Stock Holding Corporation of India Limited
(StockHolding)

RFP Reference Number: IT-11/2023-24

Date: 22.Feb.2024

GEM Reference No. - GEM/2024/B/4674569

REQUEST FOR PROPOSAL FOR APPOINTMENT OF AUDITOR FOR 2 YEARS FOR CONDUCTING INFORMATION SECURITY AND CYBER SECURITY AUDIT

DISCLAIMER

The information contained in this Request for Proposal (RFP) document or information provided subsequently to bidder(s) or applicants whether verbally or in documentary form by or on behalf of Stock Holding Corporation of India Limited *(StockHolding)*, is provided to the bidder(s) on the terms and conditions set out in this RFP document and all other terms and conditions subject to which such information is provided.

This RFP document is not an agreement and is not an offer or invitation by *StockHolding* to any parties other than the applicants who are qualified to submit the bids ("bidders"). The purpose of this RFP is to provide the bidder(s) with information to assist the formulation of their proposals. This RFP does not claim to contain all the information each bidder may require. Each bidder should conduct its own investigations and analysis and should check the accuracy, reliability and completeness of the information in this RFP and where necessary obtain independent advice. *StockHolding* makes no representation or warranty and shall incur no liability under any law, statute, rules or regulations as to the accuracy, reliability or completeness of this RFP. *StockHolding* may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFP.

RFP Document Details

Name of Organisation	Stock Holding Corporation of India Limited
RFP Reference No.	IT-11/2023-24
Requirement	Appointment of auditor for conducting Information Security & Cyber Security Audits for a period of 2 years
Interest free Earnest Money Deposit (EMD) [*]	Rs.1,00,000/- (Indian Rupees One Lakh Only) by way of RTGS/NEFT to be paid to Stock Holding Corporation of India Limited as Earnest Money Deposit should be submitted separately before submission of online bids by way of RTGS/NEFT on/or before bid submission date to StockHolding's Bank Account No.: 004103000033442 Bank: IDBI Bank (Nariman Point Branch) IFSC: IBKL0000004. Please share the UTR details to us on below mentioned email address.
Date of issue of RFP document	22-Feb-2024
Pre-bid online meeting	28-Feb-2024 11:00 AM For participation in pre-bid meeting, please send mail for online meeting link to PRIT@stockholding.com before 27-Feb-2024 05:00 PM
Email Address	PRIT@stockholding.com
Date and Time of submission of online bid	06-Mar-2024 05:00 PM
Date of Opening Bid	06-Mar-2024 05:30 PM
This bid document is not transferable	

[*] - Bidders registered under Micro, Small and Medium Enterprises (MSME) for specific trade are exempted from EMD. Bidders shall upload the scanned copy of necessary documents as part of eligibility criteria documents.

Table of Contents

Overview – About Stock Holding Corporation of India Limited

StockHolding, a subsidiary of IFCI Limited was promoted by the public financial institutions and incorporated as a public limited company on July 28, 1986. StockHolding is a Government Organization, being a subsidiary of IFCI. StockHolding, one of the largest Depository Participants (DP) and also largest premier Custodian in terms of assets under custody, provides post trading and custodial services to institutional investors, mutual funds, banks, insurance companies, etc. StockHolding acts as a Central Record Keeping Agency (CRA) for collection of stamp duty in 21 States and Union Territories on pan India basis. StockHolding is one of the largest Professional Clearing Members of the country.

In Retail segment besides DP services, StockHolding offers stock broking services through its wholly owned subsidiary SHCIL Services Ltd. (SSL). StockHolding is also into distribution of various investment and retirement solutions viz. Fixed Deposits, Bonds & NCDs of reputed institutes and corporates, Mutual Fund Schemes, Initial Public Offers (IPOs) and National Pension System (NPS). RBI has designated StockHolding as one of the Agency Banks to distribute GoI Bonds in dematerialized form. StockHolding also offers the Government of India Sovereign Gold Bonds. StockHolding is a corporate agent registered with IRDAI for distribution of insurance (Life, Health & General) products.

StockHolding has its registered office at Mumbai, main operations office at Navi Mumbai and operates through its over 200 retail branches all over India.

Submission of Proposal:

StockHolding invites e-tender through GeM Portal from competent & reputed authorized bidders to participate in the competent bidding for “Appointment of Auditor for Conducting Information Security and Cyber Security Audit”.

Submission of Bids:

The online bids will have to be submitted within the time specified on website https://gem.gov.in/ the following manner:-

1. Technical Bid (.pdf files)
2. Commercial Bid (.pdf files)

Objective of the RFP

Considering the nature of business and the industry in which StockHolding operates i.e. Capital Markets industry, there are various audits which have to be complied with from time to time. Some are regulatory requirements and some are client requirements. Apart from the regulatory needs, StockHolding is also planning to take an initiative for making Stockholding websites, systems and applications secure and vulnerabilities free. To achieve this initiative, it has been decided that all such audit requirements must go under a bulk security audit through CERT-In empanelled Security auditor at various frequency internals by StockHolding.

As a part of the initiative, StockHolding invites the proposal for security audit of Stockholding websites, systems and applications hosted on StockHolding Data Centre which must be conducted at multiple frequency intervals from time to time.

Due Diligence:

The bidder is expected to examine all instructions, Forms, Terms, Conditions and Specifications in this RFP. Bids shall be deemed to have been made after careful study and examination of this RFP with full understanding of its Implications. The Bid should be precise, complete with all details required as per this RFP document. Failure to furnish all information required by this RFP or submission of Bid not as per RFP requirements will be at the bidder's risk and may result in rejection of the bid and the decision of *StockHolding* in this regard will be final and conclusive and binding.

Cost of Bidding:

The bidder shall bear all costs associated with preparation & submission of its bid and *StockHolding* will in no case be held responsible or liable for these costs, regardless of conduct or outcome of the bidding process.

Clarifications regarding RFP Document:

- Before bidding, the bidders are requested to carefully examine the RFP Document and the Terms and Conditions specified therein, and if there appears to be any ambiguity, contradictions, gap(s) and/or discrepancy in the RFP Document, they should forthwith refer the matter to *StockHolding* for necessary clarifications.
- *StockHolding* shall not be responsible for any external agency delays.
- *StockHolding* reserves the sole right for carrying out any amendments / modifications / changes in the bidding process including any addendum to this entire RFP
- At any time before the deadline for submission of bids / offers, *StockHolding* may, for any reason whatsoever, whether at its own initiative or in response to a clarification requested by bidders, modify this RFP Document.
- It may be noted that notice regarding corrigendum/addendums/amendments/response to bidders' queries, etc., will be published on StockHolding's website only. Prospective bidders shall regularly visit StockHolding's same website for any changes/development in relation to this RFP.
- *StockHolding* reserves the rights to extend the deadline for the submission of bids, if required. However, no request from the bidders for extending the deadline for submission of bids, shall be binding on *StockHolding*.
- StockHolding reserves the right to reject any or all the responses to RFPs / Bids received in response to this RFP at any stage without assigning any reason whatsoever and without being liable for any loss/injury that Bidder might suffer due to such reason. The decision

of StockHolding shall be final, conclusive and binding on all the parties directly or indirectly connected with the bidding process.

Requirement details with Terms & Conditions:

1. Eligibility Criteria

Only those Bidders who fulfil the following criteria are eligible to respond to the RFP. Document/s in support of all eligibility criteria are required to be submitted along with the Technical Bid. Offers received from the bidders who do not fulfil any of the following eligibility criteria are liable to be rejected.

Criteria (Documents to be submitted online along with Technical Bid)-
Table A:

SN.	Criteria	Documents to be submitted by Bidder
1	The bidder should be registered company /Corporate/ partnership firm, registered under Companies Act 2013 (erstwhile Companies Act 1956), Indian Partnership Act, operational in India since last 7 years.	Certified true copy of Certificate of Incorporation issued by Registrar of Companies and of the Memorandum and Articles of Association / Regd. Partnership Deed are required to be submitted. GST registration number, Income Tax registration/ PAN number
2	The bidder should have an annual turnover of at least Rs. 2 Crores per annum for last three financial years (2010-21, 2021-22 and 2022-23). It should be of individual company and not of Group of Companies	Copy of the audited Balance Sheet and/or Certificate of the Chartered Accountant for preceding three years.
3	The bidder should have positive profit for last 3 financial years	Copy of the audited Balance Sheet and/or Certificate of the Chartered Accountant specifying net profits.
4	Audit Firm should be based within MMRDA region	Registered office Address Proof (Self certified Copy)
5	The Bidder should have completed satisfactorily below audits/assessment for at least 03 (three) different companies each in India during last 05 years i.e. 2018-19, 2019-20, 2020-21, 2021-22 & 2022-23. 1. IT Audit 2. SOC 2 Audit 3. Red Team Assessment	Copies of at least 3 such 'LOI/PO/Work Order/Completion Certificate' received from the client must be provided.
6	The bidder should be empanelled with CERT-IN for last 5 years from RFP date	Certificate of Empanelment with CERT-IN for last 5 years from RFP date
7	For SOC 2 Audit: Bidder should be registered with the Institute of Chartered Accountants of India (ICAI)	Valid Certificate for ICAI membership

8	The bidder should have on payroll – 1. For IT Audit : at least 5 Auditors who are CISA/CISSP qualified or equivalent; 2. For SOC-2 Audit : at least 5 Auditors having ICAI / AICPA membership; 3. For Red Team Assessment : at least 05 Offensive Security Certified Professional (OSCP) from offensive-security / Certified Ethical Hacker (CEH) from EC-Council / Licensed Penetration Tester (LPT) from EC-Council / GPEN: GIAC Penetration Tester from SANS / GWAPT: GIAC Web Application Penetration Tester from SANS / any other Red Team or Penetration Testing related certification;	All Relevant certificates/documents supporting basis laid out in pre-qualification criteria.
9	The bidder should not be providing IT related service(s) to StockHolding or its subsidiaries currently and should not have conducted IT Audit consecutively during the last 3 years (From Date of Issue of this RFP) for StockHolding.	Bidder to provide a Self-Declaration on the company letter head.
10	1. For IT Audit: The proposed Lead Auditor should be Graduate with CISA/CISSP certification with minimum 05 (five) years' experience in IT Audit related activities. 2. For SOC 2 Audit: Graduate with ICAI / AICPA membership with minimum 05 (five) years' experience in SOC Audit related activities. 3. For Red Team Assessment: Relevant certifications with minimum 05 (five) years' experience in assessment related activities.	Resume of proposed resource including list of IT /SOC Audit projects/Red Team Assessment handled during last 05 years in India

2. Contract Period:

a. Contract will be for the period of 02 years with 01 year extension. However, Purchase Order (PO) will be issued annually.

b. StockHolding reserves the right to cancel the Contract during the contract period without assigning any reason whatsoever.

c. Year 2 price will have maximum escalation upto 10% on Year 1 Price.

d. StockHolding may choose to extend the contract period for another 1 year with the maximum escalation upto 10% on Year 2 Price for the selected bidder.

3. **CERT-IN Empanelment**

Considering the contract will be awarded to the winning bidder for a period of 02 years with 01 year extension, the winning bidder needs to ensure that they remain empanelled as CERT-IN Auditor for the complete duration of the contract. The winning bidder has to submit the renewal empanelment from CERT-IN incase the contract is renewed in between the contract period.

4. **Validity of bid**

Bid should be valid for a minimum period of **90 days** in the event of delay in issuance of Purchase Order (PO) by StockHolding.

5. **Location for delivery and support**

Stock Holding Corporation of India Limited, SHCIL House, Plot No. P-51, TTC Industrial Area, MIDC, Mahape, Navi-Mumbai – 400 710. However, selected auditor may visit other Stockholding offices in Mumbai (if required).

6. **Payment Terms**

100% payment on submission of invoice against completion of each audit along with Final Audit Report (duly signed by Auditor/Audit agency)

7. **Taxes & levies**

Applicable taxes payable at actual as per prevailing rate of taxes as per Government notification. Applicable deduction if any may / will be recovered (deducted) from the payment(s)

8. **Refund of Earnest Money Deposit (EMD)**

(a) EMD will be refunded through NEFT to the successful bidder on providing an acceptance confirmation against the PO issued by StockHolding.

(b) In case of unsuccessful bidders, the EMD will be refunded to them through NEFT within 15 days.

9. **Scope of Work**

9.1. **Brief overview of StockHolding's IT Infrastructure–**

Considering the nature of work within which StockHolding operates, StockHolding uses various applications which are built in house and some are third party applications. Some of the applications mentioned are:

1. Custody – PTS

2. Depository Participant Module
3. Corporate Accounts
4. CSGL Accounts
5. API Gateway
6. Professional Clearing Member Module
7. E-Sign services from UIDAI for Account Opening

All the above applications are hosted in StockHolding Data Centre situated in Mahape, Navi Mumbai with DR site situated in Bengaluru.

StockHolding has more than 210+ branches situated all over India with Regional Office setups as well. Various Branch and Regional Offices are connected over MPLS VPN with Head Office.

9.2. Audit Methodology

The IS audit work will include manual procedures, computer assisted procedures and fully automated procedures, depending on the chosen audit approach.

9.3. Phases of Audits

Considering there are different audits involved at different frequency (time intervals), however the Audit phases will remain common across various Audits namely: -

PHASE –I:

1. Submit a draft report and executive summary of the Audit exercise
2. Submit a draft report and executive summary for IT Infrastructure and support services.
3. Give recommendations to mitigate the gaps suggested in the draft report wherever possible

PHASE – II:

1. Conduct a re-validation audit after the gaps are plugged wherever required
2. Submit a final report and executive summary after conducting a re-validation audit.
3. Submit compliance certificate on completion of the above-mentioned tasks.

9.4. Audit Activities and Frequency

Below is the list of regulatory and client audit requirements along with the frequency at which the Cyber Security Audits have to be conducted

Table A:

AUDIT #	Audit Name	Frequency	Area	Date of Audit to be Completed	Circular Reference with Date
1	Cyber security/System audit report	Annual	Depository Participant (NSDL and CDSL)	30th June	SEBI Circular no: SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018 NSDL Circular No.: NSDL/POLICY/2020/0071 dated May 19, 2020
2	Vulnerability Assessment and Penetration Testing report	Annual	Depository Participant (NSDL and CDSL)	Initial Report: VAPT be carried out and completed during the period 'September to November' of every financial year and the report on the said VAPT be submitted to Depositories within one month from the date of completion of VAPT after approval by Tech committee. Confirmatory/Closure Report: All vulnerabilities to be addressed and final report be submitted within 3 months of submission of Initial VAPT Report.	SEBI/HO/MIRSD/TPD/P/CIR/2022/80 June 7, 2022 NSDL Circular No. NSDL/POLICY/2022/166 dated November 28, 2022
3	E-sign ESP audit for UIDAI	Annual	Account Opening	31st July	ASP On-boarding Guidelines Version 1.3, 26th Dec 2018 – Controller of Certifying Authorities
4	PCM System Audit Clearing Corporation's MCX,ICCL and NSCCL	Annual	Professional Clearing Member	30th June	Circulars: MCX Circular No. MCX/MCXCCL/353/2023 & MCXCCL Circular No. MCXCCL/TECH/141/2023 dated May 31, 2023.
5	CSGL System Audit for RBI	Quarterly	Constituent Subsidiary General Ledger (CSGL) Account	30 April, 30 July, 30 November, 30 January (within one month of every quarter end)	RBI operational guidelines dated Sep 22, 2021
6	OWASP API Audit	As and when	API Audit	As and when needed in case a new API is developed	

		required			
7	Custody System Audit	Annual	Custody	Before April 15 for the previous FY	The Insurance clients require an audit certificate from our Internal Auditors in which one of the confirmation is relating to System audit of Custody. Hence Annual System Audit is required from Auditor
8	Cyber Security and Cyber Resilience framework for Mutual Funds /Asset Management Companies	Half Yearly	Custody	April to September - to be completed within 90 days by 31st Dec October to March - to be completed within 90 days by 30 June	SEBI Circular - SEBI/HO/IMD/DF2/CIR/P/2019/12 dated January 10, 2019 and Circular Dated June 9, 2022
9	ISMS Audit	Quarterly	IT-Infra	Within one month of every quarter end	Internal
10	SOC 2 Type 2 Gap assessment and then Type 2 Audit Attestation	Annual	IT-Infra	Report must be submitted by 31st March of the current year, covering the period from 01st February of the previous year to 31st January of the current year.	Internal
11	Red Team Assessment: External Exercise & Internal Exercise	Annual	IT-Infra	Within April to June for every year	-

Table B: Relevant Circulars for the Audits mentioned in Table A

Audit #	Annexure Number
1	Annexure : 11
2	Annexure : 12
3	Annexure : 13
4	Annexure : 14
5	Annexure : 15
6	-
7	-
8	Annexure : 16
9	-

10	-
11	Annexure : 17

The annexures also contain audit report formats where auditor attestation are required for final submission to the concerned stakeholders.

9.5. Key Areas to be covered in every Audit

a. Below is the brief scope of activities to be conducted for every application audit and applicable for Audit # 1,4,5,7 and 8 as mentioned in the above table.

Table B:

Areas	**Activities**
Infrastructure and IT service	1) IT Governance Policies and Procedures 2) System Administration Procedures 3) Operating System Controls (vulnerability assessment) 4) Vulnerability Assessment of Network Devices i.e. Router, Firewall, Switches 5) Change Management 6) Back-up and Recovery Procedures 7) Incident Response Management from network and servers perspective
Disaster Recovery (DR)	1) DR Policies and Procedures 2) DR Implementation 3) DR Testing 4) System and device configurations for redundancy and availability
Application Security Control Review	1) User Management 2) Security Entitlements / Access Controls 3) Change Management 4) Audit trials/log monitoring

Note: It is the responsibility of the winning bidder to make sure that the Key Areas of Audit has to match with the relevant circulars as published from time to time.

b. OWASP Top 10 API (Audit # 6): OWASP Top Ten criteria as mentioned below but not limited to –

- Injection Flaws
- Broken Authentication and Session Management
- Sensitive Data Exposure
- XML External Entities (XXE)
- Broken Access Control
- Security Misconfiguration

- Cross-Site Scripting (XSS)
- Insecure Deserialization
- Using Components with Known Vulnerabilities
- Insufficient Logging & Monitoring

c. E-Sign ESP Audit for UIDAI (Audit # 3): As mentioned in Annexure 13

d. Vulnerability Assessment and Penetration Testing (Audit # 2)

I. Vulnerability Scanning:

- Service Highlights
    - Automated Scans performed for faster turn-around cycle.
    - Scan option is available in both authenticated and un-authenticated mode.
    - More information like missing patches, confirmation of certain potential vulnerabilities is possible with authenticated mode.
    - Assurance that basic Vulnerability Management program is in place and basic security level is complied.
- Scope
    - All IP addresses as documented during initiation process. 30 external facing IP's.
- Report Expectations
    - A Network Vulnerability Scan Report containing Executive Summary, Vulnerability Details, Impact, Risk Rating and Solutions in excel as well as in pdf formats.
    - This activity required to be perform on half yearly basis with review of action taken on last year's assessment report.

