

**REQUEST For PROPOSAL (RFP)**

**For**

**CONDUCTING COMPREHENSIVE SYSTEM AUDIT**

**OF**

**METROPOLITAN STOCK EXCHANGE INDIA LTD. (MSEI)**

**AND**

**METROPOLITAN CLEARING CORPORATION OF INDIA LTD.  
(MCCIL)**

Vibgyor Towers, 4th floor,  
Plot No C 62, G - Block,  
Opp. Trident Hotel,  
Bandra Kurla Complex,  
Bandra (E), Mumbai – 400 098,  
Website : [www.msei.in](http://www.msei.in)



THE INFORMATION PROVIDED BY THE SERVICE PROVIDERS IN RESPONSE TO THIS RFP WILL BECOME THE PROPERTY OF MSEI AND MCCIL AND WILL NOT BE RETURNED. MSEI AND MCCIL RESERVES THE RIGHT TO AMEND, RESCIND OR REISSUE THIS RFP AND ALL AMENDMENTS WILL BE ADVISED TO THE SERVICE PROVIDERS AND SUCH AMENDMENTS WILL BE BINDING ON THEM.

*(THIS DOCUMENT SHOULD NOT BE REUSED OR COPIED OR USED  
EITHER PARTIALLY OR FULLY IN ANY FORM)*

---

**Table of Contents**

---

<b>1.</b>	<b>INTRODUCTION .....</b>	<b>3</b>
<b>2.</b>	<b>OBJECTIVE .....</b>	<b>4</b>
<b>3.</b>	<b>DEFINITION .....</b>	<b>4</b>
<b>4.</b>	<b>SCOPE OF SYSTEM AUDIT .....</b>	<b>4</b>
<b>5.</b>	<b>AUDIT PERIOD.....</b>	<b>7</b>
<b>6.</b>	<b>DELIVERABLES.....</b>	<b>8</b>
<b>7.</b>	<b>AUDITOR SELECTION NORMS .....</b>	<b>8</b>
<b>8.</b>	<b>AUDIT FEES .....</b>	<b>9</b>
<b>9.</b>	<b>PAYMENT TERMS.....</b>	<b>9</b>
<b>10.</b>	<b>PROPOSAL SUBMISSION .....</b>	<b>9</b>
<b>11.</b>	<b>EVALUATION OF OFFERS.....</b>	<b>10</b>
<b>12.</b>	<b>DISQUALIFICATION .....</b>	<b>10</b>
<b>13.</b>	<b>NOTIFICATION.....</b>	<b>10</b>
<b>14.</b>	<b>COMMUNICATION PROCESS .....</b>	<b>10</b>
<b>15.</b>	<b>RFP TERMS &amp; CONDITIONS .....</b>	<b>10</b>
<b>16.</b>	<b>LIABILITIES OF AUDITEE.....</b>	<b>11</b>
<b>17.</b>	<b>DISCLAIMER .....</b>	<b>11</b>
<b>18.</b>	<b>PROPOSAL PROCESS MANAGEMENT .....</b>	<b>11</b>
<b>19.</b>	<b>CONFIDENTIALITY &amp; RFP OWNERSHIP .....</b>	<b>11</b>
<b>20.</b>	<b>PARTICIPANT PRESENTATION .....</b>	<b>12</b>
<b>21.</b>	<b>ACCEPTANCE OF TERMS.....</b>	<b>12</b>
<b>22.</b>	<b>ERRORS AND OMISSIONS .....</b>	<b>12</b>
<b>23.</b>	<b>JURISDICTION .....</b>	<b>12</b>

---

## 1. Introduction

### **Metropolitan Stock Exchange Of India Ltd.(MSEI):**

Metropolitan Stock Exchange Of India Ltd.(MSEI) is recognised by Securities and Exchange Board of India (SEBI) under Section 4 of Securities Contracts (Regulation) Act, 1956. The Exchange was notified a “recognised stock exchange” under Section 2(39) of the Companies Act, 1956 by Ministry of Corporate Affairs, Govt. of India, on December 21, 2012. Shareholders of the Exchange include India’s top public sector banks, private sector banks and domestic financial institutions who, together hold over 88% stake in the Exchange. MSEI is subjected to CAG Audit and has an independent professional management.

