भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

NOTICE INVITING TENDER

Subject: Tender for Special Purpose Comprehensive Validation Audit of Cybersecurity Controls on Zerodha Broking Ltd.

1. Securities and Exchange Board of India (hereinafter referred to as "Board" or "SEBI") is an autonomous, statutory organization established in accordance with the provisions of the SEBI Act, 1992 of the Parliament of India. The basic function of SEBI as mandated by the SEBI Act is "*to protect the interests of investors in securities and to promote the development of, and to regulate the securities market and for matters connected therewith or incidental thereto*".
2. The Board hereby invites online bids at https://www.mstcecommerce.com/eproc from bidders to conduct a "**Special Purpose Comprehensive Validation Audit of Cybersecurity Controls on Zerodha Broking Ltd. "** with the objective of strengthening the cybersecurity posture and resilience of the Securities Market. The validation audit will effectively analyse the Cyber Audit conducted by **Zerodha Broking Ltd.**. The validation audit shall strengthen and facilitate the process of audit by emphasizing on a direct relationship between artefacts and audit observations resulting into improved audit, cybersecurity compliance and cyber resilience of the Zerodha Broking Ltd..

Table1: Schedule of Tender (SOT)

e-Tender No.	**SEBI/HO/ITD/13/25-26/ET/29**
Name of the Work:	**Special Purpose Comprehensive Validation Audit of Cybersecurity Controls on Zerodha Broking Ltd.**
Mode of Tender:	**MODE OF TENDER: e-Tender System** Online submission of Part I – Technical Bid and Part II - Price Bid at https://www.mstcecommerce.com/eproc The bidders are required to submit their offers electronically through MSTC e-tendering portal. Physical tenders or tenders through email will not be acceptable. Bidders are requested to go through the **Annexure – A** – Important Instructions for E-procurement on MSTC Portal in this regard for any queries.
	Bidders shall submit their responses as per the formats given in this Tender in the following manner:

	1. Bidders must upload duly filled copy of the Technical Bid along with digitally signed copy of this tender in acceptance of all clauses of tender in Technical Cover at MSTC e-Procurement Portal. 2. Bidder has to quote the rates on the specified Financial Cover in the MSTC e-Procurement Portal 3. Financial bids will be opened only for the eligible bidders. **Please note that prices should not be indicated in the technical bid but should only be indicated in the financial bid. In case, prices are submitted in technical bid, the bid will be summarily rejected.**
Date of NIT (along with complete tender) available to the parties to download- Tender activation on portal	**November 25, 2025**
Date and time of Pre-Bid Meeting	**December 1, 2025 – 11.00 AM** The name, address and telephone numbers of the nodal officer is: **Ms. Jayashri D** **Assistant Manager (ITD)** **Securities and Exchange Board of India,** **SEBI Bhavan II** **Plot No. C-7, "G Block",** **Bandra Kurla Complex,** **Bandra (E), Mumbai – 400 051** **Maharashtra (India)** **+91-22-4048-9988** **jayashrid@sebi.gov.in** All queries should be received on or before November 28, 2025 by 03.00 p.m. through email (to be sent to marketaudit@sebi.gov.in)
Start date and time of submission of Tender Document	December 2, 2025 – 11.00 AM

Last date and time of submission of Tender Document	December 16, 2025 – 03.00 PM
Validity of Tender	90 days from the last date of submission of tender
Earnest Money Deposit (EMD)	**Rs. 12,000/- (Rupees Twelve Thousand only)** The EMD applicable / payable by the MSME entities for participating in a tender process would be 50% (i.e.**Rs. 6,000/-**) of that being payable by the other entities. EMD can be submitted only through NEFT/ RTGS as detailed in Table 5 of page 7.
Last date of submission of NEFT/ RTGS for EMD	December 16, 2025
Opening of Part-I (i.e. Technical Bids)	**December 17, 2025 – 11.00 AM.** The bids submitted before deadline will be opened at date and time mentioned above by the Bid Opening Committee authorized by SEBI at https://www.mstcecommerce.com/eproc.

3. Purchase Order will be issued to the successful bidder. Bidder shall quote his rates as per the various terms and conditions of this tender document which will also form part of the purchase order.

4. **Scope:**

4.1. The scope of a "Special Purpose Comprehensive Validation Audit of Cybersecurity Controls on Zerodha Broking Ltd." will be as follows:

4.1.1. Verification of the comprehensiveness of the cyber audit; the coverage and scope of the cyber audit conducted by Zerodha Broking Ltd. as per SEBI cybersecurity circular(s).

4.1.2. Analysis of the artefacts vis-à-vis audit observations.

4.1.3. An extensive analysis on the cybersecurity and cyber resilience will be conducted through verification of the indicative checklist enclosed at **Annexure – B.**

4.1.4. The closure of the observations identified shall be checked. If Zerodha Broking Ltd. is non-compliant for any control, the corresponding plan of action will also be verified.

4.1.5. The repeat observations, if any, from previous cyber audits will also be analysed.

4.1.6. Further, the auditor will be required to submit their checklist as part of the approach document before the commencement of the audit.

5. **Bidder's Eligibility Criteria**

The process is open to all Bidders who fulfil the eligibility criteria as set out below and is in agreement with SEBI as per terms & conditions of this NIT document. The Bidders should furnish necessary documentary evidence supporting to meet the eligibility criteria provided in the bidding process. Tenders not fulfilling the eligibility criteria will be rejected.

Table 2: Eligibility Criteria

SN	Parameter	Criteria	Documentary Evidence
1	Technical Criteria	Bidder should be CERT-In empanelled as on the date of publication of NIT and the certificate shall be valid at least for a period of one year from the date of publication of the NIT.	Copy of certificate
2	Bidder Turnover from Security Audit services	1. The average annual financial turnover of the bidder from Security Audit services during the last three financial years, ending 31st March of the previous financial year, should be at least **Rs. 72,000/- (Rupees Seventy-Two Thousand only) [Rs. 54,000/- for MSME].** 2. The bidder shall furnish solvency certificate issued by their banker specifically for the purpose of the work, for an amount equal to **Rs. 2,40,000/- (Rupees Two Lakhs Forty Thousand only)**.	1. Documentary evidence in the form of certified Audited Balance Sheets of relevant periods or a certificate from the Chartered Accountant / Cost Accountant indicating the turnover details for the relevant period shall be uploaded with the bid. 2. Solvency Certificate from bank. 3. MSME certificate, if applicable
3	Bidder Past Experience	1. The bidder must have successfully completed at least one Security Audit assignment costing not less than the amount equal to **Rs. 1,92,000/- (Rupees One Lakh Ninety-Two Thousand only) [Rs.1,44,000/- for MSME]** or more during the last 7 years ending last day of month	1. Bidders are required to submit the copy of Purchase Order for the audit assignment. 2. Bidders are required to submit completion certificate issued by their

SN	Parameter	Criteria	Documentary Evidence
		previous to the one in which the NIT is published for any Govt Organization / PSU / Bank/ BFSI organization in India. 2. Bidder should have completed at least one year of Security Audit of the above mentioned assignment.	client of the one-year Security Audit. 3. MSME certificate, if applicable
4	Blacklisting	The bidder should not be a debarred/blacklisted firm/company in Department of Expenditure/ Ministry of Finance or any Govt. department/Banks/ PSU/other institution in India due to unsatisfactory performance, breach of general or specific instructions, corrupt or fraudulent or any other unethical business practices.	Signed and stamped Form VI on Company's Letterhead signed by Authorized Signatory.
5	No Conflict of Interest	In order to avoid conflict of interest, bidder must not be the existing application implementer(s), VAPT or Information Security (IS) auditor and / or auditor(s) of **Zerodha Broking Ltd.** in the last 3 years from the date of issue of NIT.	Signed and stamped Form VI on Company's Letterhead signed by Authorized Signatory.

6. **Resource Deployment:**

6.1. The resources provided by the bidder should be deployed completely on site at the premises of Zerodha Broking Ltd. (and in SEBI, if required).

6.2. Total period of the audit is envisaged to be 17 days as per the timelines mentioned vide para 8.

6.3. The resources deployed for this project should be on the payroll of the bidder.

6.4. The resources should have the necessary qualification mentioned below:

a. Certified Information Systems Security Professional (CISSP), or
b. Certified Information Security Manager (CISM) of ISACA, or
c. Certified Information Systems Auditor (CISA) of ISACA, or
d. Diploma in Information Systems Audit (ISA or DISA) of ICAI or
e. Diploma in Information System Security Audit (DISSA), ICMAI or
f. Any other formal IT Security Audit related qualification.