II. Network Penetration Testing – Internal/External:

- Service Highlights
    - Provides hacker's view of network vulnerabilities in organizational assets.
    - Comprehensive methodology from Information Gathering, Fingerprinting to Vulnerability Detection, Exploitation and Reporting.
    - Tool driven automated scans for discovering breadth of security issues.
    - Expert executes in-depth manual penetration exploit steps.
    - Detailed Solution Repository for different technology platforms.
- Scope
    - All IP addresses as documented during initiation process. 30 external facing IP's.

- Report Expectations
  - A Penetration Testing Report containing Executive Summary, Vulnerability Details with screenshot evidences, Impact, Risk Rating, case-specific Solutions and Good Reads
  - This activity required to be perform on half-yearly basis with confirmatory to be perform 3 months after initial assessment report

III. Software / Tools to be used during the Audit

It is desired that IS Audit is carried out with the help of following software / tools, but not limited to:

- Burp Suite – for Application Security
- Nessus – for Vulnerability Assessment of IT Infrastructure
- DIRbuster
- SQLMap
- Nmap
- XProbe
- Hping2
- Nexpose
- Metasploit
- TCPTraceroute
- Relevant Kali LINUX TOOLS
- Accunetix
- Back Track, etc.

e. ISMS (Audit # 9)

1) Internal Audits:
   a) Conduct an internal audit quarterly. This audit shall essentially cover the effectiveness of ISMS Implementation
2) Pre-Certification Assessment:
   a) Review and ensure audit preparedness of the organization for the ISO 27001 Certification audits by authorized CAs.
   b) Measurement metrics for controls effectiveness and Management Reviews.
3) ISO Certification Audit:
   a) Provide support during certification, re-certification & surveillance audits by CAs in connection with ISO 27001 certification.
4) ISMS Documentation:
   a) Review of existing StockHolding ISMS Manual/Policy & suggest changes wherever applicable.
   b) Review of SOA and all other relevant documents relating to ISMS & suggest changes wherever applicable.
   c) Review the IT and IS Policies and Procedures' documents & suggest changes wherever applicable.
5) Risk Assessment:
   a) Review the Risk Register, Risk Assessment & Treatment Plan, and other related documents and suggest changes, if any.

b) Review the Asset Register & suggest changes wherever applicable.

6) Incident Management and Change Management:

a) Review change request documents on a random basis and suggest improvements wherever appropriate.

b) Critically evaluate the incident management reports on a random basis and suggest improvements wherever appropriate.

c) Evaluate the incident handling procedures, including RCA (Root Cause Analysis), and suggest improvement areas, if any.

d) Vendors can associate in various stages of the implementation process right from the discovery & design phase to the final implementation. Some areas of expertise are:

- Data Loss Prevention (DLP)
- Document Rights Management
- Application Security Products
- Crisis Management
- System Hardening
- Business Continuity Planning (BCP) & Disaster Recovery (DR)
- Incident Handling, Response, Recovery, and Corrective / Preventive measures
- Application Access Controls - User management, Configuration review, Role-based access, SOD conflicts, etc.
- Database controls
    - Business process and functional controls with best practices
- Migration of Data & Applications

e) **Implementation service related to Information Technology Vendor also provides value to IT services and helps to choose and implement solutions that are not only efficient but also cost-effective. Some such are**

- Optimal Software Development Life Cycle (SDLC)
- Secure Application Development
- Asset management Life Cycle
- Identifying and addressing vendor outsourcing risks
- Data governance
- IT integration
- Product selection advice - software or hardware

f) **Security of new and emerging trends in technology:**

The technology landscape is in a constant state of flux. While new technologies keep emerging, several existing ones become obsolete. It is necessary to keep pace with the developments in technology to enable them to exploit and harness the advantages brought in by these technologies. Some examples of such trends are cloud, virtualization, internet of things, AI, ML, VR, etc.

f. SOC 2 Type 2 Gap assessment and then Type 2 Audit Attestation (Audit # 10)
   1) Evaluate the service organization's controls and processes based on the criteria specified in the AICPA's Trust Services Criteria (TSC).

g. Red Team Assessment (Internal & External) (Audit # 11)

Sr. No.	**Red Teaming Exercise (External- Annual, Internal- Annual)** **Bidders shall perform External & Internal assessment each year.**
1	Conduct External red team exercise for finite period of 15 days and Internal red team exercise for 20 days.
2	1. Red Teaming of Internal Network: The objective of internal red team will be to uncover the vulnerabilities in the StockHolding's internal network (DC Mahape /DR Bengaluru/ branches) and attempt to exploit the identified vulnerabilities to gain access to the StockHolding's critical infrastructure.
3	Various methods (list not exhaustive) to be used for internal red team exercises are suggested below: A. Internal Network Scanning i. Conduct ping sweep scans and identify the reachability of IP segments ii. Identify live IP addresses within the identified IP segments, etc. B. Fingerprinting i. Detecting TCP/UDP services and version details ii. Detecting Operating systems and its version details using active and passive OS fingerprinting techniques. iii. Fingerprinting webserver and HTTP/HTTPS services running on the bank's internal servers, etc. C. Vulnerability Identification i. Attempt to identify weakly configured web applications / web servers / Operating systems/ databases ii. Attempt to identify vulnerabilities in network services, operating systems, and Network devices using combination of advanced vulnerability scanners and manual tests, etc. D. Exploitation and Post Exploitation This activity will include exploitation of vulnerabilities in operating systems, web applications and network services. Post exploitation phase may include attempts to execute following key attacks in a controlled environment as applicable i. Gain access to the underlying operating system / network ii. Exploiting OS misconfigurations and local process vulnerabilities to gain privileged access on target server

	iii. Evaluate the potential for gaining further access in the bank's internal network iv. Extract credentials and password hashes from operating systems memorv, etc.
4	2. Red Teaming of External Network: Objective of this activity is to uncover the vulnerabilities in the StockHolding's external network and attempt to exploit the identified vulnerabilities to gain access to the bank's external critical infrastructure.
5	Various methods (list not exhaustive) to be used for internal red team exercises are suggested below: A. Intelligence Gathering i. Passive Reconnaissance: Extracting subdomains, hosts using OSINT tools such as recon-ng, the Harvester, twofi etc. ii. StockHolding Internet Presence: Identify IP ranges and vulnerabilities in publicly available server/network devices, etc. B. Active Reconnaissance- i. Gathering host/ identity/ network/ organization information ii. Phishing for information, etc. C. Scanning i. Conduct ping sweep scans and confirm the reachability of the bank's external IP addresses ii. Launch stealth/noisy scans on the bank's external IP addresses and identify open TCP/UDP ports, etc. D. Fingerprinting i. Detecting TCP/UDP services and version details ii. Detecting Operating systems and its version details using active and passive OS fingerprinting techniques. iii. Fingerprinting webserver and HTTP/HTTPS services running on the bank's public facing servers, etc. E. Vulnerability Identification i. Identify weakly configured web applications / web servers ii. Script scan to identify potential vulnerabilities iii. Identify vulnerabilities in external facing web applications with Black Box approach

	iv. Identify potential exploits available for identified vulnerabilities using well known exploitation framework modules, etc. F. Exploitation and Exfiltration i. Attempt to identify if a device, web application is vulnerable to a default credential attack ii. Attempt to exploit of vulnerabilities in network/web services using exploitation frameworks and publicly available exploit codes as applicable. iii. Checking for establishing Command & Control communication, etc.
6	The popular framework for Red Teaming may be referred for the same (mapped with MITRE ATT&CK Framework)- A. Reconnaissance B. Initial Access C. Lateral Movement D. Exploitation
7	Location: DC Mahape, DR Bengaluru, Any Mumbai Branches (2 nos.)
8	The bidder shall provide detailed plan of action for red team exercise and upon StockHolding's approval conduct assessment. The assessment working/analysis sheet should provide evidence for each test case. However, bidder shall seek confirmation prior to any exploitation on production environment.
9	Time required for planning, reporting shall not be included in days allotted for exercise.

9.6. Adherence to Regulatory Circulars on Cyber Security for Capital Markets Intermediaries

Although all the relevant circulars from regulatory are listed above in table A, the Auditor has to make sure that they are aware and audit the respective application area in accordance to the latest circulars.

Auditor to ensure, whether the company has complied with the IT framework guideline as mentioned in the Master Directions of the respective circulars

9.7. Deliverables

For IT Audit:

Individual report should be provided for various IT Systems location-wise and consolidated. The Report should consist of an executive summary that expresses business risk and the technical nature of the risk and its seriousness, and a technical report that includes findings and mitigation strategies in full detail. Tools used for VAPT should also mentioned in the report.

The following reports need to be submitted by the Auditor:

a. Submit a draft report and executive summary
b. Submit a draft report and executive summary for IT Infrastructure and support services.
c. Give recommendations to mitigate the gaps suggested in the draft report.
d. Conduct a re-validation audit after the gaps are plugged.
e. Submit a final report and executive summary after conducting a re-validation audit.
f. Submit compliance certificate on completion of the above-mentioned tasks.

For SOC-2 Audit:

a. Annual Audit report starting from February to January current year covering the Data Center and IT Infra and applications. Report must be submitted by March.
b. For SOC 2 - Principles covered are Security, Confidentiality and Availability.
c. For SOC 3 report is a public version of the SOC 2 report, which means it can be freely distributed to anyone, including the general public.
d. Arrange Certified Audit report from certified member of ICAI/CPA.

For Red Team Assessment (Internal & External):

a. Document and report the attack events and timelines as per the checklist (Annexure 17)
b. Discuss the report findings with StockHolding's SOC team and understand the attack attempts detected during the activity in order to help develop mitigation strategies
c. Present the StockHolding Management the activity details & observations
d. Report the observations along with attack and detection details along with recommendations.
e. Confirmation report that observations reported have been closed.

9.8. <u>Timelines of Audit</u>

a. The successful bidder will need to complete the audit within 3 weeks before closing date of respective audit.

10. <u>Service Level Agreement (SLA)</u>

a. The successful bidder will need to complete the audit within 3 weeks for the respective audit. In case of delay, the penalty of Rs. 500 per day will be levied.
b. Time taking by StockHolding for fixing the Vulnerabilities will not be considered in the time limit.
c. The overall penalty cap for each work order shall be capped at 10% of PO value.

11. <u>Bids Preparation and Submission Details</u>

1. Technical Bid (Annexure - 2)

a. The required documents for Eligibility Criteria must be submitted (uploaded) online on GeM portal. Eligibility Criteria documents should be complete in all respects and contain all information asked for in this RFP document
b. Bidder should also submit scan copy of cancelled cheque.
c. There should not be any hidden / conditional costs in the bids and in the event of their presence in the bid, the bid is liable to be rejected.
d. No indications pertaining to price or commercial terms should be made in the Eligibility Criteria submission. If any price indications are made, then the bids is liable to be rejected.
e. No open ended / conditional bid shall be entertained and is liable for rejected.

2. Commercial (Indicative Price) Bid

a. The bidder will submit Commercial Bid must be submitted (uploaded) online on GeM portal. (refer **Annexure - 3)**
b. The bidders are expected to quote per Man Day cost for Adhoc Audit requests. The scope of Adhoc Audits will be decided mutually between StockHolding and the bidder.
c. L1 price will be based on Table A as mentioned in Annexure – 3

3. Submission of Bids

a. The required documents for Eligibility Criteria and Commercial Bid must be submitted (uploaded) online on GeM portal. Both the documents should be complete in all respects and contain all information asked for in this RFP document
b. If Interest Free Earnest Money Deposit (EMD) is not submitted by bidder / received by *StockHolding* in the form of NEFT prior to the last date of submission of bids as mentioned in this RFP, bidder will not be eligible to participate in this RFP.
c. The offer should be valid for a period of at least 90 days from the date of submission of bid.
d. The bidder shall fulfil all statutory requirements as described by the law and Government notices. The bidder shall be solely responsible for any failure to fulfil the statutory obligations and shall indemnify *StockHolding* against all such liabilities, which are likely to arise out of the bidder's failure to fulfil such statutory obligations
e. The bidder shall be solely responsible for any injury, damage, accident to the workman employed by the bidder for any loss or damage to the equipment/property in the areas of work as a result of negligence/carelessness of its deployed resources.
f. No request for any further extension of the above deadline shall be entertained. Delayed and/or incomplete bid shall not be considered.
g. All employees engaged by The bidder shall be comprehensively insured for accidents and injuries by the bidder at his/her/their cost
h. The Interest free EMD should be deposited in StockHolding's bank account on or before the bid submission date.

i. Bidders are advised to submit their Eligibility Criteria and Commercial bids well before last date of submission.

12. Evaluation of Bids

StockHolding will evaluate the bid submitted by the bidders under this RFP. It is *StockHolding'*s discretion to decide at the relevant point of time. The eligibility bid submitted by the Bidder will be evaluated against the Eligibility criteria set forth in the RFP. The Bidder needs to comply with all the eligibility criteria mentioned in the RFP to be evaluated for evaluation. Noncompliance to any of the mentioned criteria would result in outright rejection of the bidder's proposal. The decision of *StockHolding* would be final and binding on all the bidders to this document.

StockHolding may accept or reject an offer without assigning any reason whatsoever. The bidder is required to comply with the requirement mentioned in the RFP. Non-compliance to this may lead to disqualification of a bidder, which would be at the discretion of *StockHolding*.

a Please note that all the information desired needs to be provided. Incomplete information may lead to non-consideration of the proposal.

b The information provided by the bidders in response to this RFQ document will become the property of StockHolding.

Evaluation Process

Stage 1 - The 'Eligibility Criteria bid document' will be evaluated and only those bidders who qualify the requirements will be eligible for 'Technical bid'.

Stage 2 - For only those bidders who have been found eligible in Stage 1, "Technical Bids" will be evaluated, and a technical score would be arrived as per evaluation steps detailed in the RFP.

Stage 3 - Bidders, who have been found eligible in Stage 2, shall be selected for "Commercial Bid" evaluation.

Eligibility Criteria Evaluation (Stage 1)

The bidder meeting the "Eligibility Criteria" will be considered for further evaluation. Any credential/supporting detail mentioned in "Eligibility Criteria" and not accompanied by relevant proof documents will not be considered for evaluation. All credential letters should be appropriately bound, labelled and segregated in the respective areas. There is no restriction on the number of credentials a bidder can provide.

Technical Bid Evaluation (Stage 2)

The Technical bids of only those bidders shall be evaluated who have satisfied the "Eligibility Criteria" bid. StockHolding may seek clarifications from any or each bidder as a part of technical evaluation. All clarifications received by within stipulated time shall be considered for evaluation. In case a clarification is not received within the stipulated time, the respective technical parameter would be treated as non-compliant and decision to qualify the bidder shall be accordingly taken by the StockHolding.

The proposal submitted by the bidders shall, therefore, be evaluated on the following criteria:

Sl. No	Parameter	Method of Allocating Marks	Minimum Qualifying marks	Maximum Score	Documents Required
	A. Bidder's Experience & Resource Strength				
1	Bidder must be in Core business of providing IT Audit, SOC-2 Audit and Red Team Assessment services for a period during last 05 years as on RFP date.	a) 5 years = 12 Marks b) >5 and < 10 years; = 15 Marks c) =>10 years = 20 Marks	12	20	PO to be shared with StockHolding
2	The bidder should have on payroll 1. For IT Audit : at least 5 Auditors who are CISA/CISSP qualified or equivalent; 2. For SOC-2 Audit : at least 5 Auditors having ICAI / AICPA membership; 3. For Red Team Assessment : at least 05 Offensive Security Certified Professional (OSCP) from offensive-security / Certified Ethical Hacker (CEH) from EC-Council / Licensed Penetration Tester (LPT) from EC-Council / GPEN: GIAC Penetration Tester from SANS / GWAPT: GIAC Web Application Penetration Tester from SANS / any other Red Team or Penetration Testing related certification;	a) Minimum 5 in each category = 12 Marks b) More than 5 nos. to 10 nos. in each category = 15 Marks c) More than 10 nos. in each category = 20 Marks	12	20	Letter from HR along with Resume of resources with valid certifications
3	The Bidder should have completed satisfactorily below audits/assessment for at least 03 (three) different companies each in India during past 05 years i.e. 2018-19, 2019-20, 2020-21, 2021-22 & 2022-23. 1. IT Audit 2. SOC 2 Audit 3. Red Team Assessment	Projects for each audit/assessment - a) Minimum 3 Projects = 12 Marks b) >3 and < 5 Projects; = 15 Marks c) =>5 Projects = 20 Marks	12	20	PO to be shared with StockHolding

	B. Project Approach, Presentation & Team Evaluation				
4	Audit Plan approach and proposed methodology with Presentation	The overall approach adopted by the responding Audit firm to complete the Audit to meet the timelines.	21	30	Proposed Approach & methodology document along with presentation
5	Quality & Experience of Lead Auditor proposed each for the below projects – 1. IT Audit 2. SOC 2 Audit 3. Red Team Assessment	Qualification and relevant project experience	7	10	Proposed Lead Auditors resume and StockHolding internal evaluation
	Total Marks		**64**	**100**	

<u>Commercial Bid Evaluation (Stage 3)</u>

Selection of bidders for commercial evaluation stage -

1. Only bidders who achieve the specified minimum qualifying marks across each evaluation parameters/credentials for Technical Bid Evaluation, and
2. Cumulative score of 64 marks in the Technical evaluation

L1 bidder will be selected based on the lowest quote submitted. In case of tie between commercials quotes submitted, the bidder with highest technical marks will be shortlisted as L1.

Further, StockHolding reserves the right to negotiate with L1 bidder and based on the negotiation price submitted, order will be placed to the selected bidder.

13. Force Majeure:

Neither the StockHolding nor the Bidder shall be responsible for any failure to fulfil any term or condition of the CONTRACT if and to the extent that fulfilment has been delayed or temporarily prevented by a Force Majeure occurrence, defined as "Force Majeure". For purposes of this clause, “Force Majeure” mean an event beyond the control of the Parties and which prevents a Party from complying with any of its obligations under this Contract, including but not limited to: acts of God not confined to the premises of the Party claiming the Force Majeure, flood, drought, lightning or fire, earthquakes, strike, lock-outs beyond its control, labour disturbance not caused at the instance of the Party claiming Force Majeure, acts of government or other competent authority, war, terrorist activities, military operations, riots, epidemics, civil commotions etc.

The Party seeking to rely on Force Majeure shall promptly, within 5 days, notify the other Party of the occurrence of a Force Majeure event as a condition precedent to the availability of this defence with particulars detailed in writing to the other Party and shall demonstrate that it has taken and is taking all reasonable measures to mitigate the events of Force Majeure. And, all Parties will endeavour to agree on an alternate mode of performance in order to ensure the continuity of service and implementation of the obligations of a party under the Contract and to minimize any adverse consequences of Force Majeure. Each PARTY shall bear its own cost in relation to the force majeure occurrence.

However, any failure or lapse on the part of the Bidder to mitigate the damage that may be caused due to the above-mentioned events or the failure to provide adequate disaster management/recovery or any failure in setting up a contingency mechanism would not constitute force Majeure, as set out above.

