The Depositories shall put in place mechanism to implement the Risk Management Framework through a Risk Management Committee which shall be headed by a Public Interest Director[191].The responsibilities of the said Committee shall include the following:

4.38.2.1 It shall meet periodically in order to continuously identify, evaluate and assess applicable risks in depository system through various sources such as investors complaints, inspections, system audit etc.;

4.38.2.2 It shall suggest measures to mitigate risk wherever applicable;

4.38.2.3 It shall monitor and assess the adequacy and effectiveness of the risk management framework and the system of internal control;

4.38.2.4 It shall review and update the risk management framework periodically.

4.38.3 The Board of the depository shall approve the Risk Management Framework and the Chief Risk Officer shall have access to the Board. The CRO shall be responsible, accountable and answerable to the board on overall risk management issues.

4.39 <u>Code of Conduct & Institutional mechanism for prevention of Fraud or Market Abuse[192]</u>

4.39.1 Pursuant to the report of the Committee on Fair Market Conduct ('Committee'), set up inter-alia to recommend appropriate Institutional Mechanism to ensure accountability of the management/designated persons in case of negligence/failure, necessary changes have been carried out in PIT Regulations.

4.39.2 Based on the above, it has been decided that the Code of Conduct and Institutional Mechanism for prevention of fraud or market abuse shall be

[191] Reference: SEBI Circular SEBI/HO/MRD/DOP2DSA2/CIR/P/2019/13 dated January 10, 2019
[192] Reference: SEBI Circular SEBI/HO/MRD/DCAP/CIR/P/2021/23 dated March 03, 2021

applicable to Stock Exchanges, Clearing Corporations and Depositories (herein after collectively referred as 'MIIs') also, on the lines of Regulation 9(1) to 9(4) of PIT Regulations.

4.39.3 Accordingly, depositories shall do the following:

4.39.3.1 Formulate a Code of Conduct to regulate, monitor and report trading by their designated persons and immediate relative of designated persons towards achieving compliance with the PIT Regulations, by adopting the minimum standards set out in Schedule C to the PIT Regulations.

4.39.3.2 Managing Director (MD) / Chief Executive Officer (CEO) of the depository shall be obligated to frame the referred code of conduct. The Board of Directors may ensure the compliance by MD/CEO in this regard.

Explanation – For the avoidance of doubt it is clarified that a depository, which is listed, is already required to adopt minimum standards set out in Schedule B of PIT regulations. Further, such depository shall adopt minimum standards as set out in Schedule B of PIT regulations with respect to trading in its own securities and in Schedule C with respect to trading in other securities.

4.39.3.3 Depository shall identify and designate a compliance officer to administer the aforesaid code of conduct.

4.39.3.4 The Board of Directors of the depository , in consultation with the aforesaid compliance officer, shall specify the designated persons to be covered by the code of conduct on the basis of their role and function in the organisation and the access that such role and function would provide to unpublished price sensitive information in addition to seniority and professional designation and shall include the position/designation as specified in the Regulation 9(4) of the PIT Regulations.

4.39.4 Depositories shall put in place an Institutional Mechanism for prevention of fraud or market abuse covering the following:

4.39.4.1 MD / CEO of the depository shall put in place adequate and effective system of internal controls to ensure compliance with the regulations and circulars issued by the Board from time to time, to prevent fraud or market abuse by depository or its designated persons and immediate relatives of designated persons.

4.39.4.2 The Board of Directors of the depository shall ensure that the MD/CEO ensures compliance with **Para 4.39.3** and **Para 4.39.4.1**

above. The compliance officer of the depository shall administer the internal controls to prevent fraud or market abuse by designated persons and immediate relatives of designated persons of the depository.

4.39.4.3 The Regulatory Oversight Committee of the depository shall review compliance with the provisions of this Circular at least once in a financial year and shall also verify that the systems for internal control are adequate and are operating effectively.

4.39.4.4 Depository shall formulate written policies and procedures for inquiry in case of suspected fraud or market abuse by its designated persons and immediate relatives of designated persons, which shall be approved by its Board of Directors. Any enquiry / investigation against the designated persons and immediate relatives of designated persons of the depository may be undertaken under the supervision of Regulatory Oversight Committee comprising of PIDs and independent external expert with consideration of avoidance of conflict of interest, if any, so as to ensure maximum fairness and transparency.

4.39.4.5 Depository shall initiate appropriate inquiry upon becoming aware of any illegal or unethical practices or transactions of suspected fraud or market abuse by its designated persons and immediate relatives of designated persons and promptly inform its Board of Directors of such suspected fraud or market abuse and results of the inquiry.

4.39.4.6 Depository shall have an effective whistler-blower policy to enable stakeholders, including employees to freely communicate their concerns about illegal or unethical practices and report instances of fraud or market abuse or any suspicion of fraud or market abuse.

4.39.4.7 Depository shall ensure that the policy framed under **Para 4.39.4.6** provides for suitable protection against any discharge, termination, demotion, suspension, threats, harassment, directly or indirectly or discrimination against any employee who reports instances of fraud or market abuse or any suspicion of fraud or market abuse.

4.40 Outsourcing by Depositories[193]

Based on recommendations by DSRC, the depositories are advised to ensure the following:

[193] Reference: SEBI Circular CIR/MRD/DP/19/2015 dated December 09, 2015

4.40.1 Depositories shall formulate and document an outsourcing policy duly approved by their Board based on the guidelines given below and the principles outlined at **Para 2.4.4.**

Core activities of Depositories

4.40.2 Core and critical activities of depositories shall not be outsourced. The core activities of the depositories shall include but not limited to the following:

- ***4.40.2.1*** Processing of the applications for admission of Depository Participants (DPs), Issuers and Registrar & Transfer Agents (RTAs).
- ***4.40.2.2*** Facilitating Issuers/RTAs to execute Corporate Actions.
- ***4.40.2.3*** Allotting ISINs for securities.
- ***4.40.2.4*** Maintenance and safekeeping of Beneficial Owner's data.
- ***4.40.2.5*** Execution of settlement and other incidental activities for pay-in/ pay-out of securities.
- ***4.40.2.6*** Execution of transfer of securities and other transactions like pledge, freeze, etc.
- ***4.40.2.7*** Provision of internet based facilities for access to demat accounts and submitting delivery instructions.
- ***4.40.2.8*** Ensuring continuous connectivity to DPs, RTAs, Clearing Corporations and other Depository.
- ***4.40.2.9*** Monitoring and redressal of investor grievances.
- ***4.40.2.10*** Inspection of DPs and RTAs.
- ***4.40.2.11*** Surveillance Functions.
- ***4.40.2.12*** Compliance Functions.

4.40.3 Core IT (Information Technology) support infrastructure / activities for running the core activities of depositories shall not be outsourced to the extent possible.

Due Diligence

4.40.4 The depositories shall conduct appropriate due diligence in selecting the third party to whom activity is proposed to be outsourced and ensure that only reputed entities having proven high delivery standards are selected.

Risk Management & Monitoring

4.40.5 Depositories shall ensure that outsourced activities are further outsourced downstream only with the prior consent of the depository and with appropriate safeguards including proper legal documentation/ agreement.

4.40.6 Depositories shall ensure that risk impact analysis is undertaken before outsourcing any activity and appropriate risk mitigation measures like back up/ restoration system are in place.

4.40.7 An effective monitoring of the entities selected for outsourcing shall be done to ensure that there is check on the activities of outsourced entity. Depositories shall strive to automate their processes and workflows to the extent possible which shall enable real time monitoring of outsourced activities.

Audit

4.40.8 The outsourcing policy document shall act as a reference for audit of the outsourced activities. Audit of implementation of risk assessment and mitigation measures listed in the outsourcing policy document and outsourcing agreement/ service level agreements pertaining to IT systems shall be part of System Audit of Depositories.

4.41 Cyber Security and Cyber Resilience framework of Depositories[194]

4.41.1 SEBI as a member of IOSCO has adopted the Principles for Financial Market Infrastructures (PFMIs) laid down by CPMI-IOSCO and has issued guidance for implementation of the principles in the securities market.

4.41.2 Principle 17 of PFMI that relates to management and mitigation of 'Operational risk' requires that systemically important market infrastructures institutions "*should identify the plausible sources of operational risk, both internal and external, and mitigate their impact through the use of appropriate systems, policies, procedures, and controls. Systems should be designed to ensure a high degree of security and operational reliability and should have adequate, scalable capacity. Business continuity management should aim for timely recovery of operations and fulfilment of the FMI's obligations, including in the event of a wide-scale or major disruption*."

4.41.3 Stock Exchanges, Depositories and Clearing Corporations (hereafter referred as *Market Infrastructure Institutions* or *MIIs*) are systemically important market infrastructure institutions. As part of the operational risk management, these MIIs need to have robust cyber security framework to provide essential facilities and perform systemically critical functions relating to trading, clearing and settlement in securities market.

4.41.4 In view of the above, SEBI along with the TAC engaged in detailed discussions with MIIs to develop necessary guidance in the area of cyber security and cyber resilience.

4.41.5 Based on the consultations and recommendations of TAC, it has been decided to lay down the framework placed under **Para 4.41.7** below that MIIs would be required to comply with regard to cyber security and cyber resilience.

4.41.6 Further, MIIs, whose systems have been identified as Critical Information Infrastructure (CII) by National Critical Information Infrastructure Protection

[194] Reference: SEBI Circular CIR/MRD/DP/13/2015 dated July 06, 2015

Centre (NCIIPC), are mandated to send regular updates/closure status of the vulnerabilities found in their respective "protected systems" to NCIIPC.[195]

4.41.7 **Framework for cyber security and cyber resilience**

4.41.7.1 Cyberattacks and threats attempt to compromise the Confidentiality, Integrity and Availability (CIA) of the computer systems, networks and databases. Cyber security framework include measures, tools and processes that are intended to prevent cyberattacks and improve cyber resilience. Cyber Resilience is an organisation's ability to prepare and respond to a cyber-attack and to continue operation during, and recover from, a cyber-attack.

Governance

4.41.7.2 As part of the operational risk management framework to manage risk to systems, networks and databases from cyber-attacks and threats, MII should formulate a comprehensive cyber security and cyber resilience policy document encompassing the framework mentioned hereunder. The policy document should be approved by the Board, and in case of deviations from the suggested framework, reasons for such deviations should also be provided in the policy document. The policy document should be reviewed by the MII's Board atleast annually with the view to strengthen and improve its cyber security and cyber resilience framework.

4.41.7.3 The cyber security and cyber resilience policy should include the following process to identify, assess, and manage cyber security risk associated with processes, information, networks and systems.

a. 'Identify' critical IT assets and risks associated with such assets,

b. 'Protect' assets by deploying suitable controls, tools and measures,

c. 'Detect' incidents, anomalies and attacks through appropriate monitoring tools / processes,

d. 'Respond' by taking immediate steps after identification of the incident, anomaly or attack,

e. 'Recover' from incident through incident management, disaster recovery and business continuity framework.

4.41.7.4 The Cyber security policy should encompass the principles prescribed by National Critical Information Infrastructure Protection Centre (NCIIPC) of National Technical Research Organisation (NTRO), Government of India in the report titled 'Guidelines for Protection of National Critical Information Infrastructure' and subsequent revisions, if any, from time to time.

[195] Reference: SEBI Circular SEBI/HO/MRD/TPD/P/CIR/2023/147 dated August 24, 2023

4.41.7.5 MII should also incorporate best practices from standards such as ISO 27001, ISO 27002, COBIT 5, etc., or their subsequent revisions, if any, from time to time.

4.41.7.6 MII should designate a senior official as Chief Information Security Officer (CISO) whose function would be to assess, identify and reduce cyber security risks, respond to incidents, establish appropriate standards and controls, and direct the establishment and implementation of processes and procedures as per the cyber security and resilience policy approved by the Board of the MII.

4.41.7.7 The Standing Committee on Technology**[196]** of the stock exchanges, clearing corporations and the depositories should on a quarterly basis review the implementation of the cyber security and resilience policy approved by their Boards, and such review should include review of their current IT and cyber security and resilience capabilities, set goals for a target level of cyber resilience, and establish a plan to improve and strengthen cyber security and cyber resilience.

4.41.7.8 MII should establish a reporting procedure to facilitate communication of unusual activities and events to CISO or to the senior management in a timely manner.

4.41.7.9 The aforementioned committee and the senior management of the MII, including the CISO, should periodically review instances of cyber-attacks, if any, domestically and globally, and take steps to strengthen cyber security and cyber resilience framework.

4.41.7.10 MII should define responsibilities of its employees, outsourced staff, and employees of vendors, members or participants and other entities, who may have access or use systems / networks of MII, towards ensuring the goal of cyber security.

Identify

4.41.7.11 [197]MII should identify and classify/designate 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

[196] Reference SEBI Circular SMD/POLICY/Cir-2/98 dated January 14, 1998 and SEBI Circular SEBI/HO/MRD/DOP2DSA2/CIR/P/2019/13 dated January 10, 2019

[197] Reference: SEBI Circular SEBI/HO/MRD1/MRD1_DTCS/P/CIR/2022/68 dated May 20, 2022

maintenance should also be classified as critical system. The Board of the MII shall approve the list of critical systems.

To this end, MII 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.

4.41.7.12 MII should accordingly identify cyber risks (threats and vulnerabilities) that it may face, along-with the likelihood of such threats and impact on the business and thereby, deploy controls commensurate to the criticality.

4.41.7.13 MII should also encourage its third-party providers, such as service providers, stock brokers, depository participants, etc. to have similar standards of Information Security.

Protection

Access Controls

4.41.7.14 No person by virtue of rank or position should have any intrinsic right to access confidential data, applications, system resources or facilities.

4.41.7.15 Any access to MII's systems, applications, networks, databases, etc., should be for a defined purpose and for a defined period. MII should grant access to IT systems, applications, databases and networks on a need-to-use basis and based on the principle of least privilege. Such access should be for the period when the access is required and should be authorized using strong authentication mechanisms.

4.41.7.16 MII should implement strong password controls for users' access to systems, applications, networks and databases. Password controls should include a change of password upon first log-on, minimum password length and history, password complexity as well as maximum validity period. The user credential data should be stored using strong and latest hashing algorithms.

4.41.7.17 MII should ensure that records of user access are uniquely identified and logged for audit and review purposes. Such logs should be maintained and stored in encrypted form for a time period not less than two (2) years.

4.41.7.18 MII should deploy additional controls and security measures to supervise staff with elevated system access entitlements (such as admin or privileged users). Such controls and measures should inter-alia include restricting the number of privileged users, periodic review of privileged users' activities, disallow privileged users from accessing systems logs in which their activities are being captured, strong controls over remote access by privileged users, etc.

4.41.7.19 Account access lock policies after failure attempts should be implemented for all accounts.

4.41.7.20 Employees and outsourced staff such as employees of vendors or service providers, who may be given authorised access to the MII's critical systems, networks and other computer resources, should be subject to stringent supervision, monitoring and access restrictions.

4.41.7.21 Two-factor authentication at log-in should be implemented for all users that connect using online / internet facility.

4.41.7.22 MII should formulate an Internet access policy to monitor and regulate the use of internet and internet based services such as social media sites, cloud-based internet storage sites, etc.

4.41.7.23 Proper 'end of life' mechanism should be adopted to deactivate access privileges of users who are leaving the organization or who access privileges have been withdrawn.

Physical security

4.41.7.24 Physical access to the critical systems should be restricted to minimum. Physical access of outsourced staff / visitors should be properly supervised by ensuring at the minimum that outsourced staff / visitors are accompanied at all times by authorised employees.

4.41.7.25 Physical access to the critical systems should be revoked immediately if the same is no longer required.

4.41.7.26 MII should ensure that the perimeter of the critical equipment room are physically secured and monitored by employing physical, human and procedural controls such as the use of security guards, CCTVs, card access systems, mantraps, bollards, etc. where appropriate.

Network Security Management

4.41.7.27 MII should establish baseline standards to facilitate consistent application of security configurations to operating systems, databases, network devices and enterprise mobile devices within the IT environment. The MII should conduct regular enforcement checks to ensure that the baseline standards are applied uniformly.

4.41.7.28 MII should install network security devices, such as firewalls as well as intrusion detection and prevention systems, to protect its IT infrastructure from security exposures originating from internal and external sources.

4.41.7.29 Anti-virus software should be installed on servers and other computer systems. Updation of Anti-virus definition files and automatic anti-virus scanning should be done on a regular basis.

Security of Data

4.41.7.30 Data-in motion and Data-at-rest should be in encrypted form by using strong encryption methods such as Advanced Encryption Standard (AES), RSA, SHA-2, etc.

4.41.7.31 MII should implement measures to prevent unauthorised access or copying or transmission of data / information held in contractual or fiduciary capacity. It should be ensured that confidentiality of information is not compromised during the process of exchanging and transferring information with external parties.

4.41.7.32 The information security policy should also cover use of devices such as mobile phone, faxes, photocopiers, scanners, etc. that can be used for capturing and transmission of data.

4.41.7.33 MII should allow only authorized data storage devices through appropriate validation processes.

Hardening of Hardware and Software

4.41.7.34 Only a hardened and vetted hardware / software should be deployed by the MII. During the hardening process, MII should inter-alia ensure that default passwords are replaced with strong passwords and all unnecessary services are removed or disabled in equipment's / software.

4.41.7.35 All open ports which are not in use or can potentially be used for exploitation of data should be blocked. Other open ports should be monitored and appropriate measures should be taken to secure the ports.

Application Security and Testing

4.41.7.36 MII should ensure that regression testing is undertaken before new or modified system is implemented. The scope of tests should cover business logic, security controls and system performance under various stress-load scenarios and recovery conditions.

Patch Management

4.41.7.37 MII should establish and ensure that the patch management procedures include the identification, categorization and prioritisation of security patches. An implementation timeframe for each category of security patches should be established to implement security patches in a timely manner.

4.41.7.38 MII should perform rigorous testing of security patches before deployment into the production environment so as to ensure that the application of patches do not impact other systems.

Disposal of systems and storage devices

4.41.7.39 MII should frame suitable policy for disposals of the storage media and systems. The data / information on such devices and systems should be

removed by using methods viz. wiping / cleaning / overwrite, degauss and physical destruction, as applicable.

Vulnerability Assessment and Penetration Testing (VAPT)

4.41.7.40 [198]MIIs should carry out periodic vulnerability assessment and penetration testing (VAPT) which inter-alia includes all 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 MII 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.

MIIs should conduct VAPT at least once in a financial year. However, for the MIIs, whose systems have been identified as "protected system" by National Critical Information Infrastructure Protection Centre (NCIIPC), VAPT shall be conducted at least twice in a financial year. Further, all MIIs are required to engage only CERT-In empaneled organizations for conducting VAPT. The final report on said VAPT should be submitted to SEBI after approval from Standing Committee on Technology (SCOT) of respective MIIs, within 1 month of completion of VAPT activity.

4.41.7.41 [199]Any gaps/vulnerabilities detected have to 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 to SEBI.

4.41.7.42 [200]In addition, MIIs should also 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.

Monitoring and Detection

4.41.7.43 MII should establish appropriate security monitoring systems and processes to facilitate continuous monitoring of security events and timely detection of unauthorised or malicious activities, unauthorised changes, unauthorised access and unauthorised copying or transmission of data / information held in contractual or fiduciary capacity, by internal and external parties. The security logs of systems, applications and network devices should also be monitored for anomalies.

4.41.7.44 Further, to ensure high resilience, high availability and timely detection of attacks on systems and networks, MII should implement suitable

[198] Reference: SEBI Circular SEBI/HO/MRD1/MRD1_DTCS/P/CIR/2022/68 dated May 20, 2022
[199] Reference: SEBI Circular SEBI/HO/MRD1/MRD1_DTCS/P/CIR/2022/68 dated May 20, 2022
[200] Reference: SEBI Circular SEBI/HO/MRD1/MRD1_DTCS/P/CIR/2022/68 dated May 20, 2022

mechanism to monitor capacity utilization of its critical systems and networks.

4.41.7.45 Suitable alerts should be generated in the event of detection of unauthorized or abnormal system activities, transmission errors or unusual online transactions.

Response and Recovery

4.41.7.46 Alerts generated from monitoring and detection systems should be suitably investigated, including impact and forensic analysis of such alerts, in order to determine activities that are to be performed to prevent expansion of such incident of cyber-attack or breach, mitigate its effect and eradicate the incident.

4.41.7.47 The response and recovery plan of the MII should aim at timely restoration of systems affected by incidents of cyber-attacks or breaches. The recovery plan should be in line with the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) specified by SEBI.

4.41.7.48 The response plan should define responsibilities and actions to be performed by its employees and support / outsourced staff in the event of cyber-attacks or breach of cyber security mechanism.

4.41.7.49 Any incident of loss or destruction of data or systems should be thoroughly analyzed and lessons learned from such incidents should be incorporated to strengthen the security mechanism and improve recovery planning and processes.

4.41.7.50 MII should also conduct suitable periodic drills to test the adequacy and effectiveness of response and recovery plan.

Sharing of information

4.41.7.51 Quarterly reports containing information on cyber-attacks and threats experienced by MII and measures taken to mitigate vulnerabilities, threats and attacks including information on bugs / vulnerabilities / threats that may be useful for other MIIs, should be submitted to SEBI.

4.41.7.52 Such details as are felt useful for sharing with other MIIs in masked and anonymous manner shall be shared using mechanism to be specified by SEBI from time to time.

Training

4.41.7.53 MII should conduct periodic training programs to enhance awareness level among the employees and outsourced staff, vendors, etc. on IT / Cyber security policy and standards. Special focus should be given to build awareness levels and skills of staff from non-technical disciplines.

4.41.7.54 The training program should be reviewed and updated to ensure that the contents of the program remain current and relevant.

Periodic Audit

4.41.7.55 The MIIs are mandated to conduct comprehensive cyber audit at least 2 times in a financial year. Along with cyber audit reports, henceforth, MIIs are directed to submit a declaration from the MD/CEO certifying that[201]:

4.41.7.55.1 Comprehensive measures and processes including suitable incentive/disincentive structures, have been put in place for identification/detection and closure of vulnerabilities in the organization's IT systems.

4.41.7.55.2 Adequate resources have been hired for staffing their Security Operations Center (SOC).

4.41.7.55.3 There is compliance by the MII with all SEBI circulars and advisories related to cyber security.

4.41.8 Cyber Security Operation Center (C-SOC)[202]

4.41.8.1 Recognizing the need for a robust Cyber Security and Cyber Resilience framework at Market Infrastructure Institutions (MIIs), i.e., Stock Exchanges, Clearing Corporations and Depositories, under **Para 4.41.3** above, a detailed regulatory framework on cyber security and cyber resilience has been prescribed.

4.41.8.2 With the view to further strengthening the aforesaid framework, particularly in respect of monitoring of cyber threats and cyber resiliency, the matter was discussed with SEBI's TAC, SEBI's High Powered Committee on Cyber Security (HPSC-CS) and the MIIs.

4.41.8.3 Accordingly, it has been decided that MIIs shall have a Cyber Security Operation Center (C-SOC) that would be a 24x7x365 set-up manned by dedicated security analysts to identify, respond, recover and protect from cyber security incidents.

4.41.8.4 The C-SOC shall function in accordance with the framework specified at **Para 4.41.7**. Illustrative list of broad functions and objectives to be carried out by a C-SOC are mentioned below:

4.41.8.4.1 Prevention of cyber security incidents through proactive actions:

a) Continuous threat analysis,
b) Network and host scanning for vulnerabilities and breaches,
c) Countermeasure deployment coordination,

[201] Reference: SEBI Circular SEBI/HO/MRD1/MRD1_DTCS/P/CIR/2022/68 dated May 20, 2022, and SEBI Circular SEBI/HO/MRD/TPD/P/CIR/2023/147 dated August 24, 2023

[202] Reference: SEBI Circular CIR/MRD/CSC/148/2018 dated December 07, 2018

d) Deploy adequate and appropriate technology at the perimeter to prevent attacks originating from external environment and internal controls to manage insider threats. MIIs may implement necessary controls to achieve zero trust security model.

4.41.8.4.2 Monitoring, detection, and analysis of potential intrusions / security incidents in real time and through historical trending on security-relevant data sources.

4.41.8.4.3 Response to confirmed incidents, by coordinating resources and directing use of timely and appropriate countermeasures.

4.41.8.4.4 Analysis of the intrusions / security incidents (including Forensic Analysis and Root Cause Analysis) and preservation of evidence.

4.41.8.4.5 Providing situational awareness and reporting on cyber security status, incidents, and trends in adversary behaviour to appropriate organizations including to CERT- In and NCIIPC.

4.41.8.4.6 Engineer and operate network defense technologies such as Intrusion Detection Systems (IDSes) and data collection / analysis systems.

4.41.8.4.7 MIIs to adopt security automation and orchestration technologies in C-SOC to automate the incident identification, analysis and response as per the defined procedures.

4.41.8.5 Further to the above, the C-SOC of MII shall, at the minimum, undertake the following activities:

4.41.8.5.1 In order to detect intrusions / security incidents in real time, the C-SOC should monitor and analyze on a 24x7x365 basis relevant logs of MII's network devices, logs of MII's systems, data traffic, suitable cyber intelligence (intel) feeds sourced from reliable vendors, inputs received from other MIIs, inputs received from external agencies such as CERT-In, etc. The cyber intelligence (intel) feeds may include cyber news feeds, signature updates, incident reports, threat briefs, and vulnerability alerts.

4.41.8.5.2 To this end, appropriate alert mechanisms should be implemented including a comprehensive dashboard, tracking of key security metrics and provide for cyber threat scorecards.

4.41.8.5.3 The C-SOC should conduct continuous assessment of the threat landscape faced by the MII including undertaking periodic VAPT (Vulnerability Assessment and Penetration Testing).

4.41.8.5.4 The C-SOC should have the ability to perform Root Cause Analysis, Incident Investigation, Forensic Analysis, Malware Reverse

Engineering, etc. to determine the nature of the attack and corrective and/or preventive actions to be taken thereof.

4.41.8.5.5 The C-SOC should conduct periodic (at the minimum quarterly) cyber-attack simulation to aid in developing cyber resiliency measures. The C-SOC should develop and document mechanisms and standard operating procedures to recover from the cyber-attacks within the stipulated RTO of the MII. The C-SOC should also document various scenarios and standard operating procedures for resuming operations from Disaster Recovery (DR) site of MII.

4.41.8.5.6 The C-SOC should conduct periodic awareness and training programs at the MII and for its members / participants / intermediaries with regard to cyber security, situational awareness and social engineering.

4.41.8.5.7 The C-SOC should be capable to prevent attacks similar to those already faced. The C-SOC should also deploy multiple honey pot services which are dynamic in characteristics to avoid being detected as honey pot by attackers.

4.41.8.6 As building an effective C-SOC requires appropriate mix of right people, suitable security products (Technology), and well-defined processes and procedures (Processes), an indicative list of areas that MIIs should consider while designing and implementing a C-SOC are as follows:

4.41.8.6.1 The MII shall ensure that the governance and reporting structure of the C-SOC is commensurate with the risk and threat landscape of the MII. The C-SOC shall be headed by the Chief Information Security Officer (CISO) of the MII. The CISO shall be designated as a Key Managerial Personnel (KMP) and relevant provisions relating to KMPs in the Securities Contracts (Regulation) (Stock Exchanges and Clearing Corporations) Regulations, 2018 and the subsequent circulars issued by SEBI relating to KMPs, shall apply to the CISO.

4.41.8.6.2 While the CISO is expected to work closely with various departments of MIIs, including MII's Network team, Cyber Security team and Information Technology (IT) team, etc., the reporting of CISO shall be directly to the MD & CEO of the MII.

4.41.8.6.3 The roles and responsibilities of CISO may be drawn from Ministry of Electronics and IT Notification No. 6(12)/2017-PDP-CERT-In dated March 14, 2017.

4.41.8.6.4 The C-SOC should deploy appropriate technology tools of adequate capacity to cater to its requirements. Such tools shall, at the

minimum, include Security Analytics Engine, Malware detection tools, Network and User Traffic Monitoring and Behaviour Analysis systems, Predictive Threat Modelling tools, Tools for monitoring of System parameters for critical systems / servers, Deep Packet Inspection tools, Forensic Analysis tools, etc.

4.41.8.6.5 Each MII is advised to formulate a Cyber Crisis Management Plan (CCMP) based on its architecture deployed, threats faced and nature of operations. The CCMP should define the various cyber events, incidents and crisis faced by the MII, the extant cyber threat landscape, the cyber resilience envisaged, incident prevention, cyber crisis recognition, mitigation and management plan. The CCMP should be approved by the respective Standing Committee on Technology / IT- Strategy Committee of the MIIs and the governing board of the MII. The CCMP should also be reviewed and updated annually.

4.41.8.6.6 The C-SOC should have well-defined and documented processes for monitoring of its systems and networks, analysis of cyber security threats and potential intrusions / security incidents, usage of appropriate technology tools deployed by C-SOC, classification of threats and attacks, escalation hierarchy of incidents, response to threats and breaches, and reporting (internal and external) of the incidents.

4.41.8.6.7 The C-SOC should employ domain experts in the field of cyber security and resilience, network security, data security, end-point security, etc.

4.41.8.6.8 The MIIs are also advised to build a contingent C-SOC at their respective DR sites with identical capabilities w.r.t. the primary C-SOC in line with **Para 4.31**. Additionally, the MIIs should perform monthly live-operations from their DR-C-SOC.

4.41.8.6.9 The C-SOC should document the cases and escalation matrices for declaring a disaster.

4.41.8.7 In view of the feedback received from MIIs, it has been decided that MIIs may choose any of the following models to set-up their C-SOC:

i. MII's own C-SOC manned primarily by its internal staff,

ii. MII's own C-SOC, staffed by a service provider, but supervised by a full time staff of the MII. (Refer **Para 4.41.8.7.3**)

iii. C-SOC that may be shared by the MII with its group entities (that are also SEBI recognized MIIs),

iv. C-SOC that may be shared by the MII with other SEBI recognized MII(s).

4.41.8.7.1 The responsibility of cyber security of an MII, adherence to business continuity and recovery objectives, etc. should lie with the respective MII, irrespective of the model adopted for C-SOC.

4.41.8.7.2 The respective risk committee(s) of the MII should evaluate the risks of outsourcing the respective activity.

4.41.8.7.3 The MII may outsource C-SOC activities in line with the guidelines as given below:

Level of support definitions for outsourcing/in-house are as follows:

4.41.8.7.3.1 Security Analyst Level 1 (L1): This function may be mostly outsourced

a) Monitoring SIEM Solution console for identifying the security events generated by the log sources integrated with SIEM tools.

b) Identification of security events that are false +ve before qualifying event as an incident.

c) Identify the exceptions which are identified as an event (e.g. VA scanning performed by SEBI appointed 3rd party which may be identified as port scanning attack).

d) Perform first level event analysis before qualifying the incidents.

e) Qualifying the event as an incident using Knowledgebase.

f) Escalating exceptions & Events to L2 level.

g) Log Incident tickets in service management tool and assign it to the respective team.

h) Follow-up for the closure of the incident tickets generated.

4.41.8.7.3.2 Security Analyst Level 2 (L2): Combination of Outsource / In-House

a) Exception Analysis.

b) Analysis of extended events.

c) Confirmation of False +ve & update Knowledge Base.

d) Qualify Incident & provide mitigation suggestions.

e) Escalate incident to next level.

f) Update /configuration correlation rules after approval.

4.41.8.7.3.3 Security Analyst Level 3 (L3): Combination of Outsource / In-House

a) Analysis of escalated Incidents.

b) Define correlation rules.

c) Analysis of impact on SIEM over all correlation rules and operations for the correlation rules suggested by Level 2 Analyst.

d) Approve correlation rules after the impact analysis.

e) Perform impact analysis before deployment of correlation rules.

f) Perform impact analysis for update and upgrade of SIEM & Advance security solutions components.

g) Define Mitigation suggestions for newly identified incidents.

h) Approve the reports before sharing with others.

4.41.8.7.3.4 SOC Manager (L4): In-house

a) Lead and manage Security Operations Centre.

b) Provide strategic directions to SOC team and organization for security posture improvements.

c) To identify key contacts for incident escalation and change management activities.

d) Ensure compliance to SLA.

e) Ensure process adherence and process improvisation to achieve operational objectives.

f) Revise and develop processes to strengthen the current Security Operations.

g) Responsible for team and vendor management.

h) Responsible for overall use of resources and initiation of corrective action where required for Security Operations Center.

i) Escalate to the other IT Infra. Management teams or application maintenance teams, as necessary.

j) Overall responsibility for delivery of in scope activities as a part of this engagement.

k) Point of contact for problem escalation and reporting.

4.41.8.7.3.5 Security Subject Matter Expert for Security technologies: In-house with reliance on external expertise

a) Subject Matter Expert (SME) for SIEM and Advance security solutions.

b) Assist you with troubleshooting steps to be performed by you in order to re-establish connectivity between the SIEM System and SEBI's locations.

c) Provide software-level management for the SIEM System components;

d) Verify data collection and log continuity;

e) Manage user access including user and group permissions updates;

f) Review application performance, capacity, and availability make recommendations as appropriate;

g) Review SIEM System disk space usage;

h) Verify time synchronization among SIEM System components;

i) Perform archival management and retrieval per change management process;

j) Provide problem determination / problem source identification for the SIEM System, consisting of creating tickets & tracking progress of Open tickets

k) Managing tickets to resolution / closure, in accordance with the processes as defined in the Integrated and Transition vendor announcements & manage SIEM System update alerts;

l) Install application patches and software updates in order to improve performance, or enable additional functionality

Illustrative Training Requirements

Security Analyst Level 1 (L1):

1) SEC401: Security Essentials Bootcamp Style https://www.sans.org/event/cyber-defence-canberra-2018/course/security-essentials-bootcamp-style

2) SEC301: Introduction to Cyber Security https://www.sans.org/course/introduction-cyber-security

Security Analyst Level 2 (L2):

1) SEC542: Web App Penetration Testing and Ethical Hacking https://www.sans.org/event/cyber-defence-canberra-2018/course/web-app-penetration-testing-ethical-hacking

2) SEC566: Implementing and Auditing the Critical Security Controls -In-Depth https://www.sans.org/private-training/course/implementing-auditing-critical-security-controls

3) SEC575: Mobile Device Security and Ethical Hacking https://www.sans.org/private-training/course/mobile-device-security-ethical-hacking

Security Analyst Level 3 (L3):

1) SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling https://www.sans.org/event/cyber-defence-canberra-2018/course/hacker-techniques-exploits-incident-handling

2) FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting https://www.sans.org/event/digital-forensics-summit-2018/course/advanced-incident-response-threat-hunting-training

3) SEC501: Advanced Security Essentials -Enterprise Defender https://www.sans.org/private-training/course/advanced-security-essentials-enterprise-defender

4) MGT414: SANS Training Program for CISSP® Certification https://www.sans.org/course/sans-plus-s-training-program-cissp-certification-exam

SOC Manager (L4):

1) Cyber Security Specialist http://www.leaderquestonline.com/it-career-training/cybersecurity-specialist/

2) Managing Security Operations: Detection, Response, and Intelligence https://www.sans.org/event/rocky-mountain-2018/course/managing-security-operations-detection-response-and-intelligence

3) SIEM with Tactical Analytics https://www.sans.org/private-training/course/siem-with-tactical-analytics

4) SEC511: Continuous Monitoring and Security Operations https://www.sans.org/course/continuous-monitoring-security-operations

5) SEC599: Defeating Advanced Adversaries -Implementing Kill Chain Defenses https://www.sans.org/course/defeating-advanced-adversaries-kill-chain-defenses

4.41.8.8 A report on the functioning of the C-SOC, including details of cyber-attacks faced by the MII, major cyber events warded off by the MII, cyber security breaches, data breaches should be placed on a quarterly basis before the board of the MII.

4.41.8.9 The system auditor of the MII shall audit the implementation of the aforesaid guidance in the annual system audit of the MII. The Scope and/or Terms of Reference (ToR) of the annual system would accordingly be modified to include audit of the implementation of the aforementioned areas.

4.41.8.10 Further, in continuation to the requirement specified at **Para 4.41.7.52**, the C-SOC shall share relevant alerts and attack information with members / participants / intermediaries of the MII, other MIIs, external cyber response agencies such as CERT-In, and SEBI.

4.41.8.11 Guidelines for MIIs regarding Cyber security and Cyber resilience[203]

4.41.8.11.1 Market Infrastructure Institutions (i.e. Stock Exchanges, Clearing Corporations and Depositories) are systemically important institutions as they, inter-alia, provide infrastructure necessary for the smooth and uninterrupted functioning of the securities market. As part of the operational risk management, these Market Infrastructure Institutions (MIIs) need to have robust cyber security framework to provide essential

[203] Reference: SEBI Circular SEBI/HO/MRD/TPD/P/CIR/2023/146 dated August 29, 2023

facilities and perform systemically critical functions relating to trading, clearing and settlement in securities market. It is also important that MIIs establish and continuously improve their Information Technology (IT) processes and controls to preserve confidentiality, integrity and availability of data and IT systems.

4.41.8.11.2 Market Infrastructure Institutions (i.e. Stock Exchanges, Clearing Corporations and Depositories) are systemically important institutions as they, inter-alia, provide infrastructure necessary for the smooth and uninterrupted functioning of the securities market. As part of the operational risk management, these Market Infrastructure Institutions (MIIs) need to have robust cyber security framework to provide essential facilities and perform systemically critical functions relating to trading, clearing and settlement in securities market. It is also important that MIIs establish and continuously improve their Information Technology(IT) processes and controls to preserve confidentiality, integrity and availability of data and IT systems.

4.41.8.11.3 With the change in market dynamics in the Indian Securities markets, the interdependence among the MIIs has seen significant increase. Considering the interconnectedness and interdependency of the MIIs to carry out their functions, the cyber risk of any MII is no longer limited to the MII's owned or controlled systems, networks and assets.

4.41.8.11.4 In view of the same, the guidelines for strengthening the existing cyber security and cyber resilience framework for depositories is placed under **Para 4.41.8.12** and the MIIs are required to comply with the same.

4.41.8.11.5 These guidelines should be read in conjunction with the applicable SEBI circulars (including but not limited to that relating to Cybersecurity and Cyber Resilience framework, System and Network Audit framework, etc.) and subsequent updates issued by SEBI from time to time.

4.41.8.11.6 The compliance of the guidelines shall be provided by the MII along with their cybersecurity audit report (conducted as per the applicable SEBI Cybersecurity and Cyber Resilience framework). The compliance shall be submitted as per the existing reporting mechanism.

4.41.8.12 Depositories are required to implement the following practices:-

4.41.8.12.1 Depositories shall maintain offline, encrypted backups of data and shall regularly test these backups at least on a quarterly basis to ensure confidentiality, integrity and availability

4.41.8.12.2 Depositories shall maintain regularly updated "gold images" of critical systems in the event they need to be rebuilt. This entails

maintaining image "templates" that include a preconfigured operating system (OS) and associated software applications that can be quickly deployed to rebuild a system, such as a virtual machine or server.

4.41.8.12.3 Depositories should explore the possibility of retaining spare hardware in an isolated environment to rebuild systems in the event starting depositories operations from both Primary Data Centre (PDC) and Disaster Recovery Site (DRS) are not feasible. The Depositories should also try to keep spare hardware in ready to use state for delivering critical services and such systems shall be updated as and when new changes (for example OS patches, security patches) are implemented in the primary systems. This spare hardware should regularly undergo testing in line with response and recovery plan of the depositories.

4.41.8.12.4 Depositories should undertake regular business continuity drills to check the readiness of the organization and effectiveness of existing security controls at the ground level to deal with the ransomware attacks. One such drill scenario recommended to be tested is recovering from ransomware attack considering both PDC and DRS have been impacted. This would assess the effectiveness of people, process and technologies to deal with such attacks.

4.41.8.12.5 Depositories should conduct regular vulnerability scanning to identify and address vulnerabilities, especially those on internet-facing devices, to limit the attack surface.

4.41.8.12.6 Depositories should patch and update software and OSs to the latest available versions and it must be reviewed on a quarterly basis to ensure the implementation of the same.

4.41.8.12.7 Depositories should implement a cybersecurity user awareness and training program that includes guidance on how to identify and report suspicious activity (e.g. phishing) or incidents.

4.41.8.12.8 Depositories should implement filters at the email gateway to filter out emails with known malicious indicators, such as known malicious subject lines, and block suspicious Internet Protocol (IP) addresses, malicious domains/URLs at the firewall.

4.41.8.12.9 Depositories should ensure Endpoint Detection and Response (EDR)/ Endpoint Protection Platform (EPP), antivirus and anti-malware software and signatures are up to date on all IT systems.

4.41.8.12.10 Depositories should use application directory whitelisting on all assets to ensure that only authorized software is run and all unauthorized software is blocked from installations/executing.

4.41.8.12.11 Depositories should employ Multi Factor Authentication (MFA) for all services.

4.41.8.12.12 Depositories should apply the principle of least privilege to all the systems and services so that users have the access to the jobs they need to perform along with solutions like Privileged Identity Management (PIM)/ Privileged Access Management (PAM) in place.

4.41.8.12.13 Depositories should put in place configuration management database approach to.-

4.41.8.12.14 Understand and inventorise their IT assets, both logical (e.g., data, software) and physical (e.g., hardware).

4.41.8.12.15 Understand which data or systems are most critical for providing critical services, as well as any associated interdependencies (i.e., "critical asset or system list").

4.41.8.12.16 Depositories shall regularly review the Active Directory (AD) to locate and close existing backdoors such as compromised service accounts, which often have administrative privileges and are a potential target for attackers.

4.41.8.12.17 Secure domain controllers (DCs)- Threat actors often target and use DCs as a staging point to spread ransomware network-wide.

a) Depositories should ensure that DCs are patched as and when patch is released and it must be reviewed on a quarterly basis to ensure the implementation of the same.

b) Depositories should ensure that no unnecessary software is installed on DCs, as these can be leveraged to run arbitrary code on the system.

c) Depositories should ensure that access to DCs should be restricted to the Administrators group- Users within this group should be limited and have separate accounts used for day-to-day operations with non-administrative permissions.

d) Depositories should ensure that DC host firewalls are configured to prevent direct internet access.

e) Depositories shall undertake the penetration testing activity (internal and external) for known Active Directory Domain Controller abuse attacks. Weaknesses shall be remediated on topmost priority.

4.41.8.12.18 Delegated access and unused tokens should be reviewed and cleaned at least on quarterly basis.

4.41.8.12.19 Depositories should retain and adequately secure logs for security devices, applications, databases, operating systems, servers, public facing servers hosted on clouds, end points and network devices etc., with full verbosity.

4.41.8.12.20 Network devices of Depositories should also be configured in line with whitelist approach including IPs, ports and services for inbound and outbound communication with proper Access Control List (ACL) implementation.

4.41.8.12.21 Depositories should build effective network segregation for containing cyber incidents and minimizing disruption to business operations.

4.41.8.12.22 Depositories should ensure secure usage of RDP (Remote Desktop Protocol) in IT systems. Further, it must be implemented on need to use basis only and it must employ MFA (Multi Factor Authentication) service. Remote access, if necessary, should be given to authorised personnel from whitelisted IP for predefined time period only with a provision to log all activities.

4.41.8.12.23 Connecting to Depositories via Application Programming Interface(API) should be strictly on whitelisting approach. Depositories should have API security solution in place for securing services and data transferred through APIs.

4.41.8.12.24 Depositories should implement Domain name system (DNS) filtering services to ensure clean DNS traffic is allowed in the environment. Domain name system security extensions (DNS-Sec) for secure communication shall be used.

4.41.8.12.25 Management of the critical servers / applications / services / network elements should only be restricted through enterprise identified intranet systems.

4.41.8.12.26 Depositories should have system(s) in place to manage and incorporate IOCs /malware alert/vulnerability-alert (received from CERT-in or NCIIPC or any linked MII or any other government agency) in their systems.

4.41.8.12.27 Depositories shall devise standard operating procedure (SoP) to implement the advisories issued by CERT-In, NCIIPC or any other government agency in their IT environment within defined timeframe and the said SoP shall be shared with SEBI.

4.41.8.12.28 Depository's response and recovery plan should be subjected to review and testing. Tests should address an appropriate broad scope of scenarios including simulation of extreme but plausible cyber-attacks. Tests should be designed to challenge the assumptions of response, resumption and recovery practices, including governance arrangements and communication plans. These tests must include the critical service provider, vendors and linked MIIs.

4.41.8.12.29 Depositories should explore the possibility of running the systems on dissimilar/different application architecture in order to ensure the high availability in the event of disaster.

