REQUEST FOR PROPOSAL (RFP)
FOR

MIGRATION AUDIT, INFORMATION SYSTEM AUDIT AND VULNERABILITY ASSESSMENT AND PENETRATION TESTING (VAPT) OF CORE BANKING SOLUTION, DATA CENTRE, DR SITE, HARDWARE, NETWORKING INFRASTRUCTURE AND OTHER ALLIED SYSTEMS

Ref No: MSCB/ITD/SYS-AUDIT/ 139/2021-22

The Maharashtra State Co-operative Bank Limited
(Incorporating The Vidarbha Co-op Bank Ltd.)
Sir Vithaldas Thackersey Memorial Building,
9, Maharashtra Chamber of Commerce Lane,
Fort, Mumbai 400001.

Cost of Document : Rs 1000/- plus GST

Commencement of Sale of Document : 30th August, 2021

Last Date of Submission: 20th September, 2021 till 3:00 PM

TABLE OF CONTENT

1. TENDER NOTICE

Sealed commercial bids are invited from **CERT-IN empaneled Information Security Auditing Organisations** for Information System Audit of Core Banking Solution, Digital Banking, Data Centre, DR Site, Networking Infrastructure and Other Integrated Systems of The Maharashtra State Co-Operative Bank Ltd. (MSCB) Head Office, Fort, Mumbai.

2. TENDER HIGHLIGHTS

Tender Reference No.	MSCB/ITD/SYS-AUDIT/139/2021-22
Price of Tender Document	Rs. 1000/- (Rupees One Thousand) plus 18% GST By Cash/ NEFT to A/c No **0002117030003377** (IFS Code – MSCI0082002, title of account – Other receipts account)
Date of Commencement of Sale of Document	30th August, 2021 11:00 AM
Last date of submission of the Pre bid Queries27	6th September, 2021 05:00 PM
Date of Pre-bid Meeting	7th September, 2021 03:00 PM
Last date of submission of Bids	20th September, 2021 03:00 PM
Opening of Offer	Will be communicated to the vendor on email
Address for Communication:	The Managing Director, The Maharashtra State Coop. Bank Ltd. Head Office, Sir Vithhaldas Thackersey Memorial Building, 9, Maharashtra Chambers of Commerce Lane, Fort, MUMBAI - 400001. Tel Nos: 022-22800527 / 22800711 Email: mscb.it@mscbank.com

3. ABOUT MSCB

The Maharashtra State Cooperative Bank Ltd, Mumbai is a premier Co-operative institute at State level established in 1911. It is rendering its services to its increasing number of clientele in more diversified and multifarious banking services and facilities over last 10 decades and has established itself as a leader of co-operative movement in the state of Maharashtra. It has been in the process of helping the economic development of rural Maharashtra through its 6 regional offices 50 Branches in the State.

The main business of the MSCB can be classified as direct financing for the cooperative societies, engaged in various fields like Sugar production, Marketing, Spinning Mills, various types of agriculture processing units; direct financing to some State level and National level co-operatives and indirect financing through three tier system i.e. MSCB at apex level, DCC Banks at middle level and primary agriculture societies at grass root level.

MSCB has 50 branches, 3 Extension Counters, Administrative Office, 6 regional offices and Head office that have fully computerized operations running on Core Banking Solution. The bank has DC & DR.

The bank is direct member of NFS and is live on RuPay ATM, POS, AEPS/ E-KYC, SMS Banking, Internet Banking (view only), UPI, and ECOM services. It is live on Mobile Banking services for its customers.

4. ABOUT BANK COMPUTERISATION

The MSCB initiated the process of computerization of its operations in a phased manner starting in 1998-99. MSCB focused on implementation of the Core Banking Software and development of an effective and timely MIS. In addition the Bank attempted to cover other corporate function like International Banking Transactions, Bank Guarantees, and Letter of Credits etc. By the time computerization of Branches was nearing completion, the Bank realized the need to implement the Core Banking System ("CBS") with centralized architecture so as to cater to functional requirements of the Bank, client / customer expectations for new services, and technological advancements.