If the duration of delay exceeds ninety (90) consecutive or one hundred eighty (180) cumulative days, StockHolding and the Bidder shall hold consultations with each other in an endeavour to find a solution to the problem. Notwithstanding above, the decision of the StockHolding, shall be final and binding on the bidder.

14. Dispute Resolution

In the event of any dispute arising out of or in connection with this purchase order, the parties shall use their best endeavour to resolve the same amicably AND if the dispute could not be settled amicably, the matter shall be settled in the court under Mumbai jurisdiction only. The final payment will be released only after the bidder complies with above-mentioned clause

15. Right to alter RFP

a. StockHolding reserves the right to alter the RFP terms and conditions at any time before submission of the bids.

b. StockHolding reserves the right to cancel the RFP/contract.

c. StockHolding reserves the right to modify, amend, alter and/or cancel the entire RFP at any stage without assigning any reason whatsoever.
StockHolding's decision in this regard will be final and binding on all bidders.

16. Integrity Pact

The bidder will have to enter into an Integrity Pact with StockHolding Corporation of India Limited. The format (text) for the Integrity Pact is provided as **Annexure – 6**. The bidder will have to submit a signed and stamped copy of the Integrity Pact by the authorized signatory.

17. Non-Disclosure Agreement (NDA)

The successful bidder will sign a Non-Disclosure Agreement (NDA) with Stock Holding Corporation of India Limited. The draft text of the NDA is enclosed in Annexure – 9.

18. **Indemnify**

The bidder should hereby indemnify, protect and save *StockHolding* against all claims, losses, costs, damages, expenses, action suits and other proceedings, resulting from infringement of any patent, trademarks, copyrights etc. or such other statutory infringements in respect of all the equipment offered by the bidder. Any publicity by bidder in which name of *StockHolding* is used should be done only with the explicit permission of *StockHolding*.

19. **Order Cancellation**

StockHolding reserves the right to cancel the order by giving a notice of 30 days in the event of the L1 Bidder failing to deliver services as specified by Stockholding as per the Service Level Agreements. Stockholding reserves full right and authority to cancel such order and will also be entitled to claim liquidated damages for the same in addition to and without prejudice to all other rights and remedies that may be available to StockHolding. In case of serious discrepancy in services provided by L1 Bidder, Stockholding may cancel the entire purchase order.

StockHolding reserves the right to award order to L2 Bidder with same terms and conditions in event of cancellation of order to L1 Bidder.

Incase the L1 Bidder is not able to renew the CERT-IN empanelment for whatever reason or does not share the renewal certificate during the contract period, the contract will be cancelled by StockHolding.

20. **Exclusivity**

StockHolding will choose one (1) successful bidder to provide the required services. Further, No Consortium bids as well as sub-contracting in any form shall be accepted.

21. **Performance Security / Bank Guarantee**

The Successful Bidder needs to deposit a Performance Bank Guarantee within 30 days from the date of acceptance of purchase order, for an amount of 5% (Five percent) of the Annual Purchase Order Value from scheduled commercial banks. PBG format attached as per Annexure-10. This Bank Guarantee shall be valid up to 60 days beyond the completion of the contract period. No payment will be due to the successful bidder based on performance, until the BG verification is pending. Also, for Year 3, BG has to be extended to cover extended contract period years plus a claim period of 3 months.

Failure to comply with the above requirement, or failure to enter into contract within 30 days or within such other extended period, as may be decided by StockHolding, shall constitute sufficient ground, among others, if any, for the annulment of the award of the tender.

In the event the selected bidder is unable to provide the services as mentioned in this RFP, during the engagement period as per the contract for whatever reason, the Performance Bank Guarantee would be invoked by StockHolding.

No Bank Charges/interest shall be payable by StockHolding for issuance of Performance Security / Bank Guarantee.

22. Return of Performance Security / Bank Guarantee

The Performance Bank Guarantee may be discharged/ returned by StockHolding after the completion of the contract and upon being satisfied for the performance of the obligations of selected bidder under the contract.

In the event the bidder is unable to provide the services, during the engagement period as per the contract for whatever reason, the Performance Bank Guarantee would be invoked by StockHolding.

Annexure – 1 - Details of Bidder's Profile

(To be submitted along with technical bid on Company letter head)

Details filled in this form must be accompanied by sufficient documentary evidence, in order to verify the correctness of the information.

Sl. No.	Parameters	Response	
1	Name of the Firm/Company		
2	Year of Incorporation in India		
3	Names of the Partners/Directors		
4	Company PAN no		
5	Company GSTN no. (please mention for all states)		
4	Name and Address of the Principal Banker		
5	Addresses of Firm/Company		
	a) Head Office		
	b) Local Office in Mumbai(if any)		
6	Authorized Contact person		
	a) Name and Designation		
	b) Telephone number		
	c) E-mail ID.		
7	**Financial parameters**		
	Business Results (last two years)	Annual Turnover (Rs. in Crores)	Net Profit (Rs. in Crores)
	2020-21		
	2021-22		
	2022-23		
	(Only Company figures need to be mentioned not to include group/subsidiary Company figures}	(Mention the above Amount in INR only)	
	Details of Reference Customer		
	Customer Name and Contact No.	Brief Details of licenses supplied	PO number and Date(Attached PO with masked price)
	1		
	2		
	3		

N.B. Enclose copies of Audited Balance Sheet along with enclosures

Dated this........ Day of 2024

(Signature)

(In the capacity of)

Duly authorized to sign bid with seal for & on behalf of (Name & Address of the Bidder)

Note:

1. Letter of Authorization shall be issued by either Managing Director having related Power of Attorney issued in his favour or a Director of the Board for submission of Response to RFP/ Tender.
2. All self-certificates shall be duly signed and Stamped by Authorized signatory of the bidder Firm unless specified otherwise.
3. Bidder response should be complete; Yes/No answer is not acceptable…
4. Details of clients and relevant contact details are mandatory. Bidder may take necessary approval of the clients in advance before submission of related information. StockHolding will not make any separate request for submission of such information.

Annexure – 2 - Eligibility Criteria

(Documents to be submitted online along with Technical Bid)

SN.	Criteria	Documents to be submitted by Bidder
1	The bidder should be registered company /Corporate/ partnership firm, registered under Companies Act 2013 (erstwhile Companies Act 1956), Indian Partnership Act, operational in India since last 7 years.	Certified true copy of Certificate of Incorporation issued by Registrar of Companies and of the Memorandum and Articles of Association / Regd. Partnership Deed are required to be submitted. GST registration number, Income Tax registration/ PAN number
2	The bidder should have an annual turnover of at least Rs. 2 Crores per annum for last three financial years (2010-21, 2021-22 and 2022-23). It should be of individual company and not of Group of Companies	Copy of the audited Balance Sheet and/or Certificate of the Chartered Accountant for preceding three years.
3	The bidder should have positive profit for last 3 financial years	Copy of the audited Balance Sheet and/or Certificate of the Chartered Accountant specifying net profits.
4	Audit Firm should be based within MMRDA region	Registered office Address Proof (Self certified Copy)
5	The Bidder should have completed satisfactorily below audits/assessment for at least 03 (three) different companies each in India during last 05 years i.e. 2018-19, 2019-20, 2020-21, 2021-22 & 2022-23. 4. IT Audit 5. SOC 2 Audit 6. Red Team Assessment	Copies of at least 3 such 'LOI/PO/Work Order/Completion Certificate' received from the client must be provided.
6	The bidder should be empanelled with CERT-IN for last 5 years from RFP date	Certificate of Empanelment with CERT-IN for last 5 years from RFP date
7	For SOC 2 Audit: Bidder should be registered with the Institute of Chartered Accountants of India (ICAI)	Valid Certificate for ICAI membership
8	The bidder should have on payroll – 4. For IT Audit : at least 5 Auditors who are CISA/CISSP qualified or equivalent; 5. For SOC-2 Audit : at least 5 Auditors having ICAI / AICPA membership; 6. For Red Team Assessment : at least 05 Offensive Security Certified Professional (OSCP) from offensive-security / Certified Ethical Hacker	All Relevant certificates/documents supporting basis laid out in pre-qualification criteria.

	(CEH) from EC-Council / Licensed Penetration Tester (LPT) from EC-Council / GPEN: GIAC Penetration Tester from SANS / GWAPT: GIAC Web Application Penetration Tester from SANS / any other Red Team or Penetration Testing related certification;	
9	The bidder should not be providing IT related service(s) to StockHolding or its subsidiaries currently and should not have conducted IT Audit consecutively during the last 3 years (From Date of Issue of this RFP) for StockHolding.	Bidder to provide a Self-Declaration on the company letter head.
10	4. For IT Audit: The proposed Lead Auditor should be Graduate with CISA/CISSP certification with minimum 05 (five) years' experience in IT Audit related activities. 5. For SOC 2 Audit: Graduate with ICAI / AICPA membership with minimum 05 (five) years' experience in SOC Audit related activities. 6. For Red Team Assessment: Relevant certifications with minimum 05 (five) years' experience in assessment related activities.	Resume of proposed resource including list of IT /SOC Audit projects/Red Team Assessment handled during last 05 years in India

Note:

a. Letter of Authorization shall be issued by either Managing Director having related Power of Attorney issued in his favour or a Director of the Board for submission of Response to RFP
b. All self-certificates shall be duly signed and Stamped by Authorized signatory of the Bidder Firm unless specified otherwise.
c. Bidder response should be complete; Yes/No answer is not acceptable.
d. Details of clients and relevant contact details are mandatory. Bidders may take necessary approval of the clients in advance before submission of related information. StockHolding will not make any separate request for submission of such information.

Dated this........ Day of 2024
(Signature)

(In the capacity of)
Duly authorized to sign bid with seal for & on behalf of (Name & Address of the Bidder)

Annexure – 3: Commercial bid format

APPOINTMENT OF AUDITOR FOR CONDUCTING INFORMATION SECURITY AND CYBER SECURITY AUDIT

Table A:

AUDIT #	Audit Name	Frequency	Qty* (A)	Year 1		Year 2	
				Unit Rate (₹) (B)	Total Cost (₹) (C= A*B)	Unit Rate (₹) (B)	Total Cost (₹) (C= A*B)
1	Cyber security/System audit report	Annual	1				
2	Vulnerability Assessment and Penetration Testing report	Annual	1				
3	E-sign ESP audit for UIDAI	Annual	1				
4	PCM System Audit Clearing Corporation's MCX,ICCL and NSCCL	Annual	1				
5	CSGL System Audit for RBI	Quarterly	1x4				
6	OWASP API Audit	As and When required	1				
7	Custody System Audit	Annual	1				
8	Cyber Security and Cyber Resilience framework for Mutual Funds /Asset Management Companies	Half Yearly	1x2				
9	ISMS Audit	Quarterly	1x4				
10	SOC 2 Type 2 Gap assessment and then Type 2 Audit Attestation	Annual	1				
11	Red Team Assessment: External Exercise & Internal Exercise	Annual	1x2				
Total Cost (₹)							
GST (₹)							
Total Cost with GST (₹)				A		B	
Grand Total Cost for 3 years (₹)				[A + B]			

Terms & Conditions:

a. Price to be quoted is for contract period of 02 (two) years including GST while uploading financial bids on GeM portal.

b. In case the L1 bidder doesn't accept the offer or accepts the offer and doesn't proceed with the agreement within 7 working days, the offer to the L1 bidder will stand terminated. StockHolding reserves the right to negotiate with the L2 bidder. Likewise, if the L2 bidder doesn't accept the offer or accepts the order and doesn't proceed with the agreement within 7 working days, the offer to the L2 bidder will stand terminate.

c. StockHolding reserves the right to negotiate with L1 bidder.

d. Contract will be awarded to bidder with highest technical score in case of multiple L1 bidders.

e. Bidder must take care in filling price information in the Commercial Offer, to ensure that there are no typographical or arithmetic errors. All fields must be filled in correctly. Please note that any Commercial Offer, which is conditional and / or qualified or subjected to suggestions, will also be summarily rejected. This offer shall not contain any deviation in terms & conditions or any specifications, if so such an offer will also be summarily rejected.

f. All payments will be made in INR.

g. Year 2 price will have maximum escalation upto 10% on Year 1 Price.

h. StockHolding may choose to extend the contract period for another 1 year with the maximum escalation upto 10% on Year 2 Price for the selected bidder.

Dated this........ Day of 2024

(Signature)
(In the capacity of)
Duly authorized to sign bid with seal for & on behalf of (Name & Address of the Bidder)

Annexure – 4: Interest Free Earnest Money Deposit (EMD) Format for Appointment of Auditor

PAN & GST number of bidder	Bank Name & branch address ,IFSC code	Bank account number	EMD amount paid in INR	UTR No.	Date of Payment (NEFT)	EMD Bank receipt to be uploaded
1.						

Dated this........ Day of 2024

(Signature)

(In the capacity of)
Duly authorized to sign bid with seal for & on behalf of (Name & Address of the Bidder)

Annexure – 5: Covering Letter-1

(To be executed on plain paper and submitted only by the successful bidder)

(__________________________________ Name of the Department / Office) RFP No: IT-11/2023-24 dated 22-Feb-2024 for______________________________

This pre-bid pre-contract Integrity Pact (Agreement) (hereinafter called the Integrity Pact) (IP) is made on ______ day of the _______________________, between, on one hand, *StockHolding* ., a company incorporated under Companies Act, 1956, with its Registered Office at 301, Centre Point Building, Dr. Babasaheb R. Ambedkar Road, Parel, Mumbai – 400012 , acting through its authorized officer, (hereinafter called **Principal**), which expression shall mean and include unless the context otherwise requires, his successors in office and assigns) of the First Part **And** M/s.____(with complete address and contact details)represented by Shri ____ (i.e. s (bidders) hereinafter called the **`Counter Party'**) which expression shall mean and include , unless the context otherwise requires, his successors and permitted assigns) of the Second Part.

AND WHEREAS the PRINCIPAL/Owner values full compliance with all relevant laws of the land, rules, regulations economic use of resources and of fairness/transparency in its relation with Bidder(s) /Contractor(s)/Counter Party(ies).

AND WHEREAS, in order to achieve these goals, the Principal/Owner has appointed Independent External Monitors (IEM) to monitor the Tender (RFP) process and the execution of the Contract for compliance with the principles as laid down in this Agreement.

WHEREAS THE Principal proposes to procure the Goods/services and Counter Party is willing to supply/has promised to supply the goods OR to offer/has offered the services and WHEREAS the Counter Party is a private Company/Public Company/Government Undertaking/ Partnership, constituted in accorded with the relevant law in the matter and the Principal is a Government Company performing its functions as a registered Public Limited Company regulated by Securities Exchange Board of India. **NOW THEREFORE**, To avoid all forms of corruption by following a system that is fair, transparent and free from any influence prejudiced dealings prior to, during and subsequent to the tenor of the contract to be entered into with a view to "- Enabling the PRINCIPAL to obtain the desired goods/services at competitive price in conformity with the defined specifications by avoiding the high cost and the distortionary impact of corruption on public procurement, and Enabling the Counter Party to abstain from bribing or indulging in any type of corrupt practice in order to secure the contract by providing assurance to them that their competitors will also abstain from bribing and other corrupt practices and the PRINCIPAL will commit to prevent corruption, in any form, by its officials by following transparent procedures. The parties hereto hereby agree to enter into this Integrity Pact and agree as follows:

I. Commitment of the Principal / Buyer

1. The Principal Owner commits itself to take all measures necessary to prevent corruption and to observe the following principles: -

   a) No employee of the Principal/Owner, personally or through any of his/her family members, will in connection with the Tender (RFP) or the execution of the contract, procurement or services/goods, demand, take a promise for or accept for self or third person, any material or immaterial benefit which the person not legally entitled to.
   b) The Principal/Owner will, during the Tender (RFP) Process treat all Bidder(s)/Counter Party(ies) with equity and reason. The Principal / Owner will, in particular, before and during the Tender (RFP) Process, provide to all Bidder(s) / Counter Party(ies) the same information and will not provide to any Bidder(s)/Counter Party(ies) confidential / additional information through which the Bidder(s)/Counter Party(ies) could obtain an advantage in relation to the Tender (RFP) Process or the Contract execution.
   c) The Principal / Owner shall endeavour to exclude from the Tender (RFP) process any person, whose conduct in the past been of biased nature.

2. If the Principal / Owner obtains information on the conduct of any of its employees which is a criminal offence under the Indian Penal Code (IPC) / Prevention of Corruption Act, 1988 (PC Act) or is in violation of the principles herein mentioned or if there is a substantive suspicion in this regard, the Principal / Owner / *StockHolding* will inform the Chief Vigilance Officer through the Vigilance Officer and in addition can also initiate disciplinary actions as per its internal laid down policies and procedures.

II. Commitments of Counter Parties/Bidders

1. The Counter Party commits itself to take all measures necessary to prevent corrupt practices, unfair means and illegal activities during any stage of bid or during any pre-contract stage in order to secure the contract or in furtherance to secure it and in particular commit itself to the following. Counter Party (ies) / Bidders commits himself to observe these principles during participation in the Tender (RFP) Process and during the Contract execution.
2. The Counter Party will not offer, directly or through intermediaries, any bribe, gift, consideration, reward, favour, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of the PRINCIPAL, connected directly or indirectly with the bidding process, or to any person organization or third party related to the contract in exchange for any advantage in the bidding, evaluation, contracting and implementation of the contract.

3. The Counter Party further undertakes that it has not given, offered or promised to give directly or indirectly any bribe, gift, consideration, reward, favour, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of the Principal / *StockHolding* or otherwise in procurement the Contract or forbearing to do or having done any act in relation to the obtaining or execution of the contract or any other contract with the Principal / *StockHolding* for forbearing to show favour or disfavour to any person in relation to the contract or any other contract with the Principal / *StockHolding*.
4. Bidder / Counter Party shall disclose the name and address of agents and representatives, if any, handling the procurement / service contract.
5. Bidder / Counter Party shall disclose the payments to be made by them to agents / brokers; or any other intermediary if any, in connection with the bid / contract.
6. The Bidder / Counter Party has to further confirm and declare to the Principal / *StockHolding* that the Bidder / Counter Party is the original integrator and has not engaged any other individual or firm or company, whether Indian or foreign to intercede, facilitate or in any way to recommend to Principal / *StockHolding* or any of its functionaries whether officially or unofficially to the award of the contract to the Bidder / Counter Party nor has any amount been paid, promised or intended to the be paid to any such individual, firm or company in respect of any such intercession, facilitation or recommendation.
7. The Bidder / Counter Party has to submit a Declaration along with Technical Bid, as given at Annexure 6. If bids are invited through a Consultant a Declaration has to be submitted along with the Technical Bids as given at Annexure.
8. The Bidder / Counter Party, either while presenting the bid or during pre- contract negotiation or before signing the contract shall disclose any payments made, is committed to or intends to make to officials of *StockHolding* /Principal, or their family members, agents, brokers or any other intermediaries in connection with the contract and the details of services agreed upon for such payments.
9. The Bidder / Counter Party will not collude with other parties interested in the contract to impair the transparency, fairness and progress of bidding process, bid evaluation, contracting and implementation of the Contract.
10. The Bidder / Counter Party shall not accept any advantage in exchange for any corrupt practice, unfair means and illegal activities.
11. The Bidder shall not use improperly, for purposes of competition or personal gain, or pass on to others, any information provided by the Principal / *StockHolding* as part of the business relationship, regarding plans, technical proposals and business details, including information contained in any electronic data carrier. The Bidder / Counter Party also undertakes to exercise due and adequate care lest any such information is divulged.
12. The Bidder / Counter Party commits to refrain from giving any complaint directly or through any other manner without supporting it with full and verifiable facts.