4.41.8.12.30 Depositories should engage Dark Web monitoring services to check for any brand abuse, data/ credential leak etc.

4.42 Recommendations of high powered steering Committee[204]

4.42.1 **High Powered Steering Committee**: Cyber Security (Committee) in its meeting dated February 21, 2019 has recommended the following actions to be undertaken by all MIIs in the context of their information technology infrastructure:

4.42.1.1 No applications should be introduced in the production environment without adequate testing. Certificates on testing of software should be mandatorily provided.

4.42.1.2 MIIs formulate its own system specific SOPs to implement SEBI guidelines. Further, MIIs should prepare and maintain a control document elaborating the implementation and methodology of the SOPs.

4.42.2 With regards to comprehensive review of cyber security at MIIs, the committee recommended that:

4.42.2.1 The review should have same time frame across all MIIs. The time frame of the review should be from April to September and October to March of the specific financial year. Organizations with review time frame not in sync with the prescribed time frame should make necessary changes.

4.42.2.2 The audit report to include time required for implementation of observation and business impact of the observations.

4.42.2.3 The audit report should mention all the control areas prescribed in the scope of audit

4.42.2.4 The audit process and submission of report should strictly follow the time lines provided in **Para 4.82**.

4.42.3 MIIs are advised to implement the same.

[204] Reference: SEBI Letter SEBI/HO/MRD/CSC/OW/P/2019/10055 dated April 22, 2019

4.43 Database for Distinctive Number (DN) of Shares[205]

4.43.1 Share capital reconciliation of the entire issued capital of the company by the issuer or its agent is a mandatory requirement under Regulation 75 of the DP Regulations.

4.43.2 In order to ensure centralised record of all securities, including both physical and dematerialised shares, issued by the company and its reconciliation thereof, the Depositories are advised to create and maintain a database of distinctive numbers (DN) of equity shares of listed companies with details of DN in respect of all physical shares and overall DN range for dematerialised shares.

4.43.3 The DN database shall make available, information in respect of issued capital, such as DN Range, number of equity shares issued, name of stock exchange where the shares are listed, date of in-principle listing / final trading approval / dealing permission, shares held in physical or demat form, date of allotment, shares dematerialized under temporary (frozen) ISIN (International Securities Identification Number) or Permanent (active) ISIN etc., at one place.

4.43.4 Based on consultations with the Depositories and Stock Exchanges, the following guidelines are given for the operationalisation of the DN database –

4.43.4.1 **Instructions to the Depositories**

4.43.4.1.1 The depositories shall create and maintain a database to capture DN in respect of all physical equity shares and overall DN range for dematerialised equity shares issued by listed companies.

4.43.4.1.2 The depositories shall provide an interface to the Stock Exchange, Issuers/RTAs for online updation and to the DPs for online enquiry.

4.43.4.1.3 The database shall include the following information -

i. Distinctive Numbers (From)	vii. Trading start date
ii. Distinctive Numbers (To)	viii. Physical/demat
iii. Number of Equity shares	ix. Date of allotment and date of issue (date of credit to BO account)
iv. Name of stock exchange	x. ISIN along with name of company
v. Date of in-principle listing approval	xi. Nature of ISIN [Temporary (Frozen) or Permanent (Active)]
vi. Date of final trading approval/dealing permission	

[205] Reference: SEBI Circular CIR/MRD/DP/10/2015 dated June 05, 2015

4.43.4.1.4 The depositories shall ensure that the database maintained by them is continuously updated and synchronised. The initial synchronisation may be in batch mode and shall thereafter shift to online mode.

4.43.4.1.5 The Depositories, in co-ordination with the Stock Exchanges, having nationwide trading terminals and the Issuers/RTAs, shall facilitate the process of populating the database with details of equity share capital and the corresponding DN information.

4.43.4.2 **Instructions to the Stock Exchanges**

4.43.4.2.1 The Stock Exchanges shall provide the following information of all companies listed on the concerned Stock Exchange-

i. Total number of equity shares (A) for which final trading approval / dealing permission has been granted.

ii. Total number of equity shares (B) for which in-principle listing approval has been granted but final trading approval / dealing permission is pending.

iii. Total number of equity shares comprising the paid-up capital i.e. (A+B).

4.43.4.2.2 The Stock Exchanges shall use the interface provided by the Depositories for the following -

i. In respect of further issue of shares by listed companies, consequent to update of DN information by Issuers/RTAs, the stock exchange shall validate the DN information updated by the Issuer/RTA and update the date of 'in-principle' listing approval, date of final trading approval / dealing permission and trading start date, immediately upon granting of such permissions.

ii. In respect of companies coming out with initial public offer or new listings on stock exchanges, the stock exchange shall update the DN database with the total number of equity shares for which final trading approval / dealing permission has been granted.

iii. In respect of companies whose capital is changed/altered for any reason other than further issuance of shares such as buy-back of shares, forfeiture of shares, capital reduction, etc., the stock exchange shall confirm such change/alteration in the capital as updated by the Issuer/RTA in the DN database.

4.43.4.2.3 In case the DN data on listed shares as per the records of Issuers/RTAs does not match with records of the Stock Exchanges, the Stock Exchanges shall coordinate with the Issuer/RTA to reconcile such differences.

4.43.4.3 **Instructions to the Issuers/RTAs**

4.43.4.3.1 Issuers/RTAs shall use the interface provided by the Depositories for the following -

i. To update DN information in respect of all physical share capital and overall DN range for dematerialised share capital for all listed companies.

ii. Updating the fields (i)-(iv), (viii) and (ix) given in **Para 4.43.4.1.3**, on a continuous basis for subsequent changes including changes in case of further issue, fresh issuance / new listing and other change / alteration in capital (such as buy-back of shares, forfeiture of shares, capital reduction, etc.).

iii. Capturing / updating the DN information on a continuous basis while processing, dematerialisation / rematerialisation requests confirmation, executing corporate action, etc.

4.43.4.3.2 Issuers/RTAs shall take all necessary steps to update the DN database. If there is mismatch in the DN information with the data provided/updated by the Stock Exchanges in the DN database, the Issuer/RTA shall take steps to match the records and update the same.

4.43.4.3.3 Failure by the Issuers/RTAs to ensure reconciliation of the records as required in terms of para above shall attract appropriate actions under the extant laws.

4.43.4.4 **Instructions to the DPs**

4.43.4.4.1 The DPs shall use the interface provided by the Depositories to check the DNs of certificates of equity shares submitted for dematerialisation and ensure that appropriate ISIN is filled in Dematerialisation Request Form, as applicable, while processing request for dematerialisation.

4.43.5 Despite follow-ups by Depositories, certain companies were yet to comply with the above provisions. Hence, in order to protect the interest of investors the following is directed[206]:-

4.43.5.1 **Action against non-compliant companies**

4.43.5.1.1 With effect from August 01, 2019:-

i. The depositories shall freeze all the securities held by the promoters and directors of the listed companies that are not in compliance with the above provisions.

ii. The depositories shall not effect any transfer, by way of sale, pledge, etc., of any of the securities, held by the promoters and directors of such non-compliant companies.

iii. The depositories shall freeze all related corporate benefits on the Beneficiary Owner a/c frozen as above.

[206] Reference: SEBI Circular SEBI/HO/MRD/DOP2DSA2/CIR/P/2019/87 dated August 01, 2019

iv. The depositories shall retain the freeze on the securities held by promoters and directors of non-compliant companies till such time the company complies with the directions provided above (**Para 4.43.1 to Para 4.43.4**). Depositories are advised to keep in abeyance the action mentioned above in specific cases where moratorium on enforcement proceedings has been provided for under any Act, Court/ Tribunal Orders, etc.

4.43.5.1.2 The names of companies that are not in compliance with aforementioned provisions shall be prominently disseminated on the website of the exchanges/depositories, indicating that the concerned companies have not complied with the above provisions.

4.43.5.1.3 Prior to revocation of suspension of trading of shares of any company, exchanges shall ensure compliance by the company with the above provisions and ensure availability of updated details of company's promoters (especially their PAN) and directors (especially their PAN and DIN), apart from ensuring compliance with other applicable regulatory norms.

4.43.5.2 The concerned Stock Exchanges and Depositories shall coordinate with each other and take necessary steps to implement these provisions.

4.43.5.3 SEBI may also take any other appropriate action(s) against the concerned listed companies and its promoters/directors for non-compliance with the above provisions.

4.44 Ticker on Website - For Investor awareness[207]

4.44.1 In order to create wider awareness about the same, Depositories and Depository Participants are advised to run the following ticker on their websites:

"No need to issue cheques by investors while subscribing to IPO. Just write the bank account number and sign in the application form to authorise your bank to make payment in case of allotment. No worries for refund as the money remains in investor's account."

4.44.2 Depositories are advised to communicate the above to their depository participants and ensure its implementation.

4.45 Separate mobile number/ email id for the clients of Depository Participants (DPs)[208]

4.45.1 It has been observed that DPs do not have the procedure to check that separate mobile number/ email id is uploaded for each client.

[207] Reference: SEBI Email on "Ticker on Website - For Investor awareness" dated November 05, 2015

[208] Reference: SEBI Email on Separate mobile number/ email id for the clients of Depository Participants (DPs) dated January 16, 2015.

4.45.2 In view of the same, Depositories are advised to instruct their participants to ensure that separate mobile number/E-mail address is uploaded for each client. However, under exceptional circumstances, the participants may, at the specific written request of a client, upload the same mobile number/E-mail address for more than one client provided such clients belong to one family.

'Family' for this purpose would mean self, spouse, dependent children and dependent parents.

4.46 Comprehensive guidelines for Investor Protection Fund (IPF) and Investor Services Fund (ISF) at Stock Exchanges and Depositories[209]

4.46.1 The comprehensive guidelines for IPF are as under:

4.46.1.1 **Investor Protection Fund**

A. Constitution and Management of the IPF

i. All depositories shall establish an IPF. The IPF of the depository shall be administered through separate trusts created for the purpose.

ii. The IPF Trust of depository shall consist of five trustees as under:

a) Three Public Interest Directors (PIDs);

b) One representative from the investor associations recognized by SEBI; and

c) Chief Regulatory Officer or Compliance Officer.

iii. The maximum tenure of a trustee (excluding the Chief Regulatory Officer or Compliance Officer, whose trusteeship would be co-terminus with their service) shall be five years or as specified by SEBI.

iv. The depository shall provide the secretariat for their IPF Trusts respectively.

v. The depository shall ensure that the funds in the IPF are well segregated and that their IPF is immune from any liabilities of the depository. Further, supervision of utilization of IPF and interest or income from IPF will rest with the IPF Trust.

B. Contribution to IPF of Depository

i. The following contributions shall be made by the Depository to the IPF:

a. 5% of their profits from depository operations every year.

b. All fines and penalties recovered from Depository Participants (DPs) and other users including clearing member pool account penalty as specified in SEBI circular no. SMDRP/Policy/Cir-05/2001 dated February 01, 2001.

c. Interest or income received out of any investments made from the IPF.

[209] Reference: SEBI Circular SEBI/HO/MRD/MRD-PoD-3/P/CIR/2023/81 dated May 30, 2023 (superceded SEBI Circular SEBI/HO/MRD/DP/CIR/P/2016/58 dated June 07, 2016)

d. Funds lying to the credit of IPR (Investor Protection Reserve) / BOPF (Beneficial Owners Protection Fund) of the Depository or any other such fund / reserve of the Depository shall be transferred to IPF.

e. Any other contribution as may be specified by SEBI from time to time.

C. Utilization of IPF and interest or income from IPF

i. The amount in IPF and any interest or income generated from the IPF of the depositories shall be utilized for the purposes as stated in the table below:

SN	Particulars	Utilization
1	IPF	a) Promotion of investor education and investor awareness programmes through seminars, lectures, workshops, publications (print and electronic media), training programmes, etc. aimed at enhancing securities market literacy and promoting retail participation in securities market; b) To utilize the fund for supporting initiatives of DPs for promotion of investor education and investor awareness programmes; c) To meet the legitimate claims of the beneficial owners, upto the maximum cap as to be determined by the depository, in case the same is not settled by the beneficial owner indemnity insurance; d) To utilize the fund in any other manner as may be prescribed or permitted by SEBI in the interest of investors;
2	Interest or income received out of any investments made from the IPF	To further strengthen the corpus, 100% of interest or income from IPF shall be treated as corpus of IPF.

D. Deployment of Funds of IPF Depositories

i. Funds of the IPF Trust shall be invested in instruments such as Central Government securities, fixed deposits of scheduled banks and any such instruments which are allowed as per the investment policy approved by the governing boards of depository. The investments shall be adequately

diversified with single issuer exposure, excluding Government securities, not exceeding 10% of the IPF corpus. The investment policy shall be devised with an objective of capital protection, portfolio diversification, liquidity, along with highest degree of safety and least market risk.

ii. The balance available in the IPF as at the end of each month and the amount utilised during the month including the manner of utilization shall be reported to SEBI in the Monthly Development Reports of the depository.

E. <u>Review of IPF Corpus</u>

i. The depositories shall conduct half-yearly review (by end of March and September every year) to ascertain the adequacy of the IPF corpus. In case the IPF corpus is found to be inadequate, the same shall be enhanced appropriately.

F. <u>Disclosures</u>

i. The depositories are advised to

a) Disclose the corpus of the IPF on its website and update the same on a monthly basis.

b) Disseminate its policy on processing investor claims from IPF on their website including the compensation limit fixed by them per investor.

c) To frame FAQs on their policy on processing investor claims for easy understanding of investors.

d) Give adequate notice (including a press release) to the investors before implementing any amendment in the policy on processing of claims. In case of any amendment in the policy on processing of investor claims, the same should not be applicable to the TMs who have been disabled or suspended or declared defaulter by the exchange prior to the effective date of implementation of policy.

4.46.1.2 <u>Miscellaneous</u>

If a depository is wound up or derecognized or exits, then the balance in the IPF and/or ISF lying un-utilised with depository shall be transferred to Investor Protection and Education Fund of SEBI in terms of SEBI (Investor Protection and Education Fund) Regulations, 2009. The funds shall be utilised for purposes of Investor education

4.47 <u>Enhanced Supervision of Depository Participant</u>[210]

[210] Reference: SEBI Circular SEBI/HO/MIRSD/MIRSD2/CIR/P/2016/95 dated September 26, 2016, SEBI Circular CIR/HO/MIRSD/MIRSD2/CIR/P/2017/64 dated June 22,2017 & SEBI Circular SEBI/HO/MIRSD/ MIRSD_DPIEA/P/CIR/2022/83 dated June 20, 2022

Kindly refer para titled 'Enhanced Supervision of Stock Brokers / Depository Participants' of SEBI Circular SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2023/71 dated May 17, 2023 (Master circular for Stock Brokers)

4.48 Amendment pursuant to comprehensive review of Investor Grievance Redressal Mechanism[211]

The respective provisions dealing with mediation, conciliation and have been superseded with the introduction of Online Dispute Resolution (ODR) Mechanism.

Kindly refer SEBI Circular SEBI/HO/OIAE/OIAE_IAD-1/P/CIR/2023/145 dated July 31, 2023 (Master circular for Online Resolution of Disputes in the Indian Securities Market)

4.49 Investor Grievance Redressal Mechanism[212]

Online Web Based Complaints Redressal System:

4.49.1 SEBI has implemented an online platform (SCORES) designed to help investors to lodge their complaints, pertaining to securities market, against listed companies and SEBI registered intermediaries.

4.49.2 In line with the same, to enable investors to lodge and follow up their complaints and track the status of redressal of such complaints from anywhere, all Depositories are advised to design and implement an online web based complaints redressal system of their own, which will facilitate investors to file complaints and escalate complaints for redressal in accordance with their respective byelaws, rules and regulations.

4.49.3 The system should be web enabled and provide online access 24 x 7 with the following salient features:

4.49.3.1 Complaints/Grievance Redressal Committee (GRC)* and reminders thereon are lodged online at anytime from anywhere;

4.49.3.2 An email is generated instantaneously acknowledging the receipt of the complaint and allotting a unique registration number for future reference and tracking;

4.49.3.3 The matter/case moves online to the entity (intermediary or listed company) concerned for its redressal;

4.49.3.4 The entity concerned can indicate the mode i.e. online or offline for GRC*

[211] Reference: SEBI Circular SEBI/HO/DMS/ CIR/P/2017/15 dated February 23, 2017, SEBI Circular SEBI/HO/MRD1/ICC1/CIR/P/2021/625 dated September 02, 2021 and SEBI Circular SEBI/HO/MRD1/ICC1/CIR/P/2022/94 dated July 04, 2022

[212] Reference: SEBI Circular SEBI/HO/MRD1/ICC1/CIR/P/2022/94 dated July 04, 2022 and (Amended vide SEBI Circular SEBI/HO/OIAE/OIAE_IAD-1/P/CIR/2023/145 dated July 31, 2023)

4.49.3.5 The access of the online system should be given to the Trading Members and Depository Participants.

4.49.3.6 The entity concerned uploads an Action Taken Report (ATR) on the Complaints/GRC*;

4.49.3.7 All Depositories peruse the ATR and dispose of the Complaints/GRC if it is satisfied that the complaint has been redressed adequately;

4.49.3.8 The concerned investor can view the status of the complaint online;

4.49.3.9 The entity concerned and the concerned investor can seek and provide clarification(s) online to each other;

4.49.3.10 The life cycle of a Complaints/GRC* has an audit trail; and

4.49.3.11 All the Complaints/GRC* are saved in a central database which would generate relevant MIS reports to enable all Depositories to take appropriate policy decisions and or remedial actions.

4.49.3.12 There should be a provision to link the online system with SCORES.

4.49.4 The system is intended to expedite redressal / disposal of investors' complaints as it would also obviate the need for physical movement of complaints. Further, the possibility of loss, damage or misdirection of the physical complaints would be avoided. It would also facilitate easy retrieval and tracking of complaints at any time.

4.49.5 All Depositories are advised to widely publicise (including in media) its online web based complaints redressal system.

Hybrid Mode of Conducting GRC*:

4.49.6 During the COVID pandemic, Stock Exchanges were advised to conduct GRC* and arbitration / appellate arbitration meetings/hearings online for faster redressal of complaints. The online process saves time and cost of the parties involved which is in the interest of investors.

4.49.7 Therefore, it has been decided that the depositories shall follow the hybrid mode (i.e. online and offline) of conducting GRC*.

(The provisions dealing with mediation, conciliation and arbitration have been superseded with the introduction of Online Dispute Resolution (ODR) Mechanism. Kindly refer SEBI Circular SEBI/HO/OIAE/OIAE_IAD-1/P/CIR/2023/145 dated July 31, 2023 (Master circular for Online Resolution of Disputes in the Indian Securities Market)

***Grievance redressal committee (GRC) has been abolished by the SEBI (Depositories and Participants) (Amendment) Regulations, 2023, w.e.f. 28-08-2023**

4.50 Digital Mode of Payment[213]

[213] Reference: SEBI Circular SEBI/HO/GSD/T&A/CIR/P/2017/42 dated May 16, 2017

4.50.1 SEBI has notified the SEBI (Payment of Fees and Mode of Payment) (Amendment) Regulations, 2017 on March 06, 2017 to enable digital mode of payment (RTGS/NEFT/IMPS, etc.) of fees/penalties/remittance/other payments etc.

4.50.2 Pursuant to above, SEBI has been receiving direct credit of amounts from various intermediaries / other entities.

4.50.3 In order to identify and account such direct credit in the SEBI account, intermediaries/other entities shall provide the information as mentioned in **Annexure 26** to SEBI once the payment is made.

4.50.4 The above information should be emailed to the respective department(s)as well as to Treasury &Accounts division at tad@sebi.gov.in

4.51 Framework for Innovation Sandbox[214]

4.51.1 Capital market in India have been early adopters of technology. SEBI believes that encouraging adoption and usage of financial technology ('FinTech') would have a profound impact on the development of securities market. FinTech can act as a catalyst to further develop and maintain an efficient, fair and transparent securities market ecosystem.

4.51.2 To create an ecosystem which promotes innovation in the securities market, SEBI feels that FinTech firms should have access to market related data, particularly, trading and holding data, which is otherwise not readily available to them, to enable them to test their innovations effectively before the introduction of such innovations in a live environment.

4.51.3 The "Innovation Sandbox", would be a testing environment where FinTech firms and entities not regulated by SEBI including individuals (herein afterwards referred to as participants/ applicants) may use the environment for offline testing of their proposed solutions in isolation from the live market, subject to fulfillment of the eligibility criteria, based on market related data made available by Stock Exchanges, Depositories and Qualified Registrar and Share Transfer Agents (QRTAs).

Features and Structure of Innovation Sandbox

4.51.4 The components and structure of the Innovation Sandbox can be broadly classified into design, legal and administrative categories. The method of implementation has been elaborated under the head "Implementation" in **Para 4.51.6 to 4.51.13.**

4.51.4.1 **Design Components**

A. Data Sets

[214] Reference: SEBI Circular SEBI/MRD/CSC/CIR/P/2019/64 dated May 20, 2019

a) One of the most important components of an Innovation Sandbox is access to securities market related data, which will enable participants to test and improve their FinTech solutions.

b) The datasets that will be made available to participants shall be clearly defined and known to market participants. Indicative datasets which may become part of the Innovation Sandbox are as follows:

i. Depositories data: Holding data, KYC data

ii. Stock exchange data: Transactions data like order log, trade log

iii. RTA data: Mutual fund transactions data

c) The datasets shall be historical and anonymized data and shall also contain data related to episodic market events. Live data shall not be made available to participants.

d) Access to datasets shall be provided in a phased manner starting with limited amount of data and based on validations, more exhaustive data would be provided to participants.

e) The use of datasets shall be governed by comprehensive confidentiality agreement which shall include an 'End User Agreement' clearly specifying that the datasets made available shall not be sold or sublet or shared in any manner with any other entities.

B. Infrastructure

a) The datasets to be used for testing solutions in the Innovation Sandbox shall be shared through application program interface (APIs), which will be widely published and available to all eligible participants.

b) Virtual machines may be made available with configurations similar to the live environment for testing an innovative product, service or solution on the datasets.

4.51.4.2 **Legal components**

a) Flexibility

The Innovation Sandbox shall be flexible to adapt and incorporate the changes, once the Innovation Sandbox evolves and matures.

b) Not-for-profit

The Innovation Sandbox can be set up as a separate not-for-profit entity which enhances the impartiality of the Innovation Sandbox.

c) Compliance

The Innovation Sandbox should ensure that all applicants can perform their testing without breaking any regulatory barriers, including compliance with investor protection, Know Your Client norms, data integrity or any other Indian laws.

d) Legally robust

The Innovation Sandbox should clearly define the rights and obligations of the stakeholders. Applicants are required to agree to contractually binding terms of participation.

e) Intellectual Property Rights (IPR) protection

The Innovation Sandbox should have the relevant provisions to protect the applicants' IPR. Also, it should define how the IPR which results from the collaboration can be used once the testing phase has ended.

f) Prevention of Data misuse

The Innovation Sandbox should have provision to restrict misuse of data from the stated purposes.

g) Restriction from Fraudulent purposes

The Innovation Sandbox should have provision for restricting development of any product/ solution for fraudulent/ manipulative purposes.

h) Secured

The Innovation Sandbox should be secured from cyber threats or unauthorized access.

4.51.4.3 **Administrative Components**

a) Application Assessment

Applications received for participating in the Innovation Sandbox will be assessed and rule based self-assessment process shall be formalized, in order to allow the applicants' automatic entry into the Innovation Sandbox.

b) Governance body

A governance body shall be formed comprising of representatives from the Stock Exchanges, Depositories and Qualified Registrar and Share Transfer Agents. This body shall supervise the operations of the Innovation Sandbox in the interests of its contributors, users and securities market in general. The governance body shall be responsible for ensuring that the sandbox fulfils its stated objectives. The governance of the Innovation Sandbox should be neutral and should not favor any particular participant or category of participants.

c) Operational team

An operational team shall be constituted to carry out the day-to-day activities of the Innovation Sandbox including processing applications, communicating with applicants, assisting the governance body, maintaining the infrastructure of the Innovation Sandbox, supervising the testing in Innovation Sandbox etc.

d) Rules of participation

Rules shall be framed to regulate the rights and responsibilities of the participant with respect to an Innovation Sandbox and to other participants. These rules could be same for each applicant type and may include the entry and exit criteria, operating guidelines, reporting requirements etc.

e) Grievance redressal process

A grievance redressal mechanism shall be formulated to deal with the grievances of any applicant in the Innovation Sandbox. This mechanism shall clearly define the point of contact for grievance redressal along with the escalation matrix.

4.51.4.4 **Interface for Innovation Sandbox**

The entire sandbox participation lifecycle (applying, tracking, on-boarding, monitoring, reporting, etc.) shall be completely digital to ensure transparency and efficiency.

Eligibility Criteria

4.51.5 The eligibility criteria for inclusion into the Innovation Sandbox are as follows:

a. **Applicability**

Conceptually, the Innovation Sandbox framework is applicable to any entity, who intends to innovate on the products, services, and/or solutions for the securities and commodities market in India.

b. **Genuine need to test**

The applicant should have a genuine need for testing the solution using resources available in the Innovation Sandbox. The applicant should be able to postulate that the solution cannot be developed properly without testing in the Innovation Sandbox.

c. **Testing readiness of the solution**

The applicant should have the necessary resources to support testing in the sandbox. The applicant must show testing plans with clear objectives, parameters and success criteria.

d. **Post-testing strategy**

The applicant should be able to postulate their post-testing plan.

e. **Direct benefits to consumers**

The solution should offer identifiable benefits (direct or indirect) to consumers and to the capital market and the Indian economy at large.

f. **Secure**

The solution shall be validated for cyber security parameters. The applicant is required to submit a cyber-security compliance certificate as per SEBI's Cyber Security guidelines.

Implementation

4.51.6 A Steering Committee comprising of representatives from the Market Infrastructure Institutions (MIIs) and QRTAs shall develop the operating guidelines as mentioned at **Para 4.51.4.3 (c)** towards the components and structure of the Innovation Sandbox as articulated in the Features, Structure and Eligibility criteria of Innovation Sandbox in **Para 4.51.4 and Para 4.51.5.** The Steering Committee shall also include members drawn from the areas of FinTech start-ups, academia and angel investors or any other area as may be prescribed by SEBI. At the initial stage, SEBI representative shall be a permanent invitee to this Committee.

4.51.7 Post issuance of operating guidelines, the Steering Committee shall carry out all the functions as envisaged in the Administrative Components at **Para 4.51.4** viz. receive, evaluate and process the applications received for participating in the Innovation Sandbox, approve / reject applications so received, grievance redressal etc. The Steering Committee shall also be responsible for registering/onboarding the applicant post approval of the application and monitor the participant throughout the lifecycle of the project.

4.51.8 Each of the MIIs and QRTAs shall build their own interface and APIs. Any approved sandbox applicant can then get access to the APIs of the respective MIIs and QRTAs where the applicant would test its solution

4.51.9 The Sandbox applicant may give a presentation to the Steering Committee upon completion of the testing and exit from the Innovation Sandbox.

4.51.10 The Steering Committee overseeing the testing of the applicant's solution within the sandbox shall maintain an Objective and Key Result Areas (OKRA) document for effective oversight on the entire process.

4.51.11 The entire sandbox participation lifecycle (applying, tracking, on-boarding, monitoring, reporting, etc.) should move towards a complete digital environment within a time-bound manner, not exceeding 24 months, towards ensuring transparency and efficiency.

4.51.12 The Steering Committee, to begin with, shall evolve decisions based on consensus and have a Chairperson from among the group on a rotation basis.

4.51.13 Based on the functioning of the Steering Committee, SEBI would prescribe other norms for governance, as and when required.

Outcome of Innovation Sandbox

4.51.14 SEBI envisages the Innovation Sandbox to have the following benefits:

4.51.14.1 **Product showcase**

A platform for showcasing the working prototype of the solution which may help FinTech firms secure more funding.

4.51.14.2 **Product regulation**

Assessing compliance and readiness with SEBI's regulations.

4.51.14.3 **Industry interoperability**

Providing an environment where developers could explore industry challenges and use cases for innovative technologies linked to interoperability of new solutions across the industry.

4.52 Revised Framework for Innovation Sandbox[215]

Kindly refer SEBI Circular SEBI/HO/ITD/ITD/CIR/P/2021/16/2021 dated February 02, 2021 in respect of Revised Framework for Innovation Sandbox

4.53 Framework for Regulatory Sandbox[216]

Kindly refer SEBI Circular SEBI/HO/MRD-1/CIR/P/2020/95 dated June 05, 2020 and SEBI circular SEBI/HO/ITD/ITD/CIR/P/2021/575 dated June 14, 2021 in respect of Framework & Revised Framework for Regulatory Sandbox respectively.

4.54 Monitoring of Foreign Investment limits in listed Indian companies[217]

4.54.1 As per FEMA, the onus of compliance with the various foreign investment limits rests on the Indian company. In order to facilitate the listed Indian companies to ensure compliance with the various foreign investment limits, SEBI in consultation with RBI has decided to put in place a system for monitoring the foreign investment limits.

4.54.2 For the architecture of the new system, kindly refer para titled 'Monitoring of Investment Limit at individual level' of SEBI Circular SEBI/HO/AFD-2/CIR/P/2022/175 dated December 19, 2022 (Master Circular for Foreign Portfolio Investors, Designated Depository Participants and Eligible Foreign Investors)

4.54.3 The depositories shall put in place the necessary infrastructure and IT systems for operationalizing the monitoring mechanism referred above.

4.55 Disclosure of performance of CRAs on Stock Exchange and Depository website[218]

---

[215] Reference: SEBI Circular SEBI/HO/ITD/ITD/CIR/P/2021/16/2021 dated February 02, 2021

[216] Reference: SEBI Circular SEBI/HO/MRD-1/CIR/P/2020/95 dated June 05, 2020, updated vide SEBI Circular SEBI/HO/ITD/ITD/CIR/P/2021/575 dated June 14, 2021

[217] Reference: SEBI Circular IMD/FPIC/CIR/P/2018/61 dated April 05, 2018

[218] Reference: SEBI Circular SEBI/ HO/ MIRSD/ DOS3/ CIR/ P/ 2018/ 140 dated November 13, 2018

Kindly refer Disclosure of performance of CRAs on Stock Exchange and Depository website of SEBI Circular SEBI/HO/DDHS/DDHS-POD2/P/CIR/2023/111 dated July 03, 2023 (Master Circular for Credit Rating Agencies)

4.56 Handling of Clients' Securities by Trading Members/Clearing Members[219]

Kindly refer Handling of Client's Securities by Trading Members/ Clearing Members of SEBI Circular SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2023/71 dated May 17, 2023 (Master circular for Stock Brokers)

4.57 Early Warning Mechanism to prevent diversion of client securities[220]

Kindly refer para titled 'Early Warning Mechanism to prevent diversion of client securities' of SEBI Circular SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2023/71 dated May 17, 2023 (Master circular for Stock Brokers)

4.58 Standard Operating Procedure in the cases of Trading Member /Clearing Member leading to default[221]

Kindly refer para titled 'Standard operating procedure in the cases of Trading Member / Clearing Member leading to default' of SEBI Circular SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2023/71 dated May 17, 2023 (Master circular for Stock Brokers)

4.59 Mapping of Unique Client Code (UCC) with demat account of the clients[222]

Kindly refer para titled 'Mapping of Unique Client Code(UCC) with demat account of clients' of SEBI Circular SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2023/71 dated May 17, 2023 (Master circular for Stock Brokers)

4.60 Reporting for Artificial Intelligence(AI) and Machine Learning (ML) applications and systems offered and used by Market Infrastructure Institutions (MIIs)[223]

Background

4.60.1 SEBI is conducting a survey and creating an inventory of the AI / ML landscape in the Indian financial markets to gain an in-depth understanding of the adoption of such technologies in the markets and to ensure preparedness for any AI / ML policies that may arise in the future.

Scope definition

---

[219] Reference: SEBI Circular CIR/HO/MIRSD/DOP/CIR/P/2019/75 dated June 20, 2019, SEBI Circular SEBI/HO/MIRSD/DOP/CIR/P/2019/95 dated August 29, 2019 and SEBI Circular SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2022/153 dated November 11, 2022

[220] Reference: SEBI Circular SEBI/HO/MIRSD/DOP/CIR/P/2018/153 dated December 17, 2018

[221] Reference: SEBI Circular SEBI/HO/MIRSD/DPIEA/CIR/P/2020/115 dated July 01, 2020 and SEBI Circular SEBI/HO/MIRSD/DPIEA/P/CIR/2022/72 dated May 27, 2022

[222] Reference: SEBI Circular SEBI/HO/MIRSD/DOP/CIR/P/2019/136 dated November 15, 2019

[223] Reference: SEBI Circular SEBI/HO/MRD/DOP1/CIR/P/2019/24 dated January 31, 2019

4.60.2 Any set of applications / software / programs/ executable / systems (computer systems) cumulatively called application and systems, to carry out compliance operations/activities, where AI/ML is used for compliance or management purposes, is included in the scope of this circular. In order to make the scope inclusive of various AI and ML technologies in use, the scope also covers Fin-Tech and Reg-Tech initiatives undertaken by MIIs that involves AI and ML.

4.60.3 Technologies that are considered to be categorized as AI and ML technologies in the scope of this section, are as follows:

Applications and Systems belonging but not limited to following categories or a combination of these:

4.60.3.1 Natural Language Processing (NLP), sentiment analysis or text mining systems that gather intelligence from unstructured data. – In this case, Voice to text, text to intelligence systems in any natural language will be considered in scope. E.g.: robo chat bots, big data intelligence gathering systems.

4.60.3.2 Neural Networks or a modified form of it. – In this case, any systems that uses a number of nodes (physical or software simulated nodes) mimicking natural neural networks of any scale, so as to carry out learning from previous firing of the nodes will be considered in scope. Eg: Recurrent Neural networks and Deep Learning Neural Networks

4.60.3.3 Machine learning through supervised, unsupervised learning or a combination of both. – In this case, any application or systems that carry out knowledge representation to form a knowledge base of domain, by learning and creating its outputs with real world input data and deciding future outputs based upon the knowledge base. E.g.: System based on Decision tree, random forest, K mean, Markov decision process, Gradient boosting Algorithms.

4.60.3.4 A system that uses statistical heuristics method instead of procedural algorithms or the system / application applies clustering or categorization algorithms to categorize data without a predefined set of categories

4.60.3.5 A system that uses a feedback mechanism to improve its parameters and bases it subsequent execution steps on these parameters.

4.60.3.6 A system that does knowledge representation and maintains a knowledge base.

Regulatory requirements

4.60.4 All MIIs shall fill in the AI / ML reporting form (**Annexure 27**) in respect of the AI or ML based applications or systems as defined in **Para 4.60.3** offered or used

by them, and submit the same in soft copy only at AI_MII_SE@sebi.gov.in(for stock Exchanges)/AI_MII_DEP@sebi.gov.in (for depositories) /AI_MII_CC@sebi.gov.in (for Clearing Corporations) to SEBI on a quarterly basis within 15 days of the expiry of the quarter.

4.61 Measures to expedite Dematerialisation of securities[224]

4.61.1 In order to enable prompt execution of demat requests, Depositories shall provide additional details, such as PAN, Address and Residential status of investors in the DRF itself.

4.61.2 To include a provision in DRF to capture 2 signatures – one registered with DP at the time of demat account opening and the other registered with issuer/RTA at the time of allotment /transfer. The request submitted by BO would be only processed when both two signatures i.e. one registered with RTA and other registered with DP matches with two respective signatures on DRF. In case of mismatch of any of the two signatures the existing process of verifying signature may be followed.

4.61.3 To advise Depository Participants to update bank account details of all demat account holders in their records.

4.62 Capacity Planning Framework for the Depositories[225]

4.62.1 Depositories have been identified as financial Market Infrastructure Institutions which facilitate and perform systemically critical functions in the securities market. In view of their importance in the smooth functioning of the securities market, the framework for capacity planning of the Depositories was also discussed in TAC. Based on recommendations of the committee, it has been decided to put in place following requirements for Depositories while planning capacities for their operations:

4.62.1.1 The installed capacity shall be at least 1.5 times (1.5x) of the projected peak load.

4.62.1.2 The projected peak load shall be calculated for the next 60 days based on the per hour peak load trend of the past 180 days.

4.62.1.3 The Depositories shall ensure that the utilisation of resources in such a manner so as to achieve work completion in 70% of the allocated time.

4.62.1.4 All systems pertaining to Depository operations shall be considered in this process including all technical components such as network, hardware, software, etc., and shall be adequately sized to meet the capacity requirements.

---

[224] Reference: SEBI Letter MRD/DoPII/DSAII/MIRSD/DOS3/OW/2018/28162/1 dated October 22, 2018

[225] Reference: SEBI Circular SEBI/HO/MRD/DP/CIR/P/2017/29 dated April 03, 2017

4.62.1.5 In case the actual capacity utilization exceeds 75% of the installed capacity for a period of 15 days on a rolling basis, immediate action shall be taken to enhance the capacity.

4.62.1.6 The actual capacity utilisation shall be monitored especially during the period of the day in which pay-in and pay-out of securities takes place for meeting settlement obligations.

4.62.2 Depositories shall implement suitable mechanisms, including generation of appropriate alerts, to monitor capacity utilisation on a real-time basis and shall proactively address issues pertaining to their capacity needs.

4.63 Trading Supported by Blocked Amount in Secondary Market[226]

4.63.1 In its continuing endeavour to provide protection to the investors from the default of member(s) ['trading member' (TM) / 'clearing member' (CM)], SEBI has decided to introduce a supplementary process for trading in secondary market based on blocked funds in investor's bank account, instead of transferring them upfront to the trading member, thereby providing enhanced protection of cash collateral. The said facility shall be provided by integrating Reserve Bank of India (RBI) approved Unified Payments Interface (UPI) mandate service of single-block-and-multiple-debits with the secondary market trading and settlement process and hereinafter referred as 'UPI block facility'

4.63.2 Under the proposed framework, funds shall remain in the account of client but will be blocked in favour of the clearing corporation ('CC') till the expiry date of the block mandate or till block is released by the CC, or debit of the block towards obligations arising out of the trading activity of the client, whichever is earlier. Further, settlement for funds and securities will be done by the CC without the need for handling of client funds and securities by the member.

4.63.3 Further, while a UPI block upon creation shall be considered towards collateral, the same shall also be available for settlement purposes. For the clients who prefer to block lump sum amount, their block can be debited multiple times, subject to available balance, for settlement obligations across days.

4.63.4 The main features of the framework are as under:

4.63.4.1 **General features:**

4.63.4.1.1 Availing UPI block facility shall be at the option of the investor.

4.63.4.1.2 Shall be introduced as a non-mandatory facility to be provided by the stock broker.

[226] Reference: SEBI Circular SEBI/HO/MRD/MRD-PoD-2/P/CIR/2023/99 dated June 23, 2023

4.63.4.1.3 Since an investor is allowed to have trading accounts across multiple stock brokers, an investor can choose to avail UPI block facility under some broker(s) and non-UPI based trading under others. However, once opted for UPI block facility (until they opt out after fulfilling all obligations) under particular broker(s), the following needs to be adhered to in respect of UPI block facility under that broker(s):

4.63.4.1.3.1 All cash collaterals shall be provided through UPI block only.

4.63.4.1.3.2 Cash equivalent collateral such as bank guarantees and fixed deposits shall not be permitted.

4.63.4.1.3.3 Securities collateral to be provided through pledge/re-pledge system and only those securities can be provided which are in the approved list of CC.

4.63.4.1.3.4 Funds pay-in settlement to be done through UPI block only.

4.63.4.1.4 Collateral and settlement shall continue to be segment-wise, and the client/TM/CM shall need to transfer/reallocate collateral between segments.

4.63.4.1.5 Running account settlement shall not be supported. CC shall settle the account of clients using UPI block facility on a daily basis, i.e., any pay-out due to the client shall be paid out to the client on the settlement day.

4.63.4.1.6 Single block limit of Rs. 5 lakhs shall apply [currently applicable for UPI based securities market transaction]. However, multiple blocks can co-exist subject to the overall limit applicable in UPI

4.63.4.2 **Eligibility of investors**: All investors who are permitted to use RBI's UPI facility, and meeting the criteria defined by CCs, shall be eligible.

4.63.4.3 **Process (in brief):**

4.63.4.3.1 The stock brokers providing the facility shall notify the details of investors desirous of availing the service to the stock exchange. The stock exchange shall validate the bank and demat account maintained in the Unique Client code ('UCC') systems and used for block creation and settlement. The exchanges shall provide relevant details to the CC.

4.63.4.3.2 The block shall be created by client using the UPI application ('UPI app') based on the blocking request initiated through stock broker app. While creating the blocking request under the proposed block mechanism, relevant information such as TM Code, CM Code, Unique Client Code, segment etc. shall be captured by the stock broker and sent to UPI.

4.63.4.3.3 The UPI block shall get created in favour of the CC and can be debited by the CC only.

4.63.4.3.4 The block shall support multiple debits – i.e., for a block created on day 1, it can be partially debited multiple times till the exhaustion of amount or expiry/release of the block, whichever is earlier.

4.63.4.3.5 Since the CC shall directly maintain/update the client collateral value based on the blocking information received from the UPI railroads of National Payment Corporation of India ('NPCI') through the CC's sponsor bank, the stock brokers shall not allocate any collateral for clients under the facility of UPI block. Other procedures such as deemed allocation of proprietary collateral, validation of 50:50 cash collateral, risk reduction mode monitoring etc. remain unchanged.

4.63.4.3.6 The CC shall debit the UPI block created in its favor to the extent of client level obligations, and receive the same in its account, without funds going through the clearing bank account of the CM. Securities provided as early pay-in (EPI) by the clients, using the block mechanism provided by depositories shall be received by the CC as per the prevailing process.

4.63.4.4 **Settlement**

4.63.4.4.1 There shall be two rounds of pay-in and one round of pay-out.

4.63.4.4.2 In Round 1 Pay-in, settlement obligation shall be calculated at client level, individually, for the clients opting for UPI block facility. There shall be no netting of obligations across different clients opting for UPI block facility and the settlement obligations shall be inclusive of standard statutory levies such as securities transaction tax (STT), stamp duty etc. The first deadline for pay-in shall be for the UPI clients. Clients with payable funds shall provide UPI block atleast to the extent of obligations, and clients with deliverable securities shall ensure availability of securities to the extent of obligations through the prevailing Early Pay-in (EPI) block mechanism wherein the securities given as EPI are blocked in favour of CC in the demat account of the client undertaking sale transaction. At the end of the Round 1 pay-in deadline defined by the CCs, the clients who have not provisioned for their pay-in shall be considered as short.

4.63.4.4.2.1 Round 2 Pay-in

4.63.4.4.2.1.1 The second round of funds obligation shall be a single net settlement of funds obligation at CM level for

(i) proprietary account of CM/TM,

(ii) clients not opting for UPI block facility and

(iii) shortages from UPI clients in Round 1 pay-in, including shortfall of funds in lieu of securities, if any.

[Illustration for funds in lieu of securities: Consider a scenario when a security sold for Rs. 100 was not delivered by client and last closing price available on settlement day for the said security was Rs. 105. In such a case, the CC shall not provide the payout of Rs. 100 to the client and in addition shall debit Rs. 5 from the block amount of the client. In case the blocked amount is insufficient, then CC shall debit this amount to CM.]

4.63.4.4.2.1.2 The second round of securities obligation shall be a single net settlement at CM level for

(i) proprietary account of CM/TM, and

(ii) clients not opting for UPI block facility, as per the existing process.

4.63.4.4.2.1.3 The CMs shall be required to provide the aforementioned funds/securities obligations to the CC.

4.63.4.4.2.1.4 If the CMs fail to fulfil the obligation, then such members shall be treated as short and relevant provisions for shortage handling/default management shall apply

4.63.4.4.3 Pay-out - The pay-out shall be done in a single round after the two pay-in rounds. The CC shall give pay-out of funds directly to the bank account of the clients opting for UPI block facility, provided they have fulfilled their payin obligations. The CCs shall provide instructions to depositories for securities pay-out to the clients, which shall be directly delivered to client's account without the need of handling of such securities pay-out by TM/CM. For all other clients and proprietary account of CM/TM, there shall be single net settlement by CC to CM as is currently being done.