In line with global best practices and regulatory requirements, clearing and settlement of trades done on the Exchange are conducted through a separate clearing corporation – Metropolitan Clearing Corporation of India Ltd. (MCCIL).

MSEI offers an electronic, transparent and hi-tech platform for trading in Capital Market, Futures & Options, Currency Derivatives and Debt Market segments. The Exchange has also received in-principle approval from SEBI for operationalizing SME trading platform. MSEI commenced operations in the Currency Derivatives (CD) Segment on October 7, 2008, under the regulatory framework of SEBI and Reserve Bank of India (RBI). MSEI launched Capital Market Segment, Futures and Options Segment commenced trading from February 11, 2013.

### **Metropolitan Clearing Corporation of India Ltd. (MCCIL):**

Metropolitan Clearing Corporation of India Ltd. (MCCIL) is the new age Clearing Corporation constituted to undertake clearing and settlement of deals in multi asset classes. The company offers best-in-class services to its clearing members with the help of its state of the art risk management framework and unparalleled clearing and settlement systems with dedicated linkages with clearing partners.

The company was incorporated on November 7, 2008 and was permitted by SEBI to undertake clearing and settlement functions of trades done in MSEI on January 2, 2009. The company commenced its operations on February 16, 2009.

MCCIL has adopted various best practices in the industry to make sure transactions are managed efficiently and completed seamlessly, which includes capital adequacy norms for membership, dedicated settlement guarantee fund, globally accepted systems for margining, online monitoring of member positions based on prudential position limit norms, automatic trading restriction on breach of prudential limits, multilateral netting for obligation computation and periodic back testing of margins.

## 2. Objective

To get the comprehensive system audit review done from the independent audit of The Exchange and the Clearing Corporations system as per the terms of references mentioned in the SEBI circular 'CIR/MRD/DMS/13/2011' dated November 29, 2011 and SEBI circular 'CIR/MRD/DMS/ 17 /2012', dated June 22, 2012.

## 3. Definition

"Auditee" means Metropolitan Stock Exchange of India Ltd. and Metropolitan Clearing Corporation of India Ltd.

## 4. Scope of System Audit

The scope of work will cover systems related to Stock Exchange and Clearing Corporation's operations. Specifically, the scope of work will cover following systems:

- a. Trading
- b. Monitoring and Surveillance
- c. Membership
- d. Listing
- e. Clearing and Settlement

All the areas as mentioned in the SEBI circular should be covered as part of system audit. The inclusive list of audit areas is mentioned below:-

### 1. General Controls

- a. Information Security Policy review and Quality of Implementation
- b. Application Security Controls
  - Segregation of duties
  - Audit Logging
  - Database controls
  - Application access controls
  - User Management etc.
- c. Physical and Environmental Controls related to Data Centre
- d. Maintenance of IT Facility and Infrastructure
- e. Fault resolution mechanism
- f. Folder sharing & back up controls- safeguard critical information on local desk top
- g. Review of Incident Management Process and Records

---

## 2. Change Management Controls

- a. Management of changes related to software / hardware
- b. Development/Test/ production environment - Segregation
- c. user awareness
- d. Processing of new change request
- e. Fault reporting/tracking mechanism & process of resolution.
- f. Testing of new releases / bug fixes - testing process
- g. Version control -History, change management process etc.
- h. New release in Production-Promotion, Release note approvals.
- i. Production issues/ disruptions reported during last year & corrective actions taken.

## 3. Data Communication / Network Controls including

- a. Network Administration
- b. Redundancy, Monitoring, Breakdown resolution etc.
- c. WAN Management- Connectivity provision for business continuity.
- d. Encryption - Router based as well as during transmission
- e. Connection permission - Restriction on need to have basis.
- f. Fall back mechanism - Dial up connections controls etc.
- g. Hardware based signing process
- h. Incidents of access violations in last year & corrective actions taken.