13. The Bidder / Counter Party shall not instigate or cause to instigate any third person including their competitor(s) of bidding to commit any of the actions mentioned above.
14. If the Bidder / Counter Party or any employee of the Bidder or any person acting on behalf of the Bidder / Counter Party, either directly or indirectly, is a relative of any of the official / employee of Principal / *StockHolding*, or alternatively, if any relative of an official / employee of Principal /

    StockHolding has financial interest / stake in the Bidder's / Counter Party firm, the same shall be disclosed by the Bidder / Counter Party at the time of filing of tender (RFP).
15. The term `relative" for this purpose would be as defined in Section 2 Sub Section 77 of the Companies Act, 2013.
16. The Bidder / Counter Party shall not lend to or borrow any money from or enter into any monetary dealings or transactions, directly or indirectly, with any employees / officials of the Principal / *StockHolding*
17. The Bidder / Counter Party declares that no previous transgression occurred in the last three years immediately before signing of this IP, with any other Company / Firm/ PSU/ Departments in respect of any corrupt practices envisaged hereunder that could justify Bidder / Counter Party exclusion from the Tender (RFP) Process.
18. The Bidder / Counter Party agrees that if it makes incorrect statement on this subject, Bidder / Counter Party can be disqualified from the tender (RFP) process or the contract, if already awarded, can be terminated for such reason.

III. Disqualification from Tender (RFP) Process and exclusion from Future Contracts

1. If the Bidder(s) / Contractor(s), either before award or during execution of Contract has committed a transgression through a violation of Article II above or in any other form, such as to put his reliability or credibility in question, the Principal / *StockHolding* is entitled to disqualify the Bidder / Counter Party / Contractor from the Tender (RFP) Process or terminate the Contract, if already executed or exclude the Bidder / Counter Party / Contractor from future contract award processes. The imposition and duration of the exclusion will be determined by the severity of transgression and determined by Principal / *StockHolding*. Such exclusion may be for a period of 1 year to 3 years as per the procedure prescribed in guidelines of the Principal / *StockHolding*.
2. The Bidder / Contractor / Counter Party accepts and undertake to respect and uphold the Principal / *StockHolding*'s absolute right to resort to and impose such exclusion.
3. Apart from the above, the Principal / *StockHolding* may take action for banning of business dealings / holiday listing of the Bidder / Counter Party / Contractor as deemed fit by the Principal / Owner / *StockHolding*.
4. The Bidder / Contractor / Counter Party can prove that it has resorted / recouped the damage caused and has installed a suitable corruption prevention system, the Principal / Owner/ *StockHolding* may at its own discretion, as per laid down organizational procedure, revoke the exclusion prematurely.

IV. Consequences of Breach Without prejudice to any rights that may be available to the Principal / *StockHolding* / Owner under Law or the Contract or its established policies and laid down procedure, the Principal / *StockHolding* / Owner shall have the following rights in case of breach of this Integrity Pact by the Bidder / Contractor(s) / Counter Party:-

1. Forfeiture of EMD / Security Deposit : If the Principal / *StockHolding* / Owner has disqualified the Bidder(s)/Counter Party(ies) from the Tender (RFP) Process prior to the award of the Contract or terminated the Contract or has accrued the right to terminate the Contract according the Article III, the Principal / *StockHolding* / Owner apart from exercising any legal rights that may have accrued to the Principal / *StockHolding* / Owner, may in its considered opinion forfeit the Earnest Money Deposit / Bid Security amount of the Bidder / Contractor / Counter Party.
2. Criminal Liability: If the Principal / Owner / *StockHolding* obtains knowledge of conduct of a Bidder / Counter Party / Contractor, or of an employee of a representative or an associate of a Bidder / Counter

   Party / Contractor which constitute corruption within the meaning of PC Act, or if the Principal / Owner / *StockHolding* has substantive suspicion in this regard, the Principal / *StockHolding* / Owner will inform the same to the Chief Vigilance Officer through the Vigilance Officer.

V. Equal Treatment of all Bidders/Contractors / Subcontractors / Counter Parties

1. The Principal / *StockHolding* / Owner will enter into Pacts on identical terms as this one with all Bidders / Counterparties and Contractors.
2. The Principal / *StockHolding* / Owner will disqualify Bidders / Counter Parties / Contractors who do not submit, the duly signed Pact, between the Principal / Owner / *StockHolding* and the Bidder/Counter Parties, along with the Tender (RFP) or violate its provisions at any stage of the Tender (RFP) process, from the Tender (RFP) process.

VI. Independent External Monitor (IEM)

1. The Principal / Owner / *StockHolding* has appointed competent and credible Independent External Monitor (s) (IEM) for this Pact. The task of the Monitor is to review independently and objectively, whether and to what extent the parties comply with the obligations under this Integrity Pact.
2. The IEM is not subject to instructions by the representatives of the parties and performs his functions neutrally and independently. He reports to the Chief Executive Officer and Managing Director, Stock Holding Corporation of India Limited.
3. The Bidder(s)/Contractor(s) / Counter Party(ies) accepts that the IEM has the right to access without restriction, to all Tender (RFP) documentation related papers / files of the Principal / *StockHolding* / Owner including that provided by the Contractor(s) / Bidder / Counter Party. The Counter Party / Bidder / Contractor will also grant the IEM, upon his request and demonstration of a valid interest, unrestricted and unconditional access to his Tender (RFP) Documentation / papers / files. The IEM is under contractual obligation to

treat the information and documents of the Bidder(s) / Contractor(s) / Counter Party (ies) with confidentiality.

4. In case of tender (RFP)s having value of 5 crore or more, the Principal / *StockHolding* / Owner will provide the IEM sufficient information about all the meetings among the parties related to the Contract/Tender (RFP) and shall keep the IEM apprised of all the developments in the Tender (RFP) Process.
5. As soon the IEM notices, or believes to notice, a violation of this Pact, he will so inform the Management of the Principal / Owner /*StockHolding* and request the Management to discontinue or take corrective action, or to take other relevant action. The IEM can in this regard submit non-binding recommendations. Beyond this, the IEM has no right to demand from the parties that they act in a specific manner, refrain from action or tolerate action.
6. The IEM will submit a written report to the CEO&MD, *StockHolding*. Within 6 to 8 weeks from the date of reference or intimation to him by the Principal / Owner / *StockHolding* and should the occasion arise, submit proposals for correcting problematic situations.
7. If the IEM has reported to the CEO&MD, *StockHolding* Ltd. a substantiated suspicion of an offence under the relevant IPC/PC Act, and the CEO & MD, *StockHolding* has not within reasonable time taken visible action to proceed against such offence or reported it to the Chief Vigilance Officer, the IEM may also transmit the information directly to the Central Vigilance Officer. 8. The word `IEM" would include both singular and plural.

VII. Duration of the Integrity Pact (IP)

This IP begins when both the parties have legally signed it. It expires for the Counter Party / Contractor / Bidder, 12 months after the completion of work under the Contract, or till continuation of defect liability period, whichever is more and for all other Bidders, till the Contract has been awarded. If any claim is made / lodged during the time, the same shall be binding and continue to be valid despite the lapse of this Integrity Pact as specified above, unless it is discharged / determined by the CEO&MD *StockHolding* **VIII. VIII. Other Provisions**

1. This IP is subject to Indian Law, place of performance and jurisdiction is the Head Office / Regional Offices of the Stockholding /Principal / Owner who has floated the Tender (RFP).
2. Changes and supplements in any Procurement / Services Contract / Tender (RFP) need to be made in writing. Change and supplement in IP need to be made in writing.
3. If the Contractor is a partnership or a consortium, this IP must be signed by all the partners and consortium members. In case of a Company, the IP must be signed by a representative duly authorized by Board resolution.
4. Should one or several provisions of this IP turn out to be invalid; the remainder of this Pact remains valid. In this case, the parties will strive to come to an agreement to their original intentions.

5. Any dispute or difference arising between the parties with regard to the terms of this Agreement / Pact, any action taken by the Principal / Owner / *StockHolding* in accordance with this Agreement / Pact or interpretation thereof shall not be subject to arbitration.

IX. Legal and Prior Rights

All rights and remedies of the parties hereto shall be in addition to all the other legal rights and remedies belonging to such parties under the Contract and / or law and the same shall be deemed to be cumulative and not alternative to such legal rights and remedies aforesaid. For the sake of brevity, both the Parties agrees that this Pact will have precedence over the Tender (RFP) / Contract documents with regard to any of the provisions covered under this Integrity Pact.

IN WITNESS WHEREOF the parties have signed and executed this Integrity Pact (IP) at the place and date first above mentioned in the presence of the following witnesses:-

----

(For and on behalf of Principal / Owner / *StockHolding*

(For and on behalf of Bidder / Counter Party / Contractor)

WITNESSES:

1.____ (Signature, name and address)

2.____ (Signature, name and address)

Note: In case of Purchase Orders wherein formal agreements are not signed references to witnesses may be deleted from the past part of the Agreement.

Annexure – 6: Covering Letter on bidder's letterhead (Annexure of Integrity Pact)

Date:

To,

Sub: RFP No: **IT-11/2023-24 dated 22-Feb-2024** for **Appointment of Auditor for conducting Information Security and Cyber Security Audit**

Dear Sir,

DECLARATION

Stock Holding Corporation of India Limited (*StockHolding*) hereby declares that *StockHolding* has adopted Integrity Pact (IP) Program as advised by Central Vigilance Commission vide its Letter No. ----------------- dated -------------- and stands committed to following the principles of transparency, equity and competitiveness in public procurement. The subject Notice Inviting Tender (RFP) (NIT) is an invitation to offer made on the condition that the Bidder will sign the Integrity Agreement, which is an integral part of tender (RFP) documents, failing which the tenderer / bidder will stand disqualified from the tendering process and the bid of the bidder would be summarily rejected. This Declaration shall form part and parcel of the Integrity Agreement and signing of the same shall be deemed as acceptance and signing of the Integrity Agreement on behalf of the *StockHolding*

Yours faithfully,

For and on behalf of Stock Holding Corporation of India Limited
(Authorized Signatory)

Annexure – 7: Compliance Statement

(To be submitted along with technical bid)

Subject: RFP for Appointment of Auditor for Conducting Information security and Cyber Security Audit

Ref: RFP No. **IT-11/2023-24 dated 22-Feb-2024**

DECLARATION

We understand that any deviations mentioned elsewhere in the bid will not be considered and evaluated by StockHolding. We also agree that *StockHolding* reserves its right to reject the bid, if the bid is not submitted in proper format as per RFP.

Sr. No.	**Item / Clause of the RFP**	**Confirmed and Accepted by Bidder (Yes / No)**
1	Eligibility Criteria	
2	Service Level Agreement (SLA) / Scope of Work	
3	Non-Disclosure Agreement	
4	Payment Terms	
5	Bid Validity, Order Cancellation	
6	StockHolding's Right to alter RFP	
7	Force Majeure	
8	Integrity Pact	
9	All General & Other Terms & Conditions in the RFP	
10	Requirement with terms and conditions	
11	Bid Format - Commercial Bid	
12	Annexures in the RFP	

Dated this........ Day of 2024

(Signature)

(In the capacity of)

Duly authorized to sign bid with seal for & on behalf of (Name & Address of the Bidder)

Annexure – 8 - Letter of Acceptance

(To be submitted along with Technical Bid)

To,
Stock Holding Corporation of India Limited
SHCIL House, Plot No. P-51, T.T.C. Industrial Area,
M.I.D.C., Mahape, Kalyan-Shil Road,
Navi Mumbai, PIN 400710.

Dear Sir,
Sub: RFP no: **IT-11/2023-24 dated 22-Feb-2024** for RFP for Appointment of Auditor for Conducting Information security and Cyber Security Audit

With reference to the above RFP, having examined and understood the instructions, annexures, terms and conditions forming part of the RFP.

We further confirm that the offer is in conformity with the terms and conditions as mentioned in the RFP. We also confirm that the offer shall remain valid for the entire Agreement Period from the date of the offer.

We also understand and accept that Stockholding can modify, amend, alter and/or cancel the entire RFP at any stage without assigning any reason whatsoever. We further understand and accept that *StockHolding*'s decision in this regard will be final and binding on us.

We also accept that *StockHolding*'s decisions with reference to this RFP pertaining to evaluation process of bidder responses will be final and binding on us. We also understand and accept that no queries will be entertained in this regard by *StockHolding*.

Dated this........ Day of 2024
(Signature)

(In the capacity of)
Duly authorized to sign bid with seal for & on behalf of (Name & Address of the Bidder)

Annexure – 9: Draft NDA (To be submitted on Rupees 100 Non-Judicial stamp paper)

MUTUAL NON-DISCLOSURE AGREEMENT

This Non-Disclosure Agreement (hereinafter "Agreement") is executed on this ___ day of _________________, 2024 by and between

Stock Holding Corporation of India Limited, a company incorporated under the Companies Act, 1956 and having its registered office at 301, Centre Point, Dr. Babasaheb Ambedkar Road, Parel, Mumbai 400012 (hereinafter referred to as "StockHolding" which expression shall mean and include its successors and assigns), of the One Part;

And

(Company Name) a company incorporated under the Companies Act, 1956 and having its registered office / corporate office at (Complete address) (hereinafter referred to as "Company Name" which expression shall mean and include its successors and assigns), of the Other Part.

(StockHolding and (Company Name) are individually referred to as 'Party' and collectively as 'Parties'.)

The Party disclosing Confidential Information under this Agreement shall be referred to as Disclosing Party and the Party receiving Confidential Information shall be referred to as Receiving Party.

Purpose: Whereas, the Parties wish to explore possible business opportunity, during which either Party will be required to disclose certain Confidential Information to the other.

Confidential Information and Exclusions: Confidential Information shall mean and include (a) any information received by the Receiving Party which is identified by Disclosing Party as confidential or otherwise; (b) all information including technical, data security , cyber security business, financial and marketing information, data, analysis, compilations, notes, extracts, materials, reports, drawings, designs, specifications, graphs, layouts, plans, charts, studies, memoranda or other documents, know-how, ideas, concepts, strategies, trade secrets, product or services, results obtained by using confidential information, prototype, client or vendor list, projects, employees, employees skills and salaries, future business plans disclosed by Disclosing Party whether orally or as embodied in tangible materials. Confidential Information shall however exclude any information which a) is in the public domain; (b) was known to the Party of such disclosure or becomes known to the Party without breach of any confidentiality agreement; (c) is independently developed by the Party without use of Confidential Information disclosed herein;

(d) is disclosed pursuant judicial order or requirement of the governmental agency or by operation of law, provided that the recipient party gives disclosing party a written notice of any such requirement within ten (10) days after the learning of any such requirement, and takes all reasonable measure to avoid disclosure under such requirement.

Confidentiality Obligations: The Receiving Party shall, at all times maintain confidentiality and prevent disclosure of Confidential Information of Disclosing party with at least the same degree of care as it uses to protect its own confidential information but in no event with less than reasonable care. The Receiving Party shall keep the Confidential Information and Confidential Materials and any copies thereof secure and in such a way so as to prevent unauthorized access by any third party. The Receiving Party agrees not to disclose, transmit, reproduce or make available any such Confidential Information to any third parties and shall restrict disclosure of Confidential Information only to a limited group of Recipient's directors, concerned officers, employees, attorneys or professional advisors who need to have access to the Confidential Information for the purposes of maintaining and supporting the services and each of whom shall be informed by Receiving Party of the confidential nature of Confidential Information and agree to observe the same terms and conditions set forth herein as if specifically named a Party hereto. The Receiving Party shall not, unless otherwise agreed herein, use any such Confidential Information and Confidential Materials for its own benefit or the benefit of others or do anything prejudicial to the interests of the Disclosing Party or its customers or their projects. The Receiving Party shall not use the Confidential Information in any way to create a derivative work out of it or auction engineer or use for any commercial purpose or for any purpose detrimental to the Disclosing Party. The Receiving Party shall not make copies of Confidential Information unless the same are reasonably necessary. The Receiving Party shall immediately notify Disclosing Party in the event of any unauthorized use or disclosure of the Confidential Information and reasonably support Disclosing Party in taking necessary remedial action.

No Warranty: All Confidential Information is provided ‘as is.’ Neither Party makes any warranty, express, implied or otherwise, regarding its accuracy, completeness or performance.

No License: Each Party recognizes that nothing in this Agreement is construed as granting it any proprietary rights, by license or otherwise, to any Confidential Information or to any intellectual property rights based on such Confidential Information.

Return:
The Receiving Party who receives the Confidential Information and Confidential Materials agrees that on receipt of a written demand from the Disclosing Party:
Immediately return all written Confidential Information, Confidential Materials and all copies thereof provided to, or produced by it or its advisers, as the case may be, which is in

Receiving Party’s possession or under its custody and control; (SUCH RETURN OF DOCUMENTS SHOULD BE DONE BY SIGNING A LETTER).

To the extent practicable, immediately destroy all analyses, compilations, notes, studies, memoranda or other documents prepared by it or its advisers to the extent that the same contain, reflect or derive from Confidential Information relating to the Disclosing Party;

So far as it is practicable to do so immediately expunge any Confidential Information relating to the Disclosing Party or its projects from any computer, word processor or other device in its possession or under its custody and control; and

To the extent practicable, immediately furnish a certificate signed by its director or other responsible representative confirming that to the best of his/her knowledge, information and belief, having made all proper enquiries the requirements of this paragraph have been fully complied with.
Receiving party will attempt to maintain, to the best possible extent, physical and logical segregation of the Confidential Information of the data of the Receiving party from data of any third party.

Term: The term of this Agreement shall be __(_) years from ________________(the Effective Date). Either Party may terminate this Agreement by giving a thirty (30) days written notice to the other. The confidentiality obligations stated in this Agreement shall survive for a period of three (3) years from the date of termination or expiration of this Agreement.

Remedies: The Confidential Information and Confidential Materials and all copies thereof, in whatsoever form shall at all times remain the property of the Disclosing Party and its disclosure hereunder shall not confer on the Receiving Party any rights whatsoever beyond those contained in this document.

The Parties acknowledge and agree that the Disclosing Party will suffer substantial and irreparable damage, not readily ascertainable or compensable in monetary terms, in the event of any breach of any provision of this Agreement by the Receiving Party. The Receiving Party therefore agrees that, in the event of any such breach, the Disclosing Party shall be entitled, without limitation of any other remedies otherwise available to it, to obtain an injunction or other form of equitable relief from any court of competent jurisdiction.

Governing Law and Jurisdiction: This Agreement may be governed and construed in accordance with the laws of India and shall be subject to the jurisdiction of courts in Mumbai, India.