Further, the resource deployed should have 5 years' or more experience in conducting Security Audits.

7. **Deliverables:**

7.1. An indicative list of deliverables is detailed below:

7.1.1. Approach Document

7.1.2. Report on the Special Purpose Comprehensive Validation Audit conducted.

7.1.3. Evidences for each observation identified.

7.1.4. Proof of visiting RE premises.

7.2. It may be noted that the report formats, method of artefact collection, detailed Standard Operating Procedure (SOP) for conducting the Special Purpose Comprehensive Validation Audit of Cybersecurity Controls on Zerodha Broking Ltd. will be shared only with the successful bidder.

8. **Timelines:**

Timelines and milestones for the project would be as follows:

Table 3:

Milestone / Phase of the project	**Man Days in which the activity to be completed**
A. Pre-requisite collection and submission of approach document with milestones	5 working days from the issue of purchase order.
B. Conduct of Validation Audit	6 working days from completion of previous milestone (milestone A).
C. Submission of report to SEBI	6 working days from completion of previous milestone (milestone B).

9. **Payment Terms:**

The payment milestones for the project is detailed below:

Table 4:

Milestone	**Payment Terms**
Resource Deployment and Approval of Approach Document by SEBI	15% of the purchase order amount.
Conduct of the Validation Audit	50% of the purchase order amount.

Submission of Validation Audit report to SEBI and approval of the same by SEBI	35% of the purchase order amount.

10. **Earnest Money Deposit:**

10.1. EMD of **Rs.12,000/- (Rs. 6,000/- for MSMEs)** in the form of NEFT/ RTGS is to be credited to the Securities and Exchange Board of India, Mumbai. The bank to which EMD is to be credited via NEFT/ RTGS is as per table 5. Any mode of payment other than the one mentioned above will not be accepted. EMD will not bear any interest. The scanned copy of the receipt of EMD paid via NEFT/ RTGS have to be uploaded in field provided in the MSTC portal.

Table 5:

Name of The Bank	ICICI Bank Limited
IFSC Code	ICIC0000106
Beneficiary Name	Securities and Exchange Board of India
Virtual Account Code	SEBIRCEMDEPOSIT

10.2. The EMD applicable / payable by the MSME entities for participating in a tender process would be 50% of that being payable by the other entities (i.e.**Rs. 6,000/- for MSMEs)**.

10.3. EMD of all unsuccessful Bidders would be returned by SEBI at the earliest after expiry of the final bid validity period and latest by the 30th day after the award of purchase order.

10.4. EMD will be forfeited if the bidder makes withdrawal or modification of an offer within the validity of the bid, after the deadline for submission of such documents; fails to sign the contract/ purchase order or fails to provide the required retention money; or fails to comply with any other condition precedent to issue of purchase order specified in the solicitation documents.

11. **Retention Money:**

Retention Money shall be 5% of the cost of the purchase order and shall be recovered from each on-account-bill of the successful bidder. The retention money shall be recovered from the running bills. The retention money shall be refunded to the successful bidder without interest, after the completion of the last milestone activity mentioned vide table 3 - Milestone C (i.e. submission of Validation Audit report to SEBI and approval of the same by SEBI).

12. **Terms and Conditions:**

12.1. The bidder should not be an auditor who is currently conducting / who has conducted VAPT or Information Security (IS) audit on **Zerodha Broking Ltd.** for the past three years from the date of issue of NIT.

12.2. Limited Tender Enquiry mode for tendering will be followed and Least Cost Based Selection (LCBS) method will be used to identify the successful bidder for award of work.

12.3. The GRAND TOTAL price quoted should be inclusive of all prices and all applicable taxes in Rupees.

12.4. The tender/quotation submitted should be applicable for a minimum period of ninety (90) days from the date of opening the tender/quotation.

12.5. SEBI reserves the right to accept or reject any or all quotations received without assigning any reason whatsoever and SEBI's decision in this regard will be final.

12.6. No commitment of any kind, contractual or otherwise shall exist unless and until a formal written contract has been executed by or on behalf of SEBI. Any notification of preferred Bidder status by SEBI shall not give rise to any enforceable rights by the Bidder.

12.7. This document supersedes and replaces any previous public documentation & communications, and Bidders should place no reliance on such communications.

12.8. SEBI reserves the right to change the requirements. Any changes made subsequently will be communicated through SEBI website. Hence before submitting bids, bidder must ensure that such clarifications/changes have been considered by them. SEBI will not have any responsibility in case some omission is done by any bidder.

12.9. The response to this document should be in English only. Any effort on the part of Bidder to influence evaluation process may result in rejection of the bidder.

12.10. SEBI is not responsible for non-submission of bids within the specified date and time due to any reason.

12.11. Bidders shall be deemed to have:

12.11.1. Examined the tender document and its subsequent changes, if any for the purpose of responding to it.

12.11.2. Examined all circumstances and contingencies, having an effect on their bid and which is obtainable by the making of reasonable enquiries.

12.11.3. Satisfied themselves as to the correctness and sufficiency of their bids and if any discrepancy, error or omission is noticed in the bid, the Bidder shall notify SEBI in writing on or before the end date/time.

12.12. Submission of a tender by a bidder implies that he has read this notice and all other contract documents and has made himself aware of the scope and specifications of the work to be done.

12.13. The bidder shall bear all costs associated with submission of bid, presentation/POC desired by SEBI. SEBI will not be responsible or liable for any cost thereof, regardless of the conduct or outcome of the process.

12.14. The hired resources shall work under the guidance of the SEBI team and follow the office hours of SEBI. The resource must not limit himself/herself to office hours and should be ready to contribute as and when required by SEBI. However, no overtime/ compensatory off will be provided for the same.

12.15. Service Provider must provide the competent resource(s) within 2 working days from the date of issue of the purchase order.

12.16. The service provider must provide a replacement of resource within 3 working days of the request made by SEBI if in case the deputed resource does not perform satisfactorily, shows some behaviour issues or resigns from bidder organization.

12.17. The bidder shall be liable to pay SEBI liquidated damages (LD) for delay in deliveries as specified in the milestones (clause 8)/ payment terms (clause 9).

12.17.1. In case Service Provider is unable to provide the competent resource(s), or the replacement of resource within the specified time as mentioned in point 12.15 and 12.16, the service provider will have to pay liquidated damages/ compensation of an amount equal to 0.50% (five tenths percent) of the fee/ charges payable for the assignment/ milestone for every week or part thereof that the assignment / milestone remains incomplete after the specified date, subject to a maximum of ten percent (10%) of the fee/ charges and subject to force majeure.

12.17.2. In case Service Provider is unable to meet the timelines as agreed and approved by SEBI for completion of validation audit and submission of Validation Audit report, the service provider will have to pay liquidated damages/ compensation of an amount equal to 0.50% (five tenths percent) of the fee/ charges payable for the assignment/ milestone for every week or part thereof that the assignment / milestone remains incomplete after the specified date, subject to a maximum of ten percent (10%) of the fee/ charges and subject to force majeure.

The bidder agrees and considers that the liquidated damages set out herein above are fair and reasonable and that he will raise no objection or dispute with regard to SEBI's right to recover the liquidated damages.

12.18. The bidder agrees with SEBI to execute the Purchase Order, Non-Disclosure Agreement (NDA) as per the format of SEBI. SEBI shall have the right to cancel the tendering process at any time, without thereby incurring any liabilities to the affected

Bidders. Reasons for cancellation, as determined by SEBI include but are not limited to, the following:

12.18.1. Services contemplated are no longer required

12.18.2. Scope of work not adequately or clearly defined due to unforeseen circumstance and/or factors and/or new developments

12.18.3. The project is not in the best interest of SEBI

12.18.4. Any other reason

12.19. Any bids with words/phrases such as (but not limited to) “assumption”, “it is understood that”, “conditional offer” may be subjected to rejection at any stage of evaluation and EMD of the bidder will be forfeited.

12.20. SEBI’s decision in respect to evaluation methodology and short-listing Bidders will be final and no claims whatsoever in this respect will be entertained.

12.21. The bidder understands that if at any stage, information provided by the bidder is found to be inaccurate, bidder is liable to be disqualified and EMD of the bidder will be forfeited.

12.22. The payment will be made after deducting Liquidated Damages and as per applicable taxes.

12.23. All prospective bidders are free to submit proposals for each of the 14 Regulated Entities for whom Validation Audit is to be conducted this year (FY 2025-26), provided no Conflict of Interest exists, as defined in criteria 5 of the table 2 of this tender document.

