RFP No.: PDCC/IT-RFQ/22-23/03 Date: 21.11.2022

THE PUNE DISTRICT CENTRAL CO-OPERATIVE BANK LTD.

INFORMATION TECHNOLOGY DEPARTMENT

INFORMATION TECHNOLOGY DEPARTMENT
HEAD OFFICE: Pune District Central Co-op. Bank Ltd.,
4 B , B. J. Road, Pune.
Pin – 411001

REQUEST FOR QUOTATION (RFQ)

FOR

Information System Audit, Migration Audit AND VULNERABILITY ASSESSMENT AND PENETRATION TESTING (VAPT), Cyber Security Audit of Data Centre, Critical Applications, IT Processes etc. of the Bank

RFQ No.: PDCC/IT-RFQ/22-23/03
RELEASEDATE: 21/11/2022

Disclaimer

The information contained in this RFQ document or any information provided subsequently to bidder(s) whether verbally or in documentary form by or on behalf of the Bank is provided to the bidder(s) on the terms and conditions set out in this RFQ document and all other terms and conditions subject to which such information is provided. This RFQ is neither an agreement nor an offer and is only an invitation by Bank to the interested parties for submission of corresponding bids. The purpose of this RFQ is to provide the bidder(s) with information to assist the formulation of their quotes propositions. While effort has been made to include all information and requirements of the Bank with respect to the solution requested, this RFQ does not claim to include all the information each bidder may require. Each bidder should conduct its own investigation and analysis and should check the accuracy, reliability and completeness of the information in this RFQ and wherever necessary obtain independent advice. The Bank 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 RFQ. The Bank may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFQ.

Data Sheet

The following is an indicative timeframe for the overall process. PDCC Bank reserves the right to vary this timeframe at its absolute and sole discretion and without providing any notice/intimation or reasons thereof. Changes to the timeframe will be communicated to the affected **Respondents during this RFQ process.**

Particulars	Details
RFQ Title	**Information System Audit, Migration Audit AND VULNERABILITY ASSESSMENT AND PENETRATION TESTING (VAPT), Cyber Security Audit of Data Centre, Critical Applications, IT Processes etc. of the Bank**
Date of Commencement of RFQ	**21/11/2022 10.30 HOURS**
RFQ submission last date and time	**05/12/2022 16:00 HOURS**
Submission of RFQ at (Emails can be acceptable)	**Pune District Central Co-Operative Bank Ltd.** **IT Department** **Head Office: 4 B, B. J. Road,** **Pune 411 001**
Contact Persons for any clarifications/ Submission Of RFQ	PDCC IT Department
Bank email id for RFQ related communication	cbs.rfp@pdccbank.com

One hard copy and one soft copy on email, of the Technical Bid and One Copy of the Commercial Bid must be submitted at the same time, giving full particulars in separate sealed envelopes at the Bank‟s address. Technical Bid will contain details about the Audit performed and framework leveraged by the Vendor whereas Commercial bid will contain the pricing information as per the format mentioned in section 5 given in the RFQ. The commercial bid should be password protected and password of the Commercial Bid file should be shared in separate mail.

The bids shall be dropped / submitted at PDCC Bank‟s address given in the above Bid Detail – Table, on or before the date specified therein.

All envelopes must be super-scribed with the following information:

- Name of the Service Provider
- Offer Reference
- Type of Offer (Technical or Commercial)

The email ID is as follows: cbs.rfp@pdccbank.com

The Bank reserves the right to accept or not to accept any bid or to reject a particular bid at its sole discretion without assigning any reason whatsoever.

TABLE OF CONTENT

Contents

1 Introduction

The Bank intends to appoint CERT-IN empanelled Information Systems Security Auditor to conduct Information Systems Security Audit. The purpose of RFQ is to shortlist IS Auditor/ Firm for audit of activities at Data Center, Disaster Recovery Site and other activities mentioned in the RFQ, for providing independent reasonable assurance to the management on:

- Robust IT security,
- Mitigation of risks where there are significant control weaknesses
- Safeguarding the information assets viz. hardware, network etc.,
- Maintaining security, confidentiality, integrity and availability of data,
- Efficient utilization of resources-IT.
- Ensuring compliance of IT Security Policy and procedures defined by the Bank.
- Ensuring compliance of RBI/ NABARD Information Security Guidelines/recommendation and other applicable external regulations.
- Cyber Security Audit Of the Bank.

The selection of auditor will be based on 1) Conformity with Minimum Eligibility Criteria 2) Technical bid 3) Commercial bid. Selected bidder is expected to make all efforts and commit all resources to make this project meet its objective.