Miscellaneous: This Agreement constitutes the entire agreement between the Parties with respect to the subject matter hereof and supersedes all prior commitments/ understanding in this regard and may not be amended or modified except by a writing signed by a duly authorized representative of the respective Parties. This Agreement may be executed in several counterparts (physical or electronic form), each of which shall be deemed an original, but all of which together shall constitute one and the same instrument. This Agreement may not be assigned or transferred except by a mutual written consent of both the Parties.

For Stock Holding Corporation of India Limited	For (Company Name)
Name:	Name:
Title:	Title:
In the Presence of	
Name:	Name:
Title:	Title:

Annexure – 10 – Template for Bank Guarantee

This Bank Guarantee is executed by the ------------------------- (Bank name) a Banking Company incorporated under the Companies Act, 1956 and a Scheduled Bank within the meaning of the Reserve Bank of India Act, 1934 and having its head office at ------------------------ and branch office at _______________(hereinafter referred to as the "Bank", which term shall mean and include, unless to repugnant to the context or meaning thereof, its successors and permitted assigns) and Branch office at _________________ in favour of Stock Holding Corporation of India Limited, a Company incorporated under the Companies Act, 1956 and having its Registered Office at 301, Centre Point, Dr. Babasaheb Ambedkar Road, Parel, Mumbai 400 012 (hereinafter referred to as "StockHolding", which term shall mean and include, unless to repugnant to the context or meaning thereof, its successors and permitted assigns) at the request of ________________, a Company incorporated under the Companies Act, 1956 and having its Registered Office at (hereinafter referred to as the "Service Provider", which term shall mean and include, unless to repugnant to the context or meaning thereof, its successors and permitted assigns).

Whereas

A. StockHolding has, pursuant to the Tender No. ___________, issued the Purchase Order dated __________ to the Service Provider for providing _________________
B. In terms of the said Tender, the Service Provider has agreed to furnish to StockHolding, a Bank guarantee for Rs. ____________ /- (Rupees _______________ only) till _________ (date).
C. The Bank has, at the request of the Service Provider, agreed to give this guarantee as under.

NOW IN CONSIDERATION OF THE FOREGOING:

1. We, the Bank, at the request the Service Provider, do hereby unconditionally provide this guarantee to StockHolding as security for due performance and fulfilment by the Service Provider of its engagements, commitments, operations, obligations or liabilities including but not limited to any sums / obligations / claims due by the Service Provider to StockHolding for meeting, satisfying, discharging or fulfilling all or any obligation or liability of the Service Provider, under the said Tender / Purchase Order.

2. We, the Bank, hereby guarantee and undertake to pay StockHolding up to a total amount of Rs. ________/- (Rupees _______________ only) under this guarantee, upon first written demand of StockHolding and without any demur, protest and without any reference to the Service Provider.
3. Any such demand made by StockHolding shall be conclusive and binding on the Bank as regards the amount due and payable notwithstanding any disputes pending before any court, Tribunal, or any other authority and/ or any other matter or thing

whatsoever as the liability of the Bank under these presents being absolute and unequivocal.

4. We, the Bank, agree that StockHolding shall have the fullest liberty without consent of the Bank to vary the terms of the said Tender/ Purchase Order or to postpone for any time or time to time exercise of any powers vested in StockHolding against the Service Provider and to forbear or enforce any of the Terms & Conditions relating to the said Tender / Purchase Order and the Bank shall not be relieved from its liability by the reason of any such variation, or extension being granted to the Service Provider or for any forbearance, act or omission or any such matter or thing whatsoever.
5. We, the Bank, agree that the guarantee herein contained shall be irrevocable and shall continue to be enforceable until it is discharged.
6. This Guarantee shall not be affected by any change in the Constitution of the Bank or the Service Provider or StockHolding.

NOTWITHSTANDING ANYTHING CONTAINED HEREIN ABOVE:

1. The liability of the bank under this guarantee is restricted to a sum of Rs. ________/- (Rupees _______________ only).
2. This Bank Guarantee will be valid for a period up to ______________ (date).
3. A written claim or demand for payment under this Bank Guarantee on or before ______________ (date) is the only condition precedent for payment of part/full sum under this guarantee.

<u>For Issuing Bank</u>

Name of Issuing Authority:

Designation of Issuing Authority:

Employee Code:

Contact Number:

Email ID:

भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

CIRCULAR

SEBI/HO/MIRSD/CIR/PB/2018/147 December 03, 2018

To,

The Managing Directors of all Recognized Stock Exchanges and Depositories

Dear Sir / Madam,

Subject: Cyber Security & Cyber Resilience framework for Stock Brokers / Depository Participants

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. Since stock brokers and depository participants perform significant functions in providing services to holders of securities, it is desirable that these entities have robust cyber security and cyber resilience framework in order to provide essential facilities and perform systemically critical functions relating to securities market.

3. Accordingly, after discussions with Exchanges, Depositories and Stock Brokers' and Depository Participants' associations, a framework on cyber security and cyber resilience has been designed, which is placed at Annexure 1. The framework would be required to be complied by all Stock Brokers and Depository Participants registered with SEBI.

4. The guidelines annexed with this circular shall be effective from April 1, 2019.

5. Stock Exchanges and Depositories shall;

   a) make necessary amendments to the relevant byelaws, rules and regulations for the implementation of the above direction;
   b) bring the provisions of this circular to the notice of their members/participants and also disseminate the same on their websites; and
   c) communicate to SEBI, the status of implementation of the provisions of this circular in their Monthly Report.

6. This circular is being issued in exercise of powers conferred under Section 11 (1) of the Securities and Exchange Board of India Act, 1992, to protect the interests of investors in securities and to promote the development of, and to regulate the securities market.

Yours faithfully

Debashis Bandyopadhyay
General Manager
Market Intermediaries Regulations and Supervision Department

Annexure – 1

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. 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.

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.

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 Organization (NTRO), Government of India (titled ‘Guidelines for Protection of National Critical Information Infrastructure’) and subsequent revisions, if any, from time to time.

5. Stock Brokers trading through APIs based terminal / Depository Participants may refer to best practices from international standards like ISO 27001, COBIT 5, etc., or their subsequent revisions, if any, from time to time.

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 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.

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.

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.

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.

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 privileged access or use systems / networks of Stock Brokers / Depository Participants towards ensuring the goal of Cyber Security.

Identification

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.

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.

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.

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.

15. Stock Brokers / 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 in Annexure C.

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.)

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.

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.

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

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

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.

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

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.

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.

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.

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.

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

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 in Annexure A and B.

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. Illustrative measures to ensure security during transportation of data over the internet are given in Annexure B.

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.

32. Stock Brokers / Depository Participants should allow only authorized data storage devices within their IT infrastructure through appropriate validation processes.

Hardening of Hardware and Software

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.

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

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.

Certification of off-the-shelf products

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.

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.

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.

Disposal of data, systems and storage devices

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.

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.

Vulnerability Assessment and Penetration Testing (VAPT)

41. Stock Brokers / Depository Participants should regularly conduct vulnerability assessment to detect security vulnerabilities in their IT environments exposed to the internet.

42. Stock Brokers / 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-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.

In addition, Stock Brokers / Depository Participants should perform vulnerability scanning and conduct penetration testing prior to the commissioning of a new system that is accessible over the internet.

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.

44. Remedial actions should be immediately taken to address gaps that are identified during vulnerability assessment and penetration testing.

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.

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.

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.

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 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.

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.

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

Sharing of Information

52. Quarterly reports containing information on cyber-attacks and threats experienced by Stock Brokers / Depository Participants and measures taken to mitigate vulnerabilities, threats and attacks including information on bugs / vulnerabilities / threats that may be useful for other Stock Brokers / Depository Participants should be submitted to Stock Exchanges / Depositories.

Training and Education

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).

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.

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

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.

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.

Annexure A

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 B

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 C

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.

7. 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.

NSDL
Technology, Trust & Reach

Participant Interface Circular

Circular No.: NSDL/POLICY/2020/0071 May 19, 2020

Subject: Annual System Audit Report.

Attention of Participants is invited to Circular No. NSDL/POLICY/2018/0069 dated December 05, 2018 regarding Cyber Security & Cyber Resilience framework for Depository Participants. With regards to Paragraph 58 of Annexure 1 of the SEBI circular dated December 03, 2018, participants are directed to 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 Depositories along with the comments of the Board / Partners / Proprietor of Participant within three months of the end of the financial year.

Further, as Participants are aware that SEBI vide its circular no. SEBI/HO/MIRSD/DOP/CIR/P/2020/62 dated April 24, 2020, has extended the deadline for submission of the annual system audit report to July 31, 2020 for the financial year ended March 31, 2020 (communicated to all the Participants vide Circular no. NSDL/POLICY/2020/0052 dated April 24, 2020).

In this context, Participants are requested to take note of the annual system audit checklist attached at **Annexure A**. Procedure for submission of the audit report will be notified separately.

Participants are requested to take note of the above and guide their system auditors accordingly.

For and on behalf of
National Securities Depository Limited

Chirag Shah
Senior Manager

Enclosed: One

FORTHCOMING COMPLIANCE			
Particulars	**Deadline**	**Manner of sending**	**Reference**
Investor Grievance Report (Monthly)	May 18th, 2020 for the months of March 2020 and April 2020.	Through e-PASS	1. Circular No. NSDL/POLICY/2015/0096 dated October 29, 2015 2. Circular No. NSDL/ POLICY/2020/0056 dated April 29, 2020
Artificial Intelligence /Machine Learning Reporting Form (if offering or using such technologies as defined) (Quarterly)	May 31st, 2020 for quarter ended March 2020.	By email at Participant-Interface@nsdl.co.in	1. Circular No. NSDL/POLICY/2019/0016 dated March 27, 2019 2. Circular No. NSDL/ POLICY/2020/0056 dated April 29, 2020
Tariff Sheet (Yearly)	May 31st, 2020	By email at dpfees@nsdl.co.in	1. Circular No. NSDL/POLICY/2006/0064 dated December 26, 2006. 2. Circular No. NSDL/POLICY/2007/0003 dated January 8, 2007. 3. Circular No. NSDL/ POLICY/2020/0058 dated May 4, 2020
Risk based supervision of Participants (October 2019- March 2020)	May 31st, 2020	Through e-PASS	1. Circular No. NSDL/POLICY/2018/0050 dated September 25, 2018 2. Circular No.: NSDL/ POLICY/2020/0060 dated May 4, 2020
Internal/ Concurrent Audit Report (October 2019 – March 2020)	June 30th 2020	Through e-PASS	1. Circular No. NSDL/POLICY/2020/0045 dated April 7, 2020 2. Circular No. NSDL/ POLICY/2020/0056 dated April 29, 2020 3. Circular No.: NSDL/ POLICY/2020/0062 dated May 7, 2020.

Digitally signed by
Name : Chirag Shah
Date : 5/19/2020 10:18:39 PM
Reason : Authentication

Circular No.: NSDL/POLICY/2022/166 November 28, 2022

Subject: Modification in Cyber Security and Cyber resilience framework for Depository Participants

Attention of Participants is invited to NSDL Circular No. NSDL/POLICY/2022/083 dated June 13, 2022 issued with reference to the SEBI Circular No. SEBI/HO/MIRSD/TPD/P/CIR/2022/80 dated June 07, 2022 regarding modification in Cyber Security and Cyber resilience framework for Stock Brokers / Depository Participants.

As per modified para 42 prescribed under SEBI Circular SEBI/HO/MIRSD/TPD/P/CIR/2022/80 dated June 07, 2022: -

> *"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 empaneled 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."*

With respect to the above provision, it may be noted that Participants are required to carry out VAPT on or before December 15, 2022 for FY 2022-23 and submit the VAPT report on said VAPT within one month from the date of completion of VAPT after approval from Technology Committee of respective Participants. Participants are requested to email the VAPT report to NSDL at vapt-nsdl@nsdl.co.in.

Further, Participants are requested to fix all the vulnerabilities reported in the VAPT and conduct revalidation assessment and submit the report to NSDL on or before March 25, 2023. It may be noted that the revalidation VAPT report should be submitted to NSDL after approval from Technology Committee of respective Participants. Participants are requested to email the VAPT report to NSDL at vapt-nsdl@nsdl.co.in.

Further, Participants are required to conduct VAPT by August – September of every financial year and the final report on said VAPT shall be required to be submitted to NSDL within one month from the date of completion of VAPT after approval from Technology Committee of respective Participants.

Participants are requested to take note of the above and ensure compliance.

For and on behalf of

National Securities Depository Limited

Digitally signed by AROCKIARAJ
Reason: Authentication
Date: 2022.11.28 10:01:44 +05'30'

Arockiaraj

Manager

FORTHCOMING COMPLIANCE			
Particulars	**Deadline**	**Manner of sending**	**Reference**
Investor Grievance Report (Monthly)	By 10th of the following month.	Through e-PASS	Circular No. NSDL/POLICY/2015/0096 dated October 29, 2015

ASP On-Boarding Guidelines

Version 1.3

26 Dec 2018

Controller of Certifying Authorities
Ministry of Communications and Information Technology

Document Control

Document Name	ASP On-Boarding Guidelines
Status	Release
Version	1.3
Last update	26.12.2018
Document Owner	Controller of Certifying Authorities, India

Table of Content

Contents

Executive Summary

The Information Technology Act, 2000 provides the required legal sanctity to Digital signatures based on asymmetric crypto systems. Digital signatures are accepted at par with handwritten signatures and the electronic documents that have been digitally signed are treated at par with paper documents signed in the traditional way. However the scheme of physical verification, document based identity validation, and issuance of cryptographic tokens does not scale to a billion people. The eSign online Electronic Signature Service allows anyone who can be authenticated through acceptable e-KYC services to be able to easily sign a document electronically

eSign Electronic Signature Service can be integrated with various service delivery applications to facilitate digitally signing a document by authenticated through e-KYC of eSign user. It is designed for applying Digital Signature based on authenticated responses received from e-KYC service pertaining to the eSign users demographics. The benefits that eSign provides includes convenience and security to the citizens while the organizations save on time, achieve streamlined processes and reduce the costs associated with handling and storage of paper.

The stakeholders involved in the process include the Application Service Provider (ASP), eSign Service Provider (ESP), the Certifying Authority (CA) and e-KYC Providers. All these players are instrumental in signing of a document through eSign. This document details out the entire process for eSign starting from eSign user initiating the process up to the ESP signing the hash of the document and sending it back to the ASP.

In order to become an eSign enabled Application Service Provider, the organization needs to first apply to a particular ESP by filling the form and submitting the required documents as prescribed. Once the ESP has satisfied itself, the two parties will (ESP and ASP) will enter into an agreement/undertaking to decide the scope of services, service level agreements and other terms of business. Once all these formalities have been completed, the ASP will be given an integration kit to start the pre-production work.

Once the ESP team is satisfied with the preparations of ASP regarding the environment that it has, it will give its approval for the pre-production testing. The ASP needs to generate a -pubic key certificate for mapping and authentication to access the pre-production environment and perform end to end testing. The testing phase lasts for usually 7-10 days during which the main thrust is on testing the domain application and connectivity with the ESP. Once it is complete, the ASP can send a request for approval to Go-Live. The ESP on its part performs tests or checks logs to satisfy itself about the readiness of the ASP to go live.

Once approval is received from the ESP, the ASP needs to obtain a public key certificate for mapping and authentication to access the production environment. The migration from pre-production to production stage is done and after due testing, the ASP can roll out the application to provide eSign service to various eSign users who want to avail it.

The objective of this document is to provide detailed guidelines and activities on how to onboard various organizations to become Application Service Providers (ASP) for the eSign Service. The document gives a brief overview of the eSign service and the process flow for the same. It details out the various stakeholders that are involved in this process and the prerequisites that an organization needs to fulfill. An organization will gain a complete understanding on the various steps that it needs to follow to integrate eSign service in its application. The document also will include the Application form, Agreement/undertaking that the ASP needs to enter into with the eSign Service Provider. Also included are the audits requirements which the ASP needs to fulfill in order to carry out its operations.

Terminologies

"eSign" or "eSign Service" is an online Electronic Signature Service in which the key pair generation, certification of the public key by the CA and digital signature creation for electronic document are facilitated by the eSign online Electronic Signature Service provider instantaneously within a single online service based on successful authentication of individual using e-KYC services

"eSign User or eKYC user or subscriber" is an Individual requesting for eSign online Electronic Signature Service of eSign Service provider.

"e-KYC" mean the transfer of digitally signed demographic data such as Name, Address, Date of Birth, Gender, Mobile number, Email address, photograph etc of an individual collected and verified by e-KYC provider on successful authentication of same individual

"response code" is the identification number maintained by e-KYC provider to identify the authentication

1. Introduction

1.1. Information Technology Act and Digital Signatures

The Information Technology Act, 2000 provides that information or any other matter shall be authenticated by affixing signature then notwithstanding anything contained in the law, such requirement shall be deemed to be fulfilled if such information is authenticated by means of electronic signatures affixed in a manner prescribed by the Central Government.

Under the IT Act, 2000, 'Electronic signatures' means authentication of an electronic record by a subscriber by means of electronic technique specified in second schedule and includes Digital signatures. Digital Signature means authentication of any electronic record by a subscriber by means of procedure specified in Section 3 of the IT Act, 2000.

As per the Gazette notifications "Electronic Signature or Electronic Authentication Technique and Procedure Rules, 2015", Online Digital Signing through the eSign Service will be offered by Trusted Third Parties (TTP) or eSign Service Provider (ESP). Currently only licensed Certifying Authorities (CAs) can operate as ESP. The above mentioned rules states that the e-authentication issued by Controller must be followed for operating as ESP. These e-authentication guidelines, "e-authentication guidelines for eSign Online Electronic Signature Service", is available at www.cca.gov.in/esign

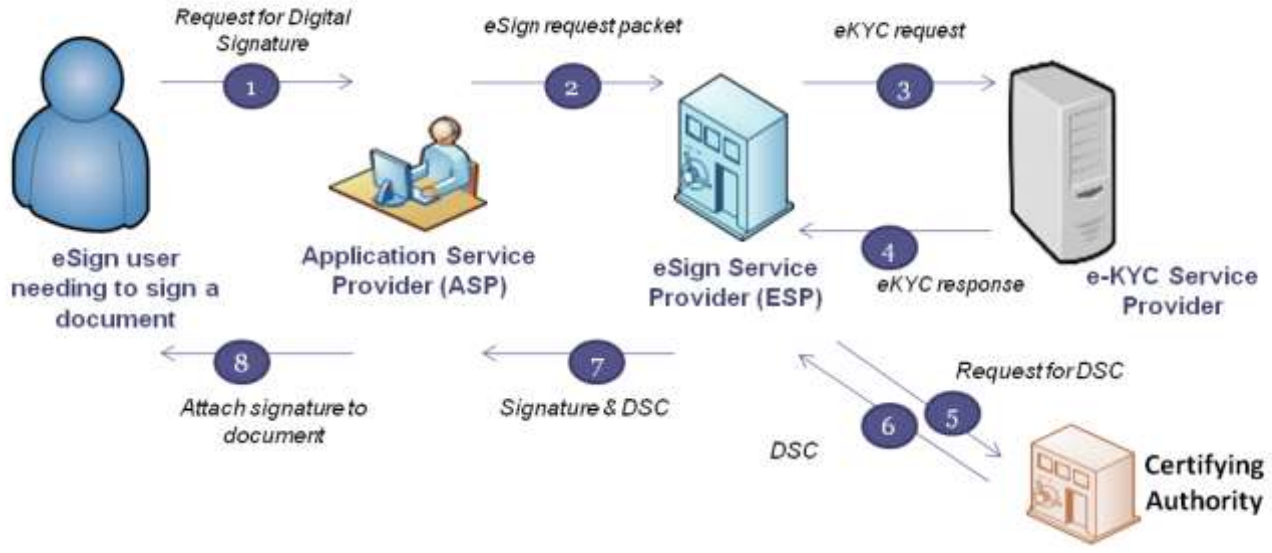
In the traditional Digital Signature system, an individual is responsible for applying for a Digital Signature Certificate to a CA, key pair generation and safe custody of keys. The Certifying Authorities issue Digital Signature Certificate to individuals after verification of credentials submitted in the application form. Such Digital Signature Certificates are valid for 2-3 years

In the eSign online Electronic Signature Service, on successful authentication of individual using e-KYC services, the key pairs generation, the certification (by the CA) of the public key based on authenticated response received and digital signature of the electronic document are facilitated by the eSign online Electronic Signature Service provider.