12.24. The audit will be conducted only onsite on the Zerodha Broking Ltd.. Therefore, no provision for any virtual / remote arrangements will be entertained. Accordingly, resources are to be deployed.

12.25. The following is a list of locations where audit will take place:

12.25.1. Bengaluru

13. **Bidder’s Authorized Signatory:**

The Proposal should be accompanied by an appropriate board resolution or power of attorney in the name of an authorized signatory of the Bidder stating that he is authorized to execute documents and to undertake any activity associated with the Bidder’s Proposal.

FORMS

FORM I - BIDDER INFORMATION DETAILS

This form includes basic information about the bidder and it should be submitted along with Bidder Eligibility Criteria

Sr. No.	Items	Bidder's Response
1	**Information**	
	a) i. Name of the organization ii. Name of the contact person	
	b) Registered office address of the organization	
	c) Contact Details of the contact person (address and phone number)	
	d) Email address of the contact person	
	e) Web site if any, of the organization	
	f) Year of commencement of business	
	g) PAN no.	
	h) Service tax registration No. / GST No.	
2	**Total number of professionals/employees on the company payroll**	

Authorized Signatory:

Name of the Authorized Signatory: Date:

Place: Seal:

FORM II – BIDDER'S BANK ACCOUNT DETAILS

Bidder is advised to provide bank details to facilitate easy and timely credit of payments for services rendered.

1	Name of the Bank	
2	Address of the Bank with Contact details (name, telephone, mobile, email, etc.)	
3	Account Type	
4	Account Title	
5	Account Number	
6	IFSC Code	
7	Organization PAN number	
8	Physical copy of a cancelled check	
9	Remarks, if any	

Signature:

Name of the Authorized Person:

Designation:

Company Seal

FORM III – ELIGIBILITY CRITERIA

The form should be submitted by the bidder in Eligibility Criteria.

<Name of the Bidder>

Special Purpose Comprehensive Validation Audit of Cybersecurity Controls on Zerodha Broking Ltd. - NIT No.:SEBI/HO/ITD/13/25-26/ET/29

SN	Parameter	Criteria	Documentary Evidence
1	Technical Criteria	Bidder should be CERT-In empaneled as on the date of publication of NIT and the certificate shall be valid at least for a period of one year from the date of publication of the NIT.	Copy of certificate
2	Bidder Turnover from Security Audit services	1. The average annual financial turnover of the bidder from Security Audit services during the last three financial years, ending 31st March of the previous financial year, should be at least **Rs. 72,000/- (Rupees Seventy-Two Thousand only) [Rs. 54,000/- for MSME].** 2. The bidder shall furnish solvency certificate issued by their banker specifically for the purpose of the work, for an amount equal to **Rs. 2,40,000/- (Rupees Two Lakhs Forty Thousand only)**.	1. Documentary evidence in the form of certified Audited Balance Sheets of relevant periods or a certificate from the Chartered Accountant / Cost Accountant indicating the turnover details for the relevant period shall be uploaded with the bid. 2. Solvency Certificate from the bank. 3. MSME certificate, if applicable.
3	Bidder Past Experience	1. The bidder must have successfully completed at least one Security Audit assignment costing not less than the amount equal to **Rs. 1,92,000/- (Rupees One Lakh Ninety-Two Thousand only) [Rs.1,44,000/-**	1. Bidders are required to submit the copy of Purchase Order for the audit assignment. 2. Bidders are required to submit completion certificate issued by their

SN	Parameter	Criteria	Documentary Evidence
		for MSME] or more during the last 7 years ending last day of month previous to the one in which the NIT is published for any Govt Organization / PSU / Bank/ BFSI organization in India. 2. Bidder should have completed at least one year of Security Audit of the above mentioned assignment.	client of the one year Security Audit. 3. MSME certificate, if applicable.
4	Blacklisting	The bidder should not be a debarred/blacklisted firm/company in Department of Expenditure/ Ministry of Finance or any Govt. department/Banks/ PSU/other institution in India due to unsatisfactory performance, breach of general or specific instructions, corrupt or fraudulent or any other unethical business practices.	Signed and stamped Form VI on Company's Letterhead signed by Authorized Signatory.
5	No Conflict of Interest	In order to avoid conflict of interest, bidder must not be the existing application implementer(s), VAPT or Information Security (IS) auditor and / or auditor(s) of **Zerodha Broking Ltd.** in the last 3 years from the date of issue of NIT.	Signed and stamped Form VI on Company's Letterhead signed by Authorized Signatory.

FORM IV – PROJECT DETAILS

Details of project successfully completed of providing Security Audit Services to any Govt. Organization/ PSU/ Bank/ BFSI organization in India (Attach Copy of Purchase orders along with project completion certificate from the client/ client email confirming project completion/ payment proof and project details)

Project no. 1 ….

SN	Items	Mandatory (Y/N)	Bidder's Response
1	Client name	Y	
2	Location of client along with contact person, contact no and email id	Y	
3	Copy of Purchase Order along with project completion proofs (s) for the project	Y	
4	a. Date of Commencement of Contract: b. Date of Completion of the project: c. Status of the Project:	Y	
5	Nature of project for the Clients (Please list the activities handled by the bidder)	Y	
6	Scope of Work	Y	
7	Team Size	Y	
8	Name of the Project Head	Y	
9	Name of the other auditors	Y	
10	Software Tools & Technology used (if any)	N	
11	Total Efforts in Man months	Y	
12	Contract Amount (in Rupees Lakhs)	Y	
13	Any other relevant information including reason for delay if any	N	

Note: The bidder should give the above information in this format only.

Authorized Signatory:

Name of the Authorized Signatory: Date:

Place: Seal:

FORM V – RESOURCE DETAILS

The bidder should provide details of the resource proposed to be deployed at **Zerodha Broking Ltd.** in the format given below. The details should be provided in the following format:

SN	Name of the Staff	Qualification	Area of Expertise	Year of joining the organization	Total Years of experience	Details of the previously conducted Security Audits for any Govt Organization/ PSU/ Bank/ BFSI Organization in India

FORM VI: Self – Declarations

(Undertaking to be submitted on Bidder Company's Letter Head)

To,

General Manager, ITD (CISO)
Securities and Exchange Board of India
SEBI Bhavan II
Plot No. C4-A, "G Block"
Bandra-Kurla Complex,
Bandra
Mumbai – 400 051

Ref: *Bid for Special Purpose Comprehensive Validation Audit of Cybersecurity Controls on* **Zerodha Broking Ltd.**

We, --------- (name and designation) on behalf of ---------having its registered office at ------have submitted a Bid proposal to SEBI for ---------- in response to the Notice Inviting Tender (NIT) dated November 25, 2025 issued by SEBI.

We are duly authorized people to submit this undertaking.

We have read and understood the aforesaid NIT and we hereby convey our absolute and unconditional acceptance to the aforesaid NIT.

We have submitted our Bid in compliance with the specific requirements as mentioned in this NIT.

We have provided with all necessary information, supporting documents which are true and accurate and shall provide with such additional information as may be required by SEBI from time to time.

Neither we nor any of our employee/director has been barred from providing the Services nor are we in negative list/blacklisted by any public sector Banks, statutory or regulatory or investigative agencies in India or abroad in the last 5 years. Also, we confirm that we are not debarred/ blacklisted by the Department of Expenditure/ Ministry of Finance.

All the information furnished here in and as per the document submitted is true and accurate and nothing has been concealed or tampered with. We have gone through all the conditions of Bid and are aware that we would be liable to any punitive action in case of furnishing of false information / documents.

We also undertake that, we were/are never involved in any legal case that may affect the solvency/ existence of our organization or in any other way that may affect capability to provide/ continue the services to SEBI.

We also undertake that we are not existing application implementer (s), VAPT or Information Security (IS) auditor and/ or auditor (s) of Zerodha Broking Ltd.in the last 3 years from the date of issue of NIT.

It is further certified that we have not modified or deleted any text/matter in this NIT. I hereby certify that this bidder fulfils all requirements in this regard and is eligible to be considered. [Where applicable, evidence of valid registration by the Competent Authority shall be attached.]"