5. PRESENT STATUS

- The primary Data Centre is presently situated at New mumbai and Disaster Recovery Centre is situated at Bengaluru.
- The current status of various applications deployed at MSC Bank are listed below:-

Applications
CBS
ATM Switch
Treasury
AML (Anti Money Laundering)
ALM (Asset Liability Management)
RTGS/NEFT
HRMS
CCIL Applications
RAM (Risk Assessment Module)
SWIFT
CTS

6. ELIGIBILITY CRITERIA

Bidder should be **CERT-IN empaneled Information Security Auditing Organisation** located in **Mumbai or Pune.**

7. OBJECTTIVES

A. BANK'S OBJECTIVES FOR CONDUCTING SYSTEM AUDIT

Bank's Objective for conducting Systems audit of Information systems and IT infrastructure is to get reasonable assurance from a third party auditor that:

- Bank's information systems and data are secure, and will remain complete, integrated, current, and accurate throughout processing.
- Bank's information assets / resources (hardware / software) are secured against unauthorized access / usage /damage / changes.
- Bank's business continuity planning is adequate enough to ensure smooth customer Service, despite interruption to technology facilities for a significant amount of time
- Bank's networks are adequately provided and protected.
- Bank's computer operations are carried out in a controlled environment.
- Bank can get independent assurance over effectiveness of controls exercised by out-sourced vendors for technology services (Facility Management Services Vendor)

- Bank has appropriate controls in its entire systems development life cycle, project management and implementation activities.
- Bank has complied for all required statutory requirements.

B. Banks Objectives of Data Migration Audit

- MSC Bank intends to appoint a third party auditor for auditing the data migration activity in order, to achieve its objective of smooth transition from Source Systems to the Target System, and to obtain a reasonable assurance for the quality of data, efficiency of data migration process and stability of data environment. In order to provide the required assurance, the bidder is required to consider and achieve the below data migration audit objectives.
- 1 To provide an assurance that data requirements for the new system have been appropriately identified and documented. In order to achieve this objective, the bidder must understand and validate the data migration related documentation such as approved data migration plan, master data requirements, transaction data requirements, historical data requirements (such as historical balances) etc.
- 2 To provide an assurance that sources for data have been appropriately identified and documented by understanding and validating information such as system source files, manual forms (if any used), new data collected for the Target System, data mapping document etc.
- 3 To provide an assurance that the collection and conversion method for each data element has be appropriately identified and documented by understanding and validating information such as details of data conversion, data translation method etc.
- 4 To provide an assurance, that the timing and sequencing for converting data elements has been appropriately identified and documented by understanding and validating information such as master data conversion methodology, transactional data conversion methodology, historical data (such as historical balances) conversion methodology etc.
- 5 To provide an assurance, that the existing source data is accurately and completely migrated by understanding and validating migration controls such as record counts / check sums etc used for the process and performing automated tool based audit of the migrated data vis-à-vis source data.

8. SCOPE OF WORK

8.1 Vulnerability Assessment of Infrastructure relating to CBS Network, Data Centre, DR Site, CBS-Back office, Head office, Regional Offices and Branches etc.

8.2 CBS Back Office and Data Centre/DR site functional. Audit covering User / Help Desk /Parameters / Access / Back end corrections /Change Management etc.

8.3 Systems audit of Core Banking Applications including OMNI ++ Enterprise - CBS main Application etc. from Infrasoft Technology India Ltd. Mumbai. Broad areas to be covered are as per Annexure - I.

8.4 Network Audit, NMS (Network Monitoring system) & Administrative Process with report and recommendations. Broad areas to be covered are as per Annexure - II.

8.5 Report on Capacity Management and performance tuning of the entire CBS architecture with recommendations, if any, for improving the performance and security. Broad areas to be covered are as per Annexure - III.

8.6 Process audit of minimum 10 CBS offices/ branches / Regional Offices with focus on critical areas like password controls, control of user ids, operating system security, anti-malware controls, maker checker controls, segregation of duties, rotation of personnel, physical security, review of exception reports/audit trails, BCP policy and testing etc.