4.63.4.5 **Release of block**

4.63.4.5.1 Client can request for release of block to TM through TM app. TM shall request CM, and CM shall request CC. In case the TM, CM and CC do not have any residual claim, the CC shall release the block through UPI. Upon release of the block, the client's bank shall unfreeze the amount in the account of the client. Information regarding release shall be shared by NPCI with CC (through CC's sponsor bank) who in-turn shall transmit it to CM and TM. Further, since the release of the block is going to result in collateral being unallocated in favour of the client, as per the existing process, the CC shall send a notification to the client regarding the collateral being removed

4.63.4.6 **Various scenarios**

4.63.4.6.1 An analysis of how various scenarios i.e.

(i) prefunded purchase by client,

(ii) delivery sale by client by EPI,

(iii) purchase/ sale by client supported by margins and

(iv) intraday cash market/ derivatives trading,

would be handled under the proposed UPI block facility vis-a-vis the current process is placed as **Annexure 28**

4.63.4.7 **Dealing with shortages:**

4.63.4.7.1 **Cash Market: Funds shortage**

4.63.4.7.1.1 CC shall provide pay-out of securities to the client's demat account and instruct the depository to auto-pledge such securities to the TM's "client unpaid securities pledgee account".

4.63.4.7.1.2 CC shall maintain the shortage amount of client. The obligation shall devolve on TM's CM, who shall settle the same with CC.

4.63.4.7.1.3 If client provides additional block subsequently, the CC shall debit the amount to the extent of shortfall and provide the same to the CM.

4.63.4.7.1.4 In case client fails to provide the amount, then TM can sell the securities pledged in favour of Client Unpaid Securities Pledgee Account (CUSPA) and/ or provided by way of margin pledge and mark early pay-in.

4.63.4.7.1.5 Out of the funds pay-out due to the client, amount to the extent of shortfall shall be paid to the CM who fulfilled the obligation. The remaining funds, if any, shall be paid out to the client.

4.63.4.7.1.6 The CC shall continue to maintain and update the residual short amount of the client, if any.

4.63.4.7.2 **Cash Market: Securities shortage**

4.63.4.7.2.1 Funds pay-out shall not be provided to the client. The amount shall be withheld by CC and used towards requirement of funds in lieu of securities delivered short.

4.63.4.7.2.2 Funds required in lieu of securities shortage in excess of funds pay-out shall be debited from block amount of client. In case of insufficient blocked amount, the same shall devolve on clearing member.

[Illustration: Consider a scenario when a share sold for Rs. 100 was not delivered and last closing price available on settlement day was Rs. 105. In such a case, the CC shall not provide the pay-out of Rs. 100 to the client and in addition shall debit Rs. 5 from the block amount of the client. In case the blocked amount is insufficient, then CC shall debit this amount to CM.]

4.63.4.7.2.3 Auction shall be conducted to buy the securities short delivered by UPI clients.

4.63.4.7.2.4 If actual amount required towards auction purchase or financial closeout exceeds the pay-out amount referred to in **Para 4.63.4.7.2.2** above, the same shall be debited from client block. In case of insufficient client block, the same shall devolve on clearing member.

4.63.4.7.2.5 In case of any devolvement on member, the short amount of client shall be maintained and in case any blocking is done in future, the block shall be debited to the extent of shortfall and provided to the clearing member

4.63.4.7.3 **Shortfall: Derivatives**

4.63.4.7.3.1 CC shall debit block to the extent of pay-in requirements, irrespective of whether such debit causes a margin shortfall. In exceptional circumstances, if pay-in exceeds the margin, the residual amount shall devolve on CM.

4.63.4.7.3.2 In case of margin shortfall, TM/CM can close-out the position of the client and resultant loss shall be debited to the block or resultant profit shall be paid out to the client by the CC. Till the time TM/CM closes out the position, the provisions related to deemed allocation of proprietary collateral shall apply.

4.63.4.7.3.3 In case obligations have devolved on CM, any pay-out resulting from close-out of positions, or any new block created by client, to the extent of devolvement, shall be provided to the CM.

4.63.5 Since the framework requires certain changes to be made in the systems and processes of clearing corporations, stock exchanges, depositories, stock brokers and NPCI, the concerned entities are expected to make requisite changes and test the systems and processes for robustness thereafter to make the facility live by January 01, 2024.

4.63.6 To begin with, the facility may be made available in the equity cash segment. The CCs may extend the facility to additional segments subsequently.

4.63.7 Further, detailed operational guidelines including mode of brokerage collection shall be issued by CCs in consultation with relevant stakeholders such as stock exchanges, depositories etc.

4.64 Enhanced Due Diligence for Dematerialization of Physical Securities[227]

4.64.1 In terms of Regulation 40 of LODR Regulations, transfer of securities held in physical mode is not permitted. Standardised norms with respect to documentation/procedure for transfer of physical securities were issued by SEBI.

4.64.2 To augment the integrity of the system in processing of dematerialization request

[227] Reference: SEBI Circular SEBI/HO/MIRSD/RTAMB/CIR/P/2019/122 dated November 05, 2019

in respect of the remaining physical shares, the Depositories and the listed companies/RTAs are directed to implement the following due diligence process:

4.64.2.1 All Listed companies or their RTAs shall provide data of their members holding shares in physical mode, viz. the name of shareholders, folio numbers, certificate numbers, distinctive numbers and PAN etc. (hereinafter, **static database**) as on March 31, 2019, to the Depositories. The common format for this data shall be specified jointly by the Depositories and be communicated to Issuer companies / their RTAs.

4.64.2.2 Depositories shall capture the relevant details from the static database as per above para and put in place systems to validate any dematerialization request received after December 31, 2019. Accordingly, the depository system shall retrieve the shareholder name(s) recorded against the folio number and certificate number in Static Data for each DRN request received after this date and validate the same against the demat account holder(s) name as available in the records of the Depositories.

4.64.2.3 In case of mismatch of name on the share certificate(s) vis-à-vis name of the beneficial owner of demat account, the depository system shall generate flag/alert. In instances, where such flags/alerts have been generated, the following additional documents explaining the difference in name shall be sought, namely

4.64.2.3.1 Copy of Passport

4.64.2.3.2 Copy of legally recognized marriage certificate

4.64.2.3.3 Copy of gazette notification regarding change in name

4.64.2.3.4 Copy of Aadhar Card

4.64.2.4 In the case of complete mismatch of name on the share certificate(s) vis-à-vis name of the beneficial owner of demat account, the applicant may approach the Issuer company/RTA for establishing his title/ownership.

4.65 Framework For Adoption Of Cloud Services By SEBI Regulated Entities (REs)[228]

Kindly refer SEBI Circular SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/033 dated March 06, 2023 in respect of Adoption Of Cloud Services By SEBI Regulated Entities for necessary compliance in respect of Depositories.

4.66 Committees at Market Infrastructure Institutions[229]

A. In order to ensure effective oversight of the functioning of depository (being an Market Infrastructure Institutions (MIIs)), Regulation 30 of the DP Regulations mandates

[228] Reference: SEBI Circular SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/033 dated March 06, 2023

[229] Reference: SEBI Circular SEBI/HO/MRD/DOP2DSA2/CIR/P/2019/13 dated January 10, 2019, and SEBI email dated February 06, 2020

depositories to constitute two functional and three oversight committees within each depository. A list of all such mandatory committees for depositories along with their functions and detailed composition requirements is provided below:

S. No.	Name of Committee	Brief terms of reference	Composition
(I) FUNCTIONAL COMMITTEES :			
1	**Member Committee**[230]	• To scrutinize, evaluate, accept or reject applications for admission of members, transfer of membership as well as approve voluntary withdrawal of membership. • Formulate policy to deal with any disciplinary matters relating to the Participants, Clients, Issuer or its Registrar and Transfer Agent, Clearing Members, Clearing Corporations and other users. This shall include termination / disciplinary action against participants, suspending, expelling or imposing penalty on the participant, freezing the account of the participant, among others. • Based on the laid down policy, consider the cases of violations observed during inspection, etc. and impose appropriate regulatory measure on the members of the depositories. • While imposing the regulatory measure, the Committee shall adopt a laid down process,	• A maximum of two key management personnel of the depositories can be on the committee one of which shall necessarily be the Managing Director of the depositories. • The committee may also include independent external persons. • SEBI may nominate members in the Committee, if felt necessary in the interest of securities market. • The number of PIDs shall not be less than the total of number of shareholder directors, KMPs and independent external persons put together.

[230] Reference: SEBI Circular SEBI/HO/MRD/DDAP/CIR/P/2020/16 dated January 28, 2020

		based on the 'Principles of natural justice'.	
2	[***][231]		
3	**Nomination and Remuneration Committee**	• Identifying a Key management personnel, other than personnel as specifically provided in its definition under DP Regulations. • Lay down the policy for compensation of key management personnel in terms of the compensation norms prescribed by SEBI. • Determining the compensation of KMPs in terms of the compensation policy. • Determining the tenure of a key management personnel, other than a director, to be posted in a regulatory department. • Selecting the Managing Director. • Framing & reviewing the performance review policy to carry out evaluation of every director's performance, including that of Public Interest Director (PID).	• The Committee shall include only public interest directors. • However, independent external persons may be part of the committee for the limited purpose of recommendation relating to selection of Managing Director; wherein the number of PIDs shall not be less than the independent external persons.

[231] Reference: "Grievance redressal committee" has been abolished by the SEBI (Depositories and Participants) (Amendment) Regulations, 2023, w.e.f. 28-08-2023

		• Recommending whether to extend the term of appointment of the PID. • Besides the above, it will also discharge the function as Nomination & Remuneration Committee under the Companies Act, 2013 and LODR Regulations as amended from time to time.	
(II) OVERSIGHT COMMITTEES :			
4	**Standing Committee on Technology**	• Monitor whether the technology used by the depository remains up to date and meets the growing demands. • Monitor the adequacy of system capacity and efficiency. • Look into the changes being suggested to the existing software/hardware. • Investigate into the problems computerised depository system, such as hanging/ slowdown/ breakdown. • Ensure that transparency is maintained in disseminating information regarding slowdown/break down in the depository system. • The Committee shall submit a report to the Governing Board of the depository. The Board will deliberate on the report and suitable action/ remedial measure will be taken.	• The Committee shall include at least two independent external persons proficient in technology. • The number of PIDs shall not be less than the total of number of shareholder directors and independent external persons put together.

		• Explain any system outage related incidents to the governing board. • Review the implementation of board approved cyber security and resilience policy and its framework. • Such other matters in the scope as may be referred by the Governing Board of the depository and/or SEBI.	
5	[***][232]		
6.	**Regulatory Oversight Committee**	• To lay down procedures for the implementation of the Code of Ethics and prescribe the reporting formats for the disclosure required under the Code of Ethics. • To oversee the implementation of the Code of Ethics. • To periodically monitor the dealings in securities of the Key Management Personnel. • To periodically monitor the trading conducted by firms/corporate entities in which the directors hold twenty percent or more beneficial interest or hold a controlling interest. • To consider and decide on the criteria for admission, withdrawal of securities and continuous compliance requirements.	• The committee shall comprise of public interest director and independent external persons. • The number of PIDs shall not be less than the total of number of independent external persons put together. • Also shareholder director and key management personnel may be invitee to the committee.

[232] Reference: "Advisory Committee" has been abolished by the SEBI (Depositories and Participants) (Amendment) Regulations, 2023, w.e.f. 28-08-2023

		• To declare any security admitted into Depository as ineligible. • To review complaint resolution process and status of redressal of grievances of demat account holders, depository participants, Issuers / RTAs with respect to depository operations. This shall include review of complaints remaining unresolved over long period of time, estimate the adequacy of resources, amongst others. • Annual review of arbitrators and arbitration awards (both quantum and quality of the awards). • To monitor compliance with DP Regulations as amended from time to time and other applicable rules and regulations along-with SEBI Circulars and other directions issued thereunder. • To review the fees and charges levied by the Depository. • Review the actions taken to implement the suggestions of SEBI's Inspection Reports, place the same before the Governing Board of the depository. • To follow up and ensure compliance/implementation of the inspection observations.	

7	**Risk Management Committee**	• To formulate a detailed risk management policy which shall be approved by the governing board. • To review the Risk Management Framework & risk mitigation measures from time to time. • To monitor and review enterprise-wide risk management plan and lay down procedures to inform Board members about the risk assessment and minimisation procedures. • The head of the risk management department shall report to the risk management committee and to the managing director of the depository. • The risk management committee shall monitor implementation of the risk management policy and keep the Board and the governing board informed about its implementation and deviation, if any. • Responsibilities and other requirements provided under Para 4.38	• The risk management committee shall comprise only of the public interest directors and independent external persons, and shall report to the Governing Board. • The number of PIDs shall not be less than the total of number of independent external persons.

4.66.1 Further, while Para 4.66 A provides for the composition that is specific to each statutory committee at depository, the overarching principles for composition and quorum of the statutory committee at depositories shall be as under, which shall be applicable to all committees.

4.66.1.1 On each committees at depositories, the number of Public Interest Directors (PIDs) shall not be less than the total of number of shareholder directors,

Key Management Personnel (KMPs), independent external persons, etc. put together, wherever shareholder directors, KMPs, independent external persons, etc. are part of the concerned committee

4.66.1.2 PID shall be chairperson of each committee at depository

4.66.1.3 To constitute the quorum for the meeting of the depository committee, the number of PIDs on each of the committees at depositories shall not be less than total number of other members (shareholder directors, KMPs, independent external persons, etc. as applicable) put together.

4.66.1.4 The voting on a resolution in the meeting of the committees at depositories shall be valid only when the number of PIDs that have cast their vote on such resolution is equal to or more than the total number of other members (shareholder directors, KMPs, independent external persons, etc., as applicable) put together who have cast their vote on such resolution.

4.66.1.5 The casting vote in the meetings of the committees shall be with the chairperson of the committee.

4.66.1.6 Apart from that specifically provided in **Para 4.66 A**, whenever required, a committee may invite Managing Director, other relevant KMPs and employees of the depository. However, such invitee shall not have any voting rights.

4.66.2 Further, depositories are directed to adhere to the following:

4.66.2.1 Over and above the statutory committees mentioned at **Para 4.66 A** above, the committees that are mandated by relevant law for listed companies shall apply *mutatis mutandis* to depositories.

4.66.2.2 Depositories shall lay down policy for the frequency of meetings, etc., for the statutory committees.

4.66.2.3 PIDs in Committees at depositories:

4.66.2.3.1 DP Regulations prescribes that a PID on the board of a depository shall not act simultaneously as a member on more than five committees of that depository.

4.66.2.3.2 It is clarified that the above limitation on maximum number of committees that a PID can be member of, shall be applicable only to statutory committees prescribed by SEBI under DP Regulations, and circulars issued thereunder. The said requirement shall not be applicable to committees constituted under Companies Act, 2013, **LODR Regulations**, amongst others.

4.66.2.3.3 In case of non-availability of adequate number of PIDs in a depository, the relevant depository shall take steps to induct more

PIDs in order to fulfil the requirement of composition of committees within a depository.

4.66.2.4 Meeting of PIDs:

4.66.2.4.1 As per code of conduct for PIDs provided DP Regulations, the PIDs shall be required to meet separately every six months. It is added that all the PIDs shall necessarily attend all such meetings of PIDs

4.66.2.4.2 The objective of such meetings, shall include inter alia reviewing the status of compliance with SEBI letters/ circulars, reviewing the functioning of regulatory departments including the adequacy of resources dedicated to regulatory functions, etc. PIDs shall also prepare a report on the working of the committees of which they are member and circulate the same to other PIDs. The consolidated report in this regard shall be submitted to the governing board of the depositories. Further, PIDs shall identify the important issues which may involve conflict of interest for the depository or may have significant impact on the market and report the same to SEBI, from time to time.

4.66.2.5 Independent external persons in committees at depositories:

4.66.2.5.1 The independent external persons forming a part of committees shall be from amongst the persons of integrity, having a sound reputation and not having any conflict of interest. They shall be specialists in the field of work assigned to the committee; however, they shall not be associated in any manner with the relevant depository and its members.

4.66.2.5.2 Depositories shall frame the guidelines for appointment, tenure, code of conduct, etc., of independent external persons. Extension of the tenure may be granted to independent external persons at the expiry of the tenure, subject to performance review in the manner prescribed by SEBI for PIDs. Further, the maximum tenure limit of Independent external persons in a committee of depository shall be at par with that of PIDs, as prescribed under Regulation 25(3) of the DP Regulations.

4.66.3 **Performance review of Public Interest Directors (PIDs)[233]:**

4.66.3.1 In respect of Public Interest Directors (PIDs) appointed in the governing board of depositories, Regulation 25(3) of DP Regulations, provides the following:

[233] Reference: SEBI Circular SEBI/HO/MRD/DOP2DSA2/CIR/P/2019/26 dated February 5, 2019

"Public interest directors shall be nominated for a term of three years, extendable by another term of three years, subject to performance review in the manner as may be specified by the Board:

Provided that post the expiry of term(s) at a depository, a public interest director may be nominated for a further term of three years in other depository or recognized stock exchange or a recognized clearing corporation, only after a cooling-off period of one year:

Provided further that a person may be nominated as a public interest director for a maximum of three terms across a depository/recognized stock exchange/recognized clearing corporations, subject to a maximum age limit of seventy-five years."

4.66.3.2 For complying with the aforementioned regulation, while developing a framework for performance review of PIDs, depositories need to consider the following:

4.66.3.2.1 **Policy for Performance review of PIDs:**

4.66.3.2.1.1 The Nomination and Remuneration committee (NRC) of the depositories will be responsible for framing the performance review policy for PIDs.

4.66.3.2.1.2 Such performance review policy shall include criteria for performance evaluation, methodology adopted for such evaluation and analyzing the results, amongst others.

4.66.3.2.1.3 Performance review policy of PID shall include scope for both internal evaluation as well as external evaluation.

4.66.3.2.1.4 Further, as performance review is not a static process and requires periodical review, NRC shall also be responsible for reviewing such performance review policy, at least once in 3 years.

4.66.3.2.1.5 Such performance review policy and changes made therein, shall be approved by the governing board of depository.

4.66.3.2.2 **Guiding criteria of Performance Review:**

As a part of framing performance review policy, NRC shall be primarily responsible for formulation of performance evaluation criteria. The criteria for performance review of PIDs, which shall be considered for both internal evaluation and external evaluation, may be framed by NRC taking into consideration guiding principles provided below. These principles would serve as a guidance for depositories and the same may be adopted by respective depository, as considered appropriate, with additional principles, if any.

Guide for depositories to frame criteria for performance review of PIDs:

a. **Qualifications:** The PID's qualification in area of law, finance, accounting, economics, management, administration or another area relevant to the financial markets, including any recent updates in this regard.

b. **Experience:** The PID's prior experience in area of law, finance, accounting, economics, management, administration or any other area relevant to the financial markets, including any recent updates in this regard.

c. **Knowledge and Competency:**

- Whether the PID has sufficient understanding and knowledge of the entity in which it operates and the applicable regulatory norms.
- Whether the PID has sufficient understanding of the role, responsibilities and obligations of PID under the relevant regulatory norms.
- How the PID fares across different competencies as identified for effective functioning of Board of the concerned depository (The depository may list various competencies and mark all PIDs against every such competency e.g. Constructive and analytical decision making abilities).
- Whether the PID has sufficient understanding of the risk attached with the business structure.

d. **Fulfilment of functions:**

- Whether the PID understands and fulfils the functions as assigned to him/her by the Board and the regulatory norms.
- Whether the PID gives views and opinion on various regulatory matters when comments are invited by SEBI through various means.

e. **Ability to function as a team:**

- Whether the PID is able to function as an effective team- member.
- Whether the PID listens attentively to the contributions of others and gives adequate weightage to the views and perception of other Board members.
- Whether the PID shares good interpersonal relationship with other directors.

f. **Initiative:**

- Whether the PID actively takes initiative with respect to various areas.
- Whether the PID insists on receiving information necessary for decision making.
- Whether the concerned PID keeps himself well informed about the functioning of depository and the external environment in which it operates.
- Whether the PID remains updated in terms of developments taking place in regulatory areas.

- Whether the PID has identified any important issues concerning any matter which may involve conflict of interest for the concerned depository, or may have significant impact on their functioning, or may not be in the interest of securities market, and whether the PID reported same to SEBI.
- Whether the PID appropriately deals with critical matters.

g. **Availability and attendance:**

- Whether the PID is available for meetings of the Board and attends the meeting of Governing board and Committees regularly and timely, without delay. It must be ensured that the concerned PID hasn't remained absent for three consecutive meetings of the governing board and has attended seventy five per cent of the total meetings of the governing board in each calendar year; failing which the PID shall be liable to vacate office.

h. **Commitment:** Whether the PID is adequately committed to the Board and the depository.

i. **Contribution:**

- Whether the PID has contributed effectively to the entity and in the Board meetings.
- Whether the PID participates in the proceedings of Board meetings keeping in mind the interests of various stakeholders.
- Whether the PID actively deliberates and contributes on proposed business propositions and strategic decisions taking into consideration pros and cons of such propositions, long term outlook, business goals, cost-benefit analysis, etc.

j. **Integrity:**

- Whether the PID demonstrates highest level of integrity (including conflict of interest disclosures, maintenance of confidentiality, etc.).
- Whether the PID strictly adhere to the provisions of the Securities Contracts (Regulation) (Stock Exchanges and Clearing Corporations) Regulations, 2018, 2018, DP Regulations and any other regulatory provision, as applicable, along-with the code of conduct and code of ethics prescribed under other applicable regulatory norms.
- Whether disclosures such as dealing in securities and other regulatory disclosures are provided by the PID on timely basis.
- Confirmation on the PID being a Fit & Proper person.
- Confirmation that the PID doesn't disclose confidential information, including technologies, unpublished price sensitive information, unless

such disclosure is expressly approved by the Board of directors or required under the applicable laws.

k. **Independence:**

- Whether the PID is independent from the entity and the other directors and there is no conflict of interest.
- Confirmation as to non-association of the PID with relevant depository and its member.
- Whether the PID keeps regulators informed of material developments in the concerned depository's functioning, from time to time.

l. **Independent views and judgment:**

- Whether the PID exercises his/ her own judgment and voices opinion freely.
- Whether the PID's participation in decisions taken during meetings are unbiased, based on ethical judgment and are in strict conformity to the applicable regulatory norms.
- Whether the PID raises his/her concern if anything is observed contrary to regulatory norms and the expected norms of ethical conduct.
- Whether the PID is committed to ensure that there is fairness and integrity in depository's system, in letter as well as spirit.

***4.66.3.2.3* Evaluation mechanism:**

4.66.3.2.3.1 PIDs shall be subjected to internal evaluation as well as external evaluation, carrying equal weightage.

4.66.3.2.3.2 Internal evaluation: All the governing board members shall evaluate the performance of each PID, on an annual basis at the end of every financial year.

4.66.3.2.3.3 External evaluation: PIDs shall also be subject to external evaluation during their last year of the term in a depository , by a management or a human resources consulting firm. The consultant shall take into consideration the performance of the PID for the entire tenure served in a given depository, at least up to 4 months before expiry of his/ her term. In order to avoid any bias or conflict of interest, external consultant should not be a related party or associated with the depository, the concerned PID or any other governing board members.

4.66.3.2.3.4 Such performance review should be carried out in fair & objective manner and the review should be recorded with clarity and verifiable facts in a standardized format covering all the relevant criteria / aspects.

4.66.3.2.3.5 While evaluating conflict of interest of a PID, the governing board of the depository shall also take into consideration provisions of Clause 2(d) of Schedule II Part C of DP Regulations under the head 'Public Interest Director'; and conflict of interest, if any, of any PIDs should be disclosed to SEBI by the governing board with their comments/ views.

4.66.3.2.4 **Disclosure:** Performance evaluation criteria for PIDs shall be disclosed in their annual report as well as on the website of the concerned depository.

4.66.3.2.5 **Recommendation to SEBI:** After taking into account the performance of a PID in the concerned depository, on the basis of internal evaluation and external evaluation both carrying equal weightage, NRC shall consider and recommend extension of his / her tenure to the Governing Board of the depository. The Governing Board of the depository shall in-turn consider and recommend to SEBI if the tenure of the PID is desired to be extended by another term of three years.

4.66.3.2.6 In addition to the other requirements prescribed in performance review policy of the depositories along-with norms specified in DP Regulations, the following may be considered by NRCs of depositories:

4.66.3.2.6.1 It shall be ensured that the concerned PID hasn't remained absent for three consecutive meetings of the governing board and has attended seventy-five per cent of the total meetings of the governing board in each calendar year; failing which PID shall be liable to vacate office.

4.66.3.2.6.2 It shall be ensured that PIDs in the governing boards of depositories are selected from diverse fields of work, in terms of their qualification and experience.

4.66.3.3 The application for extension of term of a PID shall be accompanied with the attendance details of PID in the meetings of various mandatory committees and of the governing board of the depository along-with specific reasons for seeking extension of his/her term as a PID. Such specific reasons shall include facts such as whether the concerned PID, during the term served, had identified any important issues concerning any matter which may involve conflict of interest, or have significant impact on functioning of depository, or may not be in the interest of securities market as a whole, and whether the PID had reported the same to SEBI.

4.66.3.4 In terms of DP Regulations, a minimum of two names shall be submitted by the depository at the time of making request for appointment of PID and extension

of the term of existing PID, including appointment of PID for the purpose of broad basing the governing board, against each such vacancy.

4.66.3.5 The aforementioned norms specify the minimum requirements that have to be complied with by depositories, however the NRCs of depositories may adopt additional and more stringent norms while framing a policy for performance review of PIDs. With regard to the detailed criteria for performance evaluation, as provided in **Para 4.66.3.2.2,** the same shall serve as an illustrative guide for depositories to frame performance evaluation criteria, both for internal as well as external evaluation, and the same may be adopted by depositories as considered appropriate, with additional criteria, if any.

4.66.3.5.1 Additionally, with regard to tenure of existing PIDs as on February 5, 2019, following is clarified:

4.66.3.5.1.1 The term of existing PIDs serving in a MII for more than three years, can be extended, subject to his / her performance review and a maximum tenure of 6 years as PID in that particular MII.

4.66.3.5.1.2 The term of existing PIDs, that have already served for six years or more in a single MII, shall not be eligible for further extension in that MII.

4.67 Exemption from clubbing of investment limit for foreign Government agencies and its related entities[234] and Write-off of shares held by FPIs[235]

Kindly refer para titled 'Monitoring of investment limit at investor group level' and 'Write-off of securities held by FPIs' of SEBI Circular SEBI/HO/AFD-2/CIR/P/2022/175 dated December 19, 2022 (Master Circular for Foreign Portfolio Investors, Designated Depository Participants and Eligible Foreign Investors)

4.68 Stealing of Customers data registered with NSE/ BSE

4.68.1 Central Economic Intelligence Bureau, Department of Revenue, GOI brought to the notice of SEBI that certain fraudsters are collecting data of customers who already into trading either in NSE/BSE and send them bulk messages on the pretext of providing investment tips and luring them to invest with them in their bogus firms by promising huge profits. In view of the above, there is need to sensitize, create awareness among investors about the same.

4.68.2 In this regard, Stock exchanges and Depositories to advise, sensitize their stockbrokers, investors on the above issue and also that necessary steps, safeguards

[234] Reference: SEBI Circular IMD/FPI&C/CIR/P/2020/07 dated January 16, 2020
[235] Reference: SEBI Circular SEBI/HO/IMD/FPI&C/CIR/P/2020/177 dated September 21, 2020

are taken so that data of the customers/investors registered with the Members/Participants are not shared or revealed to unauthorised persons.

4.69 Advisory regarding remote access and telecommuting[236]

4.69.1 In reference to the meeting of the TAC held on April 30, 2020, the Market Infrastructure Institutions (MIIs) were advised to implement the following measures after taking into consideration the COVID-19 situation:-

4.69.1.1 The MII shall have proper remote access policy framework incorporating the specific requirements of accessing the enterprise resources securely located in the data centre from home, using internet connection.

4.69.1.2 For implementation of the concept of trusted machine as end users, the MII shall categorize the machines as official desktops/laptops and accordingly the same may be configured to ensure implementation of solution stack considering the requirements of authorized access. Official devices shall have appropriate security measures to ensure that the configuration is not tampered with. The MII shall ensure that internet connectivity provided on all official devices shall not be used for any purpose other than the use of remote access to data centre resources.

4.69.1.3 If personal devices (BYOD) are allowed for general functions, then appropriate guidelines should be issued to indicate positive and negative list of applications that are permitted on such devices. Further, these devices should be subject to periodic audit.

4.69.1.4 The MII shall implement the various measures related to Multi-Factor Authentication (MFA) for verification of user access so as to ensure better data confidentiality and accessibility. VPN remote access through MFA shall also be implemented. It is clarified that MFA refers to the use of two or more factors to verify an account holder's claimed identity.

4.69.1.5 The MII shall ensure that the trusted machine is the only client permitted to access the data centre resources. The MII shall ensure that the Virtual Private Network (VPN) remote login is device specific through the binding of the Media Access Control (MAC) address of the device with the IP address to implement appropriate security control measures.

4.69.1.6 The MII shall explore a mechanism for ensuring that the employee using remote access solution is indeed the same person to whom access has been granted and not another employee or unauthorized user. A suitable video-recognition method has to be put in place to ensure that only the intended employee uses the device after logging in through remote access. The MII shall

[236] Reference: SEBI MRD email dated May 18, 2020

implement short session timeouts for better security. Towards this end, it is suggested that the MII may consider running a mandatory monitor on the device that executes:

4.69.1.6.1 At random intervals takes a picture with the webcam and uploads the same to the MII's server,

4.69.1.6.2 At random intervals pops up and prompts biometric authentication with a timeout period of a few seconds. If there is a timeout, this is flagged on the MII server as a security event.

4.69.1.7 The MII shall ensure that appropriate risk mitigation mechanisms are put in place whenever remote access of data centre resources is permitted for service providers.

4.69.1.8 Remote access has to be monitored continuously for any abnormal access and appropriate alerts and alarms should be generated to address this breach before the damage is done. For on-site monitoring, the MII shall implement adequate safeguard mechanism such as cameras, security guards, nearby co-workers to reinforce technological activities.

4.69.1.9 The MII shall ensure that the backup, restore and archival functions work seamlessly, particularly if the users have been provided remote access to internal systems.

4.69.1.10 The MII is advised to exercise sound judgement and discretion while applying patches to existing hardware and software and apply only those patches which were necessary and applicable.

4.69.1.11 The Security Operations Centre (SOC) engine has to be periodically monitored and logs analyzed from a remote location. Alerts and alarms generated should also be analyzed and appropriate decisions should be taken to address the security concerns. The security controls implemented for the Remote Access requirements need to be integrated with the SOC Engine and should become a part of the overall monitoring of the security posture.

4.69.1.12 The MII shall update its incidence response plan in view of the current pandemic.

4.69.1.13 The MII shall implement cyber security advisories received from SEBI, CERT-IN and NCIIPC on a regular basis.

4.69.2 Further, all the guidelines developed and implemented during pandemic situation shall become SOPs post Covid-19 situation for future preparedness.

4.70 <u>Standard Operating Procedure for handling of technical glitches by Market Infrastructure Institutions (MIIs) and payment of "Financial Disincentives" thereof</u>[237]

[237] Reference: SEBI Circular SEBI/HO/MRD1/DTCS/CIR/P/2021/590 dated July 05, 2021.

4.70.1 MIIs (i.e. Stock Exchanges, Clearing Corporations and Depositories) are systemically important institutions as they, inter-alia, provide infrastructure necessary for the smooth and uninterrupted functioning of the securities market.

4.70.2 With increasing dependence on technology, as the operations and functioning of MIIs are fully automated right from order entry to order matching to trade confirmation leading up to clearing and settlement of trades, the instances of technical glitches at MIIs, leading to business disruption/unavailability of services provided by MIIs, have been occurring, despite various mechanisms stipulated by SEBI such as Business Continuity Planning, Disaster Recovery policies, System Audit etc.

4.70.3 The general practice in the computing/technology industry to deal with business disruption/unavailability of services, is to work with specified downtime and for downtimes beyond such specified time, a pre-defined penalty structure is included in Service Level Agreement.

4.70.4 Considering the criticality of smooth functioning of systems of MIIs (as any disruption adversely impacts all classes of investors / market participants as well as the credibility of the securities market), specifying a pre-defined threshold for downtime of systems of MIIs becomes desirable. For any downtime or unavailability of services, beyond such pre-defined time, there is a need to ensure that "Financial Disincentive" is paid by the MIIs as well as Managing Director (being the executive head in-charge of all the day to day operations) and Chief Technology Officer (being the executive head in charge of technology) of the MII. This will encourage MIIs to constantly monitor the performance and efficiency of their systems and upgrade/ enhance their systems etc. to avoid any possibility of technical glitches/disruption/disaster and restart their operations expeditiously in the event of glitch/disruption/disaster.

4.70.5 Accordingly, after extensive discussion with various stakeholders, it has been decided that, MIIs shall :

4.70.5.1 Follow the Standard Operating Procedure (SOP) for handling technical glitches as detailed under **Para A** below; and

4.70.5.2 Comply with the "Financial Disincentive" structure as detailed under **Para B** below.

A. <u>Standard Operating Procedure (SOP) for handling of technical glitches</u>

Definition of "Technical Glitch"

1. Technical glitch shall mean any malfunction in the systems of an MII. Malfunction in the systems of the MII shall include malfunction in its (a) hardware, or; (b) software, or; (c) any products/ services provided by the MII, whether on account

of inadequate infrastructure/ systems or otherwise, which may lead to either stoppage or variance in the normal functions/ operations of systems of the MII.

Reporting Requirements

2. The following reporting structure for technical glitches shall be adopted by the MIIs:

S. No.	Disruption	Reporting
1.	No business disruption	• Standing Committee on Technology (SCOT) of MII • Governing Board of MII
2.	Business disruption	• SCOT of MII • Governing Board of MII • SEBI

Business disruption shall mean either stoppage or variance in the normal functions/operations of systems of the MII thereby impacting normal/regular service delivery of the MII.

2.1. With regard to incidents resulting in business disruption, the following shall be submitted by the MIIs to SEBI:

i. Information of technical glitch on immediate basis but not later than 2 hours from the time of occurrence of the glitch; provided that glitches of the nature of a disaster- as defined under **Para 4.31** shall be reported immediately upon declaration of disaster.

ii. Preliminary report within 24 hours of the occurrence of the glitch.

iii. Comprehensive Root Cause Analysis (RCA) report and corrective action taken to address the technical glitch within 21 days of the incident. Such report shall be submitted to SEBI, after placing the same before the Standing Committee on Technology and the Governing Board of the MII and confirming compliance with their observations.

iv. RCA submitted by the MIIs should inter-alia include exact cause of the technical glitch (including root cause from vendor(s), if applicable), exact duration of the technical glitch, chronology of events, list of business processes/systems and time for which they were impacted, recommendations of SCOT / Governing Board of MII, details of corrective/ preventive measures taken (or to be taken) by MII along with timelines and any other aspect relevant to the technical glitch. As part of the RCA, MIIs are required to demonstrate compliance with various requirements of this SOP. The RCA shall include details regarding time of incident, time when

operations were restored and in the event of a disaster, time when disaster was declared.

2.2. All communication and information with regard to technical glitch shall be shared by the MII with SEBI through a dedicated e-mail id viz. techglitch@sebi.gov.in

Placing before TAC

3. With regard to the incidents wherein business is disrupted, the RCA and corrective action taken, as submitted by the MII, shall be placed before TAC of SEBI. TAC/ SEBI, if it so desires, may seek additional information/ clarification from the MII regarding the technical glitch.

4. In case TAC finds the actions taken by the MII as inadequate, then, based on the recommendations of TAC, the MII shall be required to address the technical glitch by taking appropriate corrective actions, within the timeline specified by TAC/SEBI. While deciding such timeline, criticality of the malfunction and/or the services/ applications affected by the same shall also be taken into consideration.

B. "Financial Disincentive" structure with regard to handling of technical glitches

Failure to timely submit RCA

1. In case of delay in submission or submission of incomplete/ inadequate RCA by an MII, a "financial disincentive" of Rs.1,00,000 per working day shall be paid by the MII for each working day of delay from the timeline specified at **clause 2.1 (iii)** of **Para 4.70.5 A** above or any revised timeline specified by TAC/SEBI for submission of exact RCA.

Failure to timely address technical glitch

2. In order to ensure that MIIs address technical glitch within the timeline specified by TAC/SEBI, the following progressive slab-wise "financial disincentive" shall be paid from the expiry of the timeline specified by TAC/ SEBI:

S No.	No. of working days during which failure continues (i.e. after expiry of the timeline specified by TAC/SEBI)	Financial disincentive to be paid by the MII (Rs.)
i.	First 15 working days	2 lakh per working day
ii.	Subsequent 15 working days	3 lakh per working day in addition to S No. (i) above
iii.	Beyond 30 working days	25 lakh in addition to S No (i) and (ii) above

Failure to declare disaster within stipulated timelines

3. It has been mandated that, in the event of disruption of any one or more of the 'Critical Systems', the MII shall, within 30 minutes of the incident, declare that incident as 'Disaster'. In case of delay in declaration of disaster beyond the timeline specified by SEBI, the following "financial disincentive" shall be paid:

S. No.	Delay in declaration of disaster beyond abovementioned timeline specified by SEBI	Financial disincentive Equivalent (Rs.)
i.	Financial disincentive on MII	10% of average of standalone net profit for previous two financial years or Rs. 2 cr., whichever is higher.
ii.	Financial disincentive on Managing Director (MD) and Chief Technology Officer (CTO) of MII separately	10% each of their annual pay (both fixed and variable components) for the financial year when the disaster occurred

Failure to restore operations within Recovery Time Objective (RTO)

4. In the event of a disaster, if an MII fails to restore its operations within the RTO prescribed by SEBI, i.e. to restore operations of 'Critical Systems' including from Disaster Recovery Site within 45 minutes of declaration of Disaster, the following "financial disincentive" shall be paid:

S No.	Failure to restore operations within the RTO prescribed by SEBI	Financial disincentive Equivalent (Rs.)
i.	Financial disincentive on MII	10% of average of standalone net profit for previous two financial years or Rs. 2 cr., whichever is higher.
ii.	Financial disincentive on MD and CTO of MII separately	10% each of their annual pay (both fixed and variable components) for the financial year when the disaster occurred

"Financial disincentive" under Clause 3 and Clause 4 above, in relation to the same disaster, shall be paid only once either under Clause 3 or Clause 4.

5. Further, if an MII fails to restore operations of Critical Systems including from Disaster Recovery Site within three hours from the occurrence of the disaster, the following additional "financial disincentive" (over and above S No 3 or 4 above) shall be paid:

S No.	Failure to Restore operations of Critical systems beyond abovementioned timeline	Financial disincentive Equivalent (Rs.)
i.	Financial disincentive on MII	10% of average of standalone net profit for previous two financial years or Rs. 2 cr., whichever is higher.
ii.	Financial disincentive on MD and CTO of MII separately	10% each of their annual pay (both fixed and variable components) for the financial year when the disaster occurred

Failure to restore normalcy in cases of business disruption, not being in the nature of a Disaster

6. In the event of any business disruption, which is not required to be declared as "Disaster", if an MII fails to restore normalcy of operations within 75 minutes of the incident, the following slab wise "financial disincentive" shall be paid by the MII:

S No.	**Failure to Restore normalcy within**	**Financial disincentive (Rs.)**
i.	75 minutes to 3 hours of the incident	Rs. 50 lacs
ii.	Beyond 3 hours of the incident	Rs.1 crore

7. The amount of "financial disincentive" paid as per the above structure shall be credited by MII to the following funds maintained by it:

S No.	Financial Disincentive on MIIs, MD and CTO	Credited to Funds
i.	Stock Exchange	Investor Protection Fund (IPF)
ii.	Clearing Corporation	Core Settlement Guarantee Fund (Core SGF)
iii.	Depositories	Investor Protection Fund (IPF)

8. Further, the MII shall submit a compliance report within 90 days of occurrence of disaster/ business disruption to SEBI providing details of payment of "financial disincentives" including computation of "financial disincentives" as per the SOP and the date when the amount was credited to the aforementioned funds. With regard to "financial disincentive" on the MD/CTO of the MII arising out of the variable pay component, the compliance report shall be submitted within 30 days

of determination of variable pay of the concerned officials for the financial year when the disaster occurred.

9. With regard to the requirement of payment of "financial disincentive" on the aforesaid officials of the MII (i.e. MD and CTO), the MII shall insert a suitable clause in the terms of appointment of these officials and/ or in the Internal Code of Conduct of the MII to comply with the "financial disincentive" requirements.

10. The financial disincentives automatically triggered under predefined circumstances as stated in clauses 1,2,3,4,5,6 above shall be paid by the MIIs. However, these financial disincentives shall be without prejudice to any action as may be initiated by SEBI.

4.70.6 The aforesaid "Financial Disincentives", when triggered automatically under predefined conditions, as detailed in **Para 4.70.5 B,** shall be credited to the Investor Protection Fund/Core Settlement Guarantee Fund maintained by the MII.

4.71 Standard Operating Procedure for handling of Stock Exchange Outage and extension of trading hours thereof[238]

4.71.1 Trading hours of stock exchanges are pre-defined and known to all market participants including the other Market Infrastructure Institutions (MIIs) to enable them to carry out activities related to continuous trading in securities.

4.71.2 If due to any technical reason or otherwise, continuous trading on stock exchanges is disrupted, it is of paramount importance that not only all market participants including other MIIs, are promptly informed about the outage but also the trading hours are extended, if required, so as to provide opportunity for smooth closure of intraday positions.

4.71.3 With a view to ensure that any outage at stock exchange(s) is handled in a harmonized and consistent manner, the matter was discussed with the MIIs and Standard Operating Procedure with regard to handling of such stock exchange outage in Cash Market and Equity Derivatives segment is detailed below.

Definition of Stock Exchange Outage

4.71.4 Stock Exchange Outage shall mean stoppage of continuous trading, either suo moto by exchange or by virtue of reasons beyond control of stock exchange. Further, stoppage of continuous trading shall not include trading halt on account of index based market-wide circuit breaker.

Reporting Requirements for outage

[238] Reference: SEBI Circular SEBI/HO/MRD-TPD-1/CIR/P/2023/7 dated January 09, 2023

4.71.5 The stock exchange that suffered the outage (referred to as affected stock exchange) shall intimate about the outage to various stakeholders as mentioned below:

Sl. No.	Communication to	Reporting
1.	Market Participants/ Trading Members/ Other MIIs	• Immediate but not later than 15 minutes from occurrence of outage. Through broadcast message and by publishing on its website
2.	SEBI	• Immediate after occurrence of outage. Through an email to dedicated email id : techglitch@sebi.gov.in

4.71.6 Further, the affected stock exchange shall update about the ongoing outage in the time intervals of 45 minutes from the initial intimation, as mentioned at **Para 4.71.5** above, until normalcy to operations is restored. Extension of trading hours, if applicable (as mentioned subsequently from **Para 4.71.10 to 4.71.16**), shall be mentioned in the intimation by the affected stock exchange.

Trading on unaffected segment(s) / exchanges and Resumption of trading on affected stock exchange

4.71.7 In the event of disruption of trading in one or more market segments of affected stock exchange, qualifying as outage, trading in other unaffected segments of the affected exchange shall continue and all other unaffected exchanges shall continue to trade in all of their market segments.

4.71.8 Affected stock exchange would restore operations to normalcy at the earliest including from the Disaster Recovery Site and carry out various activities, in terms of **Para 4.31** on **Business Continuity Planning (BCP) and Disaster Recovery (DR)** and **Para 4.70** on **Standard Operating Procedure for handling of technical glitches by Market Infrastructure Institutions (MIIs) and payment of "Financial Disincentives" thereof, as applicable**.

4.71.9 A pre-opening session similar to normal pre-opening session would be conducted for effective price discovery, before resumption of trading. Further, there shall be an advance intimation of at least 15 minutes to various market participants with regard to resumption of trading or start of pre-opening session, as applicable.

Extension of trading hours in case of outage

4.71.10 If the trading on the affected stock exchange resumes to normalcy at least one hour (excluding 15 minutes of pre-opening session, if applicable) before the normal scheduled market closure, trading hours on that day for all stock exchanges would remain unchanged.

4.71.11 If the trading on the affected stock exchange does not resume to normalcy even one hour (excluding 15 minutes of pre-opening session, if applicable) before the

scheduled market closure, trading hours for all stock exchanges would automatically get extended for additional one and half hours for that day and the same would be intimated by the affected stock exchange to market participants, other MIIs and SEBI latest by one hour fifteen minutes before the normal scheduled market closure. Subsequent to the communication from the affected stock exchange, the unaffected stock exchanges would also suitably issue a notice with regard to extension of trading hours on their stock exchanges.

4.71.12 If the trading on the affected stock exchange does not resume to normalcy even 45 minutes (excluding 15 minutes of pre-opening session, if applicable) post normal scheduled market closure, in the case of extension of trading hours, no further trading would be allowed on the affected stock exchange for that day and other stock exchanges would continue to operate till the extended time provided at **Para 4.71.11** above to enable smooth closure/settlement of intraday positions. The affected exchange would have to suitably intimate the same to market participants, other MIIs and SEBI latest by 45 minutes post normal scheduled market closure.

4.71.13 If the occurrence of outage as mentioned in **Para 4.71.4** above, happens during the last trading hour of normal operation and latest before 15 minutes of normal scheduled market closure, trading hours for all stock exchanges would automatically get extended by one and half hours for that day and the same would be intimated by the affected stock exchange to market participants, other MIIs and SEBI immediately but not later than 10 minutes from the occurrence of outage. Subsequent to the communication from the affected stock exchange, the unaffected stock exchanges would also suitably issue a notice with regard to extension of trading hours on their stock exchanges.

4.71.14 Exchanges to put in place a common close out policy, to ensure uniform methodology of settlement of open positions, in case continuous trading didn't happen in Cash Market or Equity Derivative Segment of the exchange during last half an hour of trading for the day due to outage.

4.71.15 Extension of trading hours, if any, for Cash Market would result in equivalent extension of trading hours in Equity Derivative Segment and vice versa, provided trading hours at the start of the day are aligned for both Cash Market and Equity Derivative Segment. Further, Extension of trading hours in the Cash Market would also result in equivalent extension to other secondary market mechanisms conducted during trading hours such as Offer For Sale, Buy back etc.

4.71.16 For illustration, a few scenarios pertaining to extension of trading hours are tabulated herewith with the assumptions that trading hours for two exchanges A and B in Cash Market and Equity Derivative Segment, at start of the day, are from

09:15 to 15:30 (i.e. excluding pre-opening and post-closing session) and all segments of exchange B are operating unaffected.

S No	Occurrence of outage	Event	Extension of trading hours
1	In Equity Derivative Segment of exchange A	Normalcy in the said segment restored latest by 14:30	No extension of trading hours for exchange A and B
2	In Cash Market of exchange A	Start of Pre-opening latest by 14:15	No extension of trading hours for exchange A and B
3	Any time during the trading hours in Cash Market on exchange A	Failure to start Preopening by 14:15 on exchange A	Trading hours in Cash Market and Equity Derivative Segment of exchange A and B extended till 17:00 and announcement in this regard to be made latest by 14:15 by the affected stock exchange. Note that such announcement is to be made on the basis of assessment by stock exchange on the likely resumption of normalcy
		Failure to start Preopening by 16:00 on exchange A	No trading permitted in Cash Market on exchange A for the day. Equity Derivative Segment on exchange A and Cash Market and Equity Derivative Segment on exchange B would continue to trade till 17:00. The affected stock exchange to announce latest by 16:15
4	At 15:05 on exchange A in Cash Market		Trading hours in Cash Market and Equity Derivative Segment of exchange A and B extended till 17:00 and announcement to be made by affected stock exchange within 10 minutes of occurrence of outage i.e. by 15:15
5	At 15:16 on exchange A in Cash Market		No extension of trading hours for exchange A and B

Updation of BCP document of MII

4.71.17 MIIs shall update their BCP document and submit the same to SEBI subsequent to approval of their Governing Boards within 2 months from January 9, 2023

4.71.18 This shall come into effect without prejudice to the 'Guidelines for Business Continuity Plan (BCP) and Disaster Recovery (DR) of Market Infrastructure Institutions (MIIs)' and 'Standard Operating Procedure for handling of technical

glitches by Market Infrastructure Institutions (MIIs) and Payment of "Financial Disincentives" thereof' respectively.

4.72 Standard Operating Procedure (SOP) for Reporting of Cyber Security Incidents/ breaches/ deficiencies by MIIs and Imposition of "Financial Disincentive [239]

Background

4.72.1 Stock exchanges, Depositories and Clearing Corporations are collectively referred to as securities Market Infrastructure Institutions (MIIs). These institutions are systemically important for the country's financial development and provide the infrastructure necessary for the securities market. A smooth and uninterrupted functioning of operations of the MIIs is essential for ensuring the continuity of the securities market. It is, therefore, critical for the MIIs to constantly monitor the performance of their internal processes and systems and upgrade/ enhance their systems with respect to cyber security and cyber resilience so as to eliminate cyber security deficiencies and prevent or minimize the possibility of a cyber security breach.

4.72.2 However, incidents of technical and administrative lapses at MIIs were observed some of which have arisen due to non-compliance with the extant regulatory framework for cyber security and cyber resilience and which have hindered the smooth functioning of the MIIs and threatened the continuity of the securities market. In the event of such incidents, it should be incumbent on MIIs to address cyber security deficiencies and breaches in a timely manner by taking appropriate corrective actions. It was also observed that the MIIs were non-compliant with the extant regulatory framework for cyber security and cyber resilience in the cyber audit reports and reports from other agencies.

4.72.3 It is decided to levy a "Financial Disincentive" on MIIs in the event of the following cases:

4.72.3.1 Non-compliance with the extant cyber security regulations and guidelines resulting in cyber security breaches, cyber-attacks, cyber security deficiencies or any other cyber security incidents

4.72.3.2 Lackadaisical approach or undue delay in addressing cyber security deficiencies and breaches

4.72.3.3 Non-reporting/ delay in reporting a cyber security incident/ breach

The intent of this financial disincentive is to encourage MIIs to constantly monitor the performance of their systems and upgrade/ enhance their systems so as to

[239] Reference: SEBI Letter SEBI/HO/MRD/CSC/OW/P/2019/22202/1 dated August 28, 2019

eliminate cyber security deficiencies and prevent or minimize the possibility of a cyber security breach.

4.72.4 In this regard, an SOP for reporting of cyber security breaches and deficiencies by MIIs and imposition of "Financial Disincentive" is placed below for information and necessary compliance.

Definitions

4.72.5 "Cyber security deficiency" shall be defined as loophole, vulnerability or non-compliance observed in

a. The MII's stated internal cyber security policy/cyber security protocol/operational guidelines/information security practices or
b. The cyber security guidelines specified by SEBI from time to time

which threatens or compromises the security, confidentiality, integrity or availability of the MII's computer resource or cyber assets.

4.72.6 *"Cyber security incident"* shall be defined as any real or suspected adverse event in relation to cyber security that violates, explicitly, implicitly, applicable cyber security policy resulting in unauthorized access, denial of service or disruption, unauthorized use of computer resource for processing or storage of information or changes to data or information without authorization.

4.72.7 "Cyber security breach" shall be defined as any incident or security violation that results in unauthorized or illegitimate access or use by a person as well as an entity, of data, applications, services, networks and/or devices through bypass of the underlying cyber security protocols, policies and mechanisms resulting in the compromise of the confidentiality, integrity or availability of data/information maintained in a computer resource or cyber asset. A cyber security breach is a subset security incident.

4.72.8 "Information security practices" shall be defined as implementation of cyber security policies and standards in order to minimize the cyber security incidents and cyber security breaches.

4.72.9 "Cyber security policy" shall be defined as a set of documented business rules and processes for protecting information and the computer resource.

4.72.10 "Cyber security protocol" shall be defined as the official procedure or system of rules governing the cyber security operations of a MII. The cyber security protocol is usually as subset of the cyber security policy.

4.72.11 *"Operational guidelines"* refers to any additional set of rules and procedures issued internally by a MII that compliments its cyber security protocol and information security practices.

Reporting Requirements

4.72.12 The following reporting structure for cyber security deficiencies / breach shall be adopted by the MIIs:

S. No.	Issue	Reporting
1.	Cyber Security Breach / Incident	• CERT-In • SEBI's Cyber Security Cell • Standing Committee on Technology of the MII • Governing Board of the MII
2.	Cyber Security Deficiencies	• Standing Committee on Technology of the MII • Governing Board of the MII • SEBI's Cyber Security Cell

Cases for levy of "Financial Disincentive"

4.72.13 The "Financial Disincentives" shall be levied in the following cases:

4.72.13.1 Cyber Security breaches, cyber-attacks and any other cyber security incidents occurring on account of non-compliance of SEBI cyber security policies and guidelines and delay in reporting the Root Cause Analysis to SEBI in case of breaches, attacks and incidents.

For the above, a "Financial Disincentive of Rs.10,000,00/- {ten lakhs} shall be levied for

i. each such cyber security breach, cyber-attack or any other cyber security incident on account of non-compliance of SEBI cyber security policies and guidelines

ii. delay in reporting the Root Cause Analysis to SEBI in case such breaches, attacks and incidents.

iii. for cyber security breaches, cyber-attacks and any other cyber security incidents occurring otherwise and where there is a delay in submission of the RCA reports.

SEBI prescribed a time period of two weeks from the date of the incident for submission of RCA reports.

4.72.13.2 Cyber Security deficiencies occurring on account of non-compliance of SEBI cyber security policies and guidelines observed during biannual cyber security audits mandated under **Para 4.82** or reports from other agencies.

For the above, a "Financial Disincentive" of Rs.500,000/- {five lakhs} shall be levied for each such deficiency from the date of the report.

4.72.13.3 A cyber security breach / incident should be reported as soon as it is discovered as per the reporting structure specified at **Para 4.72.12**. A "Financial Disincentive" of INR 10,000,00/- {ten lakhs} shall be levied on those MIIs that

i. Do not report a cyber security breach/incident, or

ii. Delay the reporting of the cyber security breach/incident

4.72.13.4 Failure to timely address the cyber security deficiencies / breaches within the deadline set by SEBI/ HPSC-CS. The progressive slab-wise structure for imposition of "Financial Disincentives" shall be followed from the expiry of the deadline specified by SEBI/ HPSC-CS.

No. of working days post the stated deadline during which the deficiency / cause of breach is not addressed	**"Financial Disincentive" (Rs) per working day**
First 15 working days	1 lakh per working day
Subsequent 15 working days	2 lakh per working day
Subsequent working days	5 lakh per working day

4.72.14 Notwithstanding the reporting structure mentioned at **Para 4.72.12** above, the penalties would start being levied by SEBI at **Para 4.72.13.**

Proceeds to be credited to SEBI's IPEF

4.72.15 Further, with view to making such "Financial Disincentives" effective and meaningful, the amount realized from the same may be credited to the "Investor Protection and Education Fund" of SEBI in accordance with Section 11(1) of SEBI Act, 1992 read with Regulation 4(1)(j) of the Securities and Exchange Board of India (IPEF) Regulations, 2009, which is as follows:

Amounts to be credited to the Fund.

"4. (1) The following amounts shall be credited to the Fund:-

(a)…

(b)…

(j) such other amount as the Board may specify in the interest of investors."

4.72.16 The "Financial Disincentive" specified above shall continue to accrue till the time the issue has been addressed by the MII by taking appropriate corrective actions and the same has been validated by an independent third party.

4.72.17 The amount of "Financial Disincentive" realized as per the above structure shall be credited by MII to Investor Protection and Education Fund administered by SEBI as mentioned at **Para 4.72.15**.

4.72.18 Imposition of aforesaid "Financial Disincentive" shall be irrespective of any other action(s) initiated/taken by SEBI.

4.73 Implementation of Cyber Capability Index[240]

[240] Reference: SEBI Letter SEBI/HO/MRD/CSC/OW/P/2019/28527/1 dated October 30, 2019, SEBI/HO/MRD/CSC/OW/P/2019/28517/1 dated October 30, 2019 and SEBI MRD email dated November 04, 2019

4.73.1 SEBI issued cyber-security framework/guidelines to be implemented by all the MIIs. In this regard, SEBI developed a Cyber Capability Index to gauge the cyber security preparedness of the MIIs. The index consists of the below mentioned domains:

4.73.1.1 Governance of Critical Infrastructure and Personnel

4.73.1.2 Identification of Critical Assets and Risks

4.73.1.3 Protection of Critical Assets and Infrastructure

4.73.1.4 Monitoring and Detection of Critical Assets/ Infrastructure and Detection of Intrusion/ Unauthorized Access

4.73.1.5 Response and Recovery

4.73.1.6 Sharing of Information

4.73.1.7 Training

4.73.1.8 Periodic Audit

4.73.2 Each of the eight domains contains a structured set of parameters. Each set of parameters shall determine the extent/level to which the organization has matured with respect to cyber security and cyber resilience in that domain.

4.73.3 Depositories are advised to rate itself on Cyber Capability Index based on the rating framework (given below) on a quarterly basis. Depositories are required to submit the score of the index and detailed breakup to its Standing Committee on Technology (SCOT) and its Governing board. The report on the completed maturity index rating is then required to be submitted to SEBI.

4.73.4 Depositories are requested to rate itself every quarter and submit the report to SEBI by 30th of subsequent quarter.

Please find Annexures containing the following:

a. **Annexure 29** - "MIL" containing Maturity Indicator Levels (MILs) &

b. **Annexure 30** -"Calculation" containing the illustration for Index calculation

Index Calculation Methodology

4.73.5 The parameters for evaluation of cyber security and cyber resilience of a Market Infrastructure Institution (MII), as specified in **Para 4.31**, have been divided into 8 domains:

4.73.5.1 Governance of Critical Infrastructure and Personnel

4.73.5.2 Identification of critical assets and risks

4.73.5.3 Protection of Critical Assets and Infrastructure

4.73.5.4 Monitoring and Detection of Critical Assets/ Infrastructure and Detection of Intrusion/ Unauthorized Access

4.73.5.5 Response and Recovery

4.73.5.6 Sharing of information

4.73.5.7 Training

4.73.5.8 Periodic Audit

4.73.6 Each parameter has various Maturity Indicator Levels (MIL). The MII shall apply a MIL independently to each parameter within a domain/ sub-domain. A MII aspiring to achieve the highest MIL for each and every parameter and therefore the highest possible score within a Domain, would be an ideal scenario.

4.73.7 MIL 1 represents non-compliance with the parameter and therefore shall be assigned a value of zero. At MIL 2 (for most parameters), only the initial set of practices for the parameter is expected. However, the MII should not be hindered from undertaking additional practices to achieve higher MILs for that parameter. MIL 2 shall be assigned a score of 1, MIL 3 shall be assigned a score of 2 and so on (i.e. MIL <n> shall have a score of (n-1)).

4.73.8 For the purpose of being evaluated and rated on the Cyber Capability Index, a MII has to fulfill the minimum cut-off score for each of the 8 domains and 9 sub-domains. A MII is declared "Fail" in the evaluation process when it scores below the cut-off in at least one Domain/Sub-Domain, even if the overall index score is greater than or equal to 50.

4.73.9 The Domain-wise minimum cut-off scores and weightages in the index have been provided in the worksheet "Calculation" in the excel file. The worksheet contains three sample index scores and their calculations:

a. Index on maximum permissible score for every parameter (100)
b. Index on minimum cut-off score for every parameter (50)
c. Index on a random sample score for every parameter (89.02)

4.73.10 The formula for calculation of the Cyber Capability Index is as follows:

$$\text{Index} = \sum (ScoreParameter_i * Weight_i\ (\%) * 100ii / MaxParameter_i)$$

where i ranges from 1 to 53

$ScoreParameter_i$ *is the score of the MII for that parameter*

$Weight_i\ (\%)$ is the weightage, in percentage, of the parameter in the index

$MaxParameter_i$ is the maximum permissible value of that parameter

Score based Rating

4.73.11 Based on the value of the index, the cyber security maturity level of the MIIs shall be determined as follows:

S. No.	Rating	Index Score Range
1	Exceptional Cyber Security Maturity	90-100
2	Optimal Cyber Security Maturity	80-90
3	Manageable Cyber Security Maturity	70-80
4	Developing Cyber Security Maturity	60-70
5	Bare Minimum Cyber Security Maturity	50-60

S. No.	Rating	Index Score Range
6	FAIL	Not applicable as the MII has scored below the cut-off in at least one Domain / Sub-Domain

4.73.12 Based on the sample index scores calculated in the worksheet and the abovementioned details, the sample scores would be categorized as follows (for illustrative purposes):

S. No.	Rating	Index Score
1	Exceptional Cyber Security Maturity	100
2	Optimal Cyber Security Maturity	89.02
3	Bare Minimum Cyber Security Maturity	50

Action Point

4.73.13 Depositories are advised to rate their systems and processes on the Cyber Capability Index on a quarterly basis. Additionally, they are required to submit their quarterly index scores along with the detailed breakup to their Standing Committee on Technology (SCOT) and their Governing Board.

4.73.14 Depositories are advised to commence the rating exercise from the quarter ending September 30, 2019. Thereafter, the rating exercise shall be done every quarter and the corresponding reports shall be submitted within 30 calendar days of the end of that quarter.

4.74 Advisory for SEBI Regulated Entities (REs) regarding Cybersecurity best practices[241]

Kindly refer **Para 2.31** above in respect of Advisory for SEBI Regulated Entities (REs) regarding Cybersecurity best practices.

4.75 Norms for Scheme of Arrangement by unlisted Stock Exchanges, Clearing Corporations and Depositories[242]

4.75.1 To harmonize and bring uniformity in the norms related to scheme of arrangement for unlisted MIIs in line with provisions currently applicable to listed MIIs, comments of unlisted MIIs were sought and the matter was deliberated in Secondary Market Advisory Committee (SMAC). Taking into account the recommendations of SMAC, the framework for Scheme of Arrangement by unlisted MIIs has been introduced.

4.75.2 The detailed framework for scheme of arrangement by unlisted MIIs is given as under:

[241] Reference: SEBI Circular SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/032 dated February 22, 2023
[242] Reference: SEBI Circular SEBI/HO/MRD/MRD-PoD-3/P/CIR/2023/45 dated March 28, 2023

4.75.2.1 The unlisted MII desirous of undertaking a scheme of arrangement or involved in a scheme of arrangement as per the provisions of Companies Act 2013 shall file the draft scheme of arrangement along with a non-refundable fee with SEBI for obtaining the observation letter or no-objection letter, before filing such scheme with any Court or Tribunal, in terms of requirements specified by SEBI from time to time.

4.75.2.2 The unlisted MII shall pay a fee to SEBI at the rate of 0.1% of the paid-up share capital of the unlisted or transferee or resulting company, whichever is higher, post sanction of the proposed scheme, subject to a cap of INR 5,00,000.

4.75.2.3 The provisions may not apply to schemes which solely provide for merger of a wholly owned subsidiary or its division with the parent company. However, such draft schemes shall be filed with SEBI for the purpose of disclosures and the same shall be disseminated on the websites of the unlisted MII.

4.75.3 **Information to be provided to SEBI:**

4.75.3.1 The unlisted MIIs shall provide the following information to SEBI while filing the draft scheme of arrangement for obtaining the observation letter or no objection letter:

(b) The Draft Scheme of Arrangement or Amalgamation or Merger or Demerger or Reconstruction or Reduction of Capital, etc. (hereinafter referred as "Scheme")

(c) Approval of the governing board of the unlisted MII for the proposed Scheme.

(d) Valuation Report provided by an independent registered valuer, accompanied with an undertaking from the unlisted MII stating that no material event impacting the valuation has occurred during the last 6 months. The Valuation Report is required to be placed before the Audit Committee of the unlisted MII.

For the purpose of this clause, the Registered Valuer shall be a person, registered as a valuer, having such qualifications and experience and being a member of an organization recognized, as specified in Section 247 of the Companies Act, 2013 read with the applicable Rules issued thereunder.

(e) Report from the Audit Committee recommending the draft Scheme, taking into consideration, *inter-alia*, the Valuation Report, and also having comments on the following:

i. Need for the Scheme

ii. Rationale of the Scheme

iii. Synergies of business of the entities involved in the Scheme

iv. Impact of the Scheme on the shareholders.

v. Cost benefit analysis of the Scheme.

(f) Fairness opinion on valuation of assets or shares done by the valuer for the unlisted MII shall be taken from an independent SEBI registered Merchant Banker.

(g) Shareholding pattern of the unlisted MII pre and post the Scheme.

(h) Audited financials of last 3 years (financials not being more than 6 months old) of unlisted entities.

(i) Auditor's Certificate stating that the accounting treatment contained in the Scheme is in compliance with all the Accounting Standards specified by the Central Government under Section 133 of the Companies Act, 2013 read with the rules framed thereunder or the Accounting Standards issued by ICAI, as applicable, and other generally accepted accounting principles.

(j) Declaration from the unlisted MII on any past defaults of debt obligations (including listed debt, if any) of the entities forming part of the Scheme.

(k) No Objection Certificate (NOC) from the lending scheduled commercial banks or financial institutions or debenture trustees, in case the unlisted MII or entities forming part of the Scheme have any outstanding debt obligation.

(l) Report on Complaints containing the details of complaints or comments received by it on the proposed Scheme from various sources (complaints or comments received directly or forwarded by SEBI or any other agency) as per **Annexure 31**.

(m) Detailed Compliance Report as per the format specified at **Annexure 32** duly certified by the Company Secretary, Chief Financial Officer and the Managing Director, confirming compliance with various regulatory requirements specified for the Scheme and all accounting standards.

(n) The unlisted MII shall ensure that all dues to, and fines or penalties imposed by SEBI or any other agency have been paid or settled before filing the draft Scheme. In case of unpaid dues or fines or penalties, the unlisted entity shall submit to SEBI a 'Report on the Unpaid Dues' which shall contain the details of such unpaid dues in the format given at **Annexure 33**, prior to filing the draft Scheme.

(o) The unlisted MII shall provide the information regarding any pending proceedings or litigations against the unlisted MII or entities forming part of the Scheme and the liabilities thereof, if any.

(p) Immediately upon filing of the draft Scheme with SEBI, the unlisted MII shall disclose the draft Scheme along with all relevant documents on its website.

(q) Subsequent to filing the draft Scheme with SEBI, no changes to the draft Scheme, except those mandated by the regulators or authorities or court or tribunal, shall be made without specific written consent of SEBI.

4.75.3.2 The valuation report referred to in Para 4.75.3.1(c) above and the fairness opinion referred to in Para 4.75.3.1 (e) above shall be provided by a Registered Valuer and Independent SEBI Registered Merchant Banker respectively. The Registered Valuer and the merchant banker referred therein shall not be treated as independent in case of existence of any conflict of interest among themselves or with the company, including that of common directorships or partnerships.

4.75.4 **Processing of the Draft Scheme by SEBI**

4.75.4.1 Upon receipt of the application from the unlisted MII, SEBI shall provide its observation letter or no-objection letter on the draft Scheme to the MII. While processing the draft Scheme, SEBI may seek clarifications from any person relevant in this regard including the unlisted MII and if required, may also seek an opinion from an Independent Chartered Accountant.

4.75.4.2 SEBI shall endeavour to provide its observation letter or no-objection letter on the draft Scheme within 30 days from the later of the following:

(a) date of receipt of satisfactory reply on clarifications, if any, sought from the unlisted MII; or

(b) date of receipt of opinion from Independent Chartered Accountant, if any, sought by SEBI; or

(c) All complaints or comments received by SEBI on the draft Scheme, if any, shall be forwarded to the unlisted MII, for necessary action and resolution of the same.

4.75.5 **Validity of observation letter or no-objection letter:** The validity of the observation letter or no-objection letter of SEBI shall be for six months from the date of issuance, within which the Scheme shall be filed with any Court or Tribunal, as required, for approval.

4.76 Procedures for ensuring compliance with Securities Contracts (Regulation) (Stock Exchanges and Clearing Corporations) Regulations, 2018 (SECC Regulations) by Listed Stock Exchanges[243]

4.76.1 Regulation 45 of the SECC Regulations provides for listing of stock exchanges. As per Regulation 45(1) of the SECC Regulations, the Board may specify such conditions as it may deem fit in the interest of the securities market.

4.76.2 Accordingly, it has been decided to prescribe the following modalities so as to ensure compliance with the provisions of SECC Regulations:

4.76.2.1 **Ensuring holding of 51 per cent by public at all times by the listed stock exchange:**

[243] Reference: SEBI Circular MRD/DSA/01/2016 dated January 01, 2016

4.76.2.1.1 The listed stock exchange shall disseminate the details of its shareholding with category wise breakup, on a continuous basis, on its website. Similarly, the stock exchange where the shares are listed, shall also display the above information.

4.76.2.1.2 The depositories shall put in place necessary system to ensure that the shareholding of trading members or their associates and agents does not exceed 49 per cent. For this purpose, the depositories shall put in place systems for capturing the shareholding data of trading members or their associates and agents and ensure that there is a mechanism for coordination between the depositories towards sharing of information. The depositories shall also monitor the aggregate shareholding limit of the trading members or their associates and agents based on their demat balance, on a daily basis, at the end of the day. The stock exchange where the shares are listed shall share a list of all trading members or their associates and agents with the depositories to facilitate monitoring of demat balances.

4.76.2.1.3 The trading members or their associates and agents shall obtain prior approval of the listed stock exchange for further acquisition of shares, once the aggregate shareholding of the trading members or their associates and agents crosses the limit of 45 per cent. The trading members or their associates and agents shall refer to the shareholding pattern under the category of trading members or their associates and agents, to determine/ascertain the available head room before placing the order.

4.76.2.1.4 In the event of trading members or their associates and agents making purchases without requisite approval as stated above, the depositories shall initiate consequential action such as freezing of voting rights and all corporate benefits in respect of such shareholding till the time the same is divested.

4.76.2.1.5 The divestment of any excess shareholding beyond the specified limit would be through a special window provided by the stock exchange where the shares of the stock exchange are listed.

4.76.2.2 **Ensuring shareholding threshold of 5 per cent or 15 per cent as the case may be in terms of SECC Regulations:**

4.76.2.2.1 The depositories shall put in place a mechanism to ensure that no shareholder of listed stock exchange gets credit of shares beyond 5 per cent or 15 per cent, as applicable. The depositories shall generate an alert when such holding exceeds 2 per cent and monitor the same under intimation to SEBI.

4.76.2.2.2 The Depository would inform the listed stock exchange as and when threshold limit is breached and take consequential action such as freezing of voting rights and all corporate actions in respect of such excess holding till the same is divested through the special window.

4.76.3 The stock exchanges, both listed and where the securities are listed, and depositories shall ensure that aforesaid mechanism is in place.

4.77 Measures to strengthen tracking and reporting of delay in pay-in/pay-out for rolling settlement[244]

4.77.1 SEBI carried out review of existing SOP with regard to tracking of instances of delay in normal rolling settlement and reporting thereof to SEBI along with the joint monthly report submitted by the CCs/depositories.

4.77.2 The Competent Authority has approved the following measures subsequent to the aforesaid review to strengthen tracking of intermediate activities in rolling settlement and reporting of settlement delays. This is without prejudice to financial disincentives, if any, emanating from delay in completion of pay-in/pay-out activities.

4.77.3 **For tracking of intermediate activities constituting rolling settlement**

4.77.3.1 CCs and Depositories may put in place systems to ensure:

4.77.3.1.1 All intermediate activities that may impact rolling settlement (i.e. from trade date to settlement) are streamlined and the process flow is optimized. If there are dependencies / data shared with other CC/Depository, discussions may be done with the concerned CC / Depository with regard to optimization. Further, all intermediate activities are time stamped with start and finish time of the activity.

4.77.3.1.2 Such intermediate activities are defined along with outer timelines for each activity after discussion with the concerned stakeholders such as members/participants, DVP agent, participating banks, other Market Infrastructure Institutions (MIIs) etc. to achieve final pay-in and pay-out within SEBI stipulated timelines.

4.77.3.1.3 Process flow and associated timelines, so decided, are intimated to all the stakeholders and delay in completion of any of these activities, should be traceable and attributable to one or more entity / MII, as the case may be.

4.77.3.1.4 Procedures to handle various exceptions i.e. scenarios that could result in settlement delay are documented along with the steps to be taken towards completing settlement processes at the earliest in case of exceptions.

[244] Reference: SEBI Email dated January 31, 2022

4.77.3.2 On the basis of the aforesaid, CCs and Depositories may separately prepare a Comprehensive Standard Operating Procedure (CSOP) which is mutually agreed upon by other CCs and Depositories as far as all the timelines and exception handling are concerned. This CSOP would be submitted to SEBI after approval of the Governing Boards of CCs and Depositories.

4.77.3.3 Further, the said CSOP shall also cover action points emanating from 9.4.4 below and would be reviewed periodically by the MIIs to incorporate any regulatory/system changes.

4.77.4 **For reporting of Delay in rolling settlement cycle**

4.77.4.1 In case of delay in completion of any of the intermediate activities beyond their pre-agreed time, the respective CCs/Depositories would inform the impacting CCs/Depositories regarding delay in completion of the intermediate activity at their end on immediate basis.

4.77.4.2 CCs shall intimate delay in settlement beyond the stipulated timelines for settlement for rolling settlement to SEBI (under intimation to depositories). This intimation should be given within one hour of such SEBI stipulated timelines and should inter-alia mention - reasons for delay, entity/MII responsible for the delay and likely completion time of the settlement process.

4.77.4.3 CCs and Depositories shall submit a separate report to SEBI, on a monthly basis (from February 2022 onwards, replacing the existing joint monthly report), wherein following details are inter-alia provided:

4.77.4.3.1 Day wise completion time for pay-in and pay-out activities

4.77.4.3.2 Details about settlement delays for the month

4.77.4.3.3 Intermediate activity that caused the delay and reason(s) thereof

4.77.4.3.4 Steps taken to address the root cause of the issue

4.77.4.3.5 Review of instances of delay to understand areas of improvement etc.

4.77.4.4 CCs / Depositories would also submit a report to their Governing Boards on quarterly basis with regard to instances of delay attributable to them in the said quarter. If settlement delay is on account of technical reasons, findings are to be evaluated by the SCOT of the CC / Depository before referring to the Governing Board. The report would inter-alia include the details of individual instances of settlement delay along with reasons thereof and corrective / preventive actions taken

4.78 ***<u>Advisory on Security Patch Management Policy</u>***[245]

4.78.1 All the MIIs are advised to ensure the following:

4.78.1.1 The security patch management policy is audited by an external auditor.

[245] Reference: SEBI Email dated September 12, 2022

4.78.1.2 Appropriate changes, if necessary, are made to the existing policy on security patch management.

4.79 ***Strengthening Resiliency of Websites of Stock Exchanges, Clearing Corporations and Depositories (MIIs)*** [246]

4.79.1 MII shall take necessary steps to ensure that its website(s) are resilient to cyber-attack(s).

4.79.2 Redundant websites: MII shall host its website(s) at multiple DNS (Domain Naming Servers) and hosts. MII shall put-in place suitable systems to switch to alternate website(s) hosted on a different DNS / hosts in the event of a cyber-attack on its primary website(s) and at the same time, shall take necessary steps to recover from the cyber-attack on the its primary website(s).

4.79.3 Web Application Firewall (WAF): MII shall mandatorily deploy Web Application firewalls of demonstrated capabilities.

4.79.4 Continuous monitoring of the website(s): MII shall deploy suitable and adequate resources for 24x7 monitoring of its website(s), including monitoring of their website(s) through the SOCs (Security Operations Center).

4.79.5 MII shall periodically conduct penetration testing of its website(s) and related systems, at the minimum, once in a calendar year.

4.79.6 In cases where services of 3rd party vendors / service providers are availed by the MII for hosting of its website(s) and for other related areas, MII shall ensure that the cyber security and resilience framework of such 3rd party vendors / service providers are as per the requirements specified by SEBI for MIIs. Further, MII shall include audit of the cyber security and resilience framework of such 3rd party vendors / service providers (limited to the services availed by MIIs) in the scope of its annual system audit.

4.79.7 MII shall implement the principles mentioned in the 'Guidelines for Indian Government Websites' developed by National Informatics Centre (NIC) and adopted by Department of Administrative reforms and Public Grievances (DARPG) on the areas of 'Website Hosting', 'Website Management', 'Development', etc. The said guidelines are available at ***http://web.guidelines.gov.in/assets/documents/pdf/hand_book.pdf***

4.79.8 MII shall frame and implement a Web Server Security Policy that should cover Network and Host Security Policy, Web Server Backup and Logging Policy, Web Server Administration and Updation Policy, Classification of documents to be published on Web Server, Password Management Policy, Encryption Policy, and Physical Security

4.79.9 In addition to the above, MIIs shall ensure implementation of the following:

[246] Reference: SEBI Letter SEBI/HO/MRD/DSA/OW/P/2016/31948 dated November 24, 2016 captioned "Strengthening Resiliency of Websites of Stock Exchanges, Clearing Corporations and Depositories (MIIs)"

4.79.9.1 MIIs shall advise their auditors to give additional emphasis on the Application Security audit.

4.79.9.2 MIIs shall include suitable IT / Cyber security related certifications requirements in the criteria for selection of software developers / vendors.

4.79.9.3 MIIs shall ensure that their software vendors undertake security audit of their systems on a periodic basis (at least once a year).

4.80 Bolstering Cyber Resiliency[247]

4.80.1 In order to bolster cyber resiliency MIIs should take following steps:

4.80.1.1 In addition to the current detection and prevention tools deployed at the MIIs for Network Traffic Analysis and other SIEM solutions, MIIs should start using User and Entity Behaviour Analytics (UEBA) tools for combating cyber threats.

4.80.1.2 The Indian-CERT has set-up a Cyber Swachhta Kendra for analyzing BOTs/malware characteristics and providing information and enabling citizens for removal of BOTs/malware. MIIs should share their public facing IPs with the Cyber Swachhta Kendra for monitoring purposes.

4.80.1.3 The Standing Committee on Technology (SCOT) of Exchanges and Clearing Corporations and the IT Strategy Committees (IT-CS) of Depositories should on a quarterly basis review the cyber security preparedness of the respective MIIs and also appraise the Board of MII regarding the same.

4.80.1.4 MIIs should place the details of Cyber-threat vectors and Cyber-attack scenarios and the corresponding action plan / steps taken to manage such threat vectors and scenarios, before its SCOT or IT-CS for assessing the adequacy of steps taken / efficacy of plans and further improvements. Thereafter, the MII should place a report in this regard before its Board before submitting the same to SEBI.

4.80.1.5 In addition to the periodic vulnerability assessment and penetration testing conducted by MIIs to evaluate security posture of the MII, the MIIs should also conduct periodic table-top exercises, mock drills, etc. to improve its preparedness to handle cyber breach/incident. Such exercises should be followed-up with a detailed review before its SCOT or IT-CS.

4.81 Advisory on Cyber Audit and VAPT[248]

With regard to the cyber audit of the MIIs, the following needs to be ensured by the MIIs:

4.81.1 All MIIs should update the scope of the audit as and when any guidelines or advisory related to cyber security is issued by SEBI.

---

[247] Reference: SEBI Email dated November 11, 2017 captioned Bolstering Cyber Resiliency

[248] Reference: SEBI Email dated December 28, 2022

4.81.2 During cyber audit, evidence should be collected by inspecting physical assets, records/documents, testing of relevant systems, relevant system generated reports etc. in order to ascertain the compliance of various controls defined by SEBI.

4.81.3 The cyber audit report is to be submitted in the Standardized format placed below as **Annexure 34**.

4.81.4 Along with cyber audit reports, all MIIs are required to submit to SEBI the comments of their SCOT and Governing Board.

4.81.5 Scope of cyber audit shall also include testing the functional efficacy of the SOC.

4.81.6 VAPT exercise shall cover all possible ingress and egress points including broker ICT setup, co-location facility etc.

4.81.7 All MIIs shall conduct Periodic Training for the concerned employees regarding Cyber Security in line with **Para 4.41** and the same has to be checked by the Auditors during cyber audit.

4.81.8 The audit report shall include control wise compliance of all SEBI circulars/advisories along with the evidences.

4.81.9 All MIIs are advised to include the directions issued by SEBI pursuant to discussion in HPSC-CS in their regular bi-annual cyber audit.

4.81.10 In order to ascertain the compliance of **Para 4.41.7.11** regarding identification of critical assets, process of identification of critical assets and its implementation should be assessed during cyber audit.

4.81.11 In order to ascertain the compliance of **Para 4.41.7.40**, whether minimum baseline standards followed for conducting VAPT are in line with the scope defined by SEBI should be checked during cyber audit. Minimum baseline standards defined by SEBI for conducting VAPT is placed below as **Annexure 35** for ready reference.

All MIIs are advised to ensure the strict compliance of the said advisory and shall also bring the same to the notice of the concerned cyber auditors.

4.82 *Comprehensive Review of Cyber Security at Stock Exchanges, Clearing Corporations and Depositories (MIIs)*[249]

4.82.1 Under **Para 4.41**, SEBI had prescribed the Cyber Security and Cyber Resilience framework that Stock Exchanges, Clearing Corporations and Depositories are required to implement.

4.82.2 With the view to further strengthen the said framework and increase the level of cyber security at MIIs, SEBI has been issuing various advisories based on the extant cyber threats in the Indian securities markets from time to time.

[249] Reference: SEBI Letter SEBI/HO/MRD/DSA/OW/P/2018/000005436/5 dated February 21, 2018

4.82.3 Based on internal deliberations, guidance received from CERT-In and the recommendations of SEBI's High Powered Steering Committee on Cyber Security (HPSC-CS) it has been decided that MIIs should conduct a comprehensive review/ audit of Cyber Security.

4.82.4 In this regard MIIs are advised to conduct a detailed review/ audit of the implementation of the SEBI circular and advisories issued by SEBI from time to time w.r.t. Cyber Security as per the framework enclosed. The framework includes:

4.82.4.1 **Auditor Selection Norms**

4.82.4.2 **Scope of Review/Audit for Cyber Security of MIIs**

4.82.4.3 **Format of Review/Audit Report**

4.82.4.4 **Standardized Observation Reporting Format**

4.82.5 The stipulated timeline for the auditor to submit the report from commencement of the review / audit is 6 weeks.

4.82.6 The Cyber Security Review Audit Reports and compliance status of the same should be placed before the Standing Committee on Technology (SCoT) of Stock Exchanges/ Clearing Corporations and before the IT Strategy committee (IT-SC) of Depositories for review. The SCoT / IT-SC should also review the corrective actions taken by the MII and submit its report to the Governing Board of the MII.

4.82.7 The comments of the SCoT/ IT-SC and the Governing Board of the MII should be communicated to SEBI.

4.82.8 In order to achieve uniformity in reporting across MIIs, the review/ audit report format and the format followed by the auditor while reporting findings / observations is being standardized. The draft structure of the report and the Standardized Observation Reporting Format are enclosed herein.

4.82.9 As advised by the HPSC-CS, the MIIs should conduct the comprehensive review/audit at least two times a year.

4.82.10 MIIs are advised to submit a compliance report to SEBI within one month of the review/audit and the report on corrective action report within three months post the submission of the compliance report

A. Auditor Selection Norms

1. Auditors must be compulsorily CERT-In empanelled.

2. Auditor must preferably have a minimum 3 years of experience in IT audit of Banking and Financial Services preferably in the Securities Market e.g. stock exchanges, clearing houses, depositories etc. The audit experience should have covered all the major areas mentioned under SEBI's Audit Terms of Reference (TOR). Auditing experience of the Cyber Security Framework of NIST for an organization will be an added advantage.

3. The Auditor must have experience in / direct access to experienced resources in the areas covered under TOR. IT is recommended that resources employed shall have

relevant industry recognized certifications e.g. CISA (Certified Information Systems Auditor) from ISACA, CISM (Certified Information Securities Manager) from ISACA, GSNA (GIAC Systems and Network Auditor), CISSP (Certified information Systems Security Professional) from International Information Systems Security Certification Consortium, commonly known as (ISC).

4. The Auditor should have ISMS / IT audit/governance frameworks and processes conforming to leading industry practices like CobiT.
5. The Auditor must not have any conflict of interest in conducting fair, objective and independent audit of the Exchange / Depository. IT should not have been engaged over the last three years in any consulting engagement with any departments / units of the entity being audited.
6. The Auditor may not have any cases pending against its previous auditees, which fall under SEBI's jurisdiction, which point to its incompetence and/or unsuitability to perform the audit task.
7. The auditor must have experience of performing VAPT.
8. The Auditor must compulsorily use only licensed tools.
9. The Auditor must compulsorily enter into a Non-disclosure Agreement (NDA) with the auditee. Under no circumstances, the data sought during the review or the audit report subsequently should leave the jurisdiction of India.

B. Scope of Review for Cyber Security of MIIs

1. SEBI Circular Dated July 06,2015 on Cyber Security and Cyber Resilience framework of Stock Exchanges, Clearing Corporation and Depositories
2. SEBI Advisory dated October 19,2016
3. SEBI Advisory dated November 24,2016 on Strengthening Resiliency of Websites of Stock Exchanges, Clearing Corporations and Depositories (Mils)
4. SEBI Advisory dated May 15,2017 on WannaCry Ransomware
5. SEBI Advisory dated June 30,2017 on Petya Ransomware
6. SEBI Advisory dated September 04,2017 on Locky Ransomware
7. SEBI Advisory dated August 09,2017 w.r.t. Communique from NCSC
8. Cyber Threat Vectors and Cyber Attack Scenarios communicated vide email dated August 29, 2017.

In order to achieve uniformity in reporting across MIIs, the review/ audit report format and the format followed by the auditor while reporting findings/ observations be standardized. The structure of the report and the Standardized Observation Reporting Format are also attached.

C. Format of Review / Audit Report

1. Identification of auditee (Address & contact information)
2. Dates and Location(s) of audit

3. Terms of reference (as agreed between the auditee and auditor), including the standard / specific scope for audit
4. Audit plan (audit subject identification, pre-audit planning, data gathering methodology etc.) followed.
5. Explicit reference to key auditee organizational documents (by date or version) including policy and procedure documents. (List of documentary evidence)
6. Additional mandatory or voluntary standards or regulations applicable to the auditee
7. Summary of audit findings including identification tests, tools used and results of tests performed (Standard Observation Reporting Format to be followed by auditor while reporting findings / observations)
8. Analysis of vulnerabilities and issues of concern
9. Recommendations for action
10. Specific Best practices implemented by the auditee in a generalized manner without infringing on Intellectual property rights (IPRs).
11. Personnel involved in the audit, including identification of any trainees.

***D. Standardized Observation Reporting Format* – Annexure 36**

4.83 Activity schedule for depositories for T+2 rolling Settlement[250]

4.83.1 The activity schedule for T+2 Rolling Settlement is as under:

S. No.	Day	Time	Description of activity
1	T		Trade Day
2	T+1	By 1.00 pm	Completion of custodial confirmation of trades to CC/CH. (There is no separate extended time limit for late confirmations).
		By 2.30 pm	Completion of process and download obligation files to brokers/ custodians by the CC/CH.
3	T+2	By 11.00 am	Pay-in of securities and funds.
		By 1.30 pm	Pay-out of securities and funds.

4.83.2 All Depositories shall adhere to the aforementioned activity schedule to implement T+2 rolling settlement. DPs shall adhere to the designated activities within the prescribed time limits as under:

4.83.2.1 DPs shall accept instructions for pay-in of securities from clients in the physical form atleast upto 4 p.m. and in electronic form atleast upto 6 p.m. on T+1.

[250] Reference: SEBI Circular DCC/FITTC/Cir-19/2003 dated March 4, 2003 and SEBI Circular MRD/DoP/SE/Dep/Cir-18/2005 dated September 2, 2005

4.83.2.2 DPs shall complete execution of pay-in instructions latest by 10:30 a. m. on T+2.

4.83.2.3 Depositories shall download the processed pay-in files to the Exchange / Clearing House / Clearing Corporation latest by 11:00 a.m. on T+2.

4.83.2.4 Pay-out of securities by the Exchange / Clearing House / Clearing Corporation to the Depositories shall be executed by 1:30 p.m. on T+2.

4.83.2.5 Pay-out of securities shall be completed by the Depositories by 2:00 p.m. on T+2.

4.83.3 All instructions received by the DPs shall have an execution date, which may be either a current date or a future date. Instructions shall be valid till the pay-in deadline or till 'end of day' (EOD) of the execution date, whichever is earlier. DPs shall ensure that the validity period of instructions is brought to the notice of the client while accepting the instructions. In case the client account does not have sufficient balance before pay-in deadline or till EOD, such instructions shall fail.

भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

Annexures

Annexure 1

SARAL

ACCOUNT OPENING FORM FOR RESIDENT INDIVIDUALS TRADING IN CASH SEGMENT

PHOTOGRAPH

Please affix your recent passport size photograph and sign across it

I KYC - Please fill this form in BLOCK LETTERS

A. IDENTITY DETAILS

1. Name of the Applicant: _____
2. Father's/ Spouse Name: _____
3. a. Gender: Male/ Female b. Marital status: Single/ Married c. Date of birth: ____(dd/mm/yyyy)
4. Nationality: _____
5. a. PAN: _____ b. Aadhaar Number, if any: _____
6. Specify the proof of Identity submitted: _____

B. ADDRESS DETAILS

1. Residence/ Correspondence Address: _____ City/town/village: _____ Pin Code: _____ State: _____ Country: _____
2. Contact Details: Tel. (Off.) _____ Tel. (Res.) _____ Mobile No.: _____ Fax: ___ Email id: _____
3. Permanent Address (if different from above address): _____ City/town/village: _____ Pin Code: _____ State: _____ Country: _____
4. Specify the proof of address submitted for residence/correspondence /permanent address: _____

DECLARATION

I hereby declare that the details furnished above are true and correct to the best of my knowledge and belief and I undertake to inform you of any changes therein, immediately. In case any of the above information is found to be false or untrue or misleading or misrepresenting, I am aware that I may be held liable for it.

_____ Signature of the Applicant Date: _____(dd/mm/yyyy)

☐ Originals verified and Self-Attested Document copies received (.....)

Name & Signature of the Authorised Signatory
Seal/Stamp of the intermediary

Date .....

II OTHER DETAILS:

1. Bank account details:

Bank Name	Branch address	Bank account no.	Account Type: Saving/Current/	MICR Number	IFSC code

2. Demat account details: (In case the client does not have DP account, this column may be crossed)

DP name	NSDL/CDSL	Beneficiary name	DP ID	BO ID

3. Whether DP account is also to be opened with the same intermediary (Yes/No)

4. Trading Preferences: Please sign the relevant boxes where you wish to trade.

Exchange	Sign	Exchange	Sign	Exchange	Sign
NSE		BSE		MCX-SX	

5. Mode of receiving Contract Note/ Statement of Account: Physical / Electronic (Please indicate your preference).....

6. Standing instructions to receive credits automatically into my BO account (Yes/No)

7. Nomination details (Name, PAN, Address and Phone no. of nominee); relationship with the nominee (If nominee is a minor, details of Guardian like name, address, phone no. and signature of Guardian may be obtained)

I have understood the contents of policy and procedures document, tariff sheet, 'Rights and Obligations' document and 'Risk Disclosure Document'. I do hereby agree to be bound by such provisions as outlined in these documents. I have also been informed that the standard set of documents has been displayed for information on stock broker's designated website.

_____ Signature of the Applicant Date: _____(dd/mm/yyyy)

FOR OFFICE USE ONLY

UCC Code allotted to the Client: ——————

DP name	NSDL/CDSL	Beneficiary name	DP ID	BO ID

	Documents verified with Originals	Client Interviewed By	In-Person Verification done by
Name of the Employee			
Employee Code			
Designation of the employee			
Date			
Signature			

I / We undertake that I/we have made the client aware of 'Policy and Procedures', tariff sheet. I/We have also made the client aware of 'Rights and Obligations' document (s), RDD and Guidance Note. I/We have given/sent him a copy of all the KYC documents. I/We undertake that any change in the 'Policy and Procedures', tariff sheet would be duly intimated to the clients. I/We also undertake that any change in the 'Rights and Obligations' and RDD would be made available on my/our website, if any, for the information of the clients.

If the client chooses to avail the demat facility from the same stock broker who is also a depository participant, the stock broker may use the same form and provide the details of the demat account opened for the said client to the client while providing a copy of the KYC documents.

.....

Signature of the Authorised Signatory

Date ..... **Seal/Stamp of the stock broker**

NOTE: This form is applicable for individual investors trading in the cash segment. If such investors wish to trade in segments other than cash segment and / or wish to avail facilities such as internet trading, running account, margin trading, Power of Attorney etc., they may furnish additional details required as per prescribed regulations to the concerned intermediary.

भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

Annexure 2

KNOW YOUR CLIENT (KYC) APPLICATION FORM

For Individuals

PHOTOGRAPH

Please affix your recent passport size photograph and sign across it

Please fill this form in ENGLISH and in BLOCK LETTERS.

A. IDENTITY DETAILS

1. Name of the Applicant: _____
2. Father's/ Spouse Name: _____
3. a. Gender: Male/ Female b. Marital status: Single/ Married c. Date of birth: _____(dd/mm/yyyy)
4. a. Nationality: _____ b. Status: Resident Individual/ Non Resident/ Foreign National
5. a. PAN: _____ b. Unique Identification Number (UID)/ Aadhaar, if any:_____
6. Specify the proof of Identity submitted: _____

B. ADDRESS DETAILS

1. Address for correspondence: _____
   _____ City/town/village: _____ Pin Code: _____ State: _____ Country: _____
2. Contact Details: Tel. (Off.) _____ Tel. (Res.) _____ Mobile No.: _____ Fax: _____ Email id: _____
3. Specify the proof of address submitted for correspondence address:_____
4. Permanent Address (if different from above or overseas address, mandatory for Non-Resident Applicant): _____
   _____ City/town/village: _____ Pin Code: _____ State: _____ Country: _____
5. Specify the proof of address submitted for permanent address: _____

C. OTHER DETAILS

1. Gross Annual Income Details (please specify): Income Range per annum: Below Rs 1 Lac / 1-5 Lac /5-10 Lac / 10-25 Lac / >25 Lacs or

   Net-worth as on (date)..... (----------) (Net worth should not be older than 1 year)
2. Occupation (please tick any one and give brief details): Private Sector/ Public Sector/ Government Service/Business/ Professional/ Agriculturist/ Retired/ Housewife/ Student/ Others _____
3. Please tick, if applicable: Politically Exposed Person (PEP)/ Related to a Politically Exposed Person (PEP)
4. Any other information: _____

DECLARATION

I hereby declare that the details furnished above are true and correct to the best of my knowledge and belief and I undertake to inform you of any changes therein, immediately. In case any of the above information is found to be false or untrue or misleading or misrepresenting, I am aware that I may be held liable for it.

_____

Signature of the Applicant Date: _____ (dd/mm/yyyy)

FOR OFFICE USE ONLY

☐ (Originals verified) True copies of documents received

☐ (Self-Attested) Self Certified Document copies received

(.....)
Signature of the Authorised Signatory

Date .....

Seal/Stamp of the intermediary

भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

KNOW YOUR CLIENT (KYC) APPLICATION FORM

For Non-Individuals

PHOTOGRAPH

Please affix the recent passport size photographs and sign across it

Please fill this form in ENGLISH and in BLOCK LETTERS.

A. IDENTITY DETAILS

1. **Name of the Applicant:** _____
2. **Date of incorporation:** _____(dd/mm/yyyy) **& Place of incorporation:** _____
3. **Date of commencement of business:** _____ (dd/mm/yyyy)
4. **a. PAN:** _____ **b. Registration No. (e.g. CIN):** _____
5. **Status (please tick any one):**

   Private Limited Co./Public Ltd. Co./Body Corporate/Partnership/Trust/Charities/NGO's/FI/ FII/HUF/AOP/ Bank/Government Body/Non-Government Organization/Defense Establishment/BOI/Society/LLP/ Others (please specify) _____

B. ADDRESS DETAILS

1. **Address for correspondence:** _____

   _____ City/town/village: _____ Pin Code: _____ State: _____ Country: _____
2. **Contact Details:** Tel. (Off.) _____ Tel. (Res.) _____ Mobile No.: _____ Fax: _____ Email id: _____
3. **Specify the proof of address submitted for correspondence address:** _____
4. **Registered Address** (if different from above): _____

   _____ City/town/village: _____ Pin Code: _____ State: _____ Country: _____
5. **Specify the proof of address submitted for registered address:** _____

C. OTHER DETAILS

1. **Gross Annual Income Details (please specify):** Income Range per annum: Below Rs 1 Lac / 1-5 Lac /5-10 Lac / 10-25 Lac / 25 Lacs-1 crore/ > 1 crore
2. **Net-worth as on** (date) ..... (dd/mm/yyyy): _____ *(*Net worth should not be older than 1 year)*
3. **Name, PAN, residential address and photographs of Promoters/Partners/Karta/Trustees and whole time directors:**

   _____
4. **DIN/UID of Promoters/Partners/Karta and whole time directors:** _____
5. **Please tick, if applicable, for any of your authorized signatories/Promoters/Partners/Karta/Trustees/whole time directors:** Politically Exposed Person (PEP)/ Related to a Politically Exposed Person (PEP)
6. **Any other information:** _____

DECLARATION

I/We hereby declare that the details furnished above are true and correct to the best of my/our knowledge and belief and I/we undertake to inform you of any changes therein, immediately. In case any of the above information is found to be false or untrue or misleading or misrepresenting, I am/we are aware that I/we may be held liable for it.

_____

Name & Signature of the Authorised Signatory **Date:** _____ **(dd/mm/yyyy)**

FOR OFFICE USE ONLY

☐ (Originals verified) True copies of documents received

☐ (Self-Attested) Self Certified Document copies received

(.....)

Signature of the Authorised Signatory

Date .....

Seal/Stamp of the intermediary

INSTRUCTIONS/CHECK LIST FOR FILLING KYC FORM

A. IMPORTANT POINTS:

1. Self-attested copy of PAN card is mandatory for all clients, including Promoters/Partners/Karta/Trustees and whole time directors and persons authorized to deal in securities on behalf of company/firm/others.
2. Copies of all the documents submitted by the applicant should be self-attested and accompanied by originals for verification. In case the original of any document is not produced for verification, then the copies should be properly attested by entities authorized for attesting the documents, as per the below mentioned list.
3. If any proof of identity or address is in a foreign language, then translation into English is required.
4. Name & address of the applicant mentioned on the KYC form, should match with the documentary proof submitted.
5. If correspondence & permanent address are different, then proofs for both have to be submitted.
6. Sole proprietor must make the application in his individual name & capacity.
7. For non-residents and foreign nationals, (allowed to trade subject to RBI and guidelines under Foreign Exchange Management Act, 1999 ("**FEMA**")), copy of passport/PIO Card/OCI Card and overseas address proof is mandatory.
8. For foreign entities, CIN is optional; and in the absence of DIN no. for the directors, their passport copy should be given.
9. In case of Merchant Navy NRI's, Mariner's declaration or certified copy of CDC (Continuous Discharge Certificate) is to be submitted.
10. For opening an account with Depository participant or Mutual Fund, for a minor, photocopy of the School Leaving Certificate/Mark sheet issued by Higher Secondary Board/Passport of Minor/Birth Certificate must be provided.
11. Politically Exposed Persons (PEP) are defined as individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States or of Governments, senior politicians, senior Government/judicial/ military officers, senior executives of state owned corporations, important political party officials, etc.

B. Proof of Identity (POI): - *List of documents admissible as Proof of Identity:*

1. Unique Identification Number (UID) (Aadhaar)/ Passport/ Voter ID card/ Driving license.
2. PAN card with photograph.

3. Identity card/ document with applicant's Photo, issued by any of the following: Central/State Government and its Departments, Statutory/Regulatory Authorities, Public Sector Undertakings, Scheduled Commercial Banks, Public Financial Institutions, Colleges affiliated to Universities, Professional Bodies such as ICAI, ICWAI, ICSI, Bar Council etc., to their Members; and Credit cards/Debit cards issued by Banks.

C. Proof of Address (POA): - *List of documents admissible as Proof of Address:(*Documents having an expiry date should be valid on the date of submission.)*

1. Passport/ Voters Identity Card/ Ration Card/ Registered Lease or Sale Agreement of Residence/ Driving License/ Flat Maintenance bill/ Insurance Copy.
2. Utility bills like Telephone Bill (only land line), Electricity bill or Gas bill **-** Not more than 3 months old.
3. Bank Account Statement/Passbook -- Not more than 3 months old.
4. Self-declaration by High Court and Supreme Court judges, giving the new address in respect of their own accounts.
5. Proof of address issued by any of the following: Bank Managers of Scheduled Commercial Banks/Scheduled Co-Operative Bank/Multinational Foreign Banks/Gazetted Officer/Notary public/Elected representatives to the Legislative Assembly/Parliament/Documents issued by any Govt. or Statutory Authority.
6. Identity card/document with address, issued by any of the following: Central/State Government and its Departments, Statutory/Regulatory Authorities, Public Sector Undertakings, Scheduled Commercial Banks, Public Financial Institutions, Colleges affiliated to Universities and Professional Bodies such as ICAI, ICWAI, ICSI, Bar Council etc., to their Members.
7. For FPI, Power of Attorney given by FPI to the Custodians (which are duly notarized and/or apostiled or consularised) that gives the registered address should be taken.
8. The proof of address in the name of the spouse may be accepted.
9. Aadhaar Letter issued by UIDAI[251]

D. Exemptions/clarifications to PAN

*(*Sufficient documentary evidence in support of such claims to be collected.)*

[251] Reference: SEBI Circular CIR/MIRSD/ 09 /2012 dated August 13, 2012

1. In case of transactions undertaken on behalf of Central Government and/or State Government and by officials appointed by Courts e.g. Official liquidator, Court receiver etc.
2. Investors residing in the state of Sikkim.
3. UN entities/multilateral agencies exempt from paying taxes/filing tax returns in India.
4. SIP of Mutual Funds upto Rs 50, 000/- p.a.
5. In case of institutional clients, namely, FPIs, Mutual Funds (MFs), Venture Capital Funds (VCFs), Foreign Venture Capital Funds (FVCIs), Scheduled Commercial Banks, Multilateral and Bilateral Development Financial Institutions, State Industrial Development Corporations, Insurance Companies registered with IRDA and Public Financial Institution as defined under section 2(72) of the Companies Act, 2013, Custodians shall verify the PAN card details with the original PAN card and provide duly certified copies of such verified PAN details to the intermediary.

E. List of people authorized to attest the documents:

1. Notary Public, Gazetted Officer, Manager of a Scheduled Commercial/ Co-operative Bank or Multinational Foreign Banks (Name, Designation & Seal should be affixed on the copy).
2. In case of NRIs, authorized officials of overseas branches of Scheduled Commercial Banks registered in India, Notary Public, Court Magistrate, Judge, Indian Embassy /Consulate General in the country where the client resides are permitted to attest the documents.

F. In case of Non-Individuals, additional documents to be obtained from non-individuals, over & above the POI & POA, as mentioned below:

Types of entity	Documentary requirements
Corporate	• Copy of the balance sheets for the last 2 financial years (to be submitted every year). • Copy of latest share holding pattern including list of all those holding control, either directly or indirectly, in the company in terms of Securities and Exchange Board of India (Substantial Acquisition of Shares and Takeovers) Regulations, 2011, duly certified by the company secretary/Whole time director/MD (to be submitted every year). • Photograph, POI, POA, PAN and DIN numbers of whole time directors/two directors in charge of day to day operations.

	• Photograph, POI, POA, PAN of individual promoters holding control - either directly or indirectly. • Copies of the Memorandum and Articles of Association and certificate of incorporation. • Copy of the Board Resolution for investment in securities market. • Authorised signatories list with specimen signatures.
Partnership firm	• Copy of the balance sheets for the last 2 financial years (to be submitted every year). • Certificate of registration (for registered partnership firms only). • Copy of partnership deed. • Authorised signatories list with specimen signatures. • Photograph, POI, POA, PAN of Partners.
Trust	• Copy of the balance sheets for the last 2 financial years (to be submitted every year). • Certificate of registration (for registered trust only). • Copy of Trust deed. • List of trustees certified by managing trustees/CA. • Photograph, POI, POA, PAN of Trustees.
HUF	• PAN of HUF. • Deed of declaration of HUF/ List of coparceners. • Bank pass-book/bank statement in the name of HUF. • Photograph, POI, POA, PAN of Karta.
Unincorporated association or a body of individuals	• Proof of Existence/Constitution document. • Resolution of the managing body & Power of Attorney granted to transact business on its behalf. • Authorized signatories list with specimen signatures.
Banks/Institutional Investors	• Copy of the constitution/registration or annual report/balance sheet for the last 2 financial years. • Authorized signatories list with specimen signatures.
Foreign Portfolio Investors (FPI)	• Copy of SEBI registration certificate. • Authorized signatories list with specimen signatures.
Army/Government Bodies	• Self-certification on letterhead. • Authorized signatories list with specimen signatures.

Registered Society	• Copy of Registration Certificate under Societies Registration Act, 1860. • List of Managing Committee members. • Committee resolution for persons authorised to act as authorised signatories with specimen signatures. • True copy of Society Rules and Bye Laws certified by the Chairman/Secretary.

Annexure 3

Rights and Obligations of Beneficial Owner and Depository Participant as prescribed by SEBI and Depositories

General Clause

1. The Beneficial Owner (BO) and the Depository participant (DP) shall be bound by the provisions of the Depositories Act, 1996, Securities and Exchange Board of India (Depositories and Participants) Regulations, 2018 (DP Regulations), rules and regulations of Securities and Exchange Board of India (SEBI), circulars/notifications/guidelines issued there under, bye laws and business rules/operating instructions issued by the depositories and relevant notifications of Government Authorities as may be in force from time to time.
2. The DP shall open/activate demat account of a beneficial owner in the depository system only after receipt of complete Account opening form, KYC and supporting documents as specified by SEBI from time to time.

Beneficial Owner information

3. The DP shall maintain all the details of the beneficial owner(s) as mentioned in the account opening form, supporting documents submitted by them and/or any other information pertaining to the beneficial owner confidentially and shall not disclose the same to any person except as required by any statutory, legal or regulatory authority in this regard.
4. The BO shall immediately notify the DP in writing, if there is any change in details provided in the account opening form as submitted to the DP at the time of opening the demat account or furnished to the DP from time to time.

Fees/Charges/Tariff

5. The BO shall pay such charges to the DP for the purpose of holding and transfer of securities in dematerialized form and for availing depository services as may be agreed to from time to time between the DP and the BO as set out in the Tariff Sheet provided by the DP. It may be informed to the BO that "no charges are payable for opening of demat accounts"
6. In case of Basic Services Demat Accounts, the DP shall adhere to the charge structure as laid down under the relevant SEBI and/or depository circulars/directions/notifications issued from time to time.
7. The DP shall not increase any charges/tariff agreed upon unless it has given a notice in writing of not less than thirty days to the BO regarding the same.

Dematerialization

8. The BO shall have the right to get the securities, which have been admitted on the depositories, dematerialized in the form and manner laid down under the bye laws, business rules and operating instructions of the depositories.

Separate Accounts

9. The DP shall open separate accounts in the name of each of the BOs and securities of each BO shall be segregated and shall not be mixed up with the securities of other BOs and/or DP's own securities held in dematerialized form.

10. The DP shall not facilitate the BO to create or permit any pledge and /or hypothecation or any other interest or encumbrance over all or any of such securities submitted for dematerialization and/or held in demat account except in the form and manner prescribed in the Depositories Act, 1996, DP Regulations and bye-laws/operating instructions/business rules of the depositories.

Transfer of Securities

11. The DP shall effect transfer to and from the demat accounts of the BO only on the basis of an order, instruction, direction or mandate duly authorized by the BO and the DP shall maintain the original documents and the audit trail of such authorizations.

12. The BO reserves the right to give standing instructions with regard to the crediting of securities in his demat account and the DP shall act according to such instructions.

Statement of account

13. The DP shall provide statements of accounts to the BO in such form and manner and at such time as agreed with the BO and as specified by SEBI/depository in this regard.

14. However, if there is no transaction in the demat account, or if the balance has become Nil during the year, the DP shall send one physical statement of holding annually to such BOs and shall resume sending the transaction statement as and when there is a transaction in the account.

15. The DP may provide the services of issuing the statement of demat accounts in an electronic mode if the BO so desires. The DP will furnish to the BO the statement of demat accounts under its digital signature, as governed under the Information Technology Act, 2000. However, if the DP does not have the facility of providing the statement of demat account in the electronic mode, then the DP shall be obliged to forward the statement of demat accounts in physical form.

16. In case of Basic Services Demat Accounts, the DP shall send the transaction statements as mandated by SEBI and/or Depository from time to time.

Manner of Closure of Demat account

17. The DP shall have the right to close the demat account of the BO, for any reasons whatsoever, provided the DP has given a notice in writing of not less than thirty days to the BO as well as to the Depository. Similarly, the BO shall have the right to close his/her demat account held with the DP provided no charges are payable by him/her to the DP. In such an event, the BO shall specify whether the balances in their demat

account should be transferred to another demat account of the BO held with another DP or to rematerialize the security balances held.

18. Based on the instructions of the BO, the DP shall initiate the procedure for transferring such security balances or rematerialize such security balances within a period of thirty days as per procedure specified from time to time by the depository. Provided further, closure of demat account shall not affect the rights, liabilities and obligations of either the BO or the DP and shall continue to bind the parties to their satisfactory completion.

Default in payment of charges

19. In event of BO committing a default in the payment of any amount provided in Clause 5 & 6 within a period of thirty days from the date of demand, without prejudice to the right of the DP to close the demat account of the BO, the DP may charge interest at a rate as specified by the depository from time to time for the period of such default.

20. In case the BO has failed to make the payment of any of the amounts as provided in Clause 5&6 specified above, the DP after giving two days' notice to the BO shall have the right to stop processing of instructions of the BO till such time he makes the payment along with interest, if any.

Liability of the Depository

21. As per Section 16 of Depositories Act, 1996,

a. Without prejudice to the provisions of any other law for the time being in force, any loss caused to the BO due to the negligence of the depository or the participant, the depository shall indemnify such BO.

b. Where the loss due to the negligence of the DP under Clause (a) above, is indemnified by the depository, the depository shall have the right to recover the same from such participant.

Freezing/ Defreezing of accounts

22. The BO may exercise the right to freeze/defreeze his/her demat account maintained with the DP in accordance with the procedure and subject to the restrictions laid down under the bye laws and business rules/operating instructions.

23. The DP or the depository shall have the right to freeze/defreeze the accounts of the BOs on receipt of instructions received from any regulator or court or any statutory authority.

Redressal of Investor grievance

24. The DP shall redress all grievances of the BO against the DP within a period of twenty one days from the date of receipt of the complaint.

Authorized representative

25. If the BO is a body corporate or a legal entity, it shall, along with the account opening form, furnish to the DP, a list of officials authorized by it, who shall represent and interact on its behalf with the DP. Any change in such list including additions, deletions or alterations thereto shall be forthwith communicated to the DP.

Law and Jurisdiction

26. In addition to the specific rights set out in this document, the DP and the BO shall be entitled to exercise any other rights which the DP or the BO may have under the Rules, bye laws and regulations of the respective depository in which the demat account is opened and circulars/notices issued there under or rules and regulations of SEBI.

27. The provisions of this document shall always be subject to Government notification, any rules, regulations, guidelines and circulars/ notices issued by SEBI and Rules, Regulations and Bye-laws of the relevant Depository, where the BO maintains his/her account, that may be in force from time to time.

28. The BO and the DP shall abide by the arbitration and conciliation procedure prescribed under the bye-laws of the depository and that such procedure shall be applicable to any disputes between the DP and the BO.

29. Words and expressions which are used in this document but which are not defined herein shall unless the context otherwise requires, have the same meanings as assigned thereto in the rules, bye-laws and regulations and circulars/notices issued there under by the depository and/or SEBI.

30. Any changes in the rights and obligations which are specified by SEBI/depositories shall also be brought to the notice of the clients at once.

31. If the rights and obligations of the parties hereto are altered by virtue of change in Rules and regulations of SEBI or bye-laws, rules and regulations of the relevant depository, where the BO maintains his/her account, such changes shall be deemed to have been incorporated herein in modification of the rights and obligations of the parties mentioned in this document.

Annexure 4

Intermediaries providing this facility to ensure adherence to the following:

E. The mandate provided by client should:

- ***i.*** be in favor of the concerned SEBI registered Intermediary only,
- ***ii.*** not provide the authority to transfer the mandate in favor of any assignees of the concerned Intermediary,
- ***iii.*** require the Intermediary to return the securities to the client(s) that may have been received by them erroneously or those securities that it was not entitled to receive from the client(s).

F. The mandate provided by client shall not facilitate Intermediaries to do the following:

- ***i.*** Transfer of securities for off-market trades,
- ***ii.*** To execute trades in the name of client without client's consent,
- ***iii.*** To open an email ID on behalf of the client for receiving relevant communications,
- ***iv.*** Prohibit to issue DIS to beneficial owner.
- ***v.*** Prohibit client from operating the account.

भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

Annexure 5

TM / DP Name and Address							FORM FOR NOMINATION *(To be filled in by individual applying singly or jointly)*																			
Date	D	D	M	M	Y	Y	Y	Y	UCC/ DP ID	I	N							Client ID								
I/We wish to make a nomination. [*As per details given below*]																										
Nomination Details																										
I/We wish to make a nomination and do hereby nominate the following person(s) who shall receive all the assets held in my / our account in the event of my / our death.																										

	Nomination can be made upto three nominees in the account.		**Details of 1st Nominee**		**Details of 2nd Nominee**		**Details of 3rd Nominee**	
1	**Name of the nominee(s) (Mr./Ms.)**							
2	**Share of each Nominee**	Equally [If not equally, please specify percentage]	%		%		%	
			Any odd lot after division shall be transferred to the first nominee mentioned in the form.					
3	**Relationship With the Applicant (If Any)**							
4	**Address of Nominee(s)** City / Place: State & Country:							
		PIN Code						
5	**Mobile / Telephone No. of nominee(s) #**							
6	**Email ID of nominee(s) #**							
7	**Nominee Identification details #** [Please tick any one of following and provide details of same] ☐ Photograph & Signature ☐ PAN ☐ Aadhaar ☐ Saving Bank account no. ☐ Proof of Identity ☐ Demat Account ID							
Sr. Nos. 8-14 should be filled only if nominee(s) is a minor:								
8	**Date of Birth {in case of minor nominee(s)}**							
9	**Name of Guardian (Mr./Ms.) {in case of minor nominee(s) }**							
10	**Address of Guardian(s)**							

	City / Place: State & Country:							
		PIN Code						
11	**Mobile / Telephone no. of Guardian #**							
12	**Email ID of Guardian #**							
13	**Relationship of Guardian with nominee**							
14	**Guardian Identification details #** [Please tick any one of following and provide details of same] ☐ Photograph & Signature ☐ PAN ☐ Aadhaar Saving Bank account no. ☐ Proof of Identity ☐ Demat Account ID							

Name(s) of holder(s)	**Signature(s) of holder***
Sole / First Holder (Mr./Ms.)	
Second Holder (Mr./Ms.)	
Third Holder (Mr./Ms.)	

*** Signature of witness, along with name and address are required, if the account holder affixes thumb impression, instead of signature**

 # Optional Fields (Information required at Serial nos. 5, 6, 7, 11, 12 & 14 is not mandatory)

Note:

This nomination shall supersede any prior nomination made by the account holder(s), if any.

The Trading Member / Depository Participant shall provide acknowledgement of the nomination form to the account holder(s)

Name and Signature of Holder(s)*

1._____ 2._____ 3._____

* Signature of witness, along with name and address are required, if the account holder affixes thumb impression, instead of signature

भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

Annexure 6

To Trading Member/Participant's Name Trading Member/Participant's Address	Date	D	D	M	M	Y	Y	Y	Y
UCC/DP ID	I	N							
Client ID (only for Demat account)									
Sole/First Holder Name									
Second Holder Name									
Third Holder Name									

I / We hereby confirm that I / We do not wish to appoint any nominee(s) in my / our trading / demat account and understand the issues involved in non-appointment of nominee(s) and further are aware that in case of death of all the account holder(s), my / our legal heirs would need to submit all the requisite documents / information for claiming of assets held in my / our trading / demat account, which may also include documents issued by Court or other such competent authority, based on the value of assets held in the trading / demat account.

Name and Signature of Holder(s)*

1._____ 2._____ 3._____

* Signature of witness, along with name and address are required, if the account holder affixes thumb impression, instead of signature

भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

Annexure 7

Request for Transmission of Securities by Nominee or Legal Heir (For Transmission of securities on death of the Sole holder)	ISR - 5

To:

The Listed Issuer/RTA,
(Address)

_____ **(Name of the Listed Issuer/RTA)**

Name of the Claimant(s) Mr./Ms.
Name of the Guardian ☐ *in case the claimant is a minor →* Date of Birth of the minor*   Mr./Ms. _____   Relationship with Minor: ☐ Father ☐ Mother ☐ Court Appointed Guardian*
[Multiple PAN may be entered] PAN (Claimant(s)/Guardian): | | | | | | | | | | ☐ KYC Acknowledgment attached ☐ KYC form attached
Tax Status: ☐ Resident Individual ☐ Resident Minor (through Guardian) ☐ NRI ☐ PIO ☐ Others (please specify)

**Please attach relevant proof*

I/We, the claimant(s) named hereinabove, hereby inform you about the demise of the below mentioned Securities Holder(s) and request you to transmit the securities held by the deceased holder(s) in my/our favour in my/our capacity as –
☐ Nominee ☐ Legal Heir ☐ Successor to the Estate of the deceased ☐ Administrator of the Estate of the deceased

Name of the deceased holder(s)	**Date of demise****
1)	DD / MM / YYYY
2)	DD / MM / YYYY
3)	DD / MM / YYYY

***Please attach certified copy of Death Certificate.*

Securities(s) & Folio(s) in respect of which Transmission of securities is being requested

Name of the Company	Folio No.	No. of Securities	% of Claim@
1)			
2)			
3)			
4)			

@As per Nomination OR as per the Will/Probate/Succession Certificate/Letter of Administration/ Legal Heirship Certificate (or its equivalent certificate)/ Court Decree, if applicable.

Contact details of the Claimant (s) [Provision for multiple entries may be made]

Mobile No.+91 | | | | | | | | | | **Tel. No.** STD -
Email Address

Address *(Please note that address will be updated as per address on KYC form / KYC Registration Agency records)*

Address Line 1
Address Line 2
City: State PIN | | | | | |

Bank Account Details of the Claimant

Bank Name
Account No. | | | | | | | | | | | 11-digit IFSC | | | | | | | | | | |
A/c. Type (✓) ☐SB ☐Current ☐NRO ☐NRE ☐FCNR | 9-digit MICR No. | | | | | | | | |
Name of bank branch
City PIN | | | | | |

Please attach & tick✓ ☐Cancelled cheque with claimant's name printed **OR** ☐ *Claimant's Bank Statement/Passbook (duly attested by the Bank Manager)*

I also request you to pay the UNCLAIMED amounts, *if any*, in respect of the deceased securities holder(s) by direct credit to the bank account mentioned above.

Additional KYC information (Please tick✓ whichever is applicable)

Occupation ☐ Private Sector Service ☐Public Sector Service ☐Government Service ☐Business ☐Professional ☐Agriculturist ☐Retired ☐Home Maker ☐ Student ☐Forex Dealer ☐ Others _____ (Please specify)
The Claimant is ☐ a Politically Exposed Person ☐ Related to a Politically Exposed Person ☐ Neither (Not applicable)
Gross Annual Income (₹) ☐Below 1 Lac ☐1-5 Lacs ☐ 5-10 Lacs ☐10-25 Lacs ☐ 25 Lacs-1crore ☐ >1 crore

FATCA and CRS information

Country of Birth _____ Place of Birth _____ Nationality _____		
Are you a tax resident of any country other than India? ☐Yes ☐No If Yes, please mention all the countries in which you are resident for tax purposes and the associated Taxpayer Identification Number and its identification type in the column below		
Country	Tax-Payer Identification Number	Identification Type

Nomination@ (Please ✓ one of the options below)

☐ I/We **DO NOT** wish to make a nomination. *(Please tick ✓ if you do not wish to nominate anyone)*
☐ I/We wish to make a nomination and hereby nominate the person/s more particularly described in the **attached Nomination Form** to receive the securities held in my/our folio in the event of my / our death.

@ Guardian of a minor is not allowed to make a nomination on behalf of the minor

Declaration and Signature of the Claimant(s)

I/We have attached herewith all the relevant / required documents as indicated in the attached *Ready Reckoner as per Annexure A.*

I/We confirm that the information provided above is true and correct to the best of my knowledge and belief.

I/We undertake to keep _____ (Name of the Company) / its RTA informed about any changes/modification to the above information in future and also undertake to provide any other additional information as may be required by the RTAs.

I/We hereby authorize _____ (Name of the Company) and its RTA to provide/ share any of the information provided by me/us including my holdings in the (Name of the Company) to any governmental or statutory or judicial authorities/agencies as required by law without any obligation of informing me/us of the same.

Place_____ Date	Signature of Claimant(S)

Documents Attached

- ☐ Copy of Death Certificate of the deceased holder
- ☐ Copy of Birth Certificate (in case the Claimant is a minor)
- ☐ Copy of PAN Card of Claimant / Guardian
- ☐ KYC Acknowledgment OR
- ☐ KYC form of Claimant
- ☐ Cancelled cheque with claimant's name printed OR ☐ Claimant's Bank Statement/Passbook
- ☐ Nomination Form duly completed
- ☐ Annexure D - Individual Affidavits given EACH Legal Heir
- ☐ Original security certificate(s)
- ☐ Annexure E - Bond of Indemnity furnished by Legal Heirs
- ☐ Annexure F - NOC from other Legal Heirs

*Note: **For transmission service requests, Form ISR-4 as per SEBI circular SEBI/HO/MIRSD/MIRSD_RTAMB/P/CIR/2022/8 dated January 25, 2022 will not be required.**

भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

Annexure 8

Individual Affidavits to be given by ALL the Legal Heirs OR Legal Heirs named in Succession Certificate*/ Probate of Will*/ Will*/ Letter of Administration*/ Legal Heirship Certificate*(or its equivalent certificate)*/Court Decree*

(For Transmission of securities on death of Sole Holder where NO NOMINATION has been registered)

Each Deponent (legal heir) shall sign separate Affidavits.

(To be executed on a non-judicial stamp of appropriate value and Notarized)

I,_____Son / daughter of _____ residing at _____ _____ do hereby solemnly affirm and state on oath as follows.

That Mr. /Mrs _____@ ("the deceased holder") held the following securities in his / her name as single holder:

Company Name	Folio No.	No. of securities held
1)		
2)		
3)		

☐ That the aforesaid deceased holder died *intestate* leaving behind him/her, the following persons as the only surviving heirs as per the Succession Certificate/ Legal Heirship Certificate(or its equivalent certificate)/Court Decree dated _____ / according to the Law of Intestate Succession by which he/she was governed at the time of his/her death and without registering any nominee. *

OR

☐ That the aforesaid deceased holder died leaving behind the following persons as the legatees as per the Will/ Probated Will/ Letter of Administration dated _____ and without registering any nominee. *

A copy of the **Succession Certificate*/ Probate of Will*/ Will*/ Letter of Administration*/ Legal Heirship Certificate*(or its equivalent certificate)*/ Court Decree*** is attached herewith.

Name of the Legal Heir(s)	Address and contact details	Age	Relation with the Deceased
1)			
2)			
3)			

That among the aforesaid legal heirs, Master/ Kum._____aged _____ years is a minor and is being represented by Mr./Ms. _____$ being his / her father / mother / legal guardian.

Signature of the Deponent:

X_____

VERIFICATION

I hereby solemnly affirm and state that what is stated herein above is true and correct and nothing has been concealed therein and that we I am competent to contract and entitled to rights and benefits of the abovementioned securities of the deceased.

Solemnly affirmed at **Signature of the Deponent:**

X_____

Signed before me

Place: _____

Date : _____

X ----------

Signature of Notary with Official Seal of
Notary& Regn. No.

** strikeout whichever is not applicable*

= *Name of the legal heir* @ = *Name of the deceased security holder*

$ = *Name of the Guardian*

भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

Annexure 9

Note: *To be executed in the presence of a Public Notary* / Gazetted Officer

Bond of Indemnity to be furnished jointly by all Legal Heir(s) including the Claimant(s)
(To be submitted on Non-judicial Stamp Paper of appropriate value)

[For Transmission of Securities on death of Sole Securities' Holder, where no nomination has been registered]

I/We do hereby solemnly affirm and state on oath as follows:

That Mr. /Ms. _____Name of the deceased holder_____ was holding the following securities:

Name of the Company	Certificate No.	Distinctive No.	Folio No.	No. of securities held
1				
2				
3				
4				

That the aforesaid deceased holder died *intestate* on _____, without registering any nominee, leaving behind him/her the following persons as the only surviving legal heirs, according to the laws of intestate succession applicable to him/her by which he/she was governed at the time of his/her death.

Name of the Legal Heir(s)/Claimant(s)	Address and contact details	Age	Relationship with the Deceased
1			
2			
3			
4			

OR

That the aforesaid deceased holder died on _____, without registering any nominee, leaving behind him/her the following persons as the only surviving legal heirs, according to the laws of testamentary succession.

Name of the Legal Heir(s)/Claimant(s)	Address and contact details	Age	Relationship with the Deceased
1			
2			
3			

Therefore, I/We, the Legal Heir(s)/Claimant(s) and deponent(s) herein has/have, approached _____(Name of the Company/RTA)_with a request to transmit the aforesaid securities in the name of the undersigned Mr. /Ms. [Name(s) of the legal heir(s)/claimant(s)]_____#, on my/our behalf, without insisting on production of a Succession Certificate/ Probate of Will / Letter of Administration or any Court order, for which we execute an indemnity as is herein contained and on relying on the information herein given by us, believing the same to be true.

In consideration therefore of my/our request to transfer/transmit the above said securities to the name of the undersigned Mr. /Ms. [Name(s) of the legal heir(s)/claimant(s)] #,

I/We hereby jointly and severely agree and undertake to indemnify and keep indemnified, saved, defended, harmless, [Name of the Company/ Issuer and any RTA] and its successors and assigns for all time hereafter against all losses, costs, claims, actions, demands, risks, charges, expenses, damages, etc., whatsoever which they may suffer and/or incur by reason of transferring the said securities as herein above mentioned, at my/our request to the undersigned Mr./Ms. [Name(s) of the legal heir(s)/claimant(s)]_____#, without insisting on production of a Succession Certificate / Probate of Will / Letter of Administration or any Court order.

IN WITNESS WHEREOF the said 1) Mr. /Ms. _____ (Name and signature of the witness) _____
And 2) Mr. /Ms. _____ Name and signature of the witness _____ #, have hereunto set their respective hands and seals this day of _____. Signed and delivered by the said legal heir/s.

Name the Legal Heirs	Signature of the Legal Heirs
1	X
2	X
3	X

(*) = Name of the deceased security holder (#) = Name of the claimant/s

Signed before me

at: _____

on _____
Signature of Notary

Official stamp & seal of the Notary & Regn. No.:

Annexure 10

Note: *To be executed in the presence of a Public Notary* / Gazetted Officer

[To be submitted in non-judicial stamp paper of appropriate value]

No-Objection Certificate from the Legal Heir(s)

Format of NOC from other Legal Heir(s) for Transmission of Securities in favour of the Claimant(s) wherein the Sole Holder is deceased and NO NOMINATION has been registered

DECLARATION

I/We, the legal heir(s) of late Mr. / Ms_____(name of the deceased holder) declare as follows –

(i) That the above named deceased holder was holding the following securities in his / her name as single holder:

Name of the Company	Folio No.	No. of securities held
1)		
2)		
3)		

(ii) That the deceased had died intestate on D D / M M / Y Y Y Y and without registering any nominee.

(iii) That the following Claimant(s) has/have applied for the transmission of the aforesaid securities:

Name of the Claimant(s)	Address and contact details	Age	Relationship with the deceased
1)			
2)			
3)			

(iv) That I / We are the legal heir(s) of the deceased holder, apart from the Claimant(s)who has/ have applied for transmission of the aforesaid securities and our details are as follows:

Therefore, I/We, the Legal Heir(s)/Claimant(s) and deponent(s) herein has/have, approached _____(Name of the Company/RTA) with a request to transmit the aforesaid securities in the name of the undersigned Mr. /Ms. [Name(s) of the legal heir(s)/claimant(s)]_____#, on my/our behalf, without insisting on production of a Succession Certificate/ Probate of Will / Letter of Administration or any Court order, for which we execute an indemnity as is herein contained and on relying on the information herein given by us, believing the same to be true.

In consideration therefore of my/our request to transfer/transmit the above said securities to the name of the undersigned Mr. /Ms. [Name(s) of the legal heir(s)/claimant(s)] #,

I/We hereby jointly and severely agree and undertake to indemnify and keep indemnified, saved, defended, harmless, [Name of the Company/ Issuer and any RTA] and its successors and assigns for all time hereafter against all losses, costs, claims, actions, demands, risks, charges, expenses, damages, etc., whatsoever which they may suffer and/or incur by reason of transferring the said securities as herein above mentioned, at my/our request to the undersigned Mr./Ms. [Name(s) of the legal heir(s)/claimant(s)]_____#, without insisting on production of a Succession Certificate / Probate of Will / Letter of Administration or any Court order.

IN WITNESS WHEREOF the said 1) Mr. /Ms. _____ (Name and signature of the witness) _____
And 2) Mr. /Ms. _____ Name and signature of the witness _____#, have hereunto set their respective hands and seals this day of _____. Signed and delivered by the said legal heir/s.

Name the Legal Heirs	Signature of the Legal Heirs
1	X
2	X
3	X

(*) = Name of the deceased security holder (#) = Name of the claimant/s

Signed before me

at: _____

on _____
Signature of Notary

Official stamp & seal of the Notary & Regn. No.:

भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

Annexure 11

(to circular no. SEBI/HO/MIRSD/MIRSD_RTAMB/P/CIR/2022/8dated January 25, 2022 on Issuance of Securities in dematerialized form in case of Investor Service Requests)

RTA / ISSUER COMPANY NAME AND ADDRESS

Name: Date:
Address:

Dear Sir/Madam,

LETTER OF CONFIRMATION

Sub: Issuance of Securities in dematerialized form in case of Investor Service Requests

Name of the Company:
We refer to the request received from you for issuance of securities in your name. We would like to inform you that the request has been approved as detailed below:

Name of first holder & PAN Joint holder 1 & PAN Joint holder 2 & PAN	
Number of securities	
Folio Number	
Certificate numbers	
Distinctive numbers	
Lock-In	Yes or No. If yes, lock-in from ___/___/_____ till ___/___/____ (DD/MM/YYYY)

As you may be aware, SEBI vide Gazette Notification no. SEBI/LAD-NRO/GN/2022/66 dated January 24, 2022, has mandated that the securities that are issued pursuant to investor service request shall henceforth be issued in demat mode only and hence the security certificates (wherever applicable) are retained at our end.

Accordingly, within 120 days of this letter, please request your Depository Participant (**DP**) to demat these securities using the Dematerialization Request Form (**DRF**). Please fill the DRF with the details mentioned in this letter, sign it and present this letter in original to your DP along with the DRF for enabling your DP to raise a Demat Request Number (**DRN**). In case you do not have a demat account, kindly open one with any DP. Please note that you can open Basic Service Demat Account at minimal / nil charges.

Please note that **this letter is valid only for a period of 120 days** from the date of its issue within which you have to raise demat request with the DP as above. Any request for processing demat after the expiry of aforesaid 120 days will not be entertained and as per the operating guidelines issued by SEBI, the subject securities shall be transferred to a Suspense Escrow Demat Account of the Company.

Thanking you,

Yours faithfully,
For ABCD Limited (RTA)
Authorised Signatory

Annexure 12

Illustrative Measures for Data Security on Customer Facing Applications

1. Analyse the different kinds of sensitive data shown to the Customer on the frontend application to ensure that only what is deemed absolutely necessary is transmitted and displayed.
2. Wherever possible, mask portions of sensitive data. For instance, rather than displaying the full phone number or a bank account number, display only a portion of it, enough for the Customer to identify, but useless to an unscrupulous party who may obtain covertly obtain it from the Customer's screen. For instance, if a bank account number is "123 456 789", consider displaying something akin to "XXX XXX 789" instead of the whole number. This also has the added benefit of not having to transmit the full piece of data over various networks.
3. Analyse data and databases holistically and draw out meaningful and "silos" (physical or virtual) into which different kinds of data can be isolated and cordoned off. For instance, a database with personal financial information need not be a part of the system or network that houses the public facing websites of the Stock Broker. They should ideally be in discrete silos or DMZs.
4. Implement strict data access controls amongst personnel, irrespective of their responsibilities, technical or otherwise. It is infeasible for certain personnel such as System Administrators and developers to not have privileged access to databases. For such cases, take strict measures to limit the number of personnel with direct access, and monitor, log, and audit their activities. Take measures to ensure that the confidentiality of data is not compromised under any of these scenarios.
5. Use industry standard, strong encryption algorithms (eg: RSA, AES etc.) wherever encryption is implemented. It is important to identify data that warrants encryption as encrypting all data is infeasible and may open up additional attack vectors. In addition, it is critical to identify the right personnel to be in charge of, and the right methodologies for storing the encryption keys, as any compromise to either will render the encryption useless.
6. Ensure that all critical and sensitive data is adequately backed up, and that the backup locations are adequately secured. For instance, on servers on isolated networks that have no public access endpoints, or on-premise servers or disk drives that are off-limits to unauthorized personnel. Without up-to-date backups, a meaningful recovery from a disaster or cyber-attack scenario becomes increasingly difficult.