Dated this _____ day of _____ <*YEAR*>

Name and Signature of Authorized Signatory

(Company Seal)

In the capacity of

Duly authorized to sign bids for and on behalf of:

FORM VII – EMD Details

Bidder should provide details of the EMD on the company letterhead, in the following format (details should be filled as per the type of EMD i.e. NEFT/RTGS/Bank Guarantee):

1. Sender's Name:
2. Transfer Type: (NEFT/RTGS)
3. Sender's Name:
4. Sender's Account Name:
5. Sender's Account Number:
6. Sender's bank IFSC code:
7. Bank's Branch Name:
8. Transaction Amount (in Rupees):
9. Amount in Words:
10. Date of Transaction:
11. Time of Transaction:
12. UTR No.::

Signature of Competent Authority Date:

Place:

FORM VIII - Letter of Refund of EMD

Date:

General Manager, ITD (CISO)
Securities and Exchange Board of India
SEBI Bhavan II
Plot No. C4-A, "G Block"
Bandra-Kurla Complex,
Bandra
Mumbai – 400 051

Ref: *NIT for Special Purpose Comprehensive Validation Audit of Cybersecurity Controls on* **Zerodha Broking Ltd.**

We _____ (Company Name) had participated in the tender for *Special Purpose Comprehensive Validation Audit of Cybersecurity Controls on* **Zerodha Broking Ltd..** Kindly refund and remit the EMD submitted for participation through NEFT/RTGS.

The Details of the transaction are as follows:

Sl. No.	Bidder Name	Bank Name	Amount (Rs.)	Transaction Number	Transaction Date

Bank details to which the money needs to be credited via NEFT/ RTGS are as follows:

Sl. No.	Item	Details
1	Name of the bank with Branch	
2	Account Type	
3	Account Title	
4	Account Number	
5	IFSC Code	

Sign

Name of the signatory:
Designation :
Company Seal :

FORM IX: MSME Declaration (if applicable)

Date:
General Manager – ITD (CISO)
SEBI Bhavan II
Plot No. C7-A, "G Block"
Bandra-Kurla Complex,
Bandra East
Mumbai – 400 051.

Ref: NIT for Special Purpose Comprehensive Validation Audit of Cybersecurity Controls on Zerodha Broking Ltd. - Reg;

We _____ (Company Name) had participated in the Notice Inviting Tender for Special Purpose Comprehensive Validation Audit of Cybersecurity Controls on Zerodha Broking Ltd. as MSME (Micro, Small, Medium Enterprises). Hereby attaching the certification issued by Government of India regarding the same. (Please attach the certification).(Certification of MSME should be valid atleast till 6 months from the date of publication of NIT)

Signature:

Name of the authorised signatory:

Designation :

Company Seal:

FORM X: Undertaking of Confidentiality and Non-Disclosure

1. This has reference to the data to be provided by Securities Exchange Board of India to <Organization Name> through General Manager, ITD (CISO) to undertake designated project "Special Purpose Comprehensive Validation Audit of Cybersecurity Controls on **Zerodha Broking Ltd.**" Control No <control no to be communicated by SEBI>. In this context to ensure that the confidentiality of data is maintained at all the times, it is required that an "Undertaking of confidentiality and non-disclosure" is signed by <Organization Name>.

   Parties: "<Recipient Organization>" through <Recipient Official Name> (Recipient) and [SEBI] (The Discloser, as may be nominated by SEBI from time to time on behalf of **Zerodha Broking Ltd.**).

   The Discloser on the request of the Recipient intends to share access to data records (the Information) with the Recipient for the "Special Purpose Comprehensive Validation Audit of Cybersecurity Controls on **Zerodha Broking Ltd.**".

2. The Recipient undertakes not to use the Information for any purpose except the stated Purpose.

3. The Recipient undertakes to keep the Information secure and not to disclose directly or indirectly/ allow access in any way to any third party and shall maintain its confidentiality in accordance with the terms of this undertaking and as per the law applicable from time to time. The Recipient shall ensure that all data collected, maintained and analysed by it, are at all times kept secure and fully and effectively protected against unauthorized access or discloser or transmission by accidental or intentional destruction, loss or damage. The Recipient shall adopt and implement appropriate technical and organization security measures to protect data from any kind of unauthorized access by any person including its own employees and would be liable in case of any breach of confidentiality.

4. The Recipient undertakes not to make or retain copy of the Information or results of audits, tests, analysis, extracts or usages carried out by them.

5. The Recipient undertakes not to send the Information or any other related data at any time outside the premises of the **Zerodha Broking Ltd.** for the purpose of storage, processing, analysis or handling without the express written consent from SEBI and the **Zerodha Broking Ltd.**. The Information or any other related data should be sent outside the premises of the RE only for the purpose of sharing it with SEBI.

6. The undertakings in clauses 2, 3, 4, 5 and 6 above shall apply to all of the Information disclosed by the Discloser to the Recipient, regardless of the way or form in which it is disclosed or recorded but they would not apply to:

   a. any information which is or in future comes into the public domain (unless as a result of the breach of this Undertaking); or
   b. Any information which is already in the public domain.

7. The Recipient shall, at any time on request from the Discloser and at the time of expiration/ termination of the contract, return all copies and records of the Information to the Discloser and shall not retain any copies or records of the Information. Any data kept in the computer systems in any format by all the user shall be erased and a confirmation sent to the Discloser, on or before the date as intimated by the discloser.

8. Neither this Agreement nor the supply of any information grants the Recipient any license, interest or right in respect of any intellectual property rights of the Discloser except the right to access and use the Information solely for the stated purpose.

9. In case, the Recipient is an organization, it shall obtain a similar undertaking (for their records) with all the authorized users of the data. The Recipient shall disclose the details of all the users of data of the Recipient organization to the discloser. Any misuse/unauthorized use of information by any of the users of data shall render the Recipient liable under law.

10. The undertakings in clauses 2, 3, 4, 5 and 6 will continue in force indefinitely till such time the confirmation is given under clause 5. The Recipient assumes all legal liability arising out of any precipitative action taken by such Recipient based on the data provided by the Discloser.

11. The Recipient agrees to allow and co-operate with SEBI officials during inspection undertaken to ensure appropriate usage of data or derivative thereof and the Recipient shall abide all the directions/instructions given by the Discloser as regards the usage of the data or derivative (e.g. published paper, training material etc.) thereof.

12. The Recipient agrees that in case it fails to maintain confidentiality of data or fails to abide by any clause of this undertaking or is found indulging in any kind of irregularity with regard to data usage or provides false/misleading information, the Recipient shall be solely responsible and liable for all actions as per law prevalent at the relevant point of time (including the law which may came into force after signing this undertaking). Further, the Recipient shall be liable to make good of any loss/damage caused to the Discloser/ **Zerodha Broking Ltd.** for any unauthorized use/misuse of the information by the Recipient and shall keep the Discloser (and SEBI) indemnified for the same.

	DGM-ITD(ITD_CIMG) **(On behalf of SEBI)**	**Recipient**	
		Authorizing Person (Representing the Organization)	**Recipient Person (Representing the Institute)**
Name			
Signature			
Designation			
Date			

FORM XI – Covering Letter for Financial Bid

To:

<Location, Date>

General Manager, ITD (CISO)
Securities and Exchange Board of India
SEBI Bhavan II,
Plot No. C-7, "G Block"
Bandra Kurla Complex,
Bandra (E), Mumbai – 400051
India

Subject: Submission of the Financial bid for *Special Purpose Comprehensive Validation Audit on Cybersecurity Controls on* **Zerodha Broking Ltd.**

Dear Sir/Madam,

We, the undersigned, offer to provide the validation audit services for *Special Purpose Comprehensive Validation Audit on Cybersecurity Controls on* **Zerodha Broking Ltd.** in accordance with your Notice Inviting Tender NIT No. *SEBI/HO/ITD/ 13/25-26/ET/29* dated *November 25, 2025* and our Proposal (Technical and Financial Proposals). Our attached Financial Proposal is as submitted in our Commercial Bid as per Form XII. This amount is excluding all the applicable taxes.

1. PRICE AND VALIDITY
All the prices mentioned in our Tender are in accordance with the terms as specified in the NIT documents. All the prices and other terms and conditions of this Bid are valid for a period of 90 days from the date of opening of the Bid.

2. UNIT RATES
We have indicated in the relevant forms enclosed, the unit rates for the purpose of on account of payment as well as for price adjustment in case of any increase to / decrease from the scope of work under the contract.

3. BID PRICING
We further confirm that the prices stated in our bid are in accordance with your Instruction to Bidders included in Bid documents.

4. QUALIFYING DATA
We confirm having submitted the information as required by you in your Instruction to Bidders. In case you require any other further information/documentary proof in this regard before evaluation of our Bid, we agree to furnish the same in time to your satisfaction.

5. BID PRICE
We declare that our Bid Price is for the entire scope of the work as specified in the Section 4. These prices are indicated in the Commercial Bid attached as part of the Bid.