2 Eligibility Criteria

2.1 Basic Eligibility Criteria

Sr. No.	Eligibility Criteria	Documents to be Provided
1	Bidder should be a legal entity registered in India, under Indian Companies Act 1956 or partnership/LLP act 2013.	Certificate of Incorporation/Partnership deed.
2	The IS Audit firm/company should be in the business of Information System auditing (IS Auditing) in India at least for last three years as on RFQ publication date (in case of mergers / acquisition / restructuring or name change, the date of establishment of the earlier / original Partnership Firm / Limited Company can be taken in to account).	Shops & Establishment certificate / Incorporation certificate / Memorandum & Articles of Association should be attached.
3	The bidder should be a Profit-making company for last three (3) financial years (2018-2019, 2020-2021 and 2021-2022).	Audited Balance Sheet and Profit and Loss Account Statement for last three years. In case of 2021-22 provisional financial statement signed by statutory auditor or duly certified by charted accountant will be accepted.
4	The bidder must be having on their rolls, on permanent employment basis, a minimum of 2 (two nos.) professionals who hold professional certifications like CEH / CISA / CISSP / CISM / ISO 27001 with requisite experience to handle the work as per the scope (valid as on date).	The profile of the Core Audit team must be submitted as per format given in Annexure – I format. Respective professional certificates to be submitted.
5	The bidder should have Banks / Financial Institutions as their clients for IS Audit. The bidder must have completed comprehensive System Audit in last two financial years, for at least One (01) Bank (Bank who has more than 300 Branches).	Documentary proof must be provided along with copies of Work Order along with completion certificate.
6.	To ensure audit independence, the bidder should not have been a vendor / Consultant of IT equipment / peripheral / software / Services / existing IS auditor of PDCC Bank in the past 2 years.	Undertaking on company letterhead

7.	The bidder should be an empanelled Security Auditing Firm with CERT-In as on RFQ publication date and also during the course of Audit.	Copy of valid CERT-In certificate
8.	The service provider should ensure that there are: a. No legal proceedings pending or threatened against service provider or which adversely affect / may affect performance under the contract; and No inquiries or investigations have been threatened, commenced or pending against the service provider or by any statutory or regulatory or investigative agencies.	Declaration in the letterhead of the service provider‟s company to that effect duly certified by Statutory Auditor/ Chartered Accountant / Company Secretary should be submitted.
9.	The Bidder should not have been blacklisted by any of the Ministry/ Department of Government of India/ State Governments and also neither convicted nor is any criminal case pending against it before any court of competent jurisdiction	Self-declaration by competent authority of the bidder

Please note –

1. The bidder who do not fulfill to all the above eligibility criteria will not be considered for Technical evaluation and shall be summarily rejected without any separate notice or assigning any reason whatsoever.
2. All the proofs attached should have company seal and self-attested by authorized signatory

3 Detailed Scope Of Work

Bank is inviting bids to shortlist the auditor to conduct Information System audit for FY 2022-23 as per the scope mentioned below:

The IS Audit should comply the various guidelines issued by RBI and NABARD time to time.

NABARD guidelines issued on "***Cyber Security Frameworks' vide their EC No. 32/Dos-07/2020, Ref No. NB.DoS.Pol.HO/3182/j-1/2019-2020***" dated 06.02.2020.

IS Audit should include:-

- Determining effectiveness of planning and oversight of IT activities
- Evaluating adequacy of operating processes and internal controls
- Determining adequacy of enterprise-wide compliance efforts, related to IT policies and internal control procedures
- Identifying areas with deficient internal controls, recommend corrective action to address deficiencies and follow-up, to ensure that the management effectively implements the required actions

VAPT (Vulnerability Assessment & Penetration Testing) : VA (Vulnerability Assessment) of all major applications including CBS & Delivery Channels, and Penetration Testing of public facing applications viz. Internet Banking, Mobile Banking, Bank Website etc. Vulnerability assessment of all the critical servers/ devices.

Configuration Audit :- Configuration audit of various devices, especially for network & network security devices.

Bank's Information security & Information Technology Policies & Procedures

3.1 Core Banking Software Audit

The Application Software Audit shall involve assessment of compliance with specifications, standards, contractual agreements, functionality, regulatory compliance, systems manual and user's manual, change management procedures, user training, user feedback, critical evaluation of confidentiality, integrity and availability of the applications and their interfaces which are under the purview of the audit.

I. Software audit of following applications are to be carried out –

Core Banking Software

Core Banking Software Functionality Audit (with POC screenshots) of the CBS modules purchased from CBS vendor. Database security of audit of CBS database configuration and CBS application security related observations based on Open Web Application Security Project (OWASP) guidelines. Application meets the industry best practices securities standards. Find the bottlenecks in application which may lead to frauds.

i. Authorization Control such as concept of maker checker, exceptions, overriding exceptions, and error conditions.
ii. Authentication mechanism.
iii. User Management & Password Management
iv. Parameter Maintenance
v. Access rights;
vi. Access logs/ Audit Trail generation;
vii. Change management procedures including procedures for testing;
viii. Documentation of change management;
ix. Documentation of Data Centre Operations.