Annexure 13

Illustrative Measures for Data Transport Security

1. When an Application transmitting sensitive data communicates over the Internet with the Stock Brokers' systems, it should be over a secure, encrypted channel to prevent Man- In-The-Middle (MITM) attacks, for instance, an IBT or a Back office communicating from a Customer's web browser or Desktop with the Stock Brokers' systems over the internet, or intra or inter organizational communications. Strong transport encryption mechanisms such as TLS (Transport Layer Security, also referred to as SSL) should be used.
2. For Applications carrying sensitive data that are served as web pages over the internet, a valid, properly configured TLS (SSL) certificate on the web server is mandatory, making the transport channel HTTP(S).
3. Avoid the use of insecure protocols such as FTP (File Transfer Protocol) that can be easily compromised with MITM attacks. Instead, adopt secure protocols such as FTP(S), SSH and VPN tunnels, RDP (with TLS) etc.

Annexure 14

Illustrative Measures for Application Authentication Security

1. Any Application offered by Stock Brokers to Customers containing sensitive, private, or critical data such as IBTs, SWSTs, Back office etc. referred to as "Application" hereafter) over the Internet should be password protected. A reasonable minimum length (and no arbitrary maximum length cap or character class requirements) should be enforced. While it is difficult to quantify password "complexity", longer passphrases have more entropy and offer better security in general. Stock Brokers should attempt to educate Customers of these best practices.
2. Passwords, security PINs etc. should never be stored in plain text and should be one-way hashed using strong cryptographic hash functions (e.g.: bcrypt, PBKDF2) before being committed to storage. It is important to use one-way cryptographic hashes to ensure that stored password hashes are never transformed into the original plaintext values under any circumstances.
3. For added security, a multi-factor (e.g.: two-factor) authentication scheme may be used (hardware or software cryptographic tokens, VPNs, biometric devices, PKI etc.). In case of IBTs and SWSTs, a minimum of two-factors in the authentication flow are mandatory.
4. In case of Applications installed on mobile devices (such as smartphones and tablets), a cryptographically secure biometric two-factor authentication mechanism may be used.
5. After a reasonable number of failed login attempts into Applications, the Customer's account can be set to a "locked" state where further logins are not possible until a password and authentication reset is performed via an out-of-band channel validation, for instance, a cryptographically secure unique link that is sent to the Customer's registered e-mail, a random OTP (One Time Password) that is sent as an SMS to the Customer's registered mobile number, or manually by the Broker after verification of the Customer's identity etc.
6. Avoid forcing Customers to change passwords at frequent intervals which may result in successive, similar, and enumerated passwords. Instead, focus on strong multi-factor authentication for security and educate Customers to choose strong passphrases. Customers may be reminded within reasonable intervals to update their password and multi-factor credentials, and to ensure that their out-of-band authentication reset information (such as e-mail and phone number) are up-to-date.

Both successful and failed login attempts against a Customer's account may be logged for a reasonable period of time. After successive login failures, it is recommended that measures such as CAPTCHAs or rate-limiting be used in Applications to thwart manual and automated brute force and enumeration attacks against logins.

Annexure 15

Form to report on AI and ML technologies – To be submitted quarterly

Intimation to Depository for the use of the AI and ML application and systems

S No.	Head	Value
1	Entity SEBI registration number	
2	Registered entity category	
3	Entity name	
4	Entity PAN no.	
5	Application / System name	
6	Date from when the Application / System was used	
7	Type of area where AI or ML is used	<order execution / Advisory services / KYC / AML / Surveillance / compliance/others (please specify in 256 characters)>
7.a	Does the system involve order initiation, routing and execution?	<Yes / NO>
7.b	Does the system fall under discretionary investment or Portfolio management activities?	<Yes / NO>
7.c	Does the system disseminate invest mentor trading advice or strategies?	<Yes / NO>
7.d	Is the application/system used in area of Cyber Security to detect attacks	<Yes / NO>
7.e	What claims have been made regarding AI and ML Application / System – if any?	<free text field>
8	What is the name of the Tool / Technology that is categorized as AI and ML system / Application and submissions are declared vide this response	<free text field>
9	How was the AI or ML project implemented	<Internally / through solution provider / Jointly with a solution provider or third party>

10	Are the key controls and control points in your AI or ML application or systems in accordance to circular of SEBI that mandate cyber security control requirements	<free text field>
11	Is the AI / ML system included in the system audit, if applicable?	<Yes / NO / NA>
12	Describe the application / system and how it uses AI / ML as portrayed in the product offering	<free text field>
13	What safeguards are in place to prevent abnormal behavior of the AI or ML application / System	<free text field>

भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

Annexure 16

Consolidated Quarterly Reporting Form

Consolidated Quarterly report to SEBI of all registered depository participants with Depositories using AI and ML application and systems for the Quarter Ended DD/MM/YYYY

Entity Regn. No.	Entity Name	Entity PAN no.	Application /System name	Date used from	Type of area where AI or ML is used	To be filled if System Audit is applicable			
						If system audit report is submitted by entity later than "date used from"		If system audit report is submitted with adverse remarks and Depositories are entitled to inspect the entity	
						Does system audit report comply to Para 2.20	Is there any adverse comment in the System audit report	Was the entity inspected in past 1 year	If inspected, was any irregularity noted
					<order execution/ Advisory services/KYC/AML /Surveillance/compliance/others (please specify in 256 characters)>	<Yes / NO/>	<Yes / NO/>	<Yes / NO>	<Yes / NO>

Add separate rows for each system or application.

Annexure 17

Sr. No.	Name of reporting FPI (Nodal Entity)	Registration No. of Reporting FPI (Nodal Entity) mentioned in column B	Name of FPI / ODI Subscriber with whom the applicant shares, ownership of more than 50% common control	Type of Client viz. FPI or ODI subscriber or DR holder	Registration No. of FPI mentioned at Column D	LEI No. of entity mentioned at Column D (for ODI subscriber or DR holder)	If ODI subscriber, please mention name of dealing FPI	Jurisdiction / Country of entity mentioned at Column D
A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**

Annexure 18

Sr. No.	Name of Reporting FPI (Nodal Entity)	Registration No. of Reporting FPI (Nodal Entity) mentioned in column B	Name of ODI Subscriber or DR holder having investment in Indian Securities through ODI or DR route	LEI No. of ODI subscriber or DR holder mentioned at Column D	ISIN of the Indian Security	ISIN Description or name of the security	Quantity of securities held (in ratio as being held in India)	Value of securities held	As on date (DD-MMM-YYYY)
A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**

Note

1. Reference ISIN No. – ISIN of the underlying Indian Security (ISINs issued by NSDL for underlying security).
2. The quantity of securities in the requisite ISIN / or Indian Security shall be reported in the ration as being held in India.
3. The securities shall be reported as at the end of the month.
4. For the purpose of valuation, the closing price of such security as at the end of the month in India be considered for the computation of value of securities held.

भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

Annexure 19

Format for reporting changes in "status or constitution" of Depository Participants

Name of the Depository:-

Report for the quarter ending:- June/September/December/March Year:-

Date of report:-

Sr. No	Date of receipt	Name of the Depository Participant	SEBI Regn. number	Type of change	Details of changes		PAN (incoming entities, if any)	Date of Change
					Pre	Post		

Type	Description of Change
I	Amalgamation, demerger, consolidation or any other kind of corporate restructuring falling within the scope of Chapter XV of the Companies Act, 2013 or the corresponding provision of any other law for the time being in force.
II	Change in director, including managing director/ whole-time director
III	Change in shareholding not resulting in change in control
IV	Any other purpose as may be considered appropriate by the Depositories

भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

Annexure 20

Data of complaints against the Depositories to be displayed on their websites

Data for the month ending…….

Sr. No.	Received from	Carried forward from previous month	Received during the month	Total Complaints	Resolved during the month*	Pending at the end of the month**		Average Resolution time^
						Pending for less than 3 months	Pending for more than 3 months	
1	2	3	4	5	6	7		8
1	Directly from Investors							
2	SEBI (SCORES)							
3	Members							
4	Other Sources (if any)							
	Grand Total							

*Should include complaints of previous months resolved in the current month, if any.

**Should include total complaints pending as on the last day of the month, if any.

^ Average resolution time is the sum total of time taken to resolve each complaint in the current month divided by total number of complaints resolved in the current month.

s

Month-wise data for the current financial year

Sr. No.	Month	Carried forward from previous month	Received	Resolved	Pending
1	2	3	4	5	6
1	April				
2	May				
3	June				
4	July				
	Grand Total				

Year-wise data (for 5 years on rolling basis)

Sr. No.	Year	Carried forward from previous year	Received	Resolved	Pending
1	2	3	4	5	6
1	2020-21				
2	2021-22				
3	2022-23				

4	2023-24				
5	2024-25				
	Grand Total				

भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

Annexure 21

INVESTOR CHARTER FOR DEPOSITORIES AND DEPOSITORY PARTICIPANTS

1. **Vision**

   Towards making Indian Securities Market - Transparent, Efficient, & Investor friendly by providing safe, reliable, transparent and trusted record keeping platform for investors to hold and transfer securities in dematerialized form.

2. **Mission**

   - To hold securities of investors in dematerialised form and facilitate its transfer, while ensuring safekeeping of securities and protecting interest of investors.
   - To provide timely and accurate information to investors with regard to their holding and transfer of securities held by them.
   - To provide the highest standards of investor education, investor awareness and timely services so as to enhance Investor Protection and create awareness about Investor Rights.

3. **Details of business transacted by the Depository and Depository Participant (DP)**

   A Depository is an organization which holds securities of investors in electronic form. Depositories provide services to various market participants - Exchanges, Clearing Corporations, Depository Participants (DPs), Issuers and Investors in both primary as well as secondary markets. The depository carries out its activities through its agents which are known as Depository Participants (DP). Details available on the link [*link to be provided by Depositories*]

4. **Description of services provided by the Depository through Depository Participants (DP) to investors**

   (1) Basic Services

Sr. no.	Brief about the Activity / Service	Expected Timelines for processing by the DP after receipt of proper documents
1.	Dematerialization of securities	7 days
2.	Rematerialization of securities	7 days
3.	Mutual Fund Conversion / Destatementization	5 days

Sr. no.	Brief about the Activity / Service	Expected Timelines for processing by the DP after receipt of proper documents
4.	Re-conversion / Restatementisation of Mutual fund units	7 days
5.	Transmission of securities	7 days
6.	Registering pledge request	15 days
7.	Closure of demat account	30 days
8.	Settlement Instruction	Depositories to accept physical DIS for pay-in of securities upto 4 p.m and DIS in electronic form upto 6 p.m on T+1 day

(2) Depositories provide special services like pledge, hypothecation, internet based services etc. in addition to their core services and these include

Sr. no.	Type of Activity /Service	Brief about the Activity / Service
1.	Value Added Services	Depositories also provide value added services such as a. Basic Services Demat Account(BSDA) *[link to be provided by Depositories]*[1] b. Transposition cum dematerialization *[link to be provided by Depositories]*[2] c. Linkages with Clearing System *[link to be provided by Depositories]* [3] d. Distribution of cash and non-cash corporate benefits (Bonus, Rights, IPOs etc.), stock lending, demat of NSC / KVP, demat of warehouse receipts etc.
2.	Consolidated Account statement (CAS)	CAS is issued 10 days from the end of the month (if there were transactions in the previous month) or half yearly(if no transactions) .
3.	Digitalization of services provided by the depositories	Depositories offer below technology solutions and e-facilities to their demat account holders through DPs:

Sr. no.	Type of Activity /Service	Brief about the Activity / Service
		a. E-account opening: Details available on the link [*link to be provided by Depositories*][4] b. Online instructions for execution: Details available on the link [*link to be provided by Depositories*][5] c. e-DIS / Demat Gateway: Details available on the link [*link to be provided by Depositories*][6] d. e-CAS facility: Details available on the link [*link to be provided by Depositories*][7] e. Miscellaneous services: Details available on the link [*link to be provided by Depositories*][8]

5. Details of Grievance Redressal Mechanism

(1) The Process of investor grievance redressal

1.	Investor Complaint/ Grievances	Investor can lodge complaint/ grievance against the Depository/DP in the following ways: a. Electronic mode - (i) SCORES (a web based centralized grievance redressal system of SEBI) [link to be provided by Depositories] (ii) Respective Depository's web portal dedicated for the filing of compliant [link to be provided by Depositories] (iii) Emails to designated email IDs of Depository [link to be provided by Depositories] b. Offline mode [details of link to the form to be provided by Depositories] The complaints/ grievances lodged directly with the Depository shall be resolved within 30 days.
2.	Investor Grievance Redressal Committee of Depository	*[link to be provided by Depositories]*[9]

3.	Arbitration proceedings	*[link to be provided by the Depositories]*[10]

(2) For the Multi-level complaint resolution mechanism available at the Depositories please refer to link [*link to be provided by Depositories*][11]

6. Guidance pertaining to special circumstances related to market activities: Termination of the Depository Participant

Sl No.	Type of special circumstances	Timelines for the Activity/ Service
1.	▪ Depositories to terminate the participation in case a participant no longer meets the eligibility criteria and/or any other grounds as mentioned in the bye laws like suspension of trading member by the Stock Exchanges. ▪ Participant surrenders the participation by its own wish.	Client will have a right to transfer all its securities to any other Participant of its choice without any charges for the transfer within 30 days from the date of intimation by way of letter/email.

7. Dos and Don'ts for Investors

For Do's and Don'ts please refer to the link *[link to be provided by the Depositories]*[12]

8. Rights of investors

For rights please refer to the link *[link to be provided by the Depositories]*[13]

9. Responsibilities of Investors

For responsibilities please refer to the link *[link to be provided by the Depositories]*[14]

भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

INFORMATION CONTAINED IN LINKS TO THE INVESTOR CHARTER FOR DEPOSITORIES AND DPS

This document contains the contents pertaining to the qualifier "[*Link to be provided by Depositories*]" in the Investor Charter main document. The same is to be made available by the Depositories on their websites and web-links to the same is to be provided for incorporation in the Investor Charter.

For reasons of convenience, the contents in main Charter and this document have been mapped with the same superscript.

Para 4 (2) of Investor Charter

Point 1: Value Added Services

a. Basic Services Demat Account (BSDA)[1]: The facility of BSDA with limited services for eligible individuals was introduced with the objective of achieving wider financial inclusion and to encourage holding of demat accounts. No Annual Maintenance Charges (AMC) shall be levied, if the value of securities holding is upto Rs. 50,000. For value of holdings between Rs 50,001- 2,00,000, AMC not exceeding Rs 100 is chargeable. In case of debt securities, there are no AMC charges for holding value upto Rs 1,00,000 and a maximum of Rs 100 as AMC is chargeable for value of holdings between Rs 1,00,001 and Rs 2,00,000.

b. Transposition cum dematerialization[2]: In case of transposition-cum-dematerialisation, client can get securities dematerialised in the same account if the names appearing on the certificates match with the names in which the account has been opened but are in a different order. The same may be done by submitting the security certificates along with the Transposition Form and Demat Request Form.

c. Linkages with Clearing System[3] for actual delivery of securities to the clearing system from the selling brokers and delivery of securities from the clearing system to the buying broker.

Point 3: Digitization of services provided by the depositories

a. E-account opening[4]: Account opening through digital mode, popularly known as "On-line Account opening", wherein investor intending to open the demat account can visit DP website, fill in the required information, submit the required documents, conduct video IPV and demat account gets opened without visiting DPs office.

b. Online instructions for execution[5]: internet-enabled services like Speed-e (NSDL) & Easiest (CDSL) empower a demat account holder in managing his/her securities 'anytime-anywhere' in an efficient and convenient manner and submit instructions online without the need to use paper. These facilities allows Beneficial Owner (BO) to submit transfer instructions and pledge instructions including margin pledge from their demat account. The instruction facilities are also available on mobile applications through android, windows and IOS platforms.

c. e-DIS / Demat Gateway:[6] Investors can give instructions for transfer of securities through e-DIS apart from physical DIS. Here, for on-market transfer of securities, investors need to provide settlement number along with the ISIN and quantity of securities being authorized for transfer. Client shall be required to authorize each e-DIS valid for a single settlement number / settlement date, by way of OTP and PIN/password, both generated at Depositories end. Necessary risk containment measures are being adopted by Depositories in this regard.

d. e-CAS facility[7]: Consolidated Account Statements are available online and could also be accessed through mobile app to facilitate the investors to view their holdings in demat form.

e. Miscellaneous services[8]: Transaction alerts through SMS, e-locker facilities, chatbots for instantaneously responding to investor queries etc. have also been developed.

Para 5(1) of Investor Charter

Point 2 (Investor Grievance Redressal Committee of Depository)[9]:

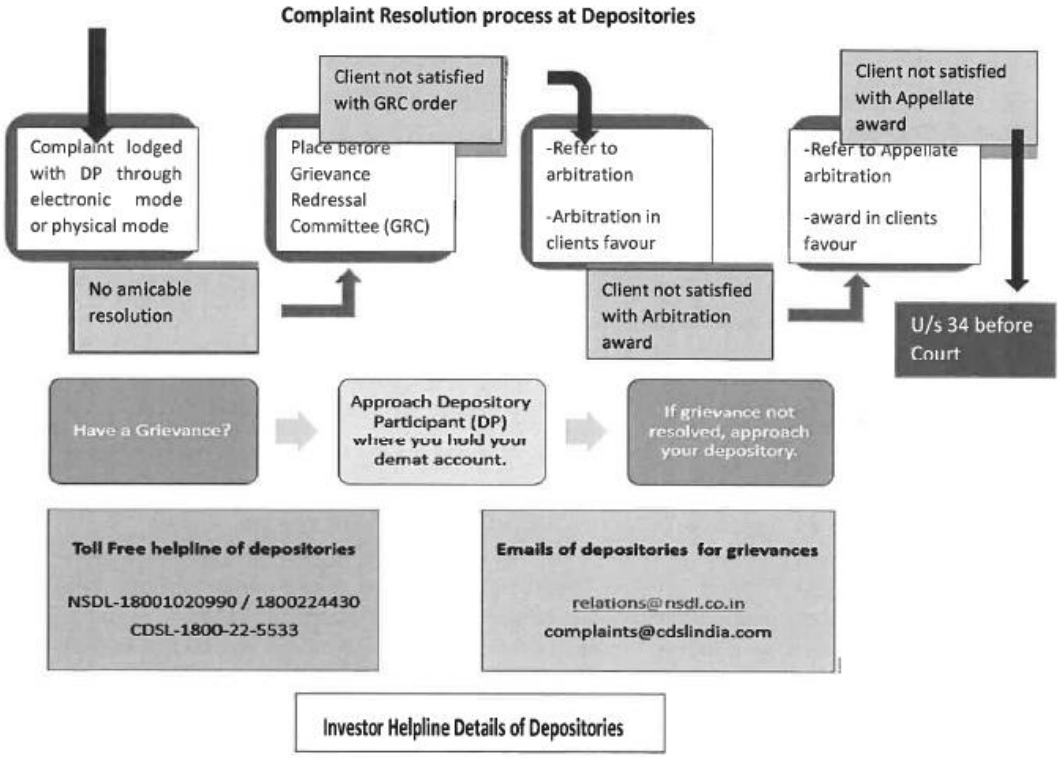
If no amicable resolution is arrived, then the Investor has the option to refer the complaint/ grievance to the Grievance Redressal Committee (GRC) of the Depository. Upon receipt of reference, the GRC will endeavor to resolve the complaint/ grievance by hearing the parties, and examining the necessary information and documents.

Point 3(Arbitration proceedings)[10]:

The Investor may also avail the arbitration mechanism set out in the Byelaws and Business Rules/Operating Instructions of the Depository in relation to any grievance, or dispute relating to depository services. The arbitration reference shall be concluded by way of issue of an arbitral award within 4 months from the date of appointment of arbitrator(s).

Para 5(2) of Investor Charter

Complaint Resolution process at Depositories[11]



Para 7 of Investor Charter

Dos and Don'ts for Investor[12]

Sl No.	Guidance
1.	Always deal with a SEBI registered Depository Participant for opening a demat account.
2.	Read all the documents carefully before signing them.
3.	Before granting Power of attorney to operate your demat account to an intermediary like Stock Broker, Portfolio Management Services (PMS) etc., carefully examine the scope and implications of powers being granted.
4.	Always make payments to registered intermediary using banking channels. No payment should be made in name of employee of intermediary.
5.	Accept the Delivery Instruction Slip (DIS) book from your DP only (pre-printed with a serial number along with your Client ID) and keep it in safe custody and do not sign or issue blank or partially filled DIS slips. Always mention the details like ISIN, number of securities accurately. In case of any queries, please contact your DP or broker and it should be signed by all demat account holders. Strike out any blank space on the slip and Cancellations or corrections on the DIS should be initialed or signed by all the account holder(s). Do not leave your instruction slip book with anyone else. Do not sign blank DIS as it is equivalent to a bearer cheque.
6.	Inform any change in your Personal Information (for example address or Bank Account details, email ID, Mobile number) linked to your demat account in the prescribed format and obtain confirmation of updation in system
7.	Mention your Mobile Number and email ID in account opening form to receive SMS alerts and regular updates directly from depository.
8.	Always ensure that the mobile number and email ID linked to your demat account are the same as provided at the time of account opening/updation.
9.	Do not share password of your online trading and demat account with anyone.

Sl No.	Guidance
10.	Do not share One Time Password (OTP) received from banks, brokers, etc. These are meant to be used by you only.
11.	Do not share login credentials of e-facilities provided by the depositories such as e-DIS/demat gateway, SPEED-e/easiest etc. with anyone else.
12.	Demat is mandatory for any transfer of securities of Listed public limited companies with few exceptions.
13.	If you have any grievance in respect of your demat account, please write to designated email IDs of depositories or you may lodge the same with SEBI online at https://scores.gov.in/scores/Welcome.html
14.	Keep a record of documents signed, DIS issued and account statements received.
15.	As Investors you are required to verify the transaction statement carefully for all debits and credits in your account. In case of any unauthorized debit or credit, inform the DP or your respective Depository.
16.	Appoint a nominee to facilitate your heirs in obtaining the securities in your demat account, on completion of the necessary procedures.
17.	Register for Depository's internet based facility or download mobile app of the depository to monitor your holdings.
18.	Ensure that, both, your holding and transaction statements are received periodically as instructed to your DP. You are entitled to receive a transaction statement every month if you have any transactions.
19.	Do not follow herd mentality for investments. Seek expert and professional advice for your investments
20.	Beware of assured/fixed returns.

Para 8 of Investor Charter

Rights of investors[13]

- Receive a copy of KYC, copy of account opening documents.
- No minimum balance is required to be maintained in a demat account.
- No charges are payable for opening of demat accounts.
- If executed, receive a copy of Power of Attorney. However, Power of Attorney is not a mandatory requirement as per SEBI / Stock Exchanges. You have the right to revoke any authorization given at any time.

- You can open more than one demat account in the same name with single DP/ multiple DPs.
- Receive statement of accounts periodically. In case of any discrepancies in statements, take up the same with the DP immediately. If the DP does not respond, take up the matter with the Depositories.
- Pledge and /or any other interest or encumbrance can be created on demat holdings.
- Right to give standing instructions with regard to the crediting of securities in demat account.
- Investor can exercise its right to freeze/defreeze his/her demat account or specific securities / specific quantity of securities in the account, maintained with the DP.
- In case of any grievances, Investor has right to approach Participant or Depository or SEBI for getting the same resolved within prescribed timelines.
- Every eligible investor shareholder has a right to cast its vote on various resolutions proposed by the companies for which Depositories have developed an internet based 'e-Voting' platform.
- Receive information about charges and fees. Any charges/tariff agreed upon shall not increase unless a notice in writing of not less than thirty days is given to the Investor.

Para 9 of Investor Charter

Responsibilities of Investors[14]

- Deal with a SEBI registered DP for opening demat account, KYC and Depository activities.
- Provide complete documents for account opening and KYC (Know Your Client). Fill all the required details in Account Opening Form / KYC form in own handwriting and cancel out the blanks.
- Read all documents and conditions being agreed before signing the account opening form.
- Accept the Delivery Instruction Slip (DIS) book from DP only (preprinted with a serial number along with client ID) and keep it in safe custody and do not sign or issue blank or partially filled DIS.

- Always mention the details like ISIN, number of securities accurately.
- Inform any change in information linked to demat account and obtain confirmation of updation in the system.
- Regularly verify balances and demat statement and reconcile with trades / transactions.
- Appoint nominee(s) to facilitate heirs in obtaining the securities in their demat account.
- Do not fall prey to fraudsters sending emails and SMSs luring to trade in stocks / securities promising huge profits.

Annexure 22

Format for Investor Complaints Data to be displayed by Depository Participants on their respective websites

Data for every month ending

SN	Received from	Carried forward from previous month	Received during the month	Total Pending	Resolved*	Pending at the end of the month**		Average Resolution time^ (in days)
						Pending for less than 3 months	Pending for more than 3 months	
1	2	3	4	5	6	7		8
1	Directly from Investors							
2	SEBI (SCORES)							
3	Depositories							
4	Other Sources (if any)							
5	**Grand Total**							

Trend of monthly disposal of complaints

SN	Month	Carried forward from previous month	Received	Resolved*	Pending**
1	2	3	4	5	6
1	April -YYYY				
2	May-YYYY				
3	June-YYYY				
4	July-YYYY				
	....				
	.....				
	March-YYYY				
	Grand Total				

*Should include complaints of previous months resolved in the current month, if any.

**Should include total complaints pending as on the last day of the month, if any.
^Average resolution time is the sum total of time taken to resolve each complaint in the current month divided by total number of complaints resolved in the current month.

Trend of annual disposal of complaints

SN	Year	Carried forward from previous year	Received during the year	Resolved during the year	Pending at the end of the year
1	2017-18				
2	2018-19				
3	2019-20				
4	2020-21				
5	2021-22				
	Grand Total				

Annexure 23

PRINCIPLES FOR FINANCIAL MARKET INFRASTRUCTURES

General Organisation

Principle 1: Legal basis

An FMI should have a well-founded, clear, transparent, and enforceable legal basis for each material aspect of its activities in all relevant jurisdictions.

Principle 2: Governance

An FMI should have governance arrangements that are clear and transparent, promote the safety and efficiency of the FMI, and support the stability of the broader financial system, other relevant public interest considerations, and the objectives of relevant stakeholders.

Principle 3: Framework for the comprehensive management of risks

An FMI should have a sound risk-management framework for comprehensively managing legal, credit, liquidity, operational, and other risks.

Credit and liquidity risk management.

Principle 4: Credit risk

An FMI should effectively measure, monitor, and manage its credit exposures to participants and those arising from its payment, clearing, and settlement processes. An FMI should maintain sufficient financial resources to cover its credit exposure to each participant fully with a high degree of confidence. In addition, a CCP that is involved in activities with a more-complex risk profile or that is systemically important in multiple jurisdictions should maintain additional financial resources sufficient to cover a wide range of potential stress scenarios that should include, but not be limited to, the default of the two participants and their affiliates that would potentially cause the largest aggregate credit exposure to the CCP in extreme but plausible market conditions. All other CCPs should maintain additional financial resources sufficient to cover a wide range of potential stress scenarios that should include, but not be limited to, the default of the participant and its affiliates that would potentially cause the largest aggregate credit exposure to the CCP in extreme but plausible market conditions.

Principle 5: Collateral

An FMI that requires collateral to manage its or its participants' credit exposure should accept collateral with low credit, liquidity, and market risks. An FMI should also set and enforce appropriately conservative haircuts and concentration limits.

Principle 6: Margin

A CCP should cover its credit exposures to its participants for all products through an effective margin system that is risk-based and regularly reviewed.

Principle 7: Liquidity risk

An FMI should effectively measure, monitor, and manage its liquidity risk. An FMI should maintain sufficient liquid resources in all relevant currencies to effect same-day and, where appropriate, intraday and multiday settlement of payment obligations with a high degree of confidence under a wide range of potential stress scenarios that should include, but not be limited to, the default of the participant and its affiliates that would generate the largest aggregate liquidity obligation for the FMI in extreme but plausible market conditions.

Settlement

Principle 8: Settlement finality

An FMI should provide clear and certain final settlement, at a minimum by the end of the value date. Where necessary or preferable, an FMI should provide final settlement intraday or in real time.

Principle 9: Money settlements

An FMI should conduct its money settlements in central bank money where practical and available. If central bank money is not used, an FMI should minimise and strictly control the credit and liquidity risk arising from the use of commercial bank money.

Principle 10: Physical deliveries

An FMI should clearly state its obligations with respect to the delivery of physical instruments or commodities and should identify, monitor, and manage the risks associated with such physical deliveries.

Central securities depositories and exchange-of-value settlement systems

Principle 11: Central securities depositories

A CSD should have appropriate rules and procedures to help ensure the integrity of securities issues and minimise and manage the risks associated with the safekeeping and transfer of securities. A CSD should maintain securities in an immobilised or dematerialised form for their transfer by book entry.

Principle 12: Exchange-of-value settlement systems

If an FMI settles transactions that involve the settlement of two linked obligations (for example, securities or foreign exchange transactions), it should eliminate principal risk by conditioning the final settlement of one obligation upon the final settlement of the other.

Default management

Principle 13: Participant-default rules and procedures

An FMI should have effective and clearly defined rules and procedures to manage a participant default. These rules and procedures should be designed to ensure that the FMI can take timely action to contain losses and liquidity pressures and continue to meet its obligations.

Principle 14: Segregation and portability

A CCP should have rules and procedures that enable the segregation and portability of positions of a participant's customers and the collateral provided to the CCP with respect to those positions.

General business and operational risk management

Principle 15: General business risk

An FMI should identify, monitor, and manage its general business risk and hold sufficient liquid net assets funded by equity to cover potential general business losses so that it can continue operations and services as a going concern if those losses materialise. Further, liquid net assets should at all times be sufficient to ensure a recovery or orderly wind-down of critical operations and services.

Principle 16: Custody and investment risks

An FMI should safeguard its own and its participants' assets and minimise the risk of loss on and delay in access to these assets. An FMI's investments should be in instruments with minimal credit, market, and liquidity risks.

Principle 17: Operational risk

An FMI should identify the plausible sources of operational risk, both internal and external, and mitigate their impact through the use of appropriate systems, policies, procedures, and controls. Systems should be designed to ensure a high degree of security and operational reliability and should have adequate, scalable capacity. Business continuity management should aim for timely recovery of operations and fulfillment of the FMI's obligations, including in the event of a wide-scale or major disruption.

Access

Principle 18: Access and participation requirements

An FMI should have objective, risk-based, and publicly disclosed criteria for participation, which permit fair and open access.

Principle 19: Tiered participation arrangements

An FMI should identify, monitor, and manage the material risks to the FMI arising from tiered participation arrangements.

Principle 20: FMI links

An FMI that establishes a link with one or more FMIs should identify, monitor, and manage link-related risks.

Efficiency

Principle 21: Efficiency and effectiveness

An FMI should be efficient and effective in meeting the requirements of its participants and the markets it serves.

Principle 22: Communication procedures and standards

An FMI should use, or at a minimum accommodate, relevant internationally accepted communication procedures and standards in order to facilitate efficient payment, clearing, settlement, and recording.

Transparency

Principle 23: Disclosure of rules, key procedures, and market data

An FMI should have clear and comprehensive rules and procedures and should provide sufficient information to enable participants to have an accurate understanding of the risks, fees, and other material costs they incur by participating in the FMI. All relevant rules and key procedures should be publicly disclosed.

Principle 24: Disclosure of market data by trade repositories

A TR should provide timely and accurate data to relevant authorities and the public in line with their respective needs.

भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

Annexure 24

Format for monitoring compliance with requirements emanating from SEBI circulars/guidelines/advisories related to technology

Sl. No.	Date of SEBI circular/ directions/advice, etc.	Subject	Technological requirements specified by SEBI in brief	Mechanism put in place by the MIIs	Non compliances with SEBI circulars/ directions, etc.	Compliance status (Open/ closed)	Comments of the Management	Time-line for taking corrective action in case of open observations

भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

Annexure 25

Exception Observation Reporting Format

Note: MIIs are expected to submit following information with regard to exceptional major non-compliances (NCs) / minor NCs observed in the System and Network Audit. MIIs should also categorically highlight those observations/NCs/suggestions pointed out in the System and Network Audit (current and previous) which are not yet complied with.

Name of the MII: _____

Name of the Auditor: _____

Systems and Network Audit Report Date:_____

Table 1: For preliminary audit

Audit period	Observation No.	Description of finding	Department of MII	Status / Nature of finding	Risk Rating of findings as per Auditor	Audit TOR clause	Root Cause Analysis	Impact Analysis	Corrective Actions proposed by auditor	Deadline for the corrective action	Management response in case of acceptance of associated risks	Whether similar issue was observed in any of the previous 3 Audits

Description of relevant Table heads

1. **Audit Period –** This indicates the period of audit
2. **Description of findings/observations –** Description of the findings in sufficient details, referencing any accompanying evidence
3. **Status/ Nature of Findings –** The category can be specified, for example:
    a. Non-compliant (Major/Minor)
    b. Work in progress
    c. Observation
    d. Suggestion
4. **Risk Rating of finding** -A rating has to be given for each of the observations based on its impact and severity to reflect the risk exposure as well as the suggested priority for action

Rating	Description

HIGH	Represents weakness in control with respect to threat(s) that is /are sufficiently capable and impacts asset (s) leading to regulatory non-compliance, significant financial, operational and reputational loss. These observations need to be addressed with utmost priority.
MEDIUM	Represents weakness in control with respect to threat(s) that is /are sufficiently capable and impacts asset (s) leading to exposure in terms of financial, operational and reputational loss. These observations need to be addressed in reasonable timeframe.
LOW	Represents weaknesses in control, which in combination with other weakness can develop into an exposure. Suggested improvements for situations not immediately/directly affecting controls. .

5. **Audit TOR clause –** The TOR clause corresponding to this observation
6. **Root Cause analysis –** A detailed analysis on the cause of the non-conformity.
7. **Impact Analysis –** An analysis of the likely impact on the operations/ activity of the organization
8. **Corrective Action –** The action taken to correct the non-conformity

Table 2: For follow on/ follow up system and Network audit

Preliminary Audit Date	Preliminary Audit Period	Preliminary Observation Number	Preliminary Status	Preliminary Corrective Action as proposed by Auditor	Current Finding	Current Status	Revised Corrective Action, if any	Deadline for the Revised Corrective Action	Reason for delay in implementation/ compliance

Description of relevant Table heads

1. **Preliminary Status –** The original finding as per the preliminary System and Network Audit Report
2. **Preliminary Corrective Action –** The original corrective action as prescribed in the preliminary System and Network audit report
3. **Current Finding –** The current finding w.r.t. the issue
4. **Current Status –** Current Status of the issue viz. compliant, non-compliant, work in progress (WIP)
5. **Revised Corrective Action –** The revised corrective action prescribed w.r.t. the Non-compliant/ WIP issues

Annexure 26

Date	Department of SEBI	Name of Intermediary / Other entities	Type of Intermediary	SEBI Regn. No. (If any)	PAN	Amount (Rs.)	Purpose of Payment (including the period for which payment was made e.g. quarterly, annually)	Bank name and Account number from which payment is remitted	UTR No.

भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

Annexure 27

Form to report on AI and ML technologies – to be submitted quarterly

S/N	Head	Value
1	Entity SEBI registration number	
2	Registered entity category	
3	Entity name	
4	Entity PAN no.	
5	Application / System name	
6	Date used from	
7	Type of area where AI or ML is used (order execution / Surveillance / compliance / others). In case of others, please specify.	
8	What is the name of the Tool / Technology that is categorized as AI and ML system / Application and submissions are declared vide this response	<free text field>
9	How was the AI or ML project implemented	<Internally / through solution provider / Jointly with a solution provider or third party>
10	Are the key controls and control points in your AI or ML application or systems in accordance with circular(s) of SEBI that mandate/s cybersecurity control requirements	<free text field>
11	Is the AI / ML system included in the system audit	<Yes / No>
12	Describe the application / system and how it uses AI / ML	<free text field>
13	What safeguards are in place to prevent abnormal behavior of the AI or ML application / System	<free text field>

Annexure 28

Various Scenarios

Current process	Proposed process
Scenario 1: Prefunded purchase by client	
• Client transfers Rs. 150 to member. • Member may retain the client funds with itself and allocate collateral to the extent of 20% margin requirements at the CC (Say Rs. 30). • Client purchases a share for Rs. 100, the margin collection requirement is Rs. 20 which is blocked from client's allocation. • Collateral is released after the member completes the net settlement with the CC.	• Client creates a block of Rs. 150 in favour of the CC. The amount shall get allocated as collateral. • The client purchases a share worth Rs. 100. The margin requirement is 20, this shall get adjusted from the block (which is allocated as collateral). • STT and stamp duty shall be 11 paise, which shall be added to the client's obligation. The CC shall debit 100.11 towards settlement at the stipulated time. • With the successful debit from the client, the securities receivable by the client shall be provided in the client's depository account directly by the CC at the time of settlement pay-out.
Scenario 2: Delivery sale by client by early pay-in	
• Client uses block mechanism for early pay-in of securities. • Such early pay-in information is received by the CC from depositories. • A sell order is executed on behalf of the client. • If sell order is executed after early pay-in, then no margin is applicable at any time. • If early pay-in is received subsequent to the sell order execution, the proprietary collateral of the member shall be blocked till receipt of early pay-in. • While providing pay-out to the client, the member may adjust other	• The client shall provide securities as early pay-in through the block mechanism only. • If the early pay-in information is received from depository before trade execution, there shall be no margin. If the information is received subsequently, the proprietary collateral of the member shall be blocked till the receipt of early pay-in. • Since the client has completed the settlement, the CC shall pay out funds directly in the client account. While providing the funds pay-out, CC shall deduct the STT and stamp duty.

statutory dues (stamp duty, STT), brokerage etc.	
Scenario 3: Purchase/sale by client supported by margins	
• Client provides 20% margin to the member. Client can execute trades based on the margins on trade date. The client shall need to provide the remaining 80% amount (in case of purchase) or deliver the security (in case of sale) till the applicable settlement deadline.	• The client may create only partial block to the extent of margin instead of entire upfront value or early pay-in through block mechanism. The client shall need to provide additional block or provide early pay-in till the stipulated time. Further process shall be same as discussed in Scenario 1 and Scenario 2.
Scenario 4: Intraday cash market/derivatives trading	
• Client provides margin money to the member. Client carries out intraday trading or trade in derivatives. There are no exchange-of-value delivery obligations (funds against securities or vice-versa), but only losses or gains. Losses shall be deducted from the margin money given by clients and gains may be added to the margin money of client or paid out.	• In case of losses, the CC shall debit the block to the extent of losses towards client pay-in. • In case of gains, the pay-out shall be given by CC in the client account. The CC shall not add the pay-out to the funds collateral of the client, and if desired the client may create another block.