Our Financial Proposal shall be binding upon us subject to the modifications resulting from Contract negotiations, up to expiration of the validity period of the Proposal, i.e., *<Last date of Validity of Proposal>.*

We understand you are not bound to accept any Proposal you receive.

We hereby declare that our Bid is made in good faith, without collusion or fraud and the information contained in the Bid is true and correct to the best of our knowledge and belief. Thanking you.

Yours sincerely,

Authorized Signature:
Name and Title of Signatory:
Name of Firm:
Address:

FORM XII – Commercial Bid Template

Format for Submission of Cost for Conducting the Special Purpose Comprehensive Validation Audit of Cybersecurity Controls on Zerodha Broking Ltd.

SN (A)	Resource (B)	Count (C)	Unit Price/ Man- Day (Man-day rate) (D)	No. of days (E)	Total (Exclusive of Taxes) (F =DxE)	Total Applicable Taxes (G)	Grand Total (H = F+G)
1.	Auditor	01	xxxx	17	xxxxx	xxxxx	xxxxx
Grand Total							xxxxx

Total Price (F) in Words: _____

Grand Total Price (H) in Words: _____

Note:

1. L1 will be computed on total amount (Column F).
2. The commercial bid should contain the Total Project cost, on a fixed cost basis. SEBI will neither provide nor reimburse any expenditure towards any type of accommodation, travel ticket, airfares, train fares, halting expenses, transport, lodging, boarding etc.
3. Payments will be made to the bidder only for the actual number of days of work/ deployment subject to the liquidated damages clause.
4. This template is for reference purpose only. Actual cost of the work shall be quoted in the price cover of the event on MSTC portal.

FORM XIII – CHECKLIST

Check list of enclosure:		
1.	Form I – Bidder Information Details attached	YES/NO
2.	Form II – Bidder's Bank Account Details	YES/NO
3.	Form III – Eligibility Criteria will all supporting documents	YES/NO
4.	Form IV- Project Details	YES/NO
5.	Form V – Resource Details	YES/NO
6.	Form VI – Self- Declarations	YES/NO
7.	Form VII – EMD Details	YES/NO
8.	Form VII – Letter of Refund of EMD	YES/NO
9.	Form IX – MSME Declaration (if applicable)	YES/NO
10.	Form X – Undertaking of Confidentiality and Non-Disclosure	YES/NO
11.	Form XI – Covering Letter for Financial Bid	YES/NO
12.	Letter regarding Bidder's Authorized Signatory	YES/NO
13.	Checklist	YES/NO

ANNEXURE – A: Important instructions for E-Procurement on MSTC Portal

Bidders are requested to read the terms & conditions of this tender before submitting their online tender.

1. Process of E-tender:

A. **Registration:** The process involves vendor's registration with MSTC e procurement portal which is free of cost. Only after registration, the vendor(s) can submit his/their bids electronically. This submission of bids shall be done over the internet. The Vendor should possess a valid Class III signing and encryption type digital signature certificate. Vendors are to make their own arrangement for bidding from a computer connected with Internet. MSTC is not responsible for making such arrangement. (Bids will not be recorded without Digital Signature).

SPECIAL NOTE: THE PRICE BID HAVE TO BE SUBMITTED ON-LINE AT www.mstcecommerce.com/eproc

i. Vendors are required to register themselves online with https://www.mstcecommerce.com/eproc → Register (Filling up details and creating own user id and password) → Submit. Please follow the 'Registration Guide' available in the Registration link before proceeding.

ii. Vendors will receive a system generated mail confirming the registration in their email which has been provided during filling the registration form.

iii. The Vendors shall have to subscribe to the buyers and categories in order to receive system generated mails. In order to subscribe, a vendor has to login and click on 'My Subscription' followed by 'Add Subscription'. On successful subscription, a system generated mail shall be forwarded to the vendor. Please follow the guide for 'Subscription' of 'Download Guides' available in the Dashboard before proceeding.

For specific queries/ clarifications, please contact MSTC

Contact person (MSTC Ltd):

1. Mr. Tanmoy Sarkar, Email id- tsarkar@mstcindia.co.in,
   Mobile no.- 8349894664
2. Ms. Rupali Pandey, Email id- rpandey@mstcindia.co.in,
   Mobile no.- 9458704037

For Technical Help: Contact 033-22901004

B. System Requirement:

a) Operating System – Windows 7 and above

b) Web Browser- Preferred 'IE 8' and above.

c) Security Settings:

i. Tools=>Internet Options=>Security=>Disable protected Mode If enabled- i.e., Remove the tick from the box mentioning "Enable Protected Mode".

ii. Tools => Internet Options => Security =>Custom Level=>

- Active X control & plug-ins: Enable all Active-X Controls
- Scripting: Enable "Allow Status Bar Update Via Script"
- Disable "Use Pop-up Blocker"

d) JAVA: JRE 8 Latest update

e) Other Settings:

i. View => Toolbars=> "Tick" Status Bar.

ii. Tools=>Internet Options=> General=> Click on Settings under "Browsing history/Delete Browsing History" => Temporary Internet Files=>Activate "Every time I Visit the Webpage".

f) For new Version of IE or other "Active –X Filtering" under Tools should not be ticked.

g) Tools =>Internet Options=> Security=> Selected Trusted Sites=> Add Website http://www.mstcecommerce.com.

2. The tender will be opened electronically on specified date and time as given in the RFP/NIT.

3. All entries in the tender should be entered in online Price Bid Formats without any ambiguity.

4. All notices and correspondence to the bidder(s) shall be sent by email only during the process, up to the finalization of tender by MSTC. Hence the bidders are required to ensure that their official email ID provided is valid and updated at the stage of registration of vendor with MSTC (i.e. Service Provider). Bidders are also requested to ensure validity of their DSCs (Digital Signature Certificates).

5. E-tender cannot be accessed after the due date and time.

5. **Bidding in e-tender:**

a. The process involves Electronic Bidding for submission of Bid.

b. The bidder(s) can submit their Bid through internet in MSTC Website www.mstcecommerce.com/eproc

c. The RFP/NIT/ Documents shall be available for download in the event catalogue available under 'Event Details' of the Event.

d. Please follow the guides for ‘Uploading encryption public key’ and ‘Bidding’ under ‘Download Guides’ available in the Dashboard before proceeding to submit bid.

e. The bidders may upload the bidding related documents in the link ‘My Documents’. The documents uploaded here shall be available for attaching with this event in the Bid Floor.

f. In order to submit bid, a vendor has to go to ‘Events’ from the menu and select ‘Bid Floor’. The vendor has to select the buyer ‘SEBI (Securities and Exchange Board of India)’ from the buyer list in order to view the live events list. The correct event has to be selected from the event list for participation. A vendor has to submit ‘Event wise bid details’ that may consist of ‘Common Terms’ and/ or ‘Document Attach’. A vendor has to save the Common Terms and/ or attach documents by clicking the respective buttons. Once the event specific bids are saved, the status is updated in ‘Event specific bid status’ and the ‘Item specific bid’ button appears on the bid floor. Thereafter vendor has to click button under ‘Technical Cover’ in order to save the technical bid for specific lots. Once the technical bid is saved, the ‘Price Cover’ button appears on the screen for respective lots. Once price bid is saved, the vendor has to click on ‘Final Submit’. On final submission of bid, the status of the bid submission shall display ‘Bid submitted’ under ‘Item specific bid status’. A vendor shall receive system generated mail.

NOTE: - The bid cannot be revised once the Final Submit button has been clicked by the bidder. However, if the bidder wishes to change his bids then he may delete the bid and re- submit the same.

g. In all cases, bidder should use their own ID and Password along with Digital Signature at the time of submission of their bid.

h. During the entire e-tender process, the bidders will remain completely anonymous to one another and also to everybody else.

i. The e-tender floor shall remain open from the pre-announced date & time and for the duration mentioned above

j. All electronic bids submitted during the e-tender process shall be legally binding on the bidder. Any bid will be considered as the valid bid offered by that bidder and acceptance of the same by Buyer will form a binding contract between Buyer and the Bidder.

k. . It is mandatory that all the bids are submitted with digital signature certificate otherwise the same will not be accepted by the system.

l. Buyer reserves the right to cancel or reject or accept or withdraw or extend the tender in full or part as the case may be without assigning any reason thereof.

m. No deviation of the terms and conditions of the tender document is acceptable. Submission of bid in the e-tender floor by any bidder confirms his acceptance of terms & conditions for the tender.

n. Unit of Measure (UOM)is indicated in the e-tender Floor. Rate to be quoted should be in Indian Rupee as per UOM indicated in the e-tender floor/tender document.