3.2 Mobile Banking Application and Internet Banking Audit

Mobile Banking & Internet Banking Application security audit based on Open Web Application Security Project (OWASP) guidelines with POC Screenshots. Information security related issues in Mobile Banking, Internet Banking and its department operations such as – customer applications, providing user account and PIN / Password to customer, customer requests / compliant handling, dispute management, NPCI Operating Circulars compliance verification (including NPCI Compliance Form). Analysis of architecture of channel from network security perspective.

i. To assess flaws in web server and Design of the Applications.
ii. Attempting to guess passwords using password-cracking tools.
iii. Search for back door traps in the software.
iv. Attempting to overload the systems using Distributed Denial of Services (DDOS) and Denial of Services (DOS) attacks.
v. Attempting penetration through perceivable network equipment/addressing and other vulnerabilities.
vi. Check Vulnerabilities like IP Spoofing, Buffer Overflows, session hijacks, account spoofing, Frame Spoofing, Caching of web pages, Cross site scripting, Cookie handling, injection flaws
vii. Check system of penetration testing and its effectiveness
viii. Sniffing.
ix. SSL Certificate & PKI verification.
x. Whether solution architecture provides 24 X 7 availability to customer. If all servers are configured to synchronize time with Central NTP server.
xi. To check whether date and time stamp are appearing correctly on all reports.
xii. To check whether servers are updated with latest security patches. Remote server Management Software used, Web logic server is up to date, IOS version in Router is vulnerable one.
xiii. Confirm Rule base in Firewall are configured properly.
xiv. To ascertain IDS is configured for intrusion detection, suspicious activity on host are monitored and reported to server, firewall and IDS logs are generated and scrutinized. IP routing is disabled.
xv. For changing system parameters whether Maker-Checker concept is followed.

xvi. Logical Access Controls Techniques viz. Passwords, Smart Cards or Other Biometric Technologies.
xvii. Proxy Server is issued between Internet and proxy systems.
xviii. Vulnerabilities of unnecessary utilities residing on Application server.
xix. Computer Access, messages are logged and security violations reported and acted upon.
xx. Effectiveness of Tools being used for monitoring systems and network against intrusions and attacks.
xxi. Proper infrastructure and schedule for back up is fixed, testing of back-up data done to ensure readability.
xxii. Legal issues.
xxiii. Electronic Record is authenticated by Asymmetric Cryptosystem and hash function.
xxiv. Secrecy and confidentiality of Customer preserved.
xxv. If any cases of unauthorized transfer through hacking, denial of service due to Technological failure is brought.
xxvi. Regulatory and Supervisory issues.
xxvii. Any other items relevant in the case of security.
xxviii. All the guidelines issued by RBI and NABARD from time to time relating to Bank's Official Website/Web hosting Software should be adhered to.

3.3 Vulnerability Assessment and Penetration testing (VAPT)

1. Auditor to perform Vulnerability Assessment and Penetration Testing on Banks:
   a. Application and its components including Web server, App server, DB Server,
   b.Mobile application,
   c.Networking systems
   d.Security devices
   e.Website
2. Auditor to carry out an assessment of Threat & Vulnerabilities assessments and assess the risks in Bank's Information Technology Infrastructure. This will include: identifying existing threats if any and suggest remedial solutions
3. VAPT should be comprehensive but not limited to following activities:
   a.Network Scanning &Port Scanning
   b.Vulnerability Scanning &Malware Scanning
   c.Application Security Testing & Code Review
   d.Denial of Service (DOS) Attacks &DDOS Attacks
   e.IDS/IPS review & Fine tuning of Signatures
   f.Social Engineering
   g.Any other attacks
4. Auditor should use the industry standard penetration test methodologies, scanning techniques and shall focus on internet and public facing applications. 5. Penetration tests should cover but not limited to OWASP Top 10 attacks for all the application servers

Note: 1.No remote access will be provided to the Auditor. 2.VA/PT will be scheduled during lean hours as per agreement with Bank

3.4 DC and DR (Current is at Collocation) Centre Operations Audit

1. Physical access controls;
   - Access control system
   - Fire / flooding / water leakage / gas leakage etc.
   - Handling of movement of man /material in /out of DC / DRC
   - Air-conditioning of DC / DRC
   - Electrical supply to DC/ DRC , Raw power / UPS / Genset
   - Surveillance system of DC / DRC
   - Redundancy of power level, UPS capacity at DC , DRC
   - Physical & environmental controls at DC & DRC
   - Assets safeguarding
   - Incident handling procedures
   - Parameters

2. Server system
   - Physical / logical access to the servers
   - Review of hardware installed in DC/DRC
   - Inventory management / movement
   - Configuration setting , parameterization
   - Performance monitoring vis –a – vis RFP and SLA
   - Audit logs / trails
   - User / privilege management, default / build-in account management
   - File system, directory & free space management
   - Domain control / administration
   - Backup and recovery policy and procedure
   - Cross check between the primary server at DC and standby server at DRS with special attention to : Configuration / file system set-up and system change management
   - Check & review application up & down time and various interfaces up time and down time

3. Environment management systems such as electrical supply, UPS, air-conditioning, fire detection and suppression, generator, etc.

I. Operating System (OS) Security :

The