8.7 Undertake Vulnerability assessment & Systems Audit of the Information Systems of Standard applications and legacy applications (either integrated with Core Banking Solution or working as standalone) such as:

- Payment Channels eg. ATM, Mega Banker Multi Kiosk machine, Mobile Banking, UPI
- Treasury
- Anti Money Laundering /KYC/Customer verification
- MIS
- RTGS / NEFT
- HRMS / Payroll / PF
- Risk Management
- Cheque Truncation System
- Forex

8.8 Review of current Security measures provided and recommendations on its improvement.

8.9 DR Site Audit

- Verification of systems/controls
- Assessment of environment and procedures
- Assessment of management parameters
- Adequacy of infrastructure (capacity to handle full traffic)
- Review of fallback procedures
- Assessment of access control

8.10 Record Management / Record processes and controls

- Policies for media handling, disposal and transit
- Periodic review of Authorization levels and distribution lists
- Procedures of handling, storage and disposal of information and media
- Storage of media backups
- Protection of records from loss, destructions and falsification in accordance to statutory, regulatory, contractual and business requirement

8.11 Vulnerability Assessment & Penetration Testing (VAPT) for entire IT ecosystem including Bank's Information System Infrastructure (Networking Systems, Security devices, Servers, Databases, Applications Systems accessible through WAN, LAN as well as with public IP's, Bank's website and email server hosted with vendor). Auditor is expected to identify existing threats and vulnerabilities and suggest remedial solutions and recommendations of the same to mitigate all identified risks, with the objective of enhancing the security of Information Systems.

8.12 Auditor's comments /Recommendations for various training, knowledge improvement program.

9. DELIVERABLES UNDER SYSTEMS AUDIT

- Data Centre Audit Report at Mahape
- Disaster Recovery Centre at Bengaluru, Audit Report
- Network Audit Report
- CBS Application System Audit
- Allied Application System Audit - Treasury, AML, Forex, ALM, RTGS/NEFT, HRMS/Payroll/PF, MIS, CTS, Risk Management, ATM/POS/ ECOM recon, IMPS recon, UPI recon, etc
- Payment Channels System Audit - ATM, Mobile Banking, Mega Banker Multi Kiosk machine, UPI etc
- Interface Application
- Branch Wise Audit Report

10. Data Migration Audit Process

1. MSC Bank has Banking Solution. The bidder is expected to go through the control specification documents, prepared by CBS Application to gain an understanding of the CBS modules being implemented by CBS Application and their data structure.
2. The CBS Vendor will migrate the source data to the Target System. The bidder is expected to study all the necessary documentation pertaining to data migration carried out by CBS Vendor.
3. The bidder should formulate and share a data migration audit plan with the bank incorporating activities to be covered as a part of data migration audit. The plan should incorporate, but notcbe limited to, the below indicative stages:
4. Validate data migration planning: The bidder should understand and validate the data migration planning done by CBS Vendor, for migrating the data from Source
   Systems to the Target System, including but not limited to,
   • Data migration strategy and methodology
   • Data migration scope
   • Data migration work plan
   • Data testing approach The bidder should also analyze and validate the tools/queries/scripts used by Polaris Software Lab Limited for extraction, transformation and migration of data.
5. Configure/develop data migration audit tool: It is up to the bidder to bring and use an automated data migration audit tool configured to suit the data audit requirements at MSC Bank. If the bidder proposes an automated tool, the Bank may decide to purchase the license of the automated tool post successful evaluation / demonstration of the tool by the bidder.
6. Understand and Validate Data mapping: The bidder is expected to understand and validate the mapping of source data fields to destination data fields defined by the CBS Vendor. The bidder should also validate the method used to create any fresh data fed into the Target System.
7. Validate data extraction and cleaning: The bidder is expected to understand and verify the integrity of data extracted from the Source Systems and the data cleansing rules/methodologies adopted by CBS Application.
8. Validate migrated data: The bidder is expected to verify the integrity and correctness of the source data reconciled and uploaded into the Target System, identify the gaps in the data migration and provide a ‘Migration audit report’ stating the gaps identified in the data migration audit. The bidder should use an automated tool for verification of data uploaded to the Target System. The details of the proposed tool should be provided in ANX1.
9. Perform recurring gap analysis: The bidder is expected to work with CBS Vendor to perform a recurring gap analysis and ensure that all the gaps/discrepancies identified in the ‘Migration Audit Report’ are rectified by CBS Vendor. The gap analysis may require to be repeated until all errors identified are closed. The bidder is expected to provide a ‘Final Compliance Report’ to certify the quality of data, efficiency of data migration process, and stability of the data environment.
10. Validation of Existing Data archival: The bidder is expected to provide reasonable assurance for the efficiency of archival of the existing data, related to the migrated regional offices, at the Data Centre of the bank. 11 The bidder is expected to audit the data migration carried out by CBS Vendor and provide an assurance for the accuracy, integrity, conformity and completeness of the data migrated from Source Systems to the Target System (This should be performed for the Data Centre- at Mahape, and Far Site- at Bengluru.)