7. Any order resulting from this e-tender shall be governed by the terms and conditions mentioned therein.

8. No deviation to the terms & conditions are allowed.

9. Buyer has the right to cancel this e-tender or extend the due date of receipt of bid(s) without assigning any reason thereof.

10. The online tender should be submitted strictly as per the terms and conditions and procedures laid down in the website www.mstcecommerce.com/eproc of MSTC Ltd.

11. The bidders should upload all the documents required (if any) as per terms of RFP/NIT. Any other document uploaded which is not required as per the terms of the RFP/NIT shall not be considered.

12. The bid will be evaluated based on the filled-in Price bid formats.

13. Canvassing in any form in connection with the Tender is strictly prohibited and the bids submitted by the bidders who resort to canvassing are liable to be rejected

ANNEXURE – B

Table 1 : Cyber Security and Cyber Resilience framework for Stock Brokers and Depository Participants Circular No. SEBI/HO/MIRSD/CIR/PB/2018/147 dated Dec 03, 2018 including modifications

SN	Circular Item	Questions	Details of the Substantiating Artefact	Additional Instructions to the inspector
1	Cyber attacks 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 cyber attacks 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	NA	Cyber security and resilience policy	*NA*
GOVERNANCE				
2	As part of the operational risk management framework to manage risk to systems, networks and databases from cyber attacks and threats, Stock Brokers/ 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 Stock Broker / 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	NA	Cyber security and resilience policy	*NA*

SN	Circular Item	Questions	Details of the Substantiating Artefact	Additional Instructions to the inspector
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. 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		Cyber security and resilience policy	
4	The Cyber security policy of Stock Brokers trading through APIs based terminal / Depository Participants should consider 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.	Refer document ['Guidelines for Protection of National Critical Information Infrastructure']	Cyber security and resilience policy	
5	Stock Brokers trading through APIs based terminal / Depository Participants may refer to best practices from standards such as ISO 27001, ISO 27002, COBIT 5, etc., or their subsequent revisions, if any, from time to time.	1. What is the validity of current certification? 2. Is the ISO certificate obtained for all the sites of the entity (DC, DR, NDR)	1. ISO certificate, any other applicable certificates	*The Inspector shall check the duration of validity of all the applicable certificates.*

SN	Circular Item	Questions	Details of the Substantiating Artefact	Additional Instructions to the inspector
6	Stock Brokers/ 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 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.	1. Who is the CISO ? 2. What are the roles and responsibilities of CISO ? Whether the roles and responsibilities are clearly defined in the policy document 3. How often does the CISO reports to the board on cybersecurity matters If applicable, Examine recent cybersecurity incidents and CISO's role in managing those incidents.	1. Information Security Policy	*The inspector shall* *1. check that the roles and responsibilities of CISO are clearly defined and implemented* *2. Check if the procedure for reporting cybersecurity incidents to CISO is followed or not.*

SN	Circular Item	Questions	Details of the Substantiating Artefact	Additional Instructions to the inspector
7	The Board / Partners / Proprietor of the Stock Brokers / Depository Participants shall constitute an internal Technology Committee 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 Stock Brokers / Depository Participants for appropriate action.	1. Whether the procedure of formulating the Technology Committee is laid down in the policy document. 2. What is the frequency of the Technology Committee meetings? What are the dates on which meetings are conducted? 3. What are the points discussed in the meeting(s) regarding: a. Review of current cyber security policy b. Review of current IT and cyber security capabilities c. Improvement in cyber security and cyber resilience 4. What are the follow up actions are taken based on the quarterly review	1. Minutes of meetings of Technology Committee Meeting 2. Quarterly reports on threats experienced 3. Incident Management Process Document	*The inspector shall* *1. verify that the quarterly Committee meetings are conducted and well documented, including agendas, minutes and actions taken for the previous Committee meeting.* *2. Check whether implementation of Cyber security policy is reviewed or not.*

SN	Circular Item	Questions	Details of the Substantiating Artefact	Additional Instructions to the inspector
8	Stock Brokers/ Depository Participants should establish a reporting procedure to facilitate communication of unusual activities and events to the Designated Officer in a timely manner.	1. What is the reporting process. What channels are used for communicating - phone, email or dedicated incident reporting systems. Check the effectiveness and security of communication channels in use. Also check whether there are multiple channels available i.e. at least one backup channel shall be there if need be. 2. What are the events that are reported to CISO? How is the distinction done for which incident to report to CISO. 3. Is there a documented policy which lays down the reporting process. 4. Instances of communication during inspection period *[may be checked on a sample basis]*	1. Cyber Security and resilience policy 2. Incident Management Process Document	*The inspector shall* *1. check for the presence of a documented policy outlining the reporting process. The policy should include sections on incident identification, reporting procedures, roles and responsibilities, and escalation criteria.* *2. Review the incident management process document for procedures on incident detection, classification, and reporting and check that it aligns with the overall cybersecurity and resilience policy. The document should include flowcharts or detailed steps for incident reporting, including specific scenarios and response actions.* 3. *Verify that incidents are documented and communicated as per the policy. The inspector can review a RCA of past incidents see if it includes details such as the incident description, date and time of detection, actions taken, and communication records with the CISO.*

SN	Circular Item	Questions	Details of the Substantiating Artefact	Additional Instructions to the inspector
9	The Designated officer and the technology committee of the Stock Brokers / 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.	1. Whether the instances of cyber attacks (domestically and globally) were reviewed or not 2. What are the sources of information you use to stay updated on domestic and global cyber attacks.	1. Minutes of meeting of Technology Committee Meeting 2. Incident management Process document	*The sources of information may also be shared with other MIIs*
10	Stock Brokers/ Depository Participants 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 Stock Brokers/ Depository Participants, towards ensuring the goal of cyber security.	Responsibility of the following shall be defined 1. Employees 2. Outsourced employees a. How does the entity assess and manage the cybersecurity practices of vendors? b. What mechanisms are present to enforce compliance and address non-compliance 3. Members of SCOT and any other relevant IT committee	1. Cyber security and resilience policy 2. Any audit, assessments or compliance checks performed during the inspection period	

SN	Circular Item	Questions	Details of the Substantiating Artefact	Additional Instructions to the inspector
IDENTIFY				
11	Stock Brokers / Depository Participants should identify critical assets based on their sensitivity and criticality for business operations, services and data management. To this end, Stock Brokers / Depository Participants should maintain up-to-date inventory of its hardware and systems and the personnel to whom these have been issued, software and information assets (internal and external), details of its network resources, connections to its network and data flows	1. What is the process for onboarding of new assets? 2. Is the entity using any tool for asset management? Is the tool providing the functionality of tracking, updating and managing asset inventory? 3. What is the process of classifying new assets into critical or non-critical? Any criteria or set of guidelines used for this classification 4. What are the timelines for classification of new assets? 5. What are the processes in place to ensure that this inventory is regularly updated?	1. Asset Management Policy 2. Asset Inventory of a. Hardware b. Software c. Information Assets (internal / external) 3. List of critical assets	*Inspector shall check* *1. the correctness of the current asset inventory by verifying the process of arriving at the current asset inventory.* *2. Inspector may also check if there are any tools used for maintaining the asset register and what part of the process is automated.* *3. check whether or not the timelines for classification of newly onboarded assets were adhered and a record of such was maintained.* *4. Check for the presence of any shadow IT assets. This can be achieved by running a network scan during working hours to identify all active IP addresses and devices and then cross-referencing these with the asset inventory to find any unlisted devices.* *5. If the entity is using cloud services, check for the CASB (Cloud Access Security Broker) tool logs for detection of access to unauthorized cloud services and applications.*

SN	Circular Item	Questions	Details of the Substantiating Artefact	Additional Instructions to the inspector
		6. How does the entity track the data flows and connection within the network.		