1.2. eSign Service

eSign facilitates digitally signing a document by an individual using an Online Service. eSign is designed for applying Digital Signature based on the response received from e-KYC service. eSign is an integrated service that facilitates issuing a Digital Signature Certificate and performing Signing of data. A unique e-KYC identifier based on response received from e-KYC services is mandatory for availing eSign Service.

Service delivery applications can integrate with eSign via an open API to facilitate digitally signing a document by an eSign user. It is designed for applying Digital Signature of eSign user who is issued a DSC based on e-KYC authentication.


Request for Digital Signature
1
eSign request packet
2
eKYC request
3
eSign user needing to sign a document
Application Service Provider (ASP)
eSign Service Provider (ESP)
4
eKYC response
e-KYC Service Provider
8
Attach signature to document
7
Signature & DSC
Request for DSC
5
6
DSC
Certifying Authority

eSign Process Flow

1.3. Types of Verification

Based on the verification of identity of the eSign user and storage of key pairs, three classes of certificates are issued in the traditional way of obtaining Digital Signatures Certificates from the Certifying Authorities. In the case of eSign Online Electronic Signature Service, the Digital Signature Certificates are issued based the following verification methods

1. **e-KYC Services**
   - **OTP:** based on **OTP authentication** of eSign user through e-KYC Service
   - **Biometric (FP/Iris):** based on **biometric authentication** of eSign user through e-KYC service**.**
   - **OTP & PIN** : based on ***OTP & PIN authentication*** of eSign user

These certificates will confirm that the information in the Digital Signature Certificate provided by the eSign user is same as information retained in the e-KYC service provider’s databases pertaining to the eSign user.

1.4. Stakeholders – Roles and Responsibilities

The entire ecosystem for providing the eSign Services will include a number of stakeholders that will come together to provide eSign service to an applicant.

S. N.	Stakeholders	Roles and Responsibilities
1.	Application Service Provider (ASP)	• Using eSign service as part of their application to digitally sign the content • Sign the contract/agreement/undertaking with the ESP • Indemnify both ESP and CA for integrity related discrepancies arises at ASP end. • Archive logs and carryout audit as per the guidelines of CCA • *ASP integrate with ESPs through standard eSign APIs • *ASP provides eSign facility to public service should integrate with all other ESPs within one month after on-boarding with first ESP. • *ASP shall protect the document URL (available within eSign request) from anyone or any system accessing it using URL and also from virus, malware, etc.

		• *ASP shall display (and allow download/print) the document that is to be signed clearly for subscribers to read before signing. • *Provision for providing/accessing the copy of the signed document to the signer ** Applicable to ASP availing eKYC service provided by CA*
2.	End User	• Represents himself/herself for signing the document under the legal framework • For the purposes of DSC by the CA, the end-user shall also be the ‘applicant/eSign User for digital certificate’, under the scope of IT Act • Provide the correct eSign user id while signing and should not impersonate anyone else
3.	eSign Service Provider	• It provides the eSign service and is a “Trusted Third Party”, as per the definitions of Second Schedule of Information Technology Act • Facilitates eSign User’s key pair-generation, storing of key pairs on hardware security module and creation of digital signature • It can be a licensed Certifying Authority (CA), or must be having an arrangement / integration with a CA for the purpose of obtaining Signature Certificate for the generated key pair
4.	Certifying Authority	• Licensed by the CCA for issuance of Digital Certificate • Carries out allied CA operations
5.	e-KYC Provider	• As per the list of e-KYC providers are given in the e-authentication Guidelines.
6.	Controller of Certifying Authority (CCA)	• Licenses and regulates the working of Certifying Authorities • Ensures that none of the provisions of the Act are violated • Performs audits and keeps checks on the functioning of the CAs to ensure it functions effectively

1.5. eSign API

eSign application programming interfaces (APIs) define the major architectural components and also describe the format and elements of communication among the stakeholders like Application Service Provider, Certifying Authorities and e-KYC service. This Standard eSign API enables Application Service Providers to integrate eSign API in their Application with minimum effort.

The various steps that are involved in the signing of document using eSign are:

1. Asks the end user to sign the document
2. Creates the document hash (to be signed) on the client side
3. Calls the e-Sign API of the eSign provider
4. eSign provider validates the calling application, obtain e-KYC response
5. Redirect eSign user to ESP for authentication by eKYC provider
6. eKYC provider validate the information obtained from eSign user and on success, provide eKYC response
7. ESP validate the authenticity of the e-KYC response.
8. On success, creates a new key pair for that eSign user
9. Signs the input document hash using the private key (The original document is not sent to eSign service provider)

   Creates an audit trail for the transaction

   a. Audit includes the transaction details, timestamp, and e-KYC response
   b. This is used for pricing and reporting
10. Sends the e-Sign API response back to the calling application

11. Attaches the signature to the document

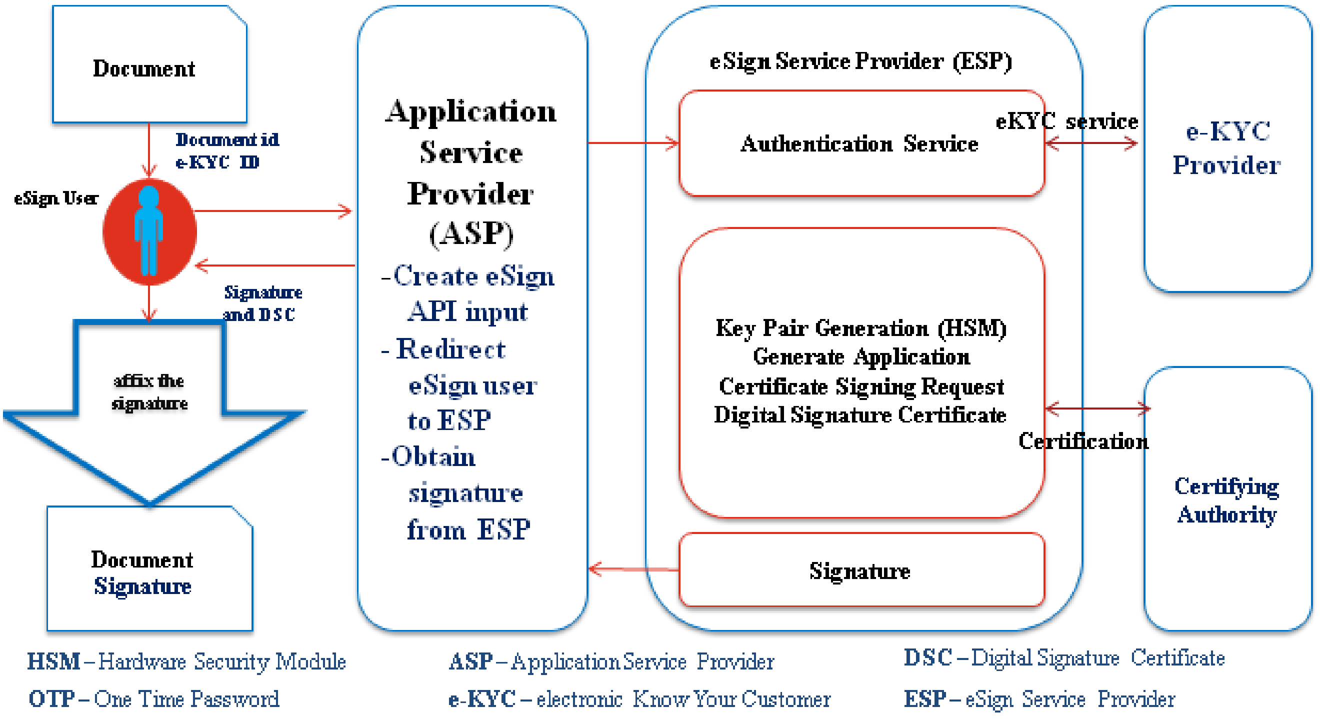
The API specifications remain common for all eSign Service providers. However, below are the things which will vary for each ESP.

- eSign Service URL
- ASP ID - Unique User ID provided by the ESP

The eSign service API can be used in different scenarios. ASPs may use:

- Single eSign Service Provider
- Multiple eSign Service Provider

The usage of single eSign Service Provider is a straight forward case. However, in case of multiple eSign service provider ASP shall have parameters configurable for each request. The routing of requests to each API can be a round-robin, a failure switchover, an end-user selection basis, or any other manner implemented by ASP.



ASP On Boarding Process for eSign

1.6. Scope

Application Service Providers (ASP) are the entities which will offer the end users, various online services through owned or operated application. However, in the case of Central or State Government, its IT department can facilitate eSign service for other departmental applications.

ASP needs to complete the on-boarding procedure with desired eSign Service Provider. On successful completion of on-boarding procedure, ESP shall grant the access to ASP for the production environment of eSign.

1.7. ASP Eligibility Criteria

A. The agency which desires to integrate eSign service should either be:

- A Central/ State Government Ministry / Department or an undertaking owned and managed by Central / State Government, or
- An Authority constituted under the Central / State Act, or
- A Not-for-profit company / Special Purpose organization of national importance, or
- A bank / financial institution / telecom company, or
- A legal entity registered in India

  Any legal entity registered in India shall be eligible subject to fulfillment of the criteria given below:

  a. Should be an organization incorporated under Companies Act, 1956, Registrar of Firms, LLP Registered; OR An association of persons or a body of individuals, in India, whether incorporated or not

  b. Should not have been blacklisted by any State Government, Central Government, Statutory, Autonomous, or Regulatory body.

1.8. Overview of on-boarding process

Below is the overview of the process, to be carried out by ASP in order to integrate eSign.

1. Application form submission by ASP.
2. Submission of supporting documents by ASP
3. Acceptance / agreement to terms of eSign service by ASP.
4. Submission of Digital Signature Certificate (public key) by ASP
5. Integration of API in ASP application in testing / preproduction environment of ESP.
6. Conducting audit and submission of Audit report by ASP
7. Grant of production access by ESP

1.9. Application form Submission

Organization intending to avail eSign service shall make a formal request to one or more ESP. Following points shall be kept in view while making an application:

1. Application form should be made specific to particular ESP. For this purpose, each ESP may share a format of application form, or ASP shall use the format in the annexure of this document by addressing it to specific ESP.

2. Application form should be submitted in original, and bear the signature / attestation of Authorized signatory of the organization.

3. In case of application form being submitted through paperless mode (email, etc), it shall be digitally / electronically signed by authorized signatory of the organization.

4. ESP shall grant the access to eSign only after receiving completed application form from ASP.

5. ESP may seek additional information over and above that already included in the application form.

1.10. Supporting Documents Submission

ASP shall submit supporting documents towards KYC verification and other requirements of on-boarding. These documents should be duly attested & forwarded by the authorized signatory of the organization.

The list of documents to be submitted shall be as given at Annexure 2.2

1.11. Acceptance / agreement to terms of eSign service

The ASP should enter / agree to the terms of service with the eSign Service Provider (ESPs) to enable eSign in their application / software. The scope of this process is:

1. To define the terms of service between ASP and ESP.
2. To define scope and obligation of ASP.
3. The terms and conditions for integration and termination of eSign service .
4. To define various inputs that are critical for success of process / activities.

Note : The sample agreement is available on the website. The eSign requirements in respect of security, consent, audit and communication shall be enforced through undertaking by ASP or an agreement between ESP and ASP

At this stage, an ASP is expected to understand the ESP services and agree to fulfill the requirements as per specifications including setting up infrastructure and aligning business process applications to the eSign services.

ASP is also expected to understand that eSign service is a regulated service under the provisions of Information Technology Act.

1.12. Digital Signature Certificate (public key) Submission by ASP

eSign is an online service provided over API. Each transaction is carried out in XML format. For the authenticity and binding of the transaction, each XML request/response Form (request / response) need to be digitally signed.

Hence, every request XML transaction needs to be digitally signed by the ASP before sending it to ESP

ASP has to submit the Digital Signature Certificate to ESP, so that ESP can configure it in their system and validate/verify each transaction received from the ASP.

Such Digital Signature Certificate should fulfill the criteria given below:

1. Should be a valid certificate issued by a CA licensed under Information technology (IT) Act.

2. Should be either an Organizational Person Digital Signature Certificate or an Organizational Document Signer Certificate. The O value in the certificate should be the legal entity name of the ASP organization.

3. Should be either Class 2 or Class 3 certificate.

4. Should be valid for at least six months from date of submission

ESP should implement necessary mechanism for mapping and carrying above validations for ASP’s Digital Signature Certificate.

1.13. Integration of API in ASP application in testing / preproduction environment of ESP.

ASP builds the required infrastructure for adopting eSign service. ESP provides access to pre-production environment and enables the ASP to establish end- to -end connectivity to carry out eSign services testing and integration

1.14. Audit: Conducting and submission of Audit report by ASP

ESP shall ensure that the ASP application is compliant to the requirement mentioned in e-authentication guidelines and all other applicable regulations. For this purpose:

1. ASP should submit the report/ certificate to ESP prior to gaining production access. The audit report shall be examined prior to completion of on-boarding.

2. ASP shall appoint eligible auditor and perform the audit.

~~3.~~ ASP shall submit the audit report in original to the ESP. Such audit report should not be older than 3 months. In case, ASP is taking service from multiple ESPs, common audit report can be submitted,

4. Audit report should comply positively to all Audit requirements. No open comments / objections should be reported by the auditor. A complete detailed checklist for Audit has been provided in Annexure 2.3.

5. ASP Audit report should be carried out by Auditor empanelled by Cert-in /IS Auditor

6. ASP should carry out the audit prior to the completion of one year from the date of completion of last audit. Audit report shall also be examined on a yearly basis by ESP by requesting a fresh audit report. ASP should submit annual compliance report with the same audit requirements and procedures provided here, upon request by ESP, within 30 days.

7. In special circumstances, ESP can initiate audit or seek audit report from ASP.

8. In respect of e-KYC compliance requirements, ESP shall carryout necessary auditing of ASP as applicable separately

1.15. Confirmation on readiness to Go Live by ASP

ASP shall notify ESP about its readiness for migration to production environment. Subsequently ASP completes the go live checklist and submits the request for Go Live checklist as provided in Annexure 2.4

ESP shall scrutinize the ASP go live request as per the Go-Live checklist and supporting documentation, before moving forward to production access.

1.16. Grant of production access by ESP

ESP shall ensure successful scrutiny of the following before granting production access:

1. Application form

2. Supporting documents

3. Acceptance of terms of service

4. Digital Signature Certificate submission

5. Integration / testing completion in preproduction / testing environment

6. Audit report

7. Go Live checklist

8. Internal approvals and clearance within ESP organization

On successful completion, ESP grants the access to production environment in the form of necessary URLs and ASP code. ESP shall ensure that such information is securely shared with the relevant person in ASP organization.

2. Annexure

2.1. Application form

ASP Application Form

Organization Name: ____

Category of Organization

□ Government Organization	□ Bank/ Financial Institution/ Telecom Company
□ Legal entity registered in India	□ Not for Profit Organization/ Special Purpose
□ Authority Constituted under Central Act	

Address:

____

Propose Business Scope____

w.r.t. eSign Service: ____

Management Point of Contact

Nodal Person Name:_________________________ Mobile No.: ___________________________________

Email-ID: _________________________________ Telephone No __________________________________

Technical Point of Contact

Nodal Person Name:_________________________ Mobile No.: ___________________________________

Email-ID:_________________________________ Telephone No __________________________________

Submitted By (*from ASP Organization*)

Signature: ____________________

Name: ____________________

Designation: ____________________

Organization: ____________________

Date: ____________________

Approved By (*from ESP*)

Signature: ___________________

Name: ___________________

Designation: ___________________

Organization: ___________________

Date: ___________________

2.2. Supporting Documents accompanying the Application

Category	Documents to be submitted
Government Organization	1. Application form. 2. KYC documents: No documents are required. 3. Audit report. 4. Go Live checklist.
Authority Constituted under Central Act	1. Application form. 2. KYC documents a. Copy of the act under which the organization is constituted. 3. Audit report. 4. Go Live checklist.
Not for Profit Organization/ Special Purpose	1. Application form. 2. KYC documents a. Letter of authority, authorizing the signatory to sign documents on behalf of the organization. b. Documentary proof for Not-for-profit company/ special purpose organization of National importance. 3. Audit report. 4. Go Live checklist.
Bank/ Financial Institution/ Telecom Company	1. Application form. 2. KYC documents a. Letter of authority, authorizing the signatory to sign documents on behalf of the organization. b. License issued by competent authority to run a bank / financial institution / telecom company in India. 3. Audit report. 4. Go Live checklist.
Legal entity registered in India	1. Application form. 2. KYC documents a. certificate of incorporation, partnership deed or any other document in support of the Agency being a legal entity registered in India b. List of names of CEO/CFO/directors/partners/trustees/person-in-charge of the agency along with the organization chart c. Letter of authority authorizing the signatory to sign documents on behalf of the organization 3. Additional documents a. Self-declaration stating that the entity has not been blacklisted by any State Government, Central Government, PSUs, Statutory, Autonomous, or Regulatory body in last five years. 4. Audit report. 5. Go Live checklist.