## 4. Security Controls – General office Infrastructure

- a. Access Policy and Controls
- b. Vulnerability Assessment and Penetration Testing of Critical Infrastructure
- c. LAN security control & monitoring.
- d. OS & database security controls & monitoring
- e. Internet connections controls - Firewall protection, Intrusion Detection system, access rights & privileges.
- f. Virus protection - Controls to mitigate the virus attack/outbreaks
- g. Secured (digitally signed) communication (electronic) with others entities like SEBI, others partner.
- h. Controls over Email Archival Process and Management.
- i. Incidents of security violations in last year & corrective action taken.
- j. Electronics Document Management
- k. General access Controls

---

5. Performance Audit

- a. Comparison of changes in transaction volumes since previous audit
- b. Review of systems (hardware, software, network) performance over a period.
- c. Review of the current volumes against the last performance test performed.

6. Review of Business Continuity / Disaster Recovery Plan and Process

- a. BCP and DR Plan including Business impact Analysis
- b. Risk assessment & DR process.
- c. Implementation of policies
- d. Back-up procedures & recovery mechanism using backups.
- e. Storage of Back up (Remote site, DRS etc.)
- f. Redundancy- Equipment, network, Site, etc.
- g. DRS installations and Drills - management statement on targeted resumption capability (in terms of time required & extent of loss of data)
- h. Evidence of achieving the set targets during DRS drills in event of various disasters scenarios.
- i. Review of any actual event when the DR/BCP was invoked during the year.

7. IT Asset Management and IT Support

- a. Utilization monitoring
- b. Capacity Planning - including projections of business volumes
- c. IT(S/W, H/W & N/W) assets, licenses & maintenance contracts
- d. Insurance
- e. Disposal- Equipment, media, etc.
- f. IT Service Desk Support
- g. Electronic Waste Disposal
- h. Asset identification and classification and labelling
- i. Asset ownership and accountability
- j. Asset inventorization

8. Review of Last Year Audit report and actions taken

9. DMZ and Network Architecture Design Review

- a. Audit the existing network architecture.
- b. Audit the configurations of critical network components such as firewall, IDS, routers, switches etc.
- c. Audit the updations / upgrades.
- d. Check the Log review process, check whether network scanning /monitoring is done on regular basis for the denial of service attack as well as other intrusion and spyware.

---

10. VPN Configuration Review

- a. User management
- b. Authentication / authorization over VPN connections
- c. Log monitoring and review
- d. Security Controls implemented on VPN device

11. IT Vendor Selection and Management

- e. identification of eligible vendors
- f. dissemination process of RFP's
- g. definition of criteria of evaluation
- h. process of competitive analysis
- i. approach for selection

12. E-Mail system

- j. Existence of policy for the acceptable use of electronic mail
- k. Regulations governing file transfer and exchange of messages with external parties
- l. Rules based on which e-mail addresses are assigned
- m. Security measures implemented and procedures for changes in filtering parameters
- n. Storage, backup and retrieval

13. Human Resource Security.

- o. Skill requirement in the operations and management
- p. Pre and Post Recruitment, Governance
- q. NDA's and confidentiality agreement
- r. Background Checks.
- s. Training for managing systems and applications.

14. Implementation review of the control areas mentioned in SEBI Circular 'CIR/MRD/DP/13/2015' dated July 06, 2015 on 'Cyber Security and Cyber Resilience framework of Stock Exchanges, Clearing Corporation and Depositories'

15. Review of provisions mentioned in SEBI CIR/MRD/DP/07/2015 May 13, 2015 on Co-location / proximity hosting facility offered by stock exchanges

16. Any other point as mentioned (TOR) in the SEBI circular, 'CIR/MRD/DMS/13/2011' dated November 29, 2011.

17. Any other additional areas subsequently asked by SEBI or other regulatory bodies.

## 5. Audit Period

January 1, 2016 to December 31, 2016

---

## 6. Deliverables

Audit reports of **initial findings** and **follow-up** audit are to be submitted to the Exchange within 10 days of completion of the audit. There would be one-three months gap between first audit and follow-up audit for implementation of recommendations

Two separate audit reports shall be issued for:

- Metropolitan Stock Exchange of India Ltd.
- Metropolitan Clearing Corporation of India Ltd.