11. The 'Final Compliance Report' submitted by the bidder should also provide assurance on the completeness and accuracy of critical data elements such as those related to the transactions and items in suspense, pending clearing entries, store and forward transactions, electronic regional offices advices, the balances at each data migration instance etc. 13 Tool proposed/used for the data migration audit should be licensed in the name of the Bank and should be made available to the bank for future use, if Bank exercises the option to do so. The bidder is also expected to train the end users (core users of the project as identified by the Bank.

11. BID SUBMISSION

- Bidders shall submit commercial bid in sealed envelope. If above bid is found not properly sealed, the bid is liable for rejection.
- Title should be mentioned on face of the envelop as Information System Audit - Ref No MSCB/ITD/SYS-AUDIT/ /2021-22.
- Bidder's name, address must be mentioned on face of the envelop. In case Bidder's name, address not clearly mentioned on envelop, the bid is liable for rejection.

12. TERMS AND CONDITIONS

12.1 **Non-transferable:** The Vendor, if selected, will not be allowed to sub contract the work under the Tender as it is non-transferable.

12.2 **Offer validity Period:** The offer should remain valid for a period of 90 days from the date of the Offer.

12.3 **No Commitment to Accept Lowest or Any Offer:** MSCB shall be under no obligation to accept the lowest or any other offer received in response to this Tender and shall be entitled to reject any or all offers, in part or in full, without assigning any reason whatsoever.

Earnest Money Deposit: The Vendors are required to deposit Rs. 25,000/- (Rupees: Twenty Five Thousand only) as Earnest Money Deposit. Offers made without EMD will be rejected. The EMD should be deposited electronically in NEFT Account No 0002116900000003 (IFS Code – MSCI0082002, title of account – "EMD for Purchase of IT Products") branch Fort.

12.4 **Erasures or Alterations:** The offers containing erasures or alterations will not be considered. There should be no hand-written material, corrections or alterations in the offer. MSCB may treat offers not adhering to these guidelines as unacceptable.

12.5 **Quality Standards:** The vendor is required to adopt highest Quality standards while working on the Project.

12.6 **Delays in the Information System Audit:** The Information System Auditor (the Vendor) must strictly adhere to the audit schedule, as committed and specified in the work order.

12.7 **Order Cancellation:** MSCB reserves its right to cancel the order in the event of one or more of the following conditions:

- Delay in delivery of services as committed
- Quality of deliverables
- Resources availability
- Skill Sets of Resources conducting Audit

12.8 **Right to Alter Scope of work:** In case it is required, in the interest of the Bank, to make any changes in the scope of the work, the Bank reserves it's right to do so with the mutual consent in writing of the bank and the vendor.

12.9 **Indemnity:** Vendor shall indemnify, protect and save MSCB against all claims, losses, costs, damages, expenses, action suits and other proceeding, resulting from infringement of any patent, trademarks, copyrights etc. or such other statutory infringements in respect of all the Services etc. supplied by him.

12.10 **Publicity:** Any publicity by the vendor in which the name of MSCB is to be used should be done only with the explicit written permission of MSCB.

12.11 **Resolution of Disputes:** MSCB and the vendor shall make every effort to resolve amicably, by direct informal negotiation, any disagreement or dispute arising between them under or in connection with the contract. If after thirty days from the commencement of such informal negotiations, MSCB and the vendor have been unable to resolve amicably a contract dispute; either party may require that the dispute be referred for resolution by formal arbitration.

All questions, disputes or differences arising under and out of, or in connection with the contract, shall be referred to two Arbitrators: One Arbitrator to be nominated by MSCB and the other to be nominated by the Vendor. In the case of the said Arbitrators not agreeing, then the matter will be referred to an umpire to be appointed by the Arbitrators in writing before proceeding with the reference. The award of the Arbitrators, and in the event of their not agreeing, the award of the Umpire appointed by them shall be final and binding on the parties. The arbitration and reconciliation act 1996 shall apply to the arbitration proceedings and the venue of the arbitration shall be Mumbai.

12.12 **Qualification of deployed Core Audit Team:** The entire Security Audit work has to be done by qualified CISA/CISSP Professionals having requisite expertise in Systems Audit. Personnel having CISA/CISSP/GIAC (SANS)/ BS7799 qualifications and with adequate experience shall be utilized by the Systems Audit firm for auditing the Information Systems security architecture.