Annexure 29

S. No	Parameter	Maturity Indicator Level (MIL)	No of Levels	Maximum Permissible Score
Domain : Governance of Critical Infrastructure and Personnel				
1	As part of the operational risk management framework to manage risk to systems, networks and databases from cyber-attacks and threats, MII should formulate a comprehensive cyber security and cyber resilience policy document encompassing the framework mentioned hereunder. The policy document should be approved by the Board, and in case of deviations from the suggested framework, reasons for such deviations should also be provided in the policy document. The policy document should be reviewed by the MII's Board at least annually with the view to strengthen and improve its cyber security and cyber resilience framework.	MIL 1: No cyber security policy document. MIL 2: Policy approved by the Board. No deviations from suggested framework or if deviations observed, reasons provided. MIL 3: Policy document reviewed by MIIs Board at least annually. MIL 4: Policy document includes security framework more stringent than SEBI guidelines/ policy document reviewed multiple times during the year.	4	3
2	The cyber security and cyber resilience policy should include the following process to identify, assess, and manage cyber security risk associated with processes, information, networks and systems. a. 'Identify' critical IT assets and risks associated with such assets, b. 'Protect' assets by deploying suitable controls, tools and measures, c. 'Detect' incidents, anomalies and attacks through appropriate monitoring tools / processes, d. 'Respond' by taking immediate steps after identification of the incident, anomaly or attack, e. 'Recover' from incident through	MIL 1: No cyber security policy document. MIL 2: Policy document includes ad-hoc process to identify, assess and manage cyber security risk. MIL 3: Policy document includes planned and documented process to identify, assess and manage cyber security risk.	3	2

S. No	Parameter	Maturity Indicator Level (MIL)	No of Levels	Maximum Permissible Score
	incident management, disaster recovery and business continuity framework.			
3	The Cyber security policy should encompass the principles prescribed by National Critical Information Infrastructure Protection Centre (NCIIPC) of National Technical Research Organisation (NTRO), Government of India in the report titled 'Guidelines for Protection of National Critical Information Infrastructure' and subsequent revisions, if any, from time to time.	MIL 1: No cyber security policy document. MIL 2: Policy document includes principles prescribed by NCIIPC, NTRO and Government of India MIL 3: Policy document is being revised annually to include changes prescribed by NCIIPC, NTRO and Government of India. MIL 4: Policy document is being revised multiple times in a year to include changes prescribed by NCIIPC, NTRO and Government of India.	4	3
4	MII should also incorporate best practices from standards such as ISO 27001, ISO 27002, COBIT 5, etc., or their subsequent revisions, if any, from time to time.	MIL 1: No cyber security policy document. MIL 2: Policy document includes best practices from standards such as ISO 27001, ISO 27002, COBIT 5, etc. MIL 3: Policy document is being revised annually to include best practices from standards such as ISO 27001, ISO 27002, COBIT 5, etc. MIL 4: Policy document is being revised multiple times in a year to include best practices	4	3

S. No	Parameter	Maturity Indicator Level (MIL)	No of Levels	Maximum Permissible Score
		from standards such as ISO 27001, ISO 27002, COBIT 5, etc.		
5	MII should designate a senior official as Chief Information Security Officer (CISO) whose function would be to assess, identify and reduce cyber security risks, respond to incidents, establish appropriate standards and controls, and direct the establishment and implementation of processes and procedures as per the cyber security and resilience policy approved by the Board of the MII.	MIL 1: No CISO appointed MIL 2: CISO appointed without well-defined functions. MIL 3: CISO appointed with well-defined functions as per the cyber security and resilience policy. MIL 4: The functions of CISO are reviewed periodically and modified accordingly.	4	3
6	The Oversight Standing Committee on Technology of the stock exchanges and of the clearing corporations and the IT Strategy Committee of the depositories should on a quarterly basis review the implementation of the cyber security and resilience policy approved by their Boards, and such review should include review of their current IT and cyber security and resilience capabilities, set goals for a target level of cyber resilience, and establish a plan to improve and strengthen cyber security and cyber resilience.	MIL 1: No review conducted. MIL 2: Review conducted with less frequency than advised. MIL 3: Review conducted quarterly and only shortcomings as pointed out addressed MIL 4: Committee reviewed quarterly and also provided inputs to improve the strengthen cyber security framework which have been carried out.	4	3

S. No	Parameter	Maturity Indicator Level (MIL)	No of Levels	Maximum Permissible Score
7	MII should establish a reporting procedure to facilitate communication of unusual activities and events to CISO or to the senior management in a timely manner.	MIL 1: No procedure established to facilitate communication of unusual activities and events to CISO or to the senior management in a timely manner. MIL 2: Procedure established to facilitate communication of unusual activities and events, but not till the level of CISO. MIL 3: Procedure established to facilitate communication of unusual activities and events to CISO or to the senior management in a timely manner. MIL 4: Procedure established to facilitate communication of unusual activities and events to MD/CEO and the Governing Board.	4	3
8	The aforementioned committee and the senior management of the MII, including the CISO, should periodically review instances of cyber-attacks, if any, domestically and globally, and take steps to strengthen cyber security and cyber resilience framework.	MIL 1: No review of cyber-attacks is conducted. MIL 2: Review of cyber-attacks is conducted, but no remedial action is taken. MIL 3: Periodic review of cyber-attacks is conducted and prompt remedial action is taken. MIL 4: Periodic review of cyber-attacks is conducted and remedial action is taken. Preventive steps to counter similar attacks is also undertaken.	4	3

S. No	Parameter	Maturity Indicator Level (MIL)	No of Levels	Maximum Permissible Score
9	MII should define responsibilities of its employees, outsourced staff, and employees of vendors, members or participants and other entities, who may have access or use systems / networks of MII, towards ensuring the goal of cyber security.	MIL 1: Responsibilities of personnel who may have access or use systems/ networks is not defined. MIL 2: Responsibilities of personnel who may have access or use systems/ networks is mentioned but not clearly defined. MIL 3: Responsibilities of personnel who may have access or use systems/ networks are clearly defined. MIL 4: Responsibilities of personnel who may have access or use systems/ networks are defined. The same are periodically reviewed and revised accordingly.	4	3
Domain : Identification critical assets and risks				
10	MII should identify critical assets based on their sensitivity and criticality for business operations, services and data management. To this end, MII 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.	MIL 1: MII has not identified any critical assets and is not maintaining any inventory of its hardware, software and information assets. MIL 2: MII has identified critical assets however is not maintaining any inventory of its hardware, software and information assets. MIL 3: MII has identified critical assets and is maintaining a basic inventory of its hardware, software and information assets.	5	4

S. No	Parameter	Maturity Indicator Level (MIL)	No of Levels	Maximum Permissible Score
		MIL 4: MII has identified critical assets and is maintaining a basic inventory of its hardware, software and information assets and is reviewing the same at least half-yearly. MIL 5: MII has identified critical assets and is maintaining a basic inventory of its hardware, software and information assets and is reviewing the same at least half-yearly. (Including its shadow inventory.)		
11	MII should accordingly identify cyber risks (threats and vulnerabilities) that it may face, alongwith the likelihood of such threats and impact on the business and thereby, deploy controls commensurate to the criticality.	MIL 1: MII has not identified / categorized / envisaged cyber threats. MIL 2: MII has identified / maintained a Software / Hardware inventory but has not categorized / envisaged cyber threats. MIL 3: MII has identified / maintained a Software / Hardware inventory and has categorized / envisaged probable cyber threats prevalent to the sector. MIL 4: MII has identified / maintained a Software / Hardware inventory and has categorized / envisaged probable cyber threats based on its deployed architecture and network architecture.	4	3

S. No	Parameter	Maturity Indicator Level (MIL)	No of Levels	Maximum Permissible Score
12	MII should also encourage its third-party providers, such as service providers, stock brokers, depository participants, etc. to have similar standards of Information Security.	MIL 1: MII has an outsourcing policy that does not enlist such a clause for its third party vendors. MIL 2: MII has an outsourcing policy that does not enlist such a clause for its vendors.	2	1
Domain : Protection of Critical Assets and Infrastructure				
Sub-Domain : Access Controls				
13	No person by virtue of rank or position should have any intrinsic right to access confidential data, applications, system resources or facilities.	MIL 1: MII has no documented and approved data classification methodology. MIL 2: MII has a documented and approved data classification methodology, however (any one) the previous 3 System Audits have pointed out observations pertaining to access matrices or email ids/ login ids of ex-employees. MIL 3: MII has a documented and approved data classification methodology, and none of the previous 3 System Audits have pointed out observations pertaining to access matrices or email ids/ login ids of ex-employees.	3	2
14	Any access to MII's systems, applications, networks, databases, etc., should be for a defined purpose and for a defined period. MII should grant access to IT systems, applications, databases and networks on a need-to-use basis and based on the principle of least privilege. Such access should be for the period when the access	MIL 1: MII has no documented and approved access control methodology for systems, applications, networks, databases of the MII. MIL 2: MII has a documented and approved access control	4	3

S. No	Parameter	Maturity Indicator Level (MIL)	No of Levels	Maximum Permissible Score
	is required and should be authorized using strong authentication mechanisms.	methodology for systems, applications, networks, databases of the MII. However the System Audit / Comprehensive review has highlighted observations pertaining to the same. MIL 3: MII has a documented and approved access control methodology for systems, applications, networks, databases of the MII. and the System Audit / Comprehensive review has no observations pertaining to the same. MIL 4 : MII has a documented and approved access control methodology for systems, applications, networks, databases of the MII. and the System Audit / Comprehensive review has no observations pertaining to the same. The MII policy for the same has a defined timelines for review.		
15	MII should implement strong password controls for users' access to systems, applications, networks and databases. Password controls should include a change of password upon first log-on, minimum password length and history, password complexity as well as maximum validity period. The user credential data should be stored using strong and latest hashing algorithms.	MIL 1: MII has no documented and approved password policy encompassing the requirements of the clause. MIL 2: MII has a documented and approved password policy however the same does not completely encompass the requirements of the clause.	3	2

S. No	Parameter	Maturity Indicator Level (MIL)	No of Levels	Maximum Permissible Score
		MIL 3: MII has a documented password policy encompassing the requirements of the clause, however the same is not approved.		
16	MII should ensure that records of user access are uniquely identified and logged for audit and review purposes. Such logs should be maintained and stored in encrypted form for a time period not less than two (2) years.	MIL 1: MII does not have an explicit (documented and approved) data retention and log management and rotation policy with relevant SOPs for the same. MIL 2: MII has an explicit (documented and approved) data retention and log management and rotation policy with relevant SOPs for the same. However the System Audit / Comprehensive review has highlighted observations pertaining to the same. MIL 3: MII has an explicit (documented and approved) data retention and log management and rotation policy with relevant SOPs for the same. And the System Audit / Comprehensive review has highlighted no observations pertaining to the same.	3	2
17	MII should deploy additional controls and security measures to supervise staff with elevated system access entitlements (such as admin or privileged users). Such controls and measures should inter-alia include restricting the number of privileged users, periodic review of privileged users' activities, disallow privileged users from accessing systems	MIL 1: The MII does not have Privilege Identity Management (PIM) solution deployed at both production systems (core Systems) as well as on non-production systems. MIL 2: The MII has a Privilege Identity Management (PIM)	3	2

S. No	Parameter	Maturity Indicator Level (MIL)	No of Levels	Maximum Permissible Score
	logs in which their activities are being captured, strong controls over remote access by privileged users, etc.	solution deployed at production systems (core Systems) but not on non-production systems. MIL 3: The MII has a Privilege Identity Management (PIM) solution deployed at production systems (core Systems) but not on non-production systems.		
18	Account access lock policies after failure attempts should be implemented for all accounts.	MIL 1: MII does not have a documented and approved account lock out policy. MIL 2 :The MII has a documented and approved account lock-out policy , however the policy doesn't segregate between different types of resources based on risk , user type etc. MIL 3: The MII has a documented and approved account lock-out policy , and the policy segregates the different types of resources based on risk , user type etc, however the System Audit / Comprehensive review has highlighted observations pertaining to the same. MIL 4: The MII has a documented and approved account lock-out policy , and the policy segregates the different types of resources	4	3

S. No	Parameter	Maturity Indicator Level (MIL)	No of Levels	Maximum Permissible Score
		based on risk , user type etc, and the System Audit / Comprehensive review has no observations pertaining to the same.		
19	Employees and outsourced staff such as employees of vendors or service providers, who may be given authorised access to the MII's critical systems, networks and other computer resources, should be subject to stringent supervision, monitoring and access restrictions.	MIL 1: MII does not have an approved policy for privileged identity management (PIM) for own staff as well as staff of vendors. MIL 2: MII has an approved policy for privileged identity management (PIM) for own staff however the same does not encompass the staff of vendors. MIL 3: MII has an approved policy for privileged identity management (PIM) for own staff which also encompass the staff of vendors, however the System Audit / Comprehensive review has highlighted observations pertaining to the same. MIL 4: MII has an approved policy for privileged identity management (PIM) for own staff which also encompass the staff of vendors , and the System Audit / Comprehensive review has no	4	3

S. No	Parameter	Maturity Indicator Level (MIL)	No of Levels	Maximum Permissible Score
		observations pertaining to the same.		
20	Two-factor authentication at log-in should be implemented for all users that connect using online / internet facility.	MIL 1: MII has not implemented a 2FA at log-in for all users that connect using online / internet facility, neither the MII has put in multi-step authentication as a compensating mechanism. MIL 2: MII has not implemented a 2FA at log-in for all users that connect using online / internet facility, neither the MII has put in multi-step authentication as a compensating mechanism. However, the MII is in process of implementing 2FA and is currently in the transition phases. MIL 3: MII has implemented a 2FA log-in for all users that connect using online / internet facility. However the System Audit / Comprehensive review has highlighted observations pertaining to the same. MIL 4: MII has implemented a 2FA log-in for all users that connect using online / internet facility and the System Audit / Comprehensive review has no observations pertaining to the same.	4	3
21	MII should formulate an Internet access policy to monitor and regulate the use of internet and internet based services such	MIL 1: MII has not formulated an internet access policy based on the controls specified in the clause.	5	4

S. No	Parameter	Maturity Indicator Level (MIL)	No of Levels	Maximum Permissible Score
	as social media sites, cloud-based internet storage sites, etc.	MIL 2: MII has formulated an internet access policy, however the same does not elaborate on the use of social media sites and / or cloud based storage sites / clients. MIL 3: MII has formulated an internet access policy and the same specifically addresses the issue of use of social media sites and / or cloud based storage sites / clients, however the System Audit / Comprehensive review has highlighted observations pertaining to the same. MIL 4: MII has formulated an internet access policy and the same specifically addresses the issue of use of social media sites and / or cloud based storage sites / clients and the System Audit / Comprehensive review has no observations pertaining to the same. The MII has not reviewed the policy in the past year. MIL 5: MII has formulated an internet access policy and the same specifically addresses the issue of use of social media sites and / or cloud based storage sites / clients and the System Audit / Comprehensive review has no observations pertaining		

S. No	Parameter	Maturity Indicator Level (MIL)	No of Levels	Maximum Permissible Score
		to the same. The MII has reviewed the policy in the past year.		
22	Proper 'end of life' mechanism should be adopted to deactivate access privileges of users who are leaving the organization or who access privileges have been withdrawn.	MIL 1: MII has no policy for 'end of life' mechanism for all users. MIL 2: MII has a documented and approved policy for 'end of life' mechanism for all users. MIL 3: MII has a documented and approved policy for 'end of life' mechanism for all users, based on a need-to-use basis and on the principle of least privilege.	3	2
Sub-Domain : Physical Security				
23	Physical access to the critical systems should be restricted to minimum. Physical access of outsourced staff / visitors should be properly supervised by ensuring at the minimum that outsourced staff / visitors are accompanied at all times by authorised employees.	MIL 1: Physical access to critical systems is not monitored. MIL 2: Physical access to critical systems is restricted to minimum, but outsourced staff / visitors are not accompanied at all times by authorised employees MIL 3: Physical access to critical systems is restricted to minimum, and outsourced staff / visitors are accompanied at all times by authorised employees	3	2

S. No	Parameter	Maturity Indicator Level (MIL)	No of Levels	Maximum Permissible Score
24	Physical access to the critical systems should be revoked immediately if the same is no longer required.	MIL 1: Physical access to critical systems is not revoked, even if it is no longer required. MIL 2: Physical access to critical systems is revoked immediately, when it is no longer required.	2	1
25	MII should ensure that the perimeter of the critical equipment's room are physically secured and monitored by employing physical, human and procedural controls such as the use of security guards, CCTVs, card access systems, mantraps, bollards, etc. where appropriate.	MIL 1: Critical equipment's room is not physically secured. MIL 2: Critical equipment's room is physically secured. MIL 3: Critical equipment's room is physically secured, and is utilizing latest security systems which is being updated on continuous basis.	3	2
Sub-Domain : Network Security Management				
26	MII should establish baseline standards to facilitate consistent application of security configurations to operating systems, databases, network devices and enterprise mobile devices within the IT environment. The MII should conduct regular enforcement checks to ensure that the baseline standards are applied uniformly.	MIL 1: No baseline standard of security configurations is implemented. MIL 2: Baseline standard of security configurations is implemented. But no regular enforcement checks are being conducted. MIL 3: Baseline standard of security configurations is implemented and regular enforcement checks are being conducted. MIL 4: Baseline standard of security configurations is implemented and regular	4	3

S. No	Parameter	Maturity Indicator Level (MIL)	No of Levels	Maximum Permissible Score
		enforcement checks are being conducted. Further, security configurations are being reviewed regularly.		
27	MII should install network security devices, such as firewalls as well as intrusion detection and prevention systems, to protect its IT infrastructure from security exposures originating from internal and external sources.	MIL 1: No firewalls and intrusion detection and prevention systems are installed. MIL 2: Firewalls and intrusion detection and prevention systems are installed. MIL 3: Firewalls and intrusion detection and prevention systems are installed. The same are patched and updated regularly.	3	2
28	Anti-virus software should be installed on servers and other computer systems. Updation of Anti-virus definition files and automatic anti-virus scanning should be done on a regular basis.	MIL 1: No anti-virus software installed on servers and other computer systems. MIL 2: Anti-virus software installed on servers and other computer systems, but is not updated on regular basis. MIL 3: Anti-virus software installed on servers and other computer systems. The same is being updated on regular basis.	3	2
Sub-Domain : Security of Data				

S. No	Parameter	Maturity Indicator Level (MIL)	No of Levels	Maximum Permissible Score
29	Data-in motion and Data-at-rest should be in encrypted form by using strong encryption methods such as Advanced Encryption Standard (AES), RSA, SHA-2, etc.	MIL 1: MII has not identified critical data / classified data and is not encrypting data-in-motion/rest. MIL 2: MII is encrypting data-in-motion/rest but has not identified critical data / classified data. MIL 3: MII is encrypting data-in-motion/rest using strong encryption methods and has identified critical data / classified data , however the System Audit / Comprehensive review has highlighted observations pertaining to the encryption of data-in-motion/rest. MIL 4: MII is encrypting data-in-motion/rest using strong encryption methods and has identified critical data / classified data, and the System Audit / Comprehensive review has no observation(s) pertaining to the encryption of data-in-motion/rest and/or classification/ identification of critical data. MIL 5: MII is encrypting data-in-motion/rest using strong encryption methods and has identified critical data / classified data , and the System Audit / Comprehensive review	5	4

S. No	Parameter	Maturity Indicator Level (MIL)	No of Levels	Maximum Permissible Score
		has no observation(s) pertaining to the encryption of data-in-motion/rest and/or classification/ identification of critical data. Additionally the MII either reviews the data classification methodology on an annual basis or the MII improves upon the encryption standards deployed periodically.		
30	MII should implement measures to prevent unauthorised access or copying or transmission of data / information held in contractual or fiduciary capacity. It should be ensured that confidentiality of information is not compromised during the process of exchanging and transferring information with external parties.	MIL 1: MII has not identified critical data / classified data and does not have an approved data leakage prevention policy. MIL 2: MII has identified critical data / classified data however it does not have an approved data leakage prevention policy. MIL 3: MII has identified critical data / classified data and has an approved data leakage prevention policy however the System Audit / Comprehensive review has highlighted observations pertaining to leakage of data. MIL 4: MII has identified critical data / classified data and has an approved data leakage prevention policy and the System Audit / Comprehensive review has no observations pertaining to leakage of data.	4	3

S. No	Parameter	Maturity Indicator Level (MIL)	No of Levels	Maximum Permissible Score
31	The information security policy should also cover use of devices such as mobile phone, faxes, photocopiers, scanners, etc. that can be used for capturing and transmission of data.	MIL 1: The MIIs information security policy does not address the usage of, security of and prevention of data leakage through, various devices that can be used for capturing and transmission of data. MIL 2: The MIIs information security policy addresses the usage of, security of and prevention of data leakage through, various devices that can be used for capturing and transmission of data however the System Audit / Comprehensive review has highlighted observations pertaining to the same. MIL 3: The MIIs information security policy addresses the usage of, security of and prevention of data leakage through, various devices that can be used for capturing and transmission of data and the System Audit / Comprehensive review has no observations pertaining to the same.	3	2

S. No	Parameter	Maturity Indicator Level (MIL)	No of Levels	Maximum Permissible Score
32	MII should allow only authorized data storage devices through appropriate validation processes.	MIL 1: MII does not have an approved hardware & software inventory management policy. MIL 2: MII has an approved hardware & software inventory management policy however it has not maintained a software and hardware inventory. (not even at a rudimentary level). MIL 3: MII has an approved hardware & software inventory management policy and it has maintained a basic software and hardware inventory. However, the System Audit / Comprehensive review has highlighted observations pertaining to the storage of data on devices without following the approved process. MIL 4: MII has an approved hardware & software inventory management policy and it has maintained a basic software and hardware inventory and the System Audit / Comprehensive review has no observations pertaining to the storage of data on devices without following the approved process.	4	3
Sub-Domain : Hardening of Hardware and Software				

S. No	Parameter	Maturity Indicator Level (MIL)	No of Levels	Maximum Permissible Score
33	Only a hardened and vetted hardware / software should be deployed by the MII. During the hardening process, MII should inter-alia ensure that default passwords are replaced with strong passwords and all unnecessary services are removed or disabled in equipment / software.	MIL 1: Hardening of hardware/ software utilized by MIIs is not being conducted. MIL 2: The hardware/ software utilized by MIIs is hardened and vetted. MIL 3: During the hardening process default passwords are replaced with strong passwords and all unnecessary services are removed or disabled. MIL 4: The hardening process is regularly reviewed to plug vulnerabilities in the system.	4	3
34	All open ports which are not in use or can potentially be used for exploitation of data should be blocked. Other open ports should be monitored and appropriate measures should be taken to secure the ports.	MIL 1: Open ports not in use are not blocked. MIL 2: Open ports which are not in use or can potentially be used for exploitation of data are blocked. MIL 3: Open ports which are not in use or can potentially be used for exploitation of data are blocked. Other open ports are monitored and measures are taken to secure the same. MIL 4: Status of open ports are reviewed regularly to decide whether the port should be kept open or not.	4	3
Sub-Domain : Application Security and Testing				

S. No	Parameter	Maturity Indicator Level (MIL)	No of Levels	Maximum Permissible Score
35	MII should ensure that regression testing is undertaken before new or modified system is implemented. The scope of tests should cover business logic, security controls and system performance under various stress-load scenarios and recovery conditions.	MIL 1: No regression testing is undertaken. MIL 2: Regression testing is undertaken, but the scope is not as per SEBI guidelines. MIL 3: Regression testing is undertaken and the scope of tests is as per SEBI guidelines.	3	2
Sub-Domain : Patch Management				
36	MII should establish and ensure that the patch management procedures include the identification, categorisation and prioritisation of security patches. An implementation timeframe for each category of security patches should be established to implement security patches in a timely manner.	MIL 1: No patch management procedures are established. MIL 2: Patch management procedures are established to include the identification, categorisation and prioritisation of security patches MIL 3: Patch management procedures and implementation timeframe for each category of security patches are established. MIL 4: Patch management procedure is periodically reviewed to ensure quick updation of patches.	4	3
37	MII should perform rigorous testing of security patches before deployment into the production environment so as to ensure that the application of patches do not impact other systems.	MIL 1: No testing of security patches undertaken. MIL 2: Testing of security patches undertaken before deployment into the production environment so as to ensure that the application of	3	2

S. No	Parameter	Maturity Indicator Level (MIL)	No of Levels	Maximum Permissible Score
		patches do not impact other systems. MIL 3: Patch testing policy has been adopted so that untested patches are not deployed in production environment.		
Sub-Domain : Disposal of Systems and Storage Devices				
38	MII should frame suitable policy for disposals of the storage media and systems. The data / information on such devices and systems should be removed by using methods viz. wiping / cleaning / overwrite, degauss and physical destruction, as applicable.	MIL 1: No policy for disposals of the storage media and systems. MIL 2: Policy for disposals of the storage media and systems is adopted and is being implemented at all times.	2	1
Sub-Domain : Vulnerability Assessment and Penetration Testing				
39	MII should regularly conduct vulnerability assessment to detect security vulnerabilities in the IT environment. MII should also carry out periodic penetration tests, at least once in a year, in order to conduct an in-depth evaluation of the security posture of the system through simulations of actual attacks on its systems and networks.	MIL 1: MII's information security policy doesn't encompass periodically conducting VA and PT. MIL 2: MII's information security policy encompasses periodically conducting VA and PT however the MII has not	5	4

S. No	Parameter	Maturity Indicator Level (MIL)	No of Levels	Maximum Permissible Score
40	Remedial actions should be immediately taken to address gaps that are identified during vulnerability assessment and penetration testing.	been conducting either VA or PT as per the approved policy. MIL 3: MII's information security policy encompasses periodically conducting VA and PT and the MII has been conducting VA and PT as per the approved policy, however the System Audit / Comprehensive review has highlighted observations pertaining to the open areas found during the VA/PT. MIL 4: MII's information security policy encompasses periodically conducting VA and PT and the MII has been conducting VA and PT as per the approved policy, however the System Audit / Comprehensive review has no observations pertaining to the open areas found during the VA/PT. (i.e. all vulnerabilities found in the VA/PT were addressed by the MII in a time-bound manner.) MIL 5: In addition to MIL 4, the MII also fine tunes its VA and or PT (based on learnings) and also periodically changes vendors.		

S. No	Parameter	Maturity Indicator Level (MIL)	No of Levels	Maximum Permissible Score
41	In addition, MII should perform vulnerability scanning and conduct penetration testing prior to the commissioning of a new system which offers internet accessibility and open network interfaces.	(For new systems built internally or owned by the MII / its subsidiary) MIL 1: MII's information security policy doesn't encompass periodically conducting VA and PT for new systems (including those which offer internet accessibility and open network interfaces). MIL 2: MII's information security policy encompasses periodically conducting VA and PT for new systems (including those which offer internet accessibility and open network interfaces), however the MII has not been conducting either VA or PT as per the approved policy. MIL 3: MII's information security policy encompasses periodically conducting VA and PT for new systems (including those which offer internet accessibility and open network interfaces) and the MII has been conducting VA and PT as per the approved policy, however the System Audit / Comprehensive review has highlighted observations pertaining to the open areas found during the VA/PT for new systems (including those which offer internet accessibility and open network interfaces). MIL 4: MII's information security policy encompasses	5	4

S. No	Parameter	Maturity Indicator Level (MIL)	No of Levels	Maximum Permissible Score
		periodically conducting VA and PT for new systems (including those which offer internet accessibility and open network interfaces) and the MII has been conducting VA and PT as per the approved policy, however the System Audit / Comprehensive review has no observations pertaining to the open areas found during the VA/PT. (i.e. all vulnerabilities found in the VA/PT were addressed by the MII in a time-bound manner.) for new systems (including those which offer internet accessibility and open network interfaces) MIL 5 : In addition to MIL 4, the MII also fine tunes its VA and or PT for new systems (including those which offer internet accessibility and open network interfaces)(based on learnings) and also periodically changes vendors.		
Domain : Monitoring of Critical Assets/Infrastructure and Detection of Intrusion/Unauthorized Access				
42	MII should establish appropriate security monitoring systems and processes to facilitate continuous monitoring of security events and timely detection of unauthorised or malicious activities, unauthorised changes, unauthorised access and unauthorised copying or transmission of data / information held in contractual or fiduciary capacity, by internal and external parties. The security logs of systems, applications and network	MIL 1: MII has not established a C-SOC. MIL 2: The MII has a C-SOC , share with other MIIs (subsidiaries etc) , however the C-SOC doesn't have separate consoles for each MII and the C-SOC does not differentiate between the traffic of different MIIs it caters to.	5	4

S. No	Parameter	Maturity Indicator Level (MIL)	No of Levels	Maximum Permissible Score
	devices should also be monitored for anomalies.	MIL 3: The MII has a C-SOC, shared with other MIIs with separate consoles for each MII and the C-SOC differentiates between the traffic of different MIIs however the System Audit / Comprehensive review has highlighted observations pertaining to the C-SOC's monitoring ability or the evaluation of logs by the C-SOC. MIL 4: The MII has a C-SOC, shared with other MIIs with separate consoles for each MII and the C-SOC differentiates between the traffic of different MIIs and the System Audit / Comprehensive review has no observations pertaining to the C-SOC's monitoring ability or the evaluation of logs by the C-SOC. MIL 5: The MII has a C-SOC, shared with other MIIs with separate consoles for each MII and the C-SOC differentiates between the traffic of different MIIs and the System Audit / Comprehensive review has no observations pertaining to the C-SOC's monitoring ability or the evaluation of logs by the C-SOC. Additionally, the C-SOC also periodically updates its monitoring parameters and has		

S. No	Parameter	Maturity Indicator Level (MIL)	No of Levels	Maximum Permissible Score
		demonstrated in pre-emptive warding-off attacks.		
43	Further, to ensure high resilience, high availability and timely detection of attacks on systems and networks, MII should implement suitable mechanism to monitor capacity utilization of its critical systems and networks.	MIL 1: The MII does not have a dedicated capacity utilization monitoring mechanism consisting of appropriate systems and dedicated in-house staff. MIL 2: The MII does has a capacity utilization monitoring mechanism consisting of appropriate systems however the same is outsourced. Additionally, not all critical systems are being monitored by the same. MIL 3: The MII does has a capacity utilization monitoring mechanism consisting of appropriate systems however the same is outsourced. All critical systems are being monitored by the same, however the thresholds set for alerts are too high to timely ward-off attacks / untoward incidents. MIL 4: The MII does has a capacity utilization monitoring mechanism consisting of appropriate systems however the same is outsourced. All critical systems are being monitored by the same, the thresholds set for alerts are appropriate to timely ward-off attacks / untoward incidents as per the System Auditor.	5	4

S. No	Parameter	Maturity Indicator Level (MIL)	No of Levels	Maximum Permissible Score
		MIL 5: The MII does has a capacity utilization monitoring mechanism consisting of appropriate systems however the same is outsourced. All critical systems are being monitored by the same, the thresholds set for alerts are appropriate to timely ward-off attacks / untoward incidents as per the System Auditor. Additionally the MII is also quarterly reviewing the threshold parameters and also monitors shadow systems deployed for new projects.		
44	Suitable alerts should be generated in the event of detection of unauthorized or abnormal system activities, transmission errors or unusual online transactions.	MIL 1: The MII does not have an alert generation system in place MIL 2 : The MII has a well-defined, robust system in place for generation of alerts MIL 3 : In addition to MIL 2, the MII has a dedicated team of experts which continuously monitor and refine the alert definitions and alert generation system	3	2
Domain : Response and Recovery				

S. No	Parameter	Maturity Indicator Level (MIL)	No of Levels	Maximum Permissible Score
45	Alerts generated from monitoring and detection systems should be suitably investigated, including impact and forensic analysis of such alerts, in order to determine activities that are to be performed to prevent expansion of such incident of cyber-attack or breach, mitigate its effect and eradicate the incident.	MIL 1: The MII does not have a SOP in place for segmenting the security alerts based on its internal criteria, investigating the security alerts, and thereafter mitigating the incidents which led to the alerts. MIL 2: The MII has a documented and approved SOP in place for segmenting the security alerts based on its internal criteria, investigating the security alerts, and thereafter mitigating the incidents which led to the alerts. MIL 3: The MII has demonstrated instances where it has been regularly monitoring the alerts, investigating relevant security alerts, and has also been taking corrective actions to avoid / mitigate instances which led to the alerts. MIL 4: The MII has demonstrated instances where it has been regularly monitoring the alerts, investigating relevant security alerts, and has also been taking corrective actions to avoid / mitigate instances which led to the alerts. The MII has also been updating its security policy	4	3

S. No	Parameter	Maturity Indicator Level (MIL)	No of Levels	Maximum Permissible Score
		based on dominant / high risk alerts received.		
46	The response and recovery plan of the MII should aim at timely restoration of systems affected by incidents of cyber-attacks or breaches. The recovery plan should be in line with the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) specified by SEBI.	MIL 1: The MII does not have an approved BCP/DR Policy independent for itself (in case of sharing of DR Sites with subsidiary companies who are also MIIs). The same may be a document pertaining to the parent MII. MIL 2: The MII has an approved BCP/DR Policy independent for its own MII (incase of sharing of DR Sites with subsidiary companies who are also MIIs). MIL 3: The MII has an approved BCP/DR Policy independent for its own MII (incase of sharing of DR Sites with subsidiary companies who are also MIIs) and has been conducting mock and live DR Drills as per frequency specified by SEBI, however the System Audit / Comprehensive review has highlighted observations	4	3

S. No	Parameter	Maturity Indicator Level (MIL)	No of Levels	Maximum Permissible Score
		pertaining to the BCP/DR Plan or the DR Site or controls pertaining to the same. The MII also conforms to the RTO and RPO requirements as relevant to it. MIL 4: The MII has an approved BCP/DR Policy independent for its own MII (incase of sharing of DR Sites with subsidiary companies who are also MIIs) and has been conducting mock and live DR Drills as per frequency specified by SEBI, and the System Audit / Comprehensive review has no observations pertaining to the BCP/DR Plan or the DR Site or controls pertaining to the same. The MII also conforms to the RTO and RPO requirements as relevant to it.		
47	The response plan should define responsibilities and actions to be performed by its employees and support / outsourced staff in the event of cyber-attacks or breach of cyber security mechanism.	MIL 1: The MII does not have an approved BCP/DR Policy independent for itself (in case of sharing of DR Sites with subsidiary companies who are also MIIs). The same may be a document pertaining to the parent MII. MIL 2: The MII has an approved BCP/DR Policy independent for its own MII (incase of sharing of DR Sites with subsidiary companies who are also MIIs). However the same	3	2

S. No	Parameter	Maturity Indicator Level (MIL)	No of Levels	Maximum Permissible Score
		does not enunciate the responsibilities and actions to be performed by its employees and support / outsourced staff in the event of cyber-attacks or breach of cyber security mechanism. MIL 3: The MII has an approved BCP/DR Policy independent for its own MII (incase of sharing of DR Sites with subsidiary companies who are also MIIs). The same enunciates the responsibilities and actions to be performed by its employees in the event of cyber-attacks or breach of cyber security mechanism. However the policy does not lay down responsibilities and action for support / outsourced staff, as may be applicable.		
48	Any incident of loss or destruction of data or systems should be thoroughly analyzed and lessons learned from such incidents should be incorporated to strengthen the security mechanism and improve recovery planning and processes.	MIL 1: The MII does not have a documented and approved policy for analyzing the incidents pertaining to system glitches, cyber incidents. MIL 2: The MII has a documented and approved policy for analyzing the incidents pertaining to system glitches, cyber incidents, which also outlines the mechanism to place the RCA before the respective technology / Cyber security committees of the MII and thereafter the Board of the MII.	4	3

S. No	Parameter	Maturity Indicator Level (MIL)	No of Levels	Maximum Permissible Score
		MIL 3: The MII has been incorporating the learnings from the incidents occurred. The MII has also been timely been incorporating security control(s) measures. MIL 4: The MII has been incorporating the learnings from the incidents occurred. The MII has also been timely been incorporating security control(s) measures. The MII has also fine-tuned its recovery planning process based on such learnings.		
49	MII should also conduct suitable periodic drills to test the adequacy and effectiveness of response and recovery plan.	MIL 1: The MII does not conduct the minimum number of mock and live drills from its DR site as specified by SEBI. MIL 2: The MII conducts the minimum number of mock and live drills from its DR site as specified by SEBI. However the scenarios developed do not include Cyber Attacks/ events. MIL 3: The MII conducts the minimum number of mock and live drills from its DR site as specified by SEBI. And the scenarios developed include Cyber Attacks/ events. MIL 4: The MII conducts the minimum number of mock and live drills from its DR site as specified by SEBI. And the scenarios developed include	4	3

S. No	Parameter	Maturity Indicator Level (MIL)	No of Levels	Maximum Permissible Score
		Cyber Attacks/ events. Additionally, the MII also conducts dedicated Cyber Drills , which may be in co-ordination with relevant agencies and its subsidiary companies who may be MIIs.		
Domain : Sharing of Information				
50	Quarterly reports containing information on cyber-attacks and threats experienced by MII and measures taken to mitigate vulnerabilities, threats and attacks including information on bugs / vulnerabilities / threats that may be useful for other MIIs, should be submitted to SEBI.	MIL 1: Quarterly reports are not being submitted. MIL 2: Quarterly reports on cyber-attacks and counter measures taken are submitted to SEBI.	2	1
51	Such details as are felt useful for sharing with other MIIs in masked and anonymous manner shall be shared using mechanism to be specified by SEBI from time to time.	NA	NA	NA
Domain : Training				
52	MII should conduct periodic training programs to enhance awareness level among the employees and outsourced staff, vendors, etc. on IT / Cyber security policy and standards. Special focus should be given to build awareness levels and skills of staff from non-technical disciplines.	MIL 1: No training programs are being conducted. MIL 2: Training programs are conducted but not periodically/or not all employees are involved. MIL 3: Periodic training programs are conducted for all the employees	4	3

S. No	Parameter	Maturity Indicator Level (MIL)	No of Levels	Maximum Permissible Score
		MIL 4: Periodic training programs are conducted for all the employees with special focus given to building awareness levels and skills of staff from non-technical disciplines		
53	The training program should be reviewed and updated to ensure that the contents of the program remain current and relevant.	MIL 1: Training program not reviewed. MIL 2: Training program reviewed and updated periodically.	2	1
Domain : Periodic Audit				
54	The Terms of Reference for the System Audit of MII specified under Para 4.29.7 shall be accordingly modified to include audit of implementation of the aforementioned areas.	MIL 1: Terms of Reference for the System Audit have not been modified. MIL 2: Terms of Reference for the System Audit have been modified to include areas mentioned in Para 4.41	2	1

Annexure 30

Calculation Methodology for Cyber Capability Index											
S. No.	**Domain**	**Sub-Domain**	**Total Parameters***	**Parameters used for scoring in the Index**	**Maximum Permissible Score (A)**	**Minimum Cut-Off Score (B)**	**Weight in the Index (C)**	**Index on min score (D)**	**Index on max score (E)**	**Sample score (F)**	**Index on sample score (G)**
1	Governance of Critical Infrastructure and Personnel	NA	9	9	26	9	11.0%	3.81	11.00	25.00	10.58
2	Identification of critical assets and risks	NA	3	3	8	3	10.0%	3.75	10.00	7.00	8.75
3	Protection of Critical Assets and Infrastructure	Access Controls	10	10	26	10	5.0%	1.92	5.00	25.00	4.81
		Physical Security	3	3	5	3	4.0%	2.40	4.00	4.00	3.20
		Network Security Management	3	3	7	3	4.0%	1.71	4.00	6.00	3.43
		Security of Data	4	4	12	4	4.0%	1.33	4.00	11.00	3.67
		Hardening of Hardware and Software	2	2	6	2	3.0%	1.00	3.00	5.00	2.50
		Application Security and Testing	1	1	2	1	3.0%	1.50	3.00	1.00	1.50

		Patch Management	2	2	5	2	3.0%	1.20	3.00	4.00	2.40
		Disposal of Systems and Storage Devices	1	1	1	1	3.0%	3.00	3.00	1.00	3.00
		Vulnerability Assessment and Penetration Testing	3	3	8	3	4.0%	1.50	4.00	7.00	3.50
4	Monitoring of Critical Assets/ Infrastructure and Detection of Intrusion/ Unauthorized Access	NA	3	3	10	3	11.0%	3.30	11.00	9.00	9.90
5	Response and Recovery	NA	5	5	14	5	10.0%	3.57	10.00	13.00	9.29
6	Sharing of Information	NA	2	1	1	1	5.0%	5.00	5.00	1.00	5.00
7	Training	NA	2	2	4	2	10.0%	5.00	10.00	3.00	7.50
8	Periodic Audit	NA	1	1	1	1	10.0%	10.00	10.00	1.00	10.00
	Total		**54**	**53**	**136**	**53**	**100.00 %**	**50.00**	**100.00**	**123.00**	**89.02**

भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

Annexure 31

Format for Report on Complaints

Part A

Sr. No.	Particulars	Number
1	Number of complaints received directly	
2	Number of complaints forwarded by SEBI	
3	Total number of complaints received (1+2)	
4	Total number of complaints resolved	
5	Total number of complaints pending (3-4)	

Part B

Sr. No.	Name of the Complainant	Date of Complaint	Status (Resolved/Pending)
1			
2			
3			

Annexure 32

Format of the Compliance Report to be submitted along with the draft Scheme

It is hereby certified that the draft Scheme involving (Name of the entities) does not, in any way violate, override or limit the provisions of securities laws and the same is in compliance with the applicable provisions of this circular.

Company Secretary *Managing Director*

Certified that the transactions / accounting treatment provided in the draft Scheme involving (Name of the entities) are in compliance with all the Accounting Standards applicable to an unlisted entity.

Chief Financial Officer *Managing Director*

भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

Annexure 33

Format for Report on Unpaid Dues

Sr. No.	Particulars	Details of dues/fine/penalty	Amount (INR)	Reason for non-payment
1.	Pending Dues of SEBI			
2.	Pending Dues of Depositories			

भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

Annexure 34

Draft Cyber Audit format

1. Background
2. Details of Auditee
3. Audit Team Member Details

Auditor name	
Auditor address	
Contact information	
Location of audit	
Audit team members and details of qualifications	

4. Scope of audit/Terms of reference (as agreed between the auditee and auditor), including the standard/specific scope for audit:
   - ***a)*** Audit Period –
   - ***b)*** Date of agreement between MII and auditor
   - ***c)*** Engagement period-
   - ***d)*** List of SEBI Circulars and Advisories covered:
   - ***e)*** List of all IT infrastructure (including IT systems of PDC, DR, Near site, Co-lo facility) covered under audit
   - ***f)*** Geographical locations covered under audit (PDC/DR/near site)
   - ***g)*** VAPT (Vulnerability assessment and penetration testing)
   - ***h)*** Any other specific item(s)
5. Methodology /Audit approach (audit subject identification, pre-audit planning, data gathering methodology, sampling methodology etc. followed)
6. Executive Summary of findings (including identification tests, tools used and results of tests performed)

S. No	Number of Non-conformity	Number of observations	Risk rating			Any other comments
			High	Medium	Low	
1						

7. Control-wise Compliance status of various SEBI Circulars /advisories

S. No	Control prescribed	*List of documentary evidence including physical inspection/sample size taken	Compliance status
1			
2			
…			
N			

*Explicit reference to the key auditee organizational documents (by date or version) including policy and procedure documents

8. Details of findings (including analysis of vulnerabilities/issues of concern and recommendation for action)

Description of finding (a)	
Name of system belongs to MII or third party vendor (b)	
Status/nature of findings (c)	
Risk rating of finding by auditor (d)	
C/I/A effected (e)	
Clause No. of SEBI Cyber security circular/advisory violated (f)	
Test cases used (g)	
Impact analysis (h)	
Root Cause analysis (i)	
Corrective Action proposed by auditor (j)	
Deadline for corrective action (k)	
Management response (l)	
Whether Similar Issue was observed in any of previous 3 audit (m)	
List of Documentary evidence verified during review/audit (n)	

a) Description of findings/observations – Description of the findings in sufficient details, referencing any accompanying evidence

b) Name of system belongs to MII or vendor-(Self Explanatory term)

c) Status/ Nature of Findings – The category can be specified, for example:

- ***a.*** Non-compliant (Major/Minor)
- ***b.*** Work in progress
- ***c.*** Observation

d) Risk Rating of finding - A rating has to be given for each of the observations based on its impact and severity to reflect the risk exposure as well as the suggested priority for action

Rating	Description
HIGH	Represents weakness in control with respect to threat(s) that is /are sufficiently capable and impacts asset (s) leading to regulatory non-

	compliance, significant financial, operational and reputational loss. These observations need to be addressed with utmost priority.
MEDIUM	Represents weakness in control with respect to threat(s) that is /are sufficiently capable and impacts asset (s) leading to exposure in terms of financial, operational and reputational loss. These observations need to be addressed reasonable timeframe.
LOW	Represents weaknesses in control, which in combination with other weakness can develop into an exposure. Suggested improvements for situations not immediately/directly affecting controls. .

e) C/I/A-Principle of Confidentiality/integrity/availability affected due to issued left unaddressed**.**

f) Clause No. of SEBI Cyber security circular/advisory violated-The clause corresponding to this observation w.r.t to SEBI circular on Cyber security/advisories issued by SEBI.

g) Test cases used **–**The details of test cases used for arriving at this observation, provide annexure numbers in case of detailed test cases.

h) Impact Analysis **–** An analysis of the likely impact on the operations/ activity of the organization

i) Root Cause analysis – A detailed analysis on the cause of the non-conformity.

j) Corrective Action proposed by auditor **–** The action taken to correct the non-conformity

k) Deadline for corrective action**-**The auditor should specify the deadline not only for the corrective action on the system where NC/observation was found, but also specify the deadline for corrective action on systems where similar observations could have been found/are found

l) Management response

m) Whether Similar Issue was observed in any of previous 3 audits

n) List of Documentary evidence verified during review/audit

9. Specific best practices implemented by the auditee in generalized manner without infringing on Intellectual Property Rights (IPRs)

10. Any other comments by auditor

11. Conclusion of cyber audit

भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

Annexure 35

Minimum baseline standards for conducting VAPT

Comprehensive Scope for Vulnerability Assessment and Penetration Testing (VAPT)

1. **Critical Asset definition:** Set-A entities shall identify and classify their critical IT systems. The systems that should essentially to be included in critical systems (not limited to):
   a. Any system that will have adverse impact on any kind of service of MIIs if compromised.
   b. Stores/transmits any type of critical data (trading data, PII etc.)
   c. Devices/Network through which any critical systems connected (either physically or virtually)
   d. Systems directly/indirectly connected to any other critical systems

2. The **scope** of the IT environment taken for VAPT should be made transparent to SEBI and should include all critical assets and infrastructure components (not limited to) like Networking systems, Security devices, Servers, Databases, Applications, Systems accessible through WAN, LAN as well as with public IP's, websites, etc.

   The scope should include (not limited to):

VA of Infrastructure-Internal & External
VA of Applications-Internal & External
External Penetration Testing-Infrastructure & Application
Internal Penetration Testing-Infrastructure & Application
WIFI Testing
Network Segmentation
VA & PT of Mobile applications
OS & DB Assessment
VAPT of Cloud implementation and deployments

3. **Testing methodology:** The VAPT should provide in-depth evaluation of the security posture of the system through simulations of actual attacks on its systems and networks. The testing methodology should adapt from the following:
   a. SEBI Circular on Cyber Security and Cyber Resilience framework
   b. National Critical Information Infrastructure Protection Centre (NCIIPC)
   c. CERT-In Guidelines
   d. The National Institute of Standards and Technology ("NIST") Special Publication 800-115
   e. Latest ISO27001
   f. PCI-DSS standards
   g. Open Source Security Testing Methodology Manual ("OSSTMM")
   h. OWASP Testing Guide

भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

Annexure 36

Standardized Observation Reporting Format

Note:

MII's are expected to submit following information with regards to each major/minor NCs/ suggestion / Observation made in the Cyber Security Review Audit

MIIs should also categorically highlight those observations/NCs/Suggestions pointed out in their System Audit (current & previous) which are not yet complied with, which corresponding to the current review finding.

I. For Preliminary Audit

(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)	(14)	(15)	(16)	(17)
Audit Period	**Observation No**	**Description of Finding**	**Department of MII**	**Status / Nature of Findings**	**C/I/A Affected**	**Risk Rating of Findings as per Auditor**	**SEBI Cyber Security Clause**	**Audited By**	**Test Cases used**	**Root Cause Analysis**	**Impact Analysis**	**Corrective Action proposed by auditor**	**Deadline for the Corrective Action**	**Management response in case of acceptance of associate Risks**	**Whether similar issue was observed in any of the previous 3 system audits**	**List of Documentary evidence verified during review / audit (Annexure Nos.)**

Description of all Table heads

1. **Audit Period –** This indicates the period of the audit**.**
2. **Observation Number –** (Self-explanatory term.)
3. **Description of Findings/ Observations –** Description of the findings in sufficient detail, referencing any accompanying evidence.
4. **Department of MII –** Corresponding Department (s) of MII where finding was observed / Department responsible for closing the finding.
5. **Status / Nature of Findings –** The category can be specified for example:
    a. Non-Conformity (Major / Minor)
    b. Work In progress
    c. Observation
    d. Suggestion
6. **C/I/A Affected –** Principle of Confidentiality / Integrity / Availability affected due to issue left unaddressed.
7. **Risk Rating of Findings as per Auditor -** A rating has to been given for each of the observations based on their impact and severity to reflect the risk exposure, as well as the suggested priority for action.