Audit reports should include at least following

- Executive Summary
- Explicit coverage of each major area mentioned the scope of work indicating any Nonconformity (NC) or Observations or lack of it.
- Tabulation of Nonconformity (NC) or Observations against each major area
- Recommendations for each NC and observation
- Qualitative input about ways to improve the process based on best practices observed for each section.
- Fully detailed report at the minimum covering all the areas mentioned in the aforesaid SEBI Circular.

Further, the Report needs to provide overall comment to indicate if a follow-on audit is required. The Report shall also indicate the timelines for respective corrective action in case of Nonconformities.

## 7. Auditor Selection Norms

1. Auditor must have minimum 3 years of experience in IT audit of Securities Industry participants e.g. stock exchanges, clearing houses, depositories etc. The audit experience should have covered all the Major Areas mentioned under SEBI's Audit Terms of Reference (TOR).
2. The Auditor must have experience in / direct access to experienced resources in the areas covered under TOR. It is recommended that resources employed shall have relevant industry recognized certifications e.g. CISA (Certified Information Systems Auditor) from ISACA, CISM (Certified Information Securities Manager) from ISACA, GSNA (GIAC Systems and Network Auditor), CISSP (Certified Information Systems Security Professional) from International Information Systems Security Certification Consortium, commonly known as (ISC)<sup>2</sup>.
3. The Auditor should have IT audit/governance frameworks and processes conforming to industry leading practices like CobiT.
4. The Auditor must not have any conflict of interest in conducting fair, objective and independent audit of the Exchange / Depository. It should not have been engaged over the last three years in any consulting engagement with any departments / units of the entity being audited.



- 
5. The Auditor may not have any cases pending against its previous auditees, which fall under SEBI's jurisdiction, which point to its incompetence and/or unsuitability to perform the audit task.

Participant not meeting the selection norms as mentioned above will not be considered for further evaluation.

## 8. Audit Fees

Audit fees should be all inclusive of

- First round of Systems audit covering above mentioned scope
- Follow-on / review audit if required
- Out of pocket expenses
- Lodging & boarding expenses for visit DR site at Delhi

## 9. Payment Terms

The Payment Terms shall be as follows and subject to the deliverables.

- 60% payment shall be made on delivery first audit report.
- 40% payment shall be made on delivery of follow-up audit report

## 10. Proposal Submission

Participants should submit Technical and Commercial proposals separately

### **Technical Proposal:**

Technical proposal should contain the company background, existing clients, audit approach, methodology and, auditor(s) profile, audit plan and schedule, and all other details as specified in the **Auditor Selection Norms** section above.

Technical Proposal should be submitted through official email to [kundan.zamvar@masi.in](mailto:kundan.zamvar@masi.in) marking cc to [shraddha.wanage@msei.in](mailto:shraddha.wanage@msei.in)

### **Commercial Proposal:**

**Commercial proposal should be submitted through courier or speed post in sealed envelope to**

**Ms. Shraddha Wanage**

Metropolitan Stock Exchange of India Ltd  
4th Floor, Vibgyor towers, plot no.C-62.  
Opp. Trident Hotel Bandra Kurla Complex,  
Bandra (East)  
Mumbai – 400098, India.

**Proposal Submission Timeline:**

Technical and Commercial proposal should be submitted on or before 31st January 2017

**11. Evaluation of Offers**

Each Participant acknowledges and accepts that Audtee may in its absolute discretion apply selection criteria specified in the document for evaluation of proposals for short listing / selecting the eligible Participants.

**12. Disqualification**

Any form of canvassing/lobbying/influence/query regarding short listing, status, etc. will be a disqualification.

If the submission does not include all the information required or is incomplete, the proposal will liable to be rejected

**13. Notification**

Auditee will notify short-listed Participant in writing as soon as practicable about the outcome of their RFP. The Auditee is not obliged to provide any reasons for any such acceptance or rejection.