2.3. ASP Audit Checklist

Sl	Audit parameters	
1.	The communication between ASP and ESP should be Digitally Signed and encrypted	
2.	Communication line between ASP and ESP should be secured. It is strongly recommended to have leased lines or similar secure private lines between ASP and ESP. If a public network is used, a secure channel such as SSL should be deployed	
3.	ASP should have a documented Information Security policy in line with security standards such as ISO 27001.	
4.	Compliance review of controls as per Information security policy	
5.	ASPs should follow standards such as ISO 27000 to maintain Information Security	
6.	Compliance to prevailing laws such as IT Act 2000 should be ensured	
7.	Software to prevent malware/virus attacks may be put in place and anti-virus software installed to protect against viruses. Additional network security controls and end point authentication schemes may be put in place.	
8.	Resident consent process must be implemented to obtain consent for every transaction carried out. The user must be asked for willingness to sign it and consent form should be stored .	
9.	Application Security Assessment of the ASP by Cert-in empanelled auditor /IS Auditor	
10.	ASP data logging for audit purposes provisioned.	
11.	ASP should not delegate any obligation to external organizations or applications.	
12.	ASP integrate with ESPs through standard eSign APIs only	
13.	Provision for providing/accessing the copy of the signed document to the signer	
14.	ASP shall display (and allow download/print) the document that is to be signed clearly for subscribers to read before signing.	
15.	ASP shall protect the document URL (available within eSign request) from anyone or any system accessing it using URL and also from virus, malware, etc.	
16.	Indemnify both ESP and CA for integrity related discrepancies arises at ASP end	

2.4. Go Live Checklist

ASP Go live Checklist

Go Live Checklist *		
1.	ASP data logging for audit purposes provisioned	□
2.	ASP has conducted end-to-end testing for 50 no of successful transactions in Pre-production environment	□

**All the above items are mandatory and need to be completed before submitting for go live approval to ESP. For additional information on the above checklist items please contact the corresponding ESP*

We understand that production ASP licence will be provided post ESP approval of this checklist. ASP hereby confirms compliance to the current standards and specifications as published.

Submitted By (*from ASP Organization*)

Signature: ________________________

Name: ________________________

Designation: ________________________

Organization: ________________________

Date: ________________________

Approved By (*from ESP*)

Signature: ________________________

Name: ________________________

Designation: ________________________

Organization: ________________________

Date: ________________________

****

MCX Circular No. MCX/MCXCCL/353/2023 May 31, 2023
MCXCCL Circular No. MCXCCL/TECH/141/2023

System Audit for Clearing Member

In terms of the provisions of the Rules, Bye-Laws and Regulations of the Multi Commodity Exchange Clearing Corporation Limited (MCXCCL), Clearing Members of the MCXCCL are notified as under:

In reference to the SEBI circular no. CIR/MRD/DMS/34/2013 dated November 06, 2013, related to “Annual System Audit of Stock Brokers/Trading Members” and SEBI advisory to extend the mentioned circular pertaining to System Audit to Clearing Members (CM).

Members are required to conduct Annual System Audit as per the framework enclosed as **Annexure-1** and Terms of Reference (TOR) enclosed as **Annexure-2**. CMs are also required to maintain a list of all the relevant SEBI/MCXCCL issued circulars/ directions/ advice, etc. pertaining to technology and compliance thereof, as per format enclosed as **Annexure-3** and Exception Observation Report as per format enclosed as **Annexire-4** and the same shall be included under the scope of System Audit.

Please note that the guidelines to submit the reports, annexed with this circular shall be **effective from immediate**.

Members are requested to take note of the same.

Anilkumar Varma
CTO

Kindly contact Customer Service Team on 022 – 6649 4040 or send an email at customersupport@mcxindia.com for any clarification.

Annexure-1

System audit Framework for Clearing Members

Audit Process

1. For the System audit, the following broad areas shall be considered in order to ensure that the audit is comprehensive and effective:

   a. The Audit shall be conducted according to the Norms, Terms of Reference (TOR) and Guidelines issued by SEBI.

   b. The Governing Board of the Clearing Members (CM) shall appoint the Auditors based on the prescribed Auditor Selection Norms and TOR.

   c. 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.

   d. 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.

   e. 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 sub-clause c above.

   f. 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.

   g. The audit shall be conducted once in a financial year and period of audit shall be 12 months. Further, the audit shall be completed within 2 months from the end of the audit period.

   h. 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, Clearing

Corporation, internal policy of the CM, 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.

i. For each of the NCs/ observations and suggestions made by the Auditor, specific corrective action as deemed fit may be taken by the CM. The management of the CM 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.

j. The Audit report along with the comments of management shall be placed before the Governing Board of the CM. The Audit report along with comments of the Governing Board shall be submitted to Clearing Corporation, within 1 month of completion of audit.

k. The follow-on audit should be completed within one month of the corrective actions taken by the CM. After the follow-on audit, the CM shall submit a report to Clearing Corporation 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.

l. In cases wherein follow-on audit is not required, the CM shall submit an Action Taken Report (ATR) to the Auditor. After verification of the ATR by the Auditor, the CM shall submit a report to Clearing Corporation 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.

m. The overall timeline from the last date of the audit period till completion of final compliance by CM, including follow-on audit, if any, should not exceed one year/6 months(as applicable). In exceptional cases, if CM is of the view that compliance with certain observations may extend beyond said period, then the concerned CM shall seek specific approval from the Governing Board.

Auditor Selection Norms

2. CM shall ensure compliance with the following norms while appointing Auditor:

a. The Auditor must have minimum 3 years of demonstrable experience in IT audit of securities market participants e.g. stock brokers, clearing members, exchanges, clearing corporations, depositories, intermediaries, etc. and/ or financial services sector i.e. banking, insurance, Fin-tech etc.

b. The team performing system 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 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).

c. 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.

d. The Auditor should have the capability to undertake forensic audit and undertake such audit as part of system audit , if required.

e. The Auditor must not have any conflict of interest in conducting fair, objective and independent audit of the clearing member. It should not have been engaged over the last three years in any consulting engagement with any departments / units of the entity being audited.

f. The Auditor should not have any cases pending against it, which point to its incompetence and/or unsuitability to perform the audit task.

g. The proposed audit agency must be empanelled with CERT-In.

h. Any criteria, in addition to the aforesaid criteria, that the CM may deem fit for the purpose of selection of Auditor.

<u>Audit Report Guidelines</u>

3. The Audit report should cover each of the major areas mentioned in the TOR and compliance with SEBI and Clearing Corporation 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. The report should also include tabulated data to show NCs / observations for each of the major areas in the TOR.
5. The audit report to include point-wise compliance of areas prescribed in Terms of Reference (TOR) and areas emanating from relevant SEBI and Clearing Corporation circulars/directions/advices along with any accompanying evidence.

6. Evidences should be specified in the audit report while reporting/ closing an issue.
7. A detailed report with regard to the system audit shall be submitted to Clearing Corporation. 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 & Clearing Corporation circulars / norms and internal policies of CM	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

Issue Log Column Heading	Description	Responsibility
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

Annexure-2
System audit Program – Terms of Reference (TOR)

1. The scope of audit shall encompass all the IT resources including hardware, software, network, policies, procedures etc. of CMs (Primary Data Centre (PDC), Disaster Recovery Site (DRS) and Near Site (NS))

2. **IT environment**

   2.1. Organization details

   a. Name

   b. Address

   c. IT team size (in house- employees)

   d. IT team size (vendors)

   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 CM.

   d. System Architecture

   e. Network architecture

   f. Telecommunication network

3. **IT Governance**

   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;

   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

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 CM?

4. Business Controls

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 CM

4.2. Risk Management System (RMS)

a. Online risk management capability – The system auditor should check whether system of online risk management including upfront real-time risk management, is in place for all orders placed through (CTCL or IML) / IBT / DMA / STWT.

b. Trading Limits – Whether a system of pre-defined limits /checks such as Order Quantity and Value Limits, Symbol wise User Order / Quantity limit, User / Branch Order Limit, Order Price limit, etc., are in place and only such orders which are within the parameters specified by the RMS are allowed to be pushed into exchange trading engines. The system auditor should check that no user or branch in the system is having unlimited limits on the above parameters.

c. Order Alerts and Reports – Whether the system has capability to generate alerts when orders that are placed are above the limits and has capability to generate reports relating to margin requirements, payments and delivery obligations.

d. Order Review – Whether the system has capability to facilitate review of such orders that were not validated by the system.

e. Back testing for effectiveness of RMS – Whether system has capability to identify trades which have exceeded the pre-defined limits (Order Quantity and Value Limits, Symbol wise User Order / Quantity limit, User / Branch Order Limit, Order Price limit) and also exceed corresponding margin availability of clients. Whether deviations from such pre-defined limits are captured by the system, documented and corrective steps taken.

f. Log Management – Whether the system maintains logs of alerts / changes / deletion / activation / deactivation of client codes and logs of changes to the risk management parameters mentioned above. Whether the system allows only authorized users to set the risk parameter in the RMS.

4.3. 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. Software Testing framework, methodology and process guideline

p. Any other controls, as deemed fit, by the CM

4.4. Data Communication/ Network Controls

a. Network Administration – Redundancy, Monitoring, breakdown resolution etc.

b. WAN Management – Connectivity provisions for business continuity.

c. Connection Permissions – Restriction on need to have basis

d. Fallback Mechanism – Dial-up connections controls etc.

e. Incidences of access violations observed in the previous report & corrective actions taken, if any

f. Any other controls, as deemed fit, by the CM

4.5. Security Controls

a. Email Archival Implementation

4.6. Access Policy and Controls

a. Review of access logs

b. Access rights and roles review procedures for all systems

c. Segregation of Duties (SOD) matrix describing key roles

d. Risk acceptance for violation of SOPs and alternate mechanism put in place

e. Privileged access to system and record of logs,

f. Periodic monitoring of access rights for privileged users

g. Authentication mechanisms used for access to systems including use of passwords, One Time Passwords (OTP), Single Sign on, etc.

h. Any other controls, as deemed fit, by the CM

4.7. Electronic Document Controls

4.8. General Access Controls

4.9. 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

4.10. Business Continuity / Disaster Recovery Facilities

a. Back-up procedures and recovery mechanism using back-ups.

b. Storage of Back-up (Remote site, DRS etc.)

c. Redundancy – Equipment, Network, Site etc.

d. DRS installation and Drills - Management statement on targeted resumption capability (in terms of time required & extent of loss of data)

e. Evidence of achieving the set targets during the DR drills in event of various disaster scenarios.

f. User awareness and training

g. Is annual review of BCP-DR or in case of major change in business/ infrastructure undertaken?

h. Is quarterly review regarding implementation of BCP policy done by Standing Committee of Technology (SCOT) of the CM?

i. Testing of BCP-DR plan through appropriate strategies including simulations, DR drills, system recovery, etc.

j. Is the recordkeeping of quarterly DR drills, live trading sessions from DRS being maintained?

k. Is BCP-DR policy document prepared and implemented in line with SEBI circular on BCP and DR of CM?

4.11. 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.

5. Entity Specific Software used for or in support of trading/clearing systems / peripheral systems and critical processes

6. **Human Resources Management**

6.1. Screening of Employee, Third party vendors / contractors

6.2. Onboarding

6.3. Offboarding

6.4. Consequence Management (Incident / Breach of policies)

6.5. Awareness and Trainings

6.6. Non-Disclosure Agreements (NDAs) and confidentiality agreement

7. **Network audit**

7.1. The audit shall require tracing of the connectivity and network diagram based on the physical audit.

7.2. The audit shall cover the link, the path, device-level redundancy, no single-point failures, high availability, and fault tolerance aspects in the network.

7.3. Network health monitoring and alert system

7.4. Service level definition for vendors/Service level management

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.

9. **E-Mail system**

9.1. Existence of policy for the acceptable use of electronic mail

9.2. Regulations governing file transfer and exchange of messages with external parties

9.3. Rules based on which e-mail addresses are assigned

9.4. Storage, backup and retrieval

10. **Redressal of Technological Complaints**

10.1. Ageing analysis of technology complaints

10.2. Whether all complaints received are brought to their logical conclusion?

11. **Any other Item(s)**

11.1. Electronic Waste Disposal

11.2. Observation(s) based on previous Audit Report (s)

11.3. Any other specific area(s) that may be informed by Clearing Corporation & SEBI.

Annexure-3

Format for monitoring compliance with requirements emanating from SEBI and Clearing Corporation (CC) circulars/guidelines/advisories related to technology

Sl. No.	Date of SEBI/CC circular/ directions/ advice, etc.	Subject	Technological requirements specified by SEBI/CC in brief	Mechanism put in place by the CMs	Non compliances with SEBI/CC circulars/ directions, etc.	Compliance status (Open/ closed)	Comments of the Management	Time-line for taking corrective action in case of open observations

Annexure-4

Exception Observation Reporting Format

Note: CMs are expected to submit following information with regard to exceptional major non-compliances (NCs) / minor NCs observed in the System audit. CMs should also categorically highlight those observations/NCs/suggestions pointed out in the System audit (current and previous) which are not yet complied with.

Name of the CM:______________________

Name of the Auditor:______________________

Systems and Network Audit Report Date:_______________________

Table 1: For preliminary audit

Audit period	Observation No.	Description of finding	Department of CM	Status / Nature of finding	Risk Rating of finding 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 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

<u>Table 2: For follow on/ follow up system audit</u>

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 audit report

2. **Preliminary Corrective Action** – The original corrective action as prescribed in the preliminary System 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.

The Gazette of India

EXTRAORDINARY

PUBLISHED BY AUTHORITY

RESERVE BANK OF INDIA

NOTIFICATION

Mumbai, the 22nd September, 2021

Subsidiary General Ledger Account: Eligibility Criteria and Operational Guidelines

No. IDMD.CDD.S788/11.22.001/2021-22. - In exercise of the powers conferred by Section 4 of the Government Securities Act, 2006 (38 of 2006) (the Act), the Reserve Bank of India (the Bank) hereby specifies the conditions applicable henceforth for opening and maintenance of a Subsidiary General Ledger (SGL) account.

I. A Subsidiary General Ledger (SGL) Account shall mean an account opened and held with the Bank for holding or/and transacting in Government Securities.

II. The Bank may open and maintain SGL accounts for conduct of its operations and for such purposes the Bank may deem necessary.

III. Eligible Entities:

The entities mentioned below are eligible to open and maintain an SGL account with the Bank:

i. Licensed Banks
ii. Primary Dealers authorised by Reserve Bank of India
iii. Financial institutions as defined in terms of Section 45-I (c) (ii) of the Reserve Bank of India Act, 1934 (2 of 1934)
iv. Central Government
v. State Governments
vi. Insurance Companies regulated by Insurance Regulatory and Development Authority
vii. Mutual Funds regulated by Securities and Exchange Board of India
viii. Provident and Pension Funds and Pension Fund Managers
ix. Foreign Central Banks with prior approval of the Bank
x. Depositories as defined under the Depositories Act 1996
xi. Stock Holding Corporation of India (SHCIL)
xii. Such other entities as may be allowed by the Bank from time to time

IV. Conditions for Opening & Maintenance of the SGL account:

i. An eligible entity, will in normal circumstances, be allowed to open and maintain only one SGL account. In certain cases, the Bank may allow an entity to open additional SGL accounts. An SGL account can be opened at its Public Debt Offices, as may be decided by the Bank from time to time.

ii. An SGL account holder shall not be eligible to open a constituent account with any Constituents' Subsidiary General Ledger (CSGL) account holder without specific approval from the Bank except in cases where the accounts are required to be opened for regulatory/margin maintenance purposes.

iii. An SGL account holder may be allowed to maintain a current account with the Bank to settle the funds in respect of transactions pertaining to the SGL account subject to obtaining specific approval of the Bank. An SGL account holder also has the option to maintain a settlement account with any designated settlement bank.

iv. The entity opening an SGL account shall submit an application form, indemnity bond and such other documents, as may be decided by the Bank from time to time.

v. The transfer of securities from/to an SGL account shall be on Delivery versus Payment basis, except as provided in paragraph vi. of the guidelines.

vi. Value Free Transfer (VFT): For the purpose of these guidelines, Value Free Transfer (VFT) of the securities shall mean transfer of securities from one SGL account to another SGL or CSGL account without corresponding payment leg in the books of RBI. Value Free Transfers of securities shall be effected by SGL holders in the manner as may be prescribed by the Bank.

vii. An SGL account can be closed by the account holders by submitting a request mentioning therein the reason(s) for closure and action, if any, required to be taken by the Bank in respect of the Government securities held in such an SGL account.

viii. The SGL holders shall abide by these Guidelines on a continuous basis. Any failure to do so will attract appropriate action by the Bank including application of penal provisions under Section 30 of the Act. A declaration to this effect shall be submitted to PDO, Mumbai on an annual basis.

ix. The Bank may at any time direct an SGL account holder to furnish to the Bank, in such form, at such intervals and within such time, such statements, information or particulars relating to the SGL account or connected with transactions in the SGL account.

x. Any misuse of the SGL facility by the entity concerned, will make the entity liable to be debarred from holding of such an account as mentioned in Section 27 of the Act, in addition to inviting the penalties as provided in Section 30 of the Act.

xi. The Reserve Bank, on being satisfied that it is necessary to do so, may exempt any SGL account holder or a class of SGL account holders either generally or for such period as may be specified, from any or all of the provisions of these Guidelines, subject to such terms or conditions or limitations or restrictions as it may think fit and proper to impose, in the interest of public or financial system of the country.

xii. These guidelines are issued in supersession of the earlier guidelines issued by the Bank vide Notification No. 1078 dated October 29, 2018 (published in The Gazette of India – Extraordinary – Part III – Section 4).

(R Subramanian)
Executive Director
Reserve Bank of India

The Gazette of India

EXTRAORDINARY

PUBLISHED BY AUTHORITY

RESERVE BANK OF INDIA

NOTIFICATION

Mumbai, the 22nd September, 2021

Constituents' Subsidiary General Ledger Account: Eligibility Criteria and Operational Guidelines

No. IDMD.CDD. S788/11.22.001/2021-22.—In exercise of the powers conferred by Section 4 of the Government Securities Act, 2006 (38 of 2006) (the Act), the Reserve Bank of India (the Bank) hereby specifies the conditions applicable henceforth for opening and maintenance of a Constituents' Subsidiary General Ledger (CSGL) account, as also the records to be maintained and procedures to be adopted by the CSGL account holders for safeguarding the interests of their constituents.

I. A Constituent Subsidiary General Ledger (CSGL) shall mean a subsidiary general ledger (SGL) account opened and maintained with the Bank by an agent on behalf of the constituents of such agent;

II. The Bank may open and maintain CSGL accounts for conduct of its operations and for such purposes the Bank may deem necessary.

III. Eligible Entities:

The entities mentioned below are eligible to open and maintain a CSGL account with the Bank on behalf of their constituents-also known as ‘Gilt Account Holders’ (GAHs):

i. Licensed banks with minimum net worth of Rs.100 cr.
ii. Primary Dealers authorised by Reserve Bank of India
iii. Depositories as defined under Depositories Act 1996
iv. Clearing Corporation of India Limited or other Clearing Corporations as may be approved by the Bank
v. National Bank for Agriculture and Rural Development (NABARD)
vi. Stock Holding Corporation of India Ltd (SHCIL)
vii. Such other entities as may be allowed by the Bank from time to time.