12.13 **Payment Terms**

- 10% on submission of audit plan/procedures and methodology covering all the points as per Scope of Work.
- 20% on submission of Draft Report/s
- 20% on presentation of and discussions on the Draft report/s with the top management
- 35% on submission of Final Audit Report/s covering all the points as per the Scope of Work
- 15% on reconfirmation after compliance (After receiving Final Audit Report Bank will try to comply points identified in the Final Audit Report in fixed time window. Auditor shall reconfirm the compliance.

ANNEXURE I

Scope for Systems Audit of Core Banking Solution ("CBS") Software

- Input controls
- Processing controls
- Output controls
- Logical access control
- Controls over automated processing /updation of records, review or check of critical calculations such as interest rates, repayment schedule, etc., review of the functioning of automated scheduled tasks, output reports design, reports distribution, etc.
- Auditability both at client side and server side including sufficiency and accuracy of event logging, SQL prompt command usage, Database level logging all other interfaces with other applications etc.
- Extent of parameterization
- Functionality
- Internal control built in at application software level, database level, server and client side
- Backup/Fallback/Restoration procedures and contingency planning
- Suggestion on segregation of roles and responsibilities with respect to application software to improve internal controls
- Review of documentation for formal naming standards, design process for job roles, activity, groups and profiles, assignment, approval and periodic review of user profiles, assignment and use of super user access
- Manageability with respect to ease of configuration, transaction roll backs, time taken for end of day, day begin operations and recovery procedures
- Special remarks may also be made on following items:
  Hard coded user-id and password, EDI, Web Server and other interfaces at Network level, Application level Recovery and restart procedures Sufficiency and coverage of UAT test cases, review of UAT defects and tracking mechanism deployed by vendor and resolution including re-testing and acceptance Review of customizations done to the software and the SDLC policy followed for such customization. Proposed change management procedure during conversion, migration of data, version control etc.
- Suggest any application specific Audit tools or programs
- Review of Software benchmark results and load and stress testing of IT infrastructure performed by the Vendors
- Adequacy of Audit trails and meaningful logs
- Adherence to Legal and Statutory Requirements
- Configuration of System mail
- Adequacy of antivirus measures at CBS environment
- Adequacy of hardening of all Servers (data center and branches) and review of Application of latest patches supplied by various vendors for known vulnerabilities as published by CERT,SANS etc.
- Apart from the Systems Audit of the application software, Systems Audit should be carried out at Data Center, DR Site, Head office, Regional office and at least ten branches.

ANNEXURE II

Scope for Systems Audit of Network Infrastructure Components, Networks and Application Security

- Net Scanning - Threat and Vulnerability Assessment: It is the process of measuring and prioritizing the risks associated with network- and host based systems and devices to allow rational planning of technologies and activities that manage business risk.
- Password Cracking
- Intrusion Detection System / Intrusion prevention system Testing
- Firewall
- Router Testing
- Denial of Service (DOS) Testing
- Distributed DOS Testing
- Containment Measures Testing
- While doing the penetration test on Servers in live environment the ISA should ensure optimum performance of the systems.
- Review of Network Monitoring Software (NMS) installed to monitor critical servers of the entire network including the branches for sizing etc., to monitor the network components of LAN & WAN, Fault Management, Performance Management of the network, Inventory Management, automatic discovery of network components etc. NMS is also implemented for Proactive Monitoring, Reporting and to Generate Performance Reports of Core Banking Network. These functional capabilities need to be reviewed and audited.
- Network Infrastructure Review : Network infrastructure at Branches, CBS-Project office, Data Centre, D R site, and NAP(network Aggregation Points)
- Network Management Review: The key management control aspects like standards for equipment, application, capacity planning, performance, reporting, problem resolution, costing and accounting are to be reviewed.
- Network Administrative Review
    - The domains that are to be reviewed for the effective administration of network
    - Monitoring of Structured Cabling and network usage
    - Optimization of setup
    - Resolution of bottlenecks
    - Bandwidth allocation (requirement/utilisation especially during peak hours for big/service branches)
    - Standard reports and Corrective action for the issues
    - Data Transmission Efficiency & Security
- Data Transmission
    - The Packet size of the message to be transmitted
    - The speed of transmission of message Security of message packets to be transmitted whether it is Tamper Proof Adequacy of Procedures for Encryption of Data to be transmitted
    - File transfer protocols FTP & SFTP
- Network Security Audit
    - Physical and logical security measures, tools and processes implemented to protect unauthorized entry into corporate network are to be reviewed. Configuration of Firewalls & Routers, effectiveness of Intrusion Detection system and / automated audit trial of all the users of network are the key areas that should undergo review. Check if adequate security is available in

the various Network connectivity provided to ensure only authorized users are accessing the system.