Rating	Description
HIGH	Weakness in control which represent exposure to the organization or risks that could lead to instances of noncompliance with the requirements of TORs. These risks need to be addressed with utmost priority.
MEDIUM	Potential weakness in controls, which could develop into an exposure or issues that represent areas of concern and may impact internal controls. These should be addressed reasonably promptly.
LOW	Potential weaknesses in controls, which in combination with other weakness can develop into an exposure. Suggested improvements for situations not immediately/directly affecting controls.

8. **SEBI Cyber Security Clause –** The clause corresponding to this observation w.r.t SEBI Circular dated July 06, 2015 on Cyber Security
9. **Audited By –** Name (s) of audit team member
10. **Test Cases used –** The details of test cases used for arriving at this observation, provide annexure numbers in case of detailed test cases.

11. **Root Cause Analysis –** A detailed analysis on the cause of the nonconformity
12. **Impact Analysis –** An analysis of the likely impact on the operations/activity of the organization
13. **Corrective Action proposed by auditor –** The action taken to correct the non-conformity
14. **Deadline for the Corrective Action –** The auditor should specify the deadline not only for the corrective action on the system where the NC/ Observation was found, but also should specify the deadline for corrective action on systems where similar observations could have been found/ are found.
15. **Management response in case of acceptance of associate Risks**
16. **Whether similar issue was observed in any of the previous 3 system audits**

List of Documentary evidence verified during review / audit (Annexure Nos.)

भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

CIRCULARS

S. No.	Circular No.
1	SEBI Circular SMD/POLICY/Cir-2/98 dated January 14, 1998
2	SEBI Circular SMDRP/Policy/Cir-9/99 dated May 6, 1999
3	SEBI Circular SMDRP/Policy/Cir-28/99 dated August 23, 1999
4	SEBI Circular SMDRP/Policy/Cir-29/99 dated August 23, 1999
5	SEBI Circular D&CC/FITTC/Cir-09/2002 dated July 4, 2002
6	SEBI Circular D&CC/FITTC/Cir-10/2002 dated September 25, 2002
7	SEBI Circular D&CC/FITTC/CIR - 12/2002 dated October 30, 2002
8	SEBI Circular D&CC/FITTC/Cir-15/2002 dated December 27, 2002
9	SEBI Circular D&CC/FITTC/CIR – 16/2002 dated December 31, 2002
10	SEBI Circular LGL/Cir-2/2003 dated February 19, 2003
11	SEBI Circular DCC/FITTC/Cir-19/2003 dated March 4, 2003
12	SEBI Circular SEBI/MRD/Policy/AT/Cir- 19/2004 dated April 21, 2004
13	SEBI Circular MRD/DoP/Dep/Cir-27/2004 dated August 16, 2004
14	SEBI Circular MRD/DoP/Dep/Cir-29/2004 dated August 24, 2004
15	SEBI Circular MRD/DoP /SE/Dep/Cir-4/2005 dated January 28, 2005
16	SEBI Circular SEBI/MRD/SE/DEP/Cir-4/2005 dated January 28, 2005
17	SEBI Circular MRD/DoP/SE/Dep/Cir-18/2005 dated September 2, 2005
18	SEBI Circular MRD/DoP/Dep/Cir-22 /05 dated November 9, 2005
19	SEBI Circular SEBI/MRD/DEP/Cir-2/06 dated January 19, 2006
20	SEBI Circular SEBI/MRD/DEP/Cir-3/06 dated February 21, 2006
21	SEBI Circular MRD/DoP/Dep/Cir-09/06 dated July 20, 2006
22	SEBI Circular MRD/DoP/Dep/SE/Cir-13/06 dated September 26, 2006
23	SEBI Circular MRD/DoP/Dep/SE/Cir-17/06 dated October 27, 2006
24	SEBI Circular MRD/Dep/Cir- 20/06 dated December 11, 2006
25	SEBI Circular MRD/DoP/Dep/SE/Cir-22/06 dated December 18, 2006
26	SEBI Circular MRD/DSA/SE/Dep/Cust/Cir-23/06 dated December 22, 2006
27	SEBI Circular SEBI/MRD/Dep/Cir-03/2007 dated February 13, 2007
28	SEBI Circular MRD/DoP/Cir-5/2007 dated April 27, 2007
29	SEBI Circular MRD/DoP/Cir-08/2007 dated June 25, 2007
30	SEBI Circular MIRSD/DPS-III/Cir-9/07 dated July 3, 2007
31	SEBI Circular SEBI/CFD/DIL/DIP/29/2008/01/02 dated February 1, 2008
32	SEBI Circular SEBI/MRD/Dep/Cir-03/2008 dated February 28, 2008
33	SEBI Circular MRD/DoP/Cir-20/2008 dated June 30, 2008
34	SEBI Circular MIRSD/DPS- III/Cir-23/08 dated July 25, 2008
35	SEBI Circular MRD/DSA/SE/Dep/Cust/CIR-30/08 dated October 23, 2008
36	SEBI Circular ISD/AML/CIR-1/2008 dated December 19, 2008
37	SEBI Circular MRD/DoP/SE/Dep/Cir-2/2009 dated February 10, 2009
38	SEBI Circular SEBI/IMD/CIR No 11/183204/2009 dated November 13, 2009

S. No.	Circular No.
39	SEBI Circular MRD/DoP/DEP/Cir 20/2009 dated December 9, 2009
40	SEBI Circular SEBI/MRD/ OIAE/ Dep/ Cir- 4/2010 dated January 29, 2010
41	SEBI Circular CIR/MRD/DMS/13/2010 dated April 23, 2010
42	SEBI Circular SEBI/MRD/ DP/ 19/2010 dated June 10, 2010
43	SEBI Circular MRD/DP/20/2010 dated July 1, 2010
44	SEBI Circular MRD/DP/22/2010 dated July 29, 2010
45	SEBI Circular CIR/MRD/DMS/28/2010 dated August 31, 2010
46	SEBI Circular CIR/MRD/DP/30/2010 dated September 06, 2010
47	SEBI Circular CIR/IMD/DF/17/2010 dated November 09, 2010
48	SEBI Circular CIR/MRD/DP/37/2010 dated December 14, 2010
49	SEBI Circular CIR/MRD/DP/4/2011 dated April 7, 2011
50	SEBI Circular CIR/MRD/ DP/05/2011 dated April 27, 2011
51	SEBI Circular CIR/MIRSD/9/2011 dated June 17, 2011
52	SEBI Circular CIR/MIRSD/16/2011 dated August 22, 2011
53	SEBI Circular MIRSD/SE/Cir-21/2011 dated October 05, 2011
54	SEBI Circular MIRSD/Cir-23/2011 dated December 02, 2011
55	SEBI Circular CIR/MIRSD/24/2011 dated December 15, 2011
56	SEBI Circular MIRSD/Cir- 26 /2011 dated December 23, 2011
57	SEBI Circular CIR/MRD/ICC/16/2012 dated June 15, 2012
58	SEBI Circular CIR/MRD/DP/ 21 /2012 dated August 02, 2012
59	SEBI Circular CIR/MIRSD/ 09 /2012 dated August 13, 2012
60	SEBI Circular MIRSD/09/2012 dated August 13, 2012
61	SEBI Circular CIR/MRD/DP/22/2012 dated August 27, 2012
62	SEBI Circular CIR/CFD/DIL/10/2012 dated August 28, 2012
63	SEBI Circular CIR/MRD/DP/24/2012 dated September 11, 2012
64	SEBI Circular CIR/MRD/DP/DA/25/2012 dated September 21, 2012
65	SEBI Circular CIR/MRD/DP/27/2012 dated November 01, 2012
66	SEBI Circular SEBI/MIRSD/01/2013 dated January 04, 2013
67	SEBI Circular CIR/MIRSD/2/2013 dated January 24, 2013
68	SEBI Circular CIR/CFD/DIL/6/2013 dated March 01, 2013
69	SEBI Circular SEBI/MRD/DRMNP/26/2013 dated September 04, 2013
70	SEBI Circular CIR/MRD/DSA/32/2013 dated October 04, 2013
71	SEBI Circular SEBI/MIRSD/09/2013 dated October 08, 2013
72	SEBI Circular SEBI/MIRSD/ 12/2013 dated December 04, 2013
73	SEBI Circular SEBI/MRD/DOP/01/2014 dated January 07, 2014
74	SEBI Circular MRD/DMS/03/2014 dated January 21, 2014
75	SEBI Circular SEBI/MRD/DMS/05/2014 dated February 07, 2014
76	SEBI Circular CIR/MRD/DP/21/2014 dated July 01, 2014
77	SEBI Circular CIR/MRD/DP/22/2014 dated July 04, 2014
78	SEBI Circular CIR/MRD/DP/31/2014 dated November 12, 2014

S. No.	Circular No.
79	SEBI Circular CIR/MRD/DSA/33/2014 dated December 09, 2014
80	SEBI Circular CIR/OIAE/1/2014 dated December 18, 2014
81	SEBI Circular CIR/MRD/DP/1/2015 dated January 12, 2015
82	SEBI Circular MIRSD/1/2015 dated March 04, 2015
83	SEBI Circular CIR/MRD/DP/10/2015 dated June 05, 2015
84	SEBI Circular CIR/MRD/DP/13/2015 dated July 06, 2015
85	SEBI Circular CIR/MIRSD/2/2015 dated August 26, 2015
86	SEBI Circular CIR/MRD/DP/18/2015 dated December 09, 2015
87	SEBI Circular CIR/MRD/DP/19/2015 dated December 09, 2015
88	SEBI Circular MRD/DSA/01/2016 dated January 01, 2016
89	SEBI Circular CIR/MIRSD/29/2016 dated January 22, 2016
90	SEBI Circular CIR/MIRSD/64/2016 dated July 12, 2016
91	SEBI Circular CIR/MIRSD/ 66/2016 dated July 21, 2016
92	SEBI Circular SEBI/HO/MIRSD/MIRSD2/CIR/P/2016/95 dated September 26, 2016
93	SEBI Circular SEBI/HO/MRD/DSA/CIR/P/2016/113 dated October 19, 2016
94	SEBI Circular CFD/DCR2/CIR/P/2016/131 dated December 09, 2016
95	SEBI Circular SEBI/HO/DMS/ CIR/P/2017/15 dated February 23, 2017
96	SEBI Circular SEBI/HO/MIRSD/MIRSD6/CIR/P/2017/20 dated March 10, 2017
97	SEBI Circular SEBI/HO/MRD/DP/CIR/P/2017/29 dated April 03, 2017
98	SEBI Circular SEBI/HO/MIRSD/MIRSD1/CIR/P/2017/38 dated May 02, 2017
99	SEBI Circular SEBI/HO/GSD/T&A/CIR/P/2017/42 dated May 16, 2017
100	SEBI Circular CIR/MRD/DP/56/2017 dated June14, 2017
101	SEBI Circular CIR/HO/MIRSD/MIRSD2/CIR/P/2017/59 dated June 15, 2017
102	SEBI Circular CIR/HO/MIRSD/MIRSD2/CIR/P/2017/64 dated June 22,2017
103	SEBI Circular CFD/CMD/CIR/P/2017/115 dated October 10, 2017
104	SEBI Circular SEBI/HO/MRD/DSA/CIR/P/2018/1 dated January 29, 2018
105	SEBI Circular SEBI/HO/OIAE/IGRD/CIR/P/2018/58 dated March 26, 2018
106	SEBI Circular IMD/FPIC/CIR/P/2018/61 dated April 05, 2018
107	SEBI Circular SEBI/HO/CFD/DIL2/CIR/P/2018/138 dated November 01, 2018
108	SEBI Circular SEBI/ HO/ MIRSD/ DOS3/ CIR/ P/ 2018/ 140 dated November 13, 2018
109	SEBI Circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018
110	SEBI Circular CIR/MRD/CSC/148/2018 dated December 07, 2018
111	SEBI Circular CIR/MRD/CSC/151/2018 dated December 14, 2018
112	SEBI Circular SEBI/HO/MIRSD/DOP/CIR/P/2018/153 dated December 17, 2018
113	SEBI Circular CIR/MRD/DP/158/2018 dated December 27, 2018
114	SEBI Circular SEBI/HO/MIRSD/DOS2/CIR/P/2019/10 dated January 04, 2019
115	SEBI Circular SEBI/HO/MRD/DOP2DSA2/CIR/P/2019/13 dated January 10, 2019
116	SEBI Circular SEBI/HO/MRD/DOP1/CIR/P/2019/24 dated January 31, 2019

S. No.	Circular No.
117	SEBI Circular SEBI/HO/MRD/DOP2DSA2/CIR/P/2019/26 dated February 5, 2019
118	SEBI Circular CIR/HO/MIRSD/DOS2/CIR/PB/2019/038 dated March 15, 2019
119	SEBI Circular MRD/DoP2DSA2/CIR/P/2019/51 dated April 10, 2019
120	SEBI Circular SEBI/MRD/CSC/CIR/P/2019/64 dated May 20, 2019
121	SEBI Circular SEBI/HO/CFD/DIL2/CIR/P/2019/67 dated May 22, 2019
122	SEBI Circular CIR/HO/MIRSD/DOP/CIR/P/2019/75 dated June 20, 2019
123	SEBI Circular SEBI/HO/MRD/DOP2DSA2/CIR/P/2019/87 dated August 01, 2019
124	SEBI Circular SEBI/HO/OIAE/IGRD/CIR/P/2019/86 dated August 02, 2019
125	SEBI Circular SEBI/HO/MIRSD/DOP/CIR/P/2019/95 dated August 29, 2019
126	SEBI Circular SEBI/HO/MRD/DOP1/CIR/P/2019/106 dated October 10, 2019
127	SEBI Circular SEBI/HO/MIRSD/DOP/CIR/P/2019/109 dated October 15, 2019
128	SEBI Circular SEBI/HO/MIRSD/DOP/CIR/P/2019/123 dated November 05, 2019
129	SEBI Circular SEBI/HO/MIRSD/RTAMB/CIR/P/2019/122 dated November 05, 2019
130	SEBI Circular SEBI/HO/MIRSD/DOP/CIR/P/2019/136 dated November 15, 2019
131	SEBI Circular SEBI/HO/MRD2/DCAP/CIR/P/2019/146 dated November 28, 2019
132	SEBI Circular IMD/FPI&C/CIR/P/2020/07 dated January 16, 2020
133	SEBI Circular SEBI/HO/CFD/CMD/CIR/P/2020/12 dated January 22, 2020
134	SEBI Circular SEBI/HO/CFD/DIL2/CIR/P/2020/13 dated January 22, 2020
135	SEBI Circular SEBI/HO/MRD/DDAP/CIR/P/2020/16 dated January 28, 2020
136	SEBI Circular IMD/FPI&C/CIR/P/2020/022 dated February 04, 2020
137	SEBI Circular SEBI/HO/MIRSD/DOP/CIR/P/2020/28 dated February 25, 2020
138	SEBI Circular SEBI/HO/MRD1/DSAP/CIR/P/2020/29 dated February 26, 2020
139	SEBI Circular SEBI/HO/MIRSD/DOP/CIR/P/2020/73 dated April 24, 2020
140	SEBI Circular SEBI/HO/MIRSD/DOP/CIR/P/2020/80 dated May 12, 2020
141	SEBI Circular SEBI/HO/MIRSD/DOP/CIR/P/2020/88 dated May 25, 2020
142	SEBI Circular SEBI/HO/MIRSD/DOP/CIR/P/2020/90 dated May 29, 2020
143	SEBI Circular SEBI/HO/MRD-1/CIR/P/2020/95 dated June 05, 2020
144	SEBI Circular SEBI/HO/MIRSD/DPIEA/CIR/P/2020/115 dated July 01, 2020
145	SEBI Circular SEBI/HO/MRD2/DDAP/CIR/P/2020/137 dated July 24, 2020
146	SEBI Circular SEBI/HO/MIRSD/DOP/CIR/P/2020/143 dated July 29, 2020
147	SEBI Circular SEBI/HO/CFD/CMD1/CIR/P/2020/144 dated July 31, 2020
148	SEBI Circular SEBI/HO/OIAE/IGRD/CIR/P/2020/152 dated August 13, 2020
149	SEBI Circular SEBI/HO/MRD2/DDAP/CIR/P/2020/153 dated August 18, 2020
150	SEBI Circular SEBI/HO/MIRSD/DOP/CIR/P/2020/158 dated August 27, 2020
151	SEBI Circular SEBI/HO/MIRSD/DOP/CIR/P/2020/167 dated September 08, 2020
152	SEBI Circular SEBI/HO/ISD/ISD/CIR/P/2020/168 dated September 09, 2020
153	SEBI Circular SEBI/HO/IMD/FPI&C/CIR/P/2020/177 dated September 21, 2020

S. No.	Circular No.
154	SEBI Circular SEBI/HO/MRD/DCAP/CIR/P/2020/190 dated October 01, 2020
155	SEBI Circular SEBI/HO/CFD/CMD/CIR/P/2020/242 dated December 09, 2020
156	SEBI Circular SEBI/HO/MRD2/DCAP/CIR/P/2020/243 dated December 18, 2020
157	SEBI Circular SEBI/HO/ITD/ITD/CIR/P/2021/16/2021 dated February 02, 2021
158	SEBI Circular SEBI/HO/MRD/DCAP/CIR/P/2021/23 dated March 03, 2021
159	SEBI Circular SEBI/HO/MIRSD/DOP/CIR/P/2021/31 dated March 10, 2021
160	SEBI Circular SEBI/HO/MRD1/DTCS/CIR/P/2021/33 dated March 22, 2021
161	SEBI Circular SEBI/HO/ITD/ITD/CIR/P/2021/575 dated June 14, 2021
162	SEBI Circular SEBI/HO/ISD/ISD/CIR/P/2021/578 dated June 16, 2021
163	SEBI Circular SEBI/HO/MRD1/DTCS/CIR/P/2021/590 dated July 05, 2021
164	SEBI Circular SEBI/HO/MIRSD/DOP/P/CIR/2021/595 dated July 16, 2021
165	SEBI Circular SEBI/HO/MIRSD/RTAMB/CIR/P/2021/601 dated July 23, 2021
166	SEBI Circular SEBI/HO/IMD/IMD-II DOF3/P/CIR/2021/604 dated July 26, 2021
167	SEBI Circular SEBI/HO/MRD1/ICC1/CIR/P/2021/625 dated September 02, 2021
168	SEBI Circular SEBI/HO/MRD2/DCAP/P/CIR/2021/628 dated September 07, 2021
169	SEBI Circular SEBI/HO/IMD/IMD-IDOF5/P/CIR/2021/635 dated October 4, 2021
170	SEBI Circular SEBI/HO/MRD1/MRD1_ICC1/P/CIR/2021/664 dated November 23, 2021
171	SEBI Circular SEBI/HO/MIRSD/MIRSD_RTAMB/P/CIR/2022/23 dated February 24, 2022
172	SEBI Circular SEBI/HO/CFD/DCR-3/P/CIR/2022/27 dated March 07, 2022
173	SEBI Circular SEBI/HO/MIRSD/DoP/P/CIR/2022/44 dated April 04, 2022
174	SEBI Circular SEBI/HO/MRD1/MRD1_DTCS/P/CIR/2022/58 dated May 02, 2022
175	SEBI Circular SEBI/HO/MIRSD/MIRSD_RTAMB/P/CIR/2022/65 dated May 18, 2022
176	SEBI Circular SEBI/HO/MRD1/MRD1_DTCS/P/CIR/2022/68 dated May 20, 2022
177	SEBI Circular SEBI/HO/MIRSD/DPIEA/P/CIR/2022/72 dated May 27, 2022
178	SEBI Circular SEBI/HO/MIRSD/TPD/P/CIR/2022/80 dated June 07, 2022
179	SEBI Circular SEBI/HO/MIRSD/ MIRSD_DPIEA/P/CIR/2022/83 dated June 20, 2022
180	SEBI Circular SEBI/HO/MIRSD/TPD/P/CIR/2022/93 dated June 30, 2022
181	SEBI Circular SEBI/HO/MRD1/ICC1/CIR/P/2022/94 dated July 04, 2022
182	SEBI Circular SEBI/HO/MIRSD/SEC-5/P/CIR/2022/99 dated July 20, 2022
183	SEBI Circular SEBI/HO/EFD1/EFD1_DRA4/P/CIR/2022/104 dated July 29, 2022
184	SEBI Circular SEBI/HO/ISD/ISD-SEC-4/P/CIR/2022/107 dated August 05, 2022
185	SEBI Circular SEBI/HO/MIRSD/DoP/P/CIR/2022/109 dated August 18, 2022
186	SEBI Circular SEBI/HO/MRD/DCAP/P/CIR/2022/110 dated August 19, 2022

S. No.	Circular No.
187	SEBI Circular SEBI/HO/MRD/MRD-POD-2/P/CIR/2022/114 dated August 26, 2022
188	SEBI Circular SEBI/HO/MIRSD/DoP/P/CIR/2022/119 dated September 19, 2022
189	SEBI Circular SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2022/137 dated October 06, 2022
190	SEBI Circular SEBI/HO/MIRSD/DoP/P/CIR/2022/143 dated October 27, 2022
191	SEBI Circular SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2022/153 dated November 11, 2022
192	SEBI Circular SEBI/HO/DDHS/RACPOD1/CIR/P/2023/0002 dated January 05, 2023
193	SEBI Circular SEBI/HO/MRD-TPD-1/CIR/P/2023/7 dated January 09, 2023
194	SEBI Circular SEBI/HO/MIRSD/SEC-5/P/CIR/2023/0026 dated February 08, 2023
195	SEBI Circular SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2023/30 dated February 15, 2023
196	SEBI Circular SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/032 dated February 22, 2023
197	SEBI Circular SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/033 dated March 06, 2023
198	SEBI Circular SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2023/37 dated March 16, 2023
199	SEBI Circular SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2023/42 dated March 27, 2023
200	SEBI Circular SEBI/HO/MRD/MRD-PoD-3/P/CIR/2023/45 dated March 28, 2023
201	SEBI Circular SEBI/HO/MRD/POD 3/CIR/P/2023/58 dated April 20, 2023
202	SEBI Circular SEBI/HO/MRD/TPD/P/CIR/2023/65 dated May 05, 2023
203	SEBI Circular SEBI/HO/MRD/MRD-PoD-3/P/CIR/2023/81 dated May 30, 2023
204	SEBI Circular SEBI/HO/MRD/MRD-PoD-2/P/CIR/2023/99 dated June 23, 2023
205	SEBI Circular SEBI/HO/OIAE/OIAE_IAD-1/P/CIR/2023/145 dated July 31, 2023
206	SEBI Circular SEBI/HO/MRD/TPD/P/CIR/2023/147 dated August 24, 2023
207	SEBI Circular SEBI/HO/MRD/TPD/P/CIR/2023/146 dated August 29, 2023

COMMUNICATIONS

S. No.	Communication Detail
1	SEBI Letter SEBI SMDRP/NSDL/4615 /2000 dated March 13, 2000
2	SEBI Letter SMDRP/NSDL/26563/2001 dated April 10, 2001
3	SEBI Letter D&CC/ 1099 / 2002 dated November 01, 2002
4	SEBI Letter MRD/VSS/ARR/ 12255/2004 dated June 10, 2004
5	SEBI Letter MRD/DoP/ Dep/82334 /2006 dated December 14, 2006
6	SEBI Letter MRD/DEP/PP/123624 /2008 dated April 23, 2008
7	SEBI Letter MRD/DoP/MC/141442 /2008 dated October 17, 2008
8	SEBI Letter MRD/CDSL/VM/155773/2009 dated February 27, 2009,

S. No.	Communication Detail
9	SEBI Letter MRD/NSDL/VM/158886 /2009 dated March 30, 2009
10	SEBI Letter MRD/DoP/NSDL/VM/ 162378 /2009 dated May 06, 2009
11	SEBI Letter MRD/CDSL/VM/168989 /2009 dated July 07, 2009
12	SEBI Letter MRD/DoP/NSDL/VM/168994 /2009 dated July 07, 2009
13	SEBI Letter SEBI/MRD/DEP/VM/169784 /09 dated July 15, 2009
14	SEBI Letter MRD/DoP/MAS – OW/16723/2010 dated August 17, 2010
15	SEBI Letter MRD/DP/SG-OW/202/2012 dated January 4, 2012
16	SEBI Letter MRD/DP/SG-OW/203/2012 dated January 4, 2012
17	SEBI Letter MRD//DP/OW/23881/2015 dated August 24, 2015
18	SEBI Letter SEBI/HO/MRD/DP/OW/2016/25739/1 dated September 14, 2016
19	SEBI Letter SEBI/HO/MRD/DP/OW/2016/25740/1 dated September 14, 2016
20	SEBI Letter SEBI/HO/MRD/DSA/OW/P/2016/31948 dated November 24, 2016
21	SEBI Letter MRD/DSA1/OW/4946/2018 dated February 14, 2018
22	SEBI Letter MRD/DSA1/OW/4947/2018 dated February 14, 2018
23	SEBI Letter SEBI/HO/MRD/DSA/OW/P/2018/000005436/5 dated February 21, 2018
24	SEBI Letter MIRSD2/DB/AEA/OW/2018/7292 dated March 07, 2018
25	SEBI Letter SEBI/MRD/ICC/OW/P/2018/27066/1 dated September 25, 2018
26	SEBI Letter MRD/DoPII/DSAII/MIRSD/DOS3/OW/2018/28162/1 dated October 22, 2018
27	SEBI Letter SEBI/HO/MRD/CSC/OW/P/2019/10055 dated April 22, 2019
28	SEBI Letter MRD/DSA/OW/11447/2/2019 dated May 8, 2019
29	SEBI Letter SEBI/MIRSD/16742/2019 dated July 03, 2019
30	SEBI Letter SEBI/HO/MRD/CSC/OW/P/2019/22202/1 dated August 28, 2019
31	SEBI Letter SEBI/HO/MRD/CSC/OW/P/2019/28517/1 dated October 30, 2019
32	SEBI Letter SEBI/HO/MRD/CSC/OW/P/2019/28527/1 dated October 30, 2019
33	SEBI Letter MRD2/DDAP/OW/P/2020/19443/1 dated November 13, 2020
34	SEBI Letter SEBI/HO/MRD2/DDAP/OW/P/2021/1632/1 dated January 20, 2021
35	SEBI Letter MRD2/DDAP/OW/P/2021/8568/1 dated April 09, 2021
36	SEBI Letter SEBI/HO/MIRSD/DPIEA/OW/2021/10188/3 dated May 11, 2021
37	SEBI Letter SEBI/HO/MIRSD/DOP/OW/P/2021/37347/1 dated December 15, 2021
38	SEBI Letter SEBI/HO/MRD/SEC-2/P/OW/2023/00001730411 dated April 28, 2023
39	SEBI MIRSD Email dated January 16, 2015
40	SEBI CFD Email dated November 05, 2015
41	SEBI Email dated November 11, 2017
42	SEBI MRD email dated November 04, 2019
43	SEBI MRD email dated February 06, 2020
44	SEBI DDHS email dated February 20, 2020
45	SEBI MRD email dated May 18, 2020

S. No.	Communication Detail
46	SEBI MIRSD email dated April 16, 2021
47	SEBI MIRSD email dated July 15, 2021
48	SEBI Email dated January 31, 2022
49	SEBI MIRSD email dated March 02, 2022
50	SEBI Email dated September 12, 2022
51	SEBI Email dated December 28, 2022

SCHEDULE A

S. No.	Circular / Communication No.
1	SEBI Circular SMD/POLICY/Cir-2/98 dated January 14, 1998
2	SEBI Circular SMDRP/Policy/Cir-9/99 dated May 6, 1999
3	SEBI Circular SMDRP/Policy/Cir-28/99 dated August 23, 1999
4	SEBI Circular SMDRP/Policy/Cir-29/99 dated August 23, 1999
5	SEBI Circular D&CC/FITTC/Cir-09/2002 dated July 4, 2002
6	SEBI Circular D&CC/FITTC/Cir-10/2002 dated September 25, 2002
7	SEBI Circular D&CC/FITTC/CIR - 12/2002 dated October 30, 2002
8	SEBI Circular D&CC/FITTC/Cir-15/2002 dated December 27, 2002
9	SEBI Circular D&CC/FITTC/CIR – 16/2002 dated December 31, 2002
10	SEBI Circular SEBI/MRD/Policy/AT/Cir- 19/2004 dated April 21, 2004
11	SEBI Circular MRD/DoP/Dep/Cir-27/2004 dated August 16, 2004
12	SEBI Circular MRD/DoP/Dep/Cir-29/2004 dated August 24, 2004
13	SEBI Circular MRD/DoP /SE/Dep/Cir-4/2005 dated January 28, 2005
14	SEBI Circular SEBI/MRD/SE/DEP/Cir-4/2005 dated January 28, 2005
15	SEBI Circular MRD/DoP/Dep/Cir-22 /05 dated November 9, 2005
16	SEBI Circular SEBI/MRD/DEP/Cir-2/06 dated January 19, 2006
17	SEBI Circular SEBI/MRD/DEP/Cir-3/06 dated February 21, 2006
18	SEBI Circular MRD/DoP/Dep/Cir-09/06 dated July 20, 2006
19	SEBI Circular MRD/DoP/Dep/SE/Cir-13/06 dated September 26, 2006
20	SEBI Circular MRD/DoP/Dep/SE/Cir-17/06 dated October 27, 2006
21	SEBI Circular MRD/Dep/Cir- 20/06 dated December 11, 2006
22	SEBI Circular MRD/DoP/Dep/SE/Cir-22/06 dated December 18, 2006
23	SEBI Circular MRD/DSA/SE/Dep/Cust/Cir-23/06 dated December 22, 2006
24	SEBI Circular SEBI/MRD/Dep/Cir-03/2007 dated February 13, 2007
25	SEBI Circular MRD/DoP/Cir-5/2007 dated April 27, 2007
26	SEBI Circular MRD/DoP/Cir-08/2007 dated June 25, 2007
27	SEBI Circular SEBI/MRD/Dep/Cir-03/2008 dated February 28, 2008
28	SEBI Circular MRD/DoP/Cir-20/2008 dated June 30, 2008
29	SEBI Circular MRD/DSA/SE/Dep/Cust/CIR-30/08 dated October 23, 2008
30	SEBI Circular MRD/DoP/SE/Dep/Cir-2/2009 dated February 10, 2009
31	SEBI Circular MRD/DoP/DEP/Cir 20/2009 dated December 9, 2009
32	SEBI Circular SEBI/MRD/ OIAE/ Dep/ Cir- 4/2010 dated January 29, 2010
33	SEBI Circular CIR/MRD/DMS/13/2010 dated April 23, 2010
34	SEBI Circular SEBI/MRD/ DP/ 19/2010 dated June 10, 2010
35	SEBI Circular MRD/DP/20/2010 dated July 1, 2010
36	SEBI Circular MRD/DP/22/2010 dated July 29, 2010
37	SEBI Circular CIR/MRD/DMS/28/2010 dated August 31, 2010
38	SEBI Circular CIR/MRD/DP/30/2010 dated September 06, 2010
39	SEBI Circular CIR/MRD/DP/37/2010 dated December 14, 2010

S. No.	Circular / Communication No.
40	SEBI Circular CIR/MRD/DP/4/2011 dated April 7, 2011
41	SEBI Circular CIR/MRD/ DP/05/2011 dated April 27, 2011
42	SEBI Circular CIR/MRD/ICC/16/2012 dated June 15, 2012
43	SEBI Circular CIR/MRD/DP/ 21 /2012 dated August 02, 2012
44	SEBI Circular CIR/MRD/DP/22/2012 dated August 27, 2012
45	SEBI Circular CIR/MRD/DP/24/2012 dated September 11, 2012
46	SEBI Circular CIR/MRD/DP/DA/25/2012 dated September 21, 2012
47	SEBI Circular CIR/MRD/DP/27/2012 dated November 01, 2012
48	SEBI Circular SEBI/MRD/DRMNP/26/2013 dated September 04, 2013
49	SEBI Circular CIR/MRD/DSA/32/2013 dated October 04, 2013
50	SEBI Circular SEBI/MRD/DOP/01/2014 dated January 07, 2014
51	SEBI Circular MRD/DMS/03/2014 dated January 21, 2014
52	SEBI Circular SEBI/MRD/DMS/05/2014 dated February 07, 2014
53	SEBI Circular CIR/MRD/DP/21/2014 dated July 01, 2014
54	SEBI Circular CIR/MRD/DP/22/2014 dated July 04, 2014
55	SEBI Circular CIR/MRD/DP/31/2014 dated November 12, 2014
56	SEBI Circular CIR/MRD/DSA/33/2014 dated December 09, 2014
57	SEBI Circular CIR/MRD/DP/1/2015 dated January 12, 2015
58	SEBI Circular CIR/MRD/DP/10/2015 dated June 05, 2015
59	SEBI Circular CIR/MRD/DP/13/2015 dated July 06, 2015
60	SEBI Circular CIR/MRD/DP/18/2015 dated December 09, 2015
61	SEBI Circular CIR/MRD/DP/19/2015 dated December 09, 2015
62	SEBI Circular MRD/DSA/01/2016 dated January 01, 2016
63	SEBI Circular SEBI/HO/MRD/DSA/CIR/P/2016/113 dated October 19, 2016
64	SEBI Circular SEBI/HO/DMS/ CIR/P/2017/15 dated February 23, 2017
65	SEBI Circular SEBI/HO/MRD/DP/CIR/P/2017/29 dated April 03, 2017
66	SEBI Circular CIR/MRD/DP/56/2017 dated June14, 2017
67	SEBI Circular SEBI/HO/MRD/DSA/CIR/P/2018/1 dated January 29, 2018
68	SEBI Circular CIR/MRD/CSC/148/2018 dated December 07, 2018
69	SEBI Circular CIR/MRD/CSC/151/2018 dated December 14, 2018
70	SEBI Circular CIR/MRD/DP/158/2018 dated December 27, 2018
71	SEBI Circular SEBI/HO/MRD/DOP2DSA2/CIR/P/2019/13 dated January 10, 2019
72	SEBI Circular SEBI/HO/MRD/DOP1/CIR/P/2019/24 dated January 31, 2019
73	SEBI Circular SEBI/HO/MRD/DOP2DSA2/CIR/P/2019/26 dated February 5, 2019
74	SEBI Circular MRD/DoP2DSA2/CIR/P/2019/51 dated April 10, 2019
75	SEBI Circular SEBI/MRD/CSC/CIR/P/2019/64 dated May 20, 2019
76	SEBI Circular SEBI/HO/MRD/DOP2DSA2/CIR/P/2019/87 dated August 01, 2019
77	SEBI Circular SEBI/HO/MRD/DOP1/CIR/P/2019/106 dated October 10, 2019
78	SEBI Circular SEBI/HO/MRD2/DCAP/CIR/P/2019/146 dated November 28, 2019

S. No.	Circular / Communication No.
79	SEBI Circular SEBI/HO/MRD/DDAP/CIR/P/2020/16 dated January 28, 2020
80	SEBI Circular SEBI/HO/MRD1/DSAP/CIR/P/2020/29 dated February 26, 2020
81	SEBI Circular SEBI/HO/MRD-1/CIR/P/2020/95 dated June 05, 2020
82	SEBI Circular SEBI/HO/MRD2/DDAP/CIR/P/2020/137 dated July 24, 2020
83	SEBI Circular SEBI/HO/MRD2/DDAP/CIR/P/2020/153 dated August 18, 2020
84	SEBI Circular SEBI/HO/MRD/DCAP/CIR/P/2020/190 dated October 01, 2020
85	SEBI Circular SEBI/HO/MRD2/DCAP/CIR/P/2020/243 dated December 18, 2020
86	SEBI Circular SEBI/HO/MRD/DCAP/CIR/P/2021/23 dated March 03, 2021
87	SEBI Circular SEBI/HO/MRD1/DTCS/CIR/P/2021/33 dated March 22, 2021
88	SEBI Circular SEBI/HO/MRD1/DTCS/CIR/P/2021/590 dated July 05, 2021
89	SEBI Circular SEBI/HO/MRD1/ICC1/CIR/P/2021/625 dated September 02, 2021
90	SEBI Circular SEBI/HO/MRD2/DCAP/P/CIR/2021/628 dated September 07, 2021
91	SEBI Circular SEBI/HO/MRD1/MRD1_ICC1/P/CIR/2021/664 dated November 23, 2021
92	SEBI Circular SEBI/HO/MRD1/MRD1_DTCS/P/CIR/2022/58 dated May 02, 2022
93	SEBI Circular SEBI/HO/MRD1/MRD1_DTCS/P/CIR/2022/68 dated May 20, 2022
94	SEBI Circular SEBI/HO/MRD1/ICC1/CIR/P/2022/94 dated July 04, 2022
95	SEBI Circular SEBI/HO/MRD/DCAP/P/CIR/2022/110 dated August 19, 2022
96	SEBI Circular SEBI/HO/MRD/MRD-POD-2/P/CIR/2022/114 dated August 26, 2022
97	SEBI Circular SEBI/HO/MRD-TPD-1/CIR/P/2023/7 dated January 09, 2023
98	SEBI Circular SEBI/HO/MRD/MRD-PoD-3/P/CIR/2023/45 dated March 28, 2023
99	SEBI Circular SEBI/HO/MRD/POD 3/CIR/P/2023/58 dated April 20, 2023
100	SEBI Circular SEBI/HO/MRD/TPD/P/CIR/2023/65 dated May 05, 2023
101	SEBI Circular SEBI/HO/MRD/MRD-PoD-3/P/CIR/2023/81 dated May 30, 2023
102	SEBI Circular SEBI/HO/MRD/MRD-PoD-2/P/CIR/2023/99 dated June 23, 2023
103	SEBI Circular SEBI/HO/MRD/TPD/P/CIR/2023/147 dated August 24, 2023
104	SEBI Circular SEBI/HO/MRD/TPD/P/CIR/2023/146 dated August 29, 2023
105	SEBI Letter SEBI SMDRP/NSDL/4615 /2000 dated March 13, 2000
106	SEBI Letter SMDRP/NSDL/26563/2001 dated April 10, 2001
107	SEBI Letter D&CC/ 1099 / 2002 dated November 01, 2002
108	SEBI Letter MRD/VSS/ARR/ 12255/2004 dated June 10, 2004
109	SEBI Letter MRD/DoP/ Dep/82334 /2006 dated December 14, 2006
110	SEBI Letter MRD/DEP/PP/123624 /2008 dated April 23, 2008
111	SEBI Letter MRD/DoP/MC/141442 /2008 dated October 17, 2008
112	SEBI Letter MRD/CDSL/VM/155773/2009 dated February 27, 2009,
113	SEBI Letter MRD/NSDL/VM/158886 /2009 dated March 30, 2009
114	SEBI Letter MRD/DoP/NSDL/VM/ 162378 /2009 dated May 06, 2009
115	SEBI Letter MRD/CDSL/VM/168989 /2009 dated July 07, 2009
116	SEBI Letter MRD/DoP/NSDL/VM/168994 /2009 dated July 07, 2009
117	SEBI Letter SEBI/MRD/DEP/VM/169784 /09 dated July 15, 2009

S. No.	Circular / Communication No.
118	SEBI Letter MRD/DoP/MAS – OW/16723/2010 dated August 17, 2010
119	SEBI Letter MRD/DP/SG-OW/202/2012 dated January 4, 2012
120	SEBI Letter MRD/DP/SG-OW/203/2012 dated January 4, 2012
121	SEBI Letter MRD//DP/OW/23881/2015 dated August 24, 2015
122	SEBI Letter SEBI/HO/MRD/DP/OW/2016/25739/1 dated September 14, 2016
123	SEBI Letter SEBI/HO/MRD/DP/OW/2016/25740/1 dated September 14, 2016
124	SEBI Letter SEBI/HO/MRD/DSA/OW/P/2016/31948 dated November 24, 2016
125	SEBI Letter MRD/DSA1/OW/4946/2018 dated February 14, 2018
126	SEBI Letter MRD/DSA1/OW/4947/2018 dated February 14, 2018
127	SEBI Letter SEBI/HO/MRD/DSA/OW/P/2018/000005436/5 dated February 21, 2018
128	SEBI Letter SEBI/MRD/ICC/OW/P/2018/27066/1 dated September 25, 2018
129	SEBI Letter MRD/DoPII/DSAII/MIRSD/DOS3/OW/2018/28162/1 dated October 22, 2018
130	SEBI Letter SEBI/HO/MRD/CSC/OW/P/2019/10055 dated April 22, 2019
131	SEBI Letter MRD/DSA/OW/11447/2/2019 dated May 8, 2019
132	SEBI Letter SEBI/HO/MRD/CSC/OW/P/2019/22202/1 dated August 28, 2019
133	SEBI Letter SEBI/HO/MRD/CSC/OW/P/2019/28517/1 dated October 30, 2019
134	SEBI Letter SEBI/HO/MRD/CSC/OW/P/2019/28527/1 dated October 30, 2019
135	SEBI Letter MRD2/DDAP/OW/P/2020/19443/1 dated November 13, 2020
136	SEBI Letter SEBI/HO/MRD2/DDAP/OW/P/2021/1632/1 dated January 20, 2021
137	SEBI Letter MRD2/DDAP/OW/P/2021/8568/1 dated April 09, 2021
138	SEBI Letter SEBl/HO/MRD/SEC-2/P/OW/2023/00001730411 dated April 28, 2023
139	SEBI MRD Email dated November 11, 2017
140	SEBI MRD Email dated November 04, 2019
141	SEBI MRD Email dated February 06, 2020
142	SEBI MRD Email dated May 18, 2020
143	SEBI MRD Email dated January 31, 2022
144	SEBI MRD Email dated September 12, 2022
145	SEBI MRD Email dated December 28, 2022

भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

CIRCULAR

SEBI/HO/MIRSD/POD-1/P/CIR/2023/158 **September 26, 2023**

To
All Recognized Stock Exchanges
All Recognized Depositories
Stock Brokers (Trading Members) through Recognized Stock Exchanges
Depository Participants through Depositories
All registered Registrars to an Issue and Share Transfer Agents (RTAs)
All Listed Companies through Recognized Stock Exchanges

Dear Sir / Madam,

Subject: Extension of timelines (i) for nomination in eligible demat accounts and (ii) for submission of PAN, Nomination and KYC details by physical security holders; and voluntary nomination for trading accounts

For trading and demat accounts

1. SEBI, vide circular no. SEBI/HO/MIRSD/RTAMB/CIR/P/2021/601 dated July 23, 2021, stipulates that trading accounts and demat account which do not have 'choice of nomination' by September 30, 2023[1] shall be frozen.

2. In this respect, based on the representations received from the Exchanges, Depositories, Brokers' Associations and various other stakeholders, the following has been decided:

   2.1. Submission of 'choice of nomination' for trading accounts has been made voluntary as a step towards ease of doing business;

   2.2. With respect to demat accounts, it has been decided to extend the last date for submission of 'choice of nomination' to **December 31, 2023.**

For physical security holders

3. As regards physical securities, SEBI, vide circular no. SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2023/37 dated March 16, 2023, stipulated that folios shall be frozen

[1] The aforesaid timeline of September 30, 2023 was prescribed by SEBI circular SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2023/42 dated March 27, 2023.

if PAN, Nomination, Contact details, Bank A/c details and Specimen signature are not submitted by the holders by September 30, 2023.

4. Based on the representations received from investors, Registrars Association of India and various other stakeholders, it has been decided to extend the last date for submission of PAN, Nomination, Contact details, Bank A/c details and Specimen signature for their corresponding folio numbers to **December 31, 2023.**

5. Stock Exchanges, Depositories, RTAs and Listed Companies are advised to:
    a) take necessary steps to implement the provisions of this circular, including making necessary amendment to the relevant bye-laws / business rules / regulations / operational instructions, as the case may be;
    b) bring the provisions of this circular to the notice of their respective constituents and also disseminate this circular on their websites;
    c) communicate to SEBI, the status of the implementation of the provisions of this circular; and
    d) monitor the compliance of this circular.

6. This circular shall come into effect immediately in supersession of relevant provisions contained in various circulars issued by SEBI including Master Circulars issued for Stock Brokers and Registrars to an Issue and Share Transfer Agents dated May 17, 2023.

7. This circular is issued in exercise of powers conferred by Section 11(1) of the Securities and Exchange Board of India Act, 1992, and Section 19 of the Depositories Act, 1996 to protect the interests of investors in securities and to promote the development of, and to regulate the securities market.

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

Yours faithfully,

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