IV. Operational Guidelines to be complied with by the CSGL Account Holders

i. An eligible entity will, in normal circumstances, be allowed to open and maintain only one CSGL account. In certain cases, the Bank may allow an entity to open additional CSGL accounts. A constituent is not permitted to open and maintain an SGL account with the Bank (except when the SGL account has been opened after specific approval of the Bank or for regulatory/margin purposes).

ii. The CSGL account holders shall ensure that the constituents for whom the gilt accounts are opened/maintained satisfy the eligibility conditions for holding Government securities in terms of the General Loan Notifications as also the specific Loan Notifications issued by the Government.

iii. The CSGL account holders, who are regulated by the Bank, shall follow guidelines on 'Know Your Customer' (KYC) Direction, 2016 issued by the Bank and as amended from time to time, in respect of their constituents. Other CSGL account holders shall follow the relevant guidelines on KYC issued by their respective regulators. The gilt accounts opened with a CSGL holder shall have unique numbers.

iv. A constituent is permitted to open one or more gilt account with any of the CSGL account holders. This permission will be subject to the relevant guidelines/instructions on their operations, if any, issued by the constituent’s respective regulators.

v. The transfer of securities from/to a CSGL account shall be on Delivery versus Payment basis, except as provided in paragraph vi. of the guidelines.

vi. Value Free transfer - For the purpose of these Guidelines, Value Free Transfers (VFT) of the securities shall mean transfer of securities from one CSGL account to another CSGL or SGL account without corresponding payment leg in the books of RBI. Value Free Transfers of securities shall be effected by CSGL holders in the manner as may be prescribed by the Bank.

vii. The CSGL account holders must have appropriate Information Technology (IT) infrastructure to maintain accounts and put through deals on behalf of their constituents with adequate contingency/back-up plan to ensure business continuity. The IT infrastructure shall be subject to Information System (IS) audit by certified professionals every year and any observations made by them shall be immediately complied with.

viii. The CSGL account holder shall execute with their constituents an agreement, which shall categorically mention the circumstances under which they will accept/release securities and accept/release funds on behalf of the constituents, as also the rights and obligations of the constituents, and the grievance redressal mechanism available for the constituents.

ix. The CSGL account holders shall ensure that deals/transactions pertaining to constituents are put through according to the instructions of the constituents concerned and appropriate records are maintained for such instructions received from their constituents. The CSGL account holder shall refrain from setting off Government securities in the CSGL account or otherwise deal with the Government securities to extinguish partly or fully any amounts due to it from the constituents without a written consent from the constituents.

x. The CSGL account holder shall be accountable/responsible for the movement of Government securities from/to the CSGL account and shall provide system generated audit trail, whenever called for by the constituent or the Bank.

xi. The CSGL account holders shall issue/post a deal slip for each buy/sell transaction put through on behalf of the constituents concerned on the transaction date itself mentioning therein the details of the deal, such as, ISIN, instrument nomenclature, buy/sell quantity, buy/sell price, service charges, etc. Further, the CSGL account holder shall send statements mentioning the outstanding/transaction details of Government securities to each constituent as per the agreement as also at the specific request of the constituents and obtain a balance confirmation certificate from the constituents.

xii. The CSGL account holder shall credit the constituents' fund account with the due amount of interest/redemption proceeds on due date itself and maintain appropriate record of the same for verification.

xiii. The CSGL account holder shall be responsible for settlement of each deal put through on behalf of the constituents and any shortfall in securities/funds will be treated as a case of SGL deal bouncing against the CSGL account holder. Further, the CSGL account holder, before submitting any deals on behalf of the constituents, shall ensure that the particular constituent is eligible, as per the latest guidelines issued by the Bank, for entering into such transactions/deals.

xiv. The CSGL account holders shall have a well-documented operational manual, duly approved by their Board, highlighting the roles/responsibilities of the dealers/mid-office/back-office and the resultant checks and balances to ensure proper dealings on behalf of the constituents so as to mitigate any risk arising out of such custodial business to the CSGL account holder as also to the constituents.

xv. The CSGL account holders shall ensure daily reconciliation of outstanding balances in their CSGL account as per the E-kuber data vis-à-vis the constituent-wise holding details maintained by them. Any mismatch in the outstanding balances shall be immediately brought to the notice of E-kuber Helpdesk, Department of Information Technology (DIT) and Public Debt Office (PDO), Mumbai to ensure reconciliation of balances before next day-end.

xvi. The CSGL account holders must put the operations of their CSGL account, as also the transactions in the gilt accounts of their constituents, under the purview of their Concurrent Auditors, who shall verify and comment, inter alia, upon the following aspects of CSGL account transactions:

a) Completion of documents for opening the constituent account;
b) Authorisation of each transaction in the CSGL account by the constituent concerned and that the securities bought/sold have been credited/debited to the gilt account on due date;

c) Issuance of debit/credit advices on time to the constituents for each transaction put through on their behalf;
d) Reconciliation of the outstanding balances in the CSGL account vis-à-vis the constituent-wise holding details on a daily basis;
e) Receipt of balance confirmation certificates from the constituents on half-yearly basis;
f) Crediting of interest/redemption proceeds to the constituents' fund account on due date; and
g) Ensuring the eligibility of the constituent, as per latest guidelines issued by the Bank, to put through the deal/transaction and that the deal price is in line with the prevailing market rates.

xvii. The CSGL account holders shall put up the information system audit report as also the concurrent auditor's report in respect of CSGL account to the Audit Committee of the Board on a quarterly basis or at more frequent intervals. The CSGL account holder may submit a quarterly certificate, confirming that the compliance of the audit observations, as also daily reconciliation exercise carried out by them, has been placed before the Audit Committee of the Board, to PDO, Mumbai (pdomumbai@rbi.org.in).

xviii. The Bank may at any time direct the CSGL Account holder to furnish to the Bank, in such form, at such intervals and within such time, such statements, information or particulars relating to CSGL account or connected with transactions in the CSGL account.

xix. The CSGL account holder shall submit constituent-wise holding details electronically, as per Annex to the Chief General Manager, Reserve Bank of India, Internal Debt Management Department, Central Office Building, 23rd Floor, Fort, Mumbai - 400001 (email id: cgmidmd@rbi.org.in) on a quarterly basis as on March 31, June 30, September 30 & December 31, by the 1st week of the following month.

xx. The CSGL account holders shall furnish copies of half-yearly review reports, as on March 31 and September 30 each year, of investments in the CSGL account on behalf of constituents, including brokers, to the Internal Debt Management Department of the Bank.

xxi. The CSGL holders shall abide by these Guidelines on a continuous basis. Any failure to do so will attract appropriate action by the Bank including application of penal provisions under Section 30 of the Act. A declaration to this effect shall be submitted to PDO, Mumbai on an annual basis.

xxii. Notwithstanding anything contained in these guidelines, the Reserve Bank reserves the right to take any action including temporary or permanent debarment of the CSGL account holder, as mentioned in Section 27 of the Act, in addition to inviting the penalties as provided in Section 30 of the Act for violation of the terms and conditions of the opening and maintenance of CSGL accounts or misuse of the CSGL facility by the entity concerned or breach of the operational guidelines issued from time to time.

xxiii. The Reserve Bank, on being satisfied that it is necessary to do so, may exempt any CSGL account holder or class of CSGL account holders either generally or for such period as may be specified, from any or all of the provisions of these Guidelines, subject to such terms or conditions or limitations or restrictions as it may think fit and proper to impose, in the interest of public or financial system of the country.

xxiv. These guidelines are issued in supersession of the earlier guidelines issued by the Bank vide **Notification No.** 1078 dated October 29, 2018 (published in The Gazette of India – Extraordinary – Part III – Section 4).

(R Subramanian)
Executive Director
Reserve Bank of India

Annex

Statement on Ownership Pattern of Government Securities Held in the Gilt Accounts as on Quarter ended

Name of the CSGL account holder:

CSGL account number:

Sr. No.	Name of Constituent	Investor Group@	Type of Security^	ISIN	Face Value
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					

@ Commercial Banks/ State or Dist. Central Co-op Banks/ Urban Co-operative Banks/ Mutual Funds/ Insurance Companies/ Financial Institutions/ Corporates/ HUF/ Individuals/ FPIs/ Provident Funds/ Others

^ Central Government Dated Security/ T-Bills/State Government Securities/Others (please specify)

भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

CIRCULAR

SEBI/HO/IMD/DF2/CIR/P/2019/12 **January 10, 2019**

**All Mutual Funds/
Asset Management Companies (AMCs)/
Trustee Companies/ Boards of Trustees of Mutual Funds/
Association of Mutual Funds in India (AMFI)**

Dear Sir / Madam,

Sub: Cyber Security and Cyber Resilience framework for Mutual Funds / Asset Management Companies (AMCs)

1. With rapid technological advancement in securities market, there is greater need for maintaining robust cyber security and to have cyber resilience framework to protect integrity of data and guard against breaches of privacy.

2. As part of the operational risk management, the Mutual Funds / Asset Management Companies (AMCs) need to have robust cyber security and cyber resilience framework in order to provide essential facilities and services and perform critical functions in securities market.

3. Based on the recommendation of SEBI's High Powered Steering Committee - Cyber Security, it has been decided that the framework prescribed vide SEBI circular CIR/MRD/DP13/2015 dated July 06, 2015 on cyber security and cyber resilience also be made applicable to all Mutual Funds / AMC. Accordingly, all Mutual Funds / AMCs shall comply with the provisions of Cyber Security and Cyber Resilience as placed at **Annexure-1**.

4. Mutual Funds / AMCs are advised to take necessary steps to put in place systems for implementation of this circular. The guidelines annexed with this circular shall be effective from April 1, 2019.

5. This circular is issued in exercise of powers conferred under Section 11 (1) of the Securities and Exchange Board of India Act, 1992, read with the provisions of 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.

Yours faithfully,

**Harini Balaji
General Manager
Investment Management Department
Tel No. 022-26449372
Email: harinib@sebi.gov.in**

Annexure - 1

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. As part of the operational risk management framework to manage risk to systems, networks and databases from cyber-attacks and threats, Mutual Funds/ Asset Management Companies (AMCs) 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 of the AMC and Trustees, 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 Board of AMC at least once annually with the view to strengthen and improve its cyber security and cyber resilience framework.

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. The Cyber security policy should encompass the principles prescribed by National Critical Information Infrastructure Protection Centre (NCIIPC) of National Technical Research Organization (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.

5. Mutual Funds/ AMCs 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.

6. Mutual Funds/ AMCs 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 AMCs.

7. The Board of the AMCs shall constitute a Technology Committee comprising experts proficient in technology. This Technology Committee should on a quarterly basis review the implementation of the cyber security and cyber resilience policy approved by their Board, 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 a plan to improve and strengthen cyber security and cyber resilience. The review shall be placed before the Board of the AMCs and Trustees for appropriate action.

8. Mutual Funds/ AMCs should establish a reporting procedure to facilitate communication of unusual activities and events to CISO or to the senior management in a timely manner.

9. The aforementioned committee and the senior management of the AMCs, 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.

10. Mutual Funds/ AMCs 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 the Mutual Funds/ AMCs, towards ensuring the goal of cyber security.

Identify

11. Mutual Funds/ AMCs should identify critical assets based on their sensitivity and criticality for business operations, services and data management and 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.

12. Mutual Funds/ AMCs 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.

13. Mutual Funds/ AMCs should also encourage its third-party service providers, if any, such as RTAs, Custodians, Brokers, Distributors, etc. to have similar standards of Information Security.

Protection

Access Controls

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

15. Any access to AMC's/ Mutual Fund's systems, applications, networks, databases, etc., should be for a defined purpose and for a defined period. AMCs/MFs 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.

16. Mutual Funds/ AMCs 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.

17. Mutual Funds/ AMCs 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.

18. Mutual Funds/ AMCs 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.

19. Account access lock policies after failure attempts should be implemented for all accounts.

20. Employees and outsourced staff such as employees of vendors or service providers, who may be given authorized access to the Mutual Fund's/ AMC's critical systems, networks and other computer resources, should be subject to stringent supervision, monitoring and access restrictions.

21. Two-factor authentication at log-in should be implemented for all users that connect using online/ internet facility.

22. Mutual Funds/ AMCs 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.

23. Proper 'end of life' mechanism should be adopted to deactivate access privileges of users who are leaving the organization or whose access privileges have been withdrawn.

Physical Security

24. Physical access to the critical systems should be restricted to minimum. Physical access of outsourced staff or visitors should be properly supervised by ensuring at the minimum that outsourced staff or visitors are accompanied at all times by authorized employees.

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

26. Mutual Funds/ AMCs should ensure that the perimeter of the critical equipments rooms 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

27. Mutual Funds/ AMCs 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 Mutual Funds/ AMCs should conduct regular enforcement checks to ensure that the baseline standards are applied uniformly.

28. Mutual Funds/ AMCs should install network security devices, such as firewalls as well as intrusion detection and prevention systems, to protect their IT infrastructure from security exposures originating from internal and external sources.

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

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.

31. Mutual Funds/ AMCs 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.

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.

33. Mutual Funds/ AMCs should allow only authorized data storage devices through appropriate validation processes.

Hardening of Hardware and Software

34. Only a hardened and vetted hardware / software should be deployed by the Mutual Funds/ AMCs. During the hardening process, Mutual Funds/ AMCs should inter-alia ensure that default passwords are replaced with strong passwords and all unnecessary services are removed or disabled in equipments / software.

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

36. Mutual Funds/ AMCs 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

37. Mutual Funds/ AMCs should establish and ensure that the patch management procedures include the identification, categorization and prioritization of security patches. An implementation timeframe for each category of security patches should be established to implement security patches in a timely manner.

38. Mutual Funds/ AMCs 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

39. Mutual Funds/ AMCs 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)

40. Mutual Funds/ AMCs should regularly conduct vulnerability assessment to detect security vulnerabilities in the IT environment. Mutual Funds/ AMCs 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.

41. Remedial actions should be immediately taken to address gaps that are identified during vulnerability assessment and penetration testing.

42. In addition, Mutual Funds/ AMCs should perform vulnerability scanning and conduct penetration testing prior to the commissioning of a new system which offers internet accessibility and open network interfaces.

Monitoring and Detection

43. Mutual Funds/ AMCs should establish appropriate security monitoring systems and processes to facilitate continuous monitoring of security events and timely detection of unauthorized or malicious activities, unauthorized changes, unauthorized access and unauthorized 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.

44. Further, to ensure high resilience, high availability and timely detection of attacks on systems and networks, Mutual Funds/ AMCs should implement suitable mechanism to monitor capacity utilization of its critical systems and networks.

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

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.

47. The response and recovery plan of the Mutual Funds/ AMCs 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) 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.

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

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.

50. Mutual Funds/ AMCs should also conduct suitable periodic drills to test the adequacy and effectiveness of response and recovery plan.

Sharing of information

51. Quarterly reports containing information on cyber-attacks and threats experienced by Mutual Funds/ AMCs and measures taken to mitigate vulnerabilities, threats and attacks including information on bugs / vulnerabilities / threats that may be useful for other AMCs/MFs should be submitted to SEBI in a soft copy.

52. Such details as are felt useful for sharing with other Mutual Funds/ AMCs in masked and anonymous manner shall be shared using mechanism to be specified by SEBI from time to time.

Training

53. Mutual Funds/ AMCs 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.

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

Periodic Audit

55. AMCs / Mutual Funds shall arrange to have its systems audited on an annual basis by an independent CISA / CISM qualified or CERT-IN empanelled auditor to check compliance with the above areas and shall submit the report to SEBI along with the comments of the Board of AMCs and Trustees within three months of the end of the financial year.

Vendors or Service Providers

56. AMCs / MFs have outsourced many of their critical activities to different agencies / vendors / service providers. The responsibility, accountability and ownership of those outsourced activities lies primarily with AMCs / MFs. Therefore, AMCs / MFs have to come out with appropriate monitoring mechanism through clearly defined framework to ensure that all the requirements as specified in this circular is complied with. The periodic report submitted to SEBI should highlight the critical activities handled by the agencies and to certify the above requirement is complied. The provisions of this circular shall also apply to those RTAs which serves AMCs as the in-house RTAs of the AMCs.

****

CIRCULAR

SEBI/HO/MIRSD/TPD/P/CIR/2022/80 **June 07, 2022**

To

All Recognised Stock Exchanges and Depositories

Dear Sir/ Madam,

<u>Sub: - Modification in Cyber Security and Cyber resilience framework for Stock Brokers / Depository Participants</u>

SEBI vide circular SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 03, 2018 prescribed framework for Cyber Security and Cyber Resilience for Stock Brokers / Depository Participants.

2. In partial modification to Annexure -1 of SEBI circular dated December 03, 2018, the paragraph-11, 41, 42 and 44 shall be read as under:

11. Stock Brokers / 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 Stock Brokers / Depository Participants shall approve the list of critical systems.

To this end, Stock Brokers / 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.

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.*

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 empaneled 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.

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.*

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

4. Stock Brokers / Depository Participants shall take necessary steps to put in place systems for implementation of the circular.

5. All Stock Brokers / Depository Participants are directed to communicate the status of the implementation of the provisions of this circular to Stock Exchanges / Depositories within 10 days from the date of this Circular.

6. Stock Exchanges and Depositories shall;
   a) make necessary amendments to the relevant byelaws, rules and regulations for the implementation of the above direction; and
   b) bring the provisions of this circular to the notice of their members/participants and also disseminate the same on their websites.

7. The provisions of the Circular shall come into force with immediate effect.

8. This circular is being issued in exercise of powers conferred under Section 11 (1) of the Securities and Exchange Board of India Act, 1992 to protect the interests of investors in securities and to promote the development of, and to regulate the securities market.

Yours faithfully,

Vishal M Padole
Deputy General Manager
MIRSD
Tel. No: 022 26449247
Email ID: vishalp@sebi.gov.in

Annexure -17
Sample Red Team Flags / Objectives

Sr. No.	Domain/ Area	Target Objective	Evidence
1	Identity and Access Management	Access to a Domain Admin Account	Change a user's properties / Add a new user account/ Screenshot
2	Communication Infrastructure	Compromise Email Infrastructure	Access Senior Exec's emails / Send Phishing emails from a company Internal account
	Compromise Messaging Infrastructure		Access Senior Exec's chats / Send messages with malicious links from a legitimate account
3	Compromise Internal Collaboration Portals	Privileged access to SharePoint / Confluence / Jive	Access to restricted content / Portal admin access / Host malicious files
4	Security Infrastructure	Privileged Access to IDS	Privileged Access to IDS Logs
		Access to SIEM	Access to Collected Logs
		Privileged access to Perimeter Firewall	Firewall admin access screenshot
5	Internal Project Management Systems	Access to Sensitive Corporate Data	Account admin access / Portal admin access / Record tampering / Access to financial reports or customer details
6	Network Routing Infrastructure	Privileged access to DNS servers	Poison DNS with a malicious record
		Privileged access to edge routers	Root access
7	Enterprise Segregation Controls	Access sensitive systems	Sensitive systems' contents
8	Transaction Systems	Compromise Transactional Systems	Access to tamper with inputs for transactional systems
9	Wholesale Payment Systems	Compromise the SWIFT Payment System	Operator access to workbench interface or backend system with STP setup
10	Customer PII	Compromise PII in RM (Relationship management) systems	List of PII database / table
11	Source Code Control	Code change access to source code repository	Tampered dummy source code file in the repository