**14. Communication Process**

Participants are required to direct all communications related to this RFP, through the Nominated Point of Contact person:

Contact : Mr. Kundan Zamvar  
Position : CISO  
Email : kundan.zamvar@msei.in  
Telephone : +91 22 22 6112 9000 (Extn. 9015 )

The Auditee may, in its absolute discretion, seek additional information or material from any Participants after the RFP closes and all such information and material provided must be taken to form part of that Participant's response.

If the Auditee, in its absolute discretion, deems that the originator of the question will gain an advantage by a response to a question, then the Auditee reserves right to communicate such response to all Participants.

**15. RFP Terms & Conditions**

Participant must accept all of the foregoing terms and conditions without exception. All submissions, including any accompanying documents, will become the property of the Auditee and will not be returned under any circumstances.

Participant shall grant all rights to the Auditee to reproduce the whole or any portion of their submission for the purpose of evaluation, to disclose the contents of the submission to other Participants and to disclose and/or use the contents of the submission as the basis for processing of RFP, notwithstanding any copyright or other intellectual property right that may subsist in the submission or accompanying documents.

The Participant should therefore provide a quote which is inclusive of all terms & conditions and therefore will not be a separate charge for any other related services.

## **16. Liabilities of Auditee**

This RFP is only an invitation for proposal and does not give rise to any contractual obligation on behalf of the Auditee whatsoever unless and until a formal contract is signed between Auditee and the Participant.

Participant understands that the Auditee shall in no manner or on any grounds whatsoever not be liable to pay any cost incurred in the preparation or submission of any proposal or to procure or for any other miscellaneous services.

## **17. Disclaimer**

Subject to any law to the contrary, and to the maximum extent permitted by law, the Auditee and its officers, employees, contractors, agents, and advisers disclaim all liability from any loss or damage (whether foreseeable or not) suffered by any person acting on or refraining from acting because of any information including forecasts, statements, estimates, or projections contained in this RFP document or conduct ancillary to it whether or not the loss or damage arises in connection with any negligence, omission, default, lack of care or misrepresentation on the part of the Auditee or any of its officers, employees, contractors, agents, or advisers.

## **18. Proposal Process Management**

The Auditee reserves the right to accept or reject any and all of the proposals, to revise the RFP, to request one or more re-submissions or clarification from one or more Participants, or to cancel the process in part or whole without any prior notice or intimation and without assigning any reasons. No Participant is obligated to respond to or to continue to respond to the RFP after the submission and closing date.

The Auditee will, at its discretion, award the contract to the responsible Participant submitting the best proposal that complies with the RFP. The Auditee may, at its sole discretion, reject any or all proposals received or waive minor defects, irregularities, or informalities therein.

## **19. Confidentiality & RFP Ownership**

This RFP is both confidential and proprietary to the Auditee. The Auditee reserves the right to recall the RFP in its entirety or in part. Participants agree that they will not duplicate, distribute or otherwise disseminate or make available this document or the information contained in it without the express written consent of the Auditee. Participant would take due care of the

information to prevent unauthorized use or disclosure of the information, as if it would exercise or do for protecting its own information of similar nature.

Participants shall not include or refer this RFP in any publicity without prior written approval from the Auditee. The Participants understand that in case of violation or material breach of any term of this clause may entitle the Auditee to all reliefs available to it under equity and law, which may include injunctive relief, losses, damages, cost, etc.

## **20. Participant Presentation**

If required, the Participant will be asked to make presentations at the Auditee. The Auditee shall not be under any obligation to bear any part of the expenses incurred by the Participants in connection for or related to presentations or any ancillary expense.

## **21. Acceptance of Terms**

The Participant will, by responding to the RFP, be deemed to have accepted the disclaimer, terms and conditions of the RFP

## **22. Errors and Omissions**

Participant may notify the Auditee of any error, omission, or discrepancy found in this RFP document.

## **23. Jurisdiction**

Any disputes of claims would be subject to the exclusive jurisdiction of Courts in Mumbai and governed by laws of India.

-----End of Document-----