SN	Circular Item	Questions	Details of the Substantiating Artefact	Additional Instructions to the inspector
12	Stock Brokers/ 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.	1. What controls are deployed to protect from such threats	1. Cyber security Policy	*The Inspector shall check the proactiveness of the entity in this regard. This can be gauged by checking if the cybersecurity threats were discussed in the subsequent Committee meetings and actions taken following that... (Pt. 9 should be taken into consideration)*
PROTECTION				
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.	1. Whether access management policy is in place. When was it last updated. 2. Is role based access control being implemented? 3. Are there exceptions to access control policies and how are these exceptions approved. 4. How does the entity ensure that these exceptions are temporary i.e. the exceptional access	1. Access Management Policy 2. Review of user access during the period of inspection	*The Inspector shall* *1. check that the privileged access to the users is reviewed from time to time.* *2. Verify the exception report duly approved by the competent authority during the inspection period.*

SN	Circular Item	Questions	Details of the Substantiating Artefact	Additional Instructions to the inspector
		given shall be terminated in a specific period of time as defined in the access management policy?		
14	Any access to Stock Brokers / Depository Participants systems, applications, networks, databases, etc., should be for a defined purpose and for a defined period. Stock Brokers / 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	1. Whether Access Management Policy is in place 2. What mechanisms are in place to establish access to i) IT systems ii) Applications iii) Databases iv) Network	1. Access Management Policy 2. 2FA screenshot 3. VPN screenshot	
15	Stock Brokers / Depository Participants should implement an access policy which addresses strong password controls for users' access to systems, applications, networks and databases.	1. Whether password management policy is defined. 2. Password Management Policy should cover i) Minimum password length and complexity requirements ii) Avoiding reuse of old passwords iii) Passwords are stored in encrypted format	Password Management Policy	*The Inspector shall* *1. verify the implementation of Password Policy* *2. Check the password change logs if they are maintained.*

SN	Circular Item	Questions	Details of the Substantiating Artefact	Additional Instructions to the inspector
16	All critical systems of the Stock Broker/ Depository Participant accessible over the internet should have two-factor security (such as VPNs, Firewall controls etc.)	1. Whether two factor security is present for all critical systems	2FA Screenshot	*The Inspector shall ask the entity to demonstrate the login process and verify the implementation of 2FA process.*
17	Stock Brokers / 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.	1. Describe the logging mechanism to check user access activities. 2. Check whether the logs include information such as user IDs, timestamps and details of accessed resources. 3. Who has the access to log data (only authorised person shall have this access)	1. Access Management Policy 2. Log retention Policy	-
18	Stock Brokers / Depository Participants should deploy controls and security measures to supervise staff with elevated system access entitlements (such as admin or privileged users) to Stock Broker/ 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.	1. Whether review of activity of privileged users is conducted and what is the frequency of such exercise. 2. Where are the logs being stored and do the privileged users have access to the systems on which logs are being stored.	1. Access Management Policy 2. Log retention Policy	-

SN	Circular Item	Questions	Details of the Substantiating Artefact	Additional Instructions to the inspector
19	Employees and outsourced staff such as employees of vendors or service providers, who may be given authorised access to the Stock Brokers/ Depository Participants critical systems, networks and other computer resources, should be subject to stringent supervision, monitoring and access restrictions.	1. List of outsourced staff who have privileged access to critical systems and reason for the same 2. What are the controls and measures that are in place for monitoring for access restrictions	-	-
20	Stock Brokers / 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 Stock Broker/ Depository Participant's critical IT infrastructure.	List of Restricted category/sites is maintained and updated from time to time.	Internet Access Policy	-
21	User Management must address deactivation of access of privileges of users who are leaving the organization or whose access privileges have been withdrawn	1. Check the process for deactivating access privileges who are a. leaving the organisation b. withdrawal / de-escalation of access privileges 2. What types of access privileges are deactivated - physical premises, IT systems, applications and other resources	Active Directory walkthrough	-

SN	Circular Item	Questions	Details of the Substantiating Artefact	Additional Instructions to the inspector
Physical Security				
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.	NA	Physical visit Physical Access policy	*The Inspector shall* *1. check whether the visitors and outsourced staff are accompanied by authorised employees when visiting critical systems or sensitive areas.* *2. Check if records of visits with In and Out times shall be properly maintained*
23	Physical access to the critical systems should be revoked immediately if the same is no longer required.	NA	Physical visit Physical Access policy	
24	Stock Brokers / Depository Participants should ensure that the perimeter of the critical equipments 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.	NA	Physical visit Physical Access policy	
Network Security Management				
25	Stock Brokers / 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 Stock Brokers / Depository Participants' premises with proper access controls.	Are there separate baseline standards established for OS, DBs, NW devices, etc.	Baseline standards /Hardening Documents	*The Inspector* *1. Shall check whether the baseline standards are properly documented.* *2. Can view the current configurations of systems selected on a sample basis and verify it against the baseline standards* *3. Can leverage the availability of any security scanning tool deployed on the entity's network, to check for*

SN	Circular Item	Questions	Details of the Substantiating Artefact	Additional Instructions to the inspector
				compliance with hardening guidelines.
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.		1. List of all the algorithmic trading systems used. 2. Access Control for these systems 3. Network Segmentation 4. System Hardening 5. Change Management	

SN	Circular Item	Questions	Details of the Substantiating Artefact	Additional Instructions to the inspector
27	Stock Brokers / 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.	If the following tools or any other tools are established and the way it is implemented - a) Firewalls *[mandatory]** b) IPS *[dedicated IPS is mandatory]** - whether implementation is in the form of dedicated NGIPS or HIPS or both c) Proxy d) Network Monitoring tool e) Firewall Analyzers *mandatory because they are mentioned in the circular	Work Order/ Purchase Order	*The inspector may review the blocking rules on firewall by viewing the entity's firewall management console.*
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.	Check whether antivirus or any other endpoint security solution is installed on all the endpoints and servers	Endpoint security Solution Dashboard	*The Inspector may* 1. *review the Endpoint security solution dashboard.* 2. *Ask the entity to show the proof of installation of endpoint security solution on endpoints.*

SN	Circular Item	Questions	Details of the Substantiating Artefact	Additional Instructions to the inspector
Security of Data				
29	Critical data must be identified and encrypted in motion and at rest by using strong encryption methods.	1. What are the data nodes where encryption is required E.g. databases, enterprise storage, data backup, communication channels, etc.? 2. Is encryption applied at file level, disk level or on database. 3. Check whether the same is verified by the auditor and reflected in the report	1. Encryption certificates, validation from Auditor	*The inspector shall* *1. Verify that data backup is encrypted during storage and transmission* *2. Check whether SSL/TLS is used on web traffic* *3. Check whether email encryption (S/MIME, PGP, etc.) is used* *4. Verify the validity of encryption certificates and are regularly updated.*
30	Stock Brokers / 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.	1. What are the scenarios where data sharing with external parties is required? 2. What is the process of approval and mode of sharing data with external parties. 3. What is the process of enabling/granting admin access, root	1. AD access logs 2. Information Security Policy	*The inspector shall* *1. Review recent access requests, approvals, and the documentation associated with each request.* *2. Access the AD console to review user and group settings.* *3. Review logs and reports generated by the DLP tool to check for incidents of sensitive data movement.*

SN	Circular Item	Questions	Details of the Substantiating Artefact	Additional Instructions to the inspector
		access on user desktops/servers. 4. What are the integrations made with AD. 5. List of Domain controllers(DC) within AD and whether DCs are equipped to have certain alerting mechanism which ensures secure internal and external access. 6. Does the MII use Data Loss Prevention (DLP) tool to monitor and control the movement of sensitive data through email. Is email traffic monitored for suspicious activities or security incidents.		
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	Scope of information Security policy	Information security policy document	1. *The inspector shall verify that the policy includes guidelines on secure usage, data protection, and incident response.*

SN	Circular Item	Questions	Details of the Substantiating Artefact	Additional Instructions to the inspector
				2. *For mobile phones, the inspector can access the MDM system console and review configurations for encryption, remote wipe, and access controls.*
32	Stock Brokers / Depository Participants should allow only authorized data storage devices within their IT infrastructure through appropriate validation processes.	1. What are the type of removable data storage devices (USB, HDD, SSD, magnetic tape, etc.) that are allowed in the organisation's environment? 2. Whether the files in authorized data storage devices are scanned for viruses. 3. In case of exchanges, what is the procedure of allowing USB access to trading server. 4. What are the whitelisted devices? 5. Process of whitelisting the devices and whether the process was followed or not.	1. Information security policy document 2. Approval process communication 3. Whitelisted device list	*The inspector shall* 1. *review Access incident logs and recent cases of unauthorized device usage.* 2. *Verify that each incident was documented, investigated, and resolved according to the incident response procedures.*
Hardening of Hardware and Software				

SN	Circular Item	Questions	Details of the Substantiating Artefact	Additional Instructions to the inspector
33	Stock Brokers / 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.	1. What are the new assets onboarded during the Inspection period? 2. Is hardening carried out for each asset and at what stage of procurement process is it carried out.		*The Inspector can* *1. Access recent port scanning reports from tools like Nmap or Nessus.* *2. Identify open ports on critical systems and verify that unused ports are blocked.* *3. Check for documentation or tickets showing the blocking of unused ports.*
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	What are the ports that are most vulnerable in the organisation's environment.		-
Application Security in Customer Facing Applications				
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 in Annexure C of the Circular.			-
Certification of off-the-shelf products				