- Check if remote logon is enabled and if so, whether it is identifiable by terminal IDs / IP addresses.
- Check if remote logon through services such as ftp, telnet, etc., is disabled. If not, ensure that the same has been implemented as instant guidelines.
- In case of WAN (Wide Area Networks), are the Router maintained securely to ensure efficient Systems Administration.
- Focus should be on detecting the system vulnerabilities arising out of multiple access levels. Standard tools to scan various entry points to the network are to be used and an exhaustive analysis of security targets are to be provided. The scope includes operating system, databases, firewalls, routers, remote access devices and switches.
- Review the activities of Network Administrator/System Administrator and suggest Improvements and controls, if any, required.

- Security Device Audit
  - Configuration, policy/rule sets, signatures, Inspection, Logging, Location, redundancy, port restrictions, patches & updates, Administration & Management
  - Firewalls (Juniper/ CISCO and FortiGATE)
  - Network Intrusion Prevention Systems
  - Host Intrusion Detection Systems
- Architecture & placement of security devices
  - Change Management Processes - Deployment of rules, policies and adequacy of change management through Trouble Ticketing tool
  - Incident Management Processes
  - Documentation
  - Adequacy of Phishing Monitoring/Antiphishing services
  - Adequacy of Security Monitoring
  - Failover/Fallback processes and testing of failover/fallback processes
- Adequacy of Reporting & Escalation Mechanisms
- Patch Management

ANNEXURE III

Scope for Systems Audit of Capacity Management and performance tuning

The goal of Audit of capacity Planning and Management is to assess whether satisfactory service levels are being provided to users in a cost effective manner.

Review of following functions carried out by Bank's I.T. department

- Determining Service Level Requirements
- Analyzing Current Capacity
- Analyzing network bandwidth availability at peak level
- Planning for the future
- Analyzing periodically Workloads and Service
- Measuring overall resource usage
- Determining a process to measure the incoming work
- Establishing service level requirements Vs performance
- Checking whether the organization will be prepared for the future

Annexure IV

Scope of Work for Migration Audit

Definitions

1 "Source Systems" are defined as the disparate systems/IT applications deployed in various functional areas to handle the banking services of MSC Bank. Current list of these systems/applications and the departments in which they are deployed are summarized below:

Applications
CBS
ATM Switch
Treasury
AML (Anti Money Laundering)
ALM (Asset Liability Management)
RTGS/NEFT
HRMS
CCIL Applications
RAM (Risk Assessment Module)
SWIFT
CTS

2 '"Target System" is defined as the Core Banking Solution (CBS) being implemented at MSC Bank.

3 "Systems in scope" are defined as the above mentioned "Source" and "Target" systems.

4 "Source data" is defined as the data to be migrated to the Target system from the Source Systems or provided otherwise by the bank.

5 "Data Migration Audit" is defined as auditing the data migration from Source Systems to the Target System, including but not limited to

- Understanding and validating the data mapping provided by CBS Vendor
- Developing/Configuring automated data audit tool for auditing the migrated data
- Obtaining the data from the Source Systems in the required format
- Obtaining the migrated data from the CBS Vendor
- Performing an audit of migrated data vis-à-vis source data to provide a 'Data Migration Audit report' highlighting errors in the data migrated to the Target System
- Working with CBS vendor to correct data migration errors and providing an assurance for efficiency of the data migration process and stability of the data environment (data relationship maintenance) and, providing a 'Final Compliance report' and a certificate of confirmation of account balances for all accounts (funds and depository)

6 "Bidder" is defined as the vendor who performs all activities mentioned above.

7 "Core Banking Solution" or "CBS" for MSC Bank shall primarily include banking modules such as current accounts, deposits, loans; debt office modules such as depository, securities settlement module, auction module etc.; and services like clearing, payment and settlement, consolidation of agency transactions, remittance etc.