SN	Circular Item	Questions	Details of the Substantiating Artefact	Additional Instructions to the inspector
36	Stock Brokers / 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.		STQC Certificate Reports on regression testing, configuration testing	
Patch Management				
37	Stock Brokers / 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.	What is the procedure for patch management? Whether any patch management tool is used. Whether approval is sought for the deployment of patch.	Patch Management Policy	-
38	Stock Brokers / 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.	Whether an impact analysis is carried out before deploying the patches. *[May be checked on a sample basis]*	-	-
Disposal of Systems and Storage Devices				

SN	Circular Item	Questions	Details of the Substantiating Artefact	Additional Instructions to the inspector
39	Stock Brokers / 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	What is the procedure and timeline for disposal of assets - both Physical and Digital Assets	Asset Disposal Policy	-
40	Stock Brokers / Depository Participants should formulate a data-disposal and data-retention policy to identify the value and lifetime of various parcels of data.		Data Disposal and Data Retention Policy with implementation evidences	
Vulnerability Assessment and Penetration Testing (VAPT)				

SN	Circular Item	Questions	Details of the Substantiating Artefact	Additional Instructions to the inspector
41	Stock Brokers / Depository Participants shall carry out periodic Vulnerability Assessment and Penetration Tests(VAPT)which inter-alia include critical assets and infrastructure components like Servers, Networking systems, Security devices, load balancers, other IT systems pertaining to the activities done as Stock Brokers / Depository Participants 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 *[Updated Jun 07, 2022]*	1. What are the timelines of VAPT a. Timelines for first cycle VAPT b. Timelines for second cycle VAPT 2. Summary statistics of reported vulnerabilities -[High, Medium, Low] 3. Timely closure of vulnerabilities	1. VAPT tracker 2. VAPT reports	*The inspector shall* *1. Check the closure of observations on sample basis. The closure shall be verified by accessing the specific IT component a* *2. Check the if any observations from the previous VAPT are repeated in this year's VAPT cycle*

SN	Circular Item	Questions	Details of the Substantiating Artefact	Additional Instructions to the inspector
42	Stock Brokers / Depository Participants shall conduct VAPT at least once in a financial year. All Stock Brokers / Depository Participants are required to engage only CERT-In empanelled organizations for conducting VAPT. The final report on said VAPT shall be submitted to the Stock Exchanges/Depositories after approval from Technology Committee of respective Stock Brokers / Depository Participants, within 1 month of completion of VAPT activity. In addition, Stock Brokers / Depository Participants shall perform vulnerability scanning and conduct penetration testing prior to the commissioning of a new system which is a critical system or part of an existing critical system. *[Updated Jun 07, 2022]*			

SN	Circular Item	Questions	Details of the Substantiating Artefact	Additional Instructions to the inspector
43	In case of vulnerabilities discovered in off-the-shelf products (used for core business) or applications provided by exchange empanelled vendors, Stock Brokers / Depository Participants should report them to the vendors and the exchanges in a timely manner.		Evidences of reporting vulnerabilities by vendors and to the Exchanges	
44	Any gaps/vulnerabilities detected shall be remedied on immediate basis and compliance of closure of findings identified during VAPT shall be submitted to the Stock Exchanges/ Depositories within 3 months post the submission of final VAPT report.		VAPT Closure evidences	
MONITORING AND DETECTION				
45	Stock Brokers / 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.	1. What are the tools and technologies deployed in SOC? 2. What are the conditions for carrying out RCA? 3. How many RCAs have been conducted during the Inspection period and was it in line with the provided conditions? 4. Whether log management policy is established and covers all the devices	1. RCA reports 2. SIEM dashboard 3. Dashboard of any other tool deployed, if required	*The Inspector should check for date of RCA, time of the incident and first alert.*

SN	Circular Item	Questions	Details of the Substantiating Artefact	Additional Instructions to the inspector
		5. Whether endpoint security agents are installed on all critical endpoints.		
46	Further, to ensure high resilience, high availability and timely detection of attacks on systems and networks exposed to the internet, Stock Brokers / 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.	1. Whether all the points with respect to capacity utilization circular are complied or not 2. What is the mechanism for monitoring capacity utilization? 3. What are the rules for which alerts are triggered	1. Capacity Utilisation reports	-
RESPONSE AND RECOVERY				
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.	1. Process carried out on reception of an alert 2. How many alerts are translated into tickets? 3. Number of forensic analysis carried out	1. Cyber Crisis Management Plan (CCMP) 2. Incident Response Procedure	-
48	The response and recovery plan of the Stock Brokers / 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. Stock	What are the RTO and RPO achieved during all the DR drills	1. DR Drill reports	-

SN	Circular Item	Questions	Details of the Substantiating Artefact	Additional Instructions to the inspector
	Brokers / Depository Participants should have the same Recovery Time Objective (RTO) and Recovery Point Objective (RPO) as specified by SEBI for Market Infrastructure Institutions vide SEBI circular CIR/MRD/DMS/17/20 dated June 22, 2012 as amended from time to time			
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	NA	1. CCMP 2. Incident Response Procedure	-
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.	NA	1. CCMP 2. Incidence Response Procedure 3. Quarterly reports on cybersecurity and threats experienced by MIIs	
51	Stock Brokers / Depository Participants should also conduct suitable periodic drills to test the adequacy and effectiveness of the aforementioned response and recovery plan	What is the frequency of DR Drills	DR Drill report	-
SHARING OF INFORMATION				
52	Quarterly reports containing information on cyber-attacksand threats experienced by Stock Brokers / Depository Participants and measures taken to mitigate vulnerabilities, threats and attacks including	NA	1. Communication with SEBI	-

SN	Circular Item	Questions	Details of the Substantiating Artefact	Additional Instructions to the inspector
	information on bugs / vulnerabilities / threats that may be useful for other Stock Brokers / Depository Participants should be submitted to Stock Exchanges / Depositories *Updated on [Oct 15, 2019]*		2. Quarterly reports on cybersecurity and threats experienced by MIIs	
TRAINING				
53	Stock Brokers / Depository Participants should work on building Cyber Security and basic system hygiene awareness of staff (with a focus on staff from non-technical disciplines).	1. Number of training programs conducted during the inspection period. 2. Details of training program and number of participants that took the training	Training Attendance sheet	-
54	Stock Brokers / 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.	3. Periodic Cyber Security training should be kept mandatory for the employees.		

SN	Circular Item	Questions	Details of the Substantiating Artefact	Additional Instructions to the inspector
55	The training program should be reviewed and updated to ensure that the contents of the program remain current and relevant.	Whether the updates to the training program was approved by the competent Authority	1. Minutes of Meeting where the agenda was discussed 2. Communication for Approval	-
Systems managed by vendors				
56	Where the systems (IBT, Back office and other Customer facing applications, IT infrastructure, etc.) of a Stock Brokers / Depository Participants are managed by vendors and the Stock Brokers / Depository Participants may not be able to implement some of the aforementioned guidelines directly, the Stock Brokers / 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				
57	Where applications are offered to customers over the internet by MIIs (Market Infrastructure Institutions), for eg.: NSE's NOW, BSE's BEST etc., the responsibility of ensuring Cyber Resilience on those applications reside with the MIIs and not with the Stock Broker/ Depository Participant. The Stock Broker/ Depository Participant is exempted from applying the aforementioned guidelines to such systems offered by MIIs such as NOW, BEST, etc			

SN	Circular Item	Questions	Details of the Substantiating Artefact	Additional Instructions to the inspector
PERIODIC AUDIT				
58	The Terms of Reference for the System Audit of Stock Brokers specified vide circular no. CIR/MRD/DMS/34/2013 dated November 06, 2013,shall accordingly stand modified to include audit of implementation of the aforementioned areas. The Depository Participants and Type I Stock Brokers (as defined in CIR/MRD/DMS/34/2013 dated November 06, 2013) shall arrange to have their systems audited on an annual basis by a CERT-IN empanelled auditor or an independent CISA/CISM qualified auditor to check compliance with the above areas and shall submit the report to Stock Exchanges / Depositories along with the comments of the Board/ Partners / Proprietor of Stock Broker/ Depository Participant within three months of the end of the financial year.	NA	Terms of Reference of System Audit	*NA*

***

D JAYASHRI

Digitally signed by D JAYASHRI
Date: 2025.11.21 16:22:40 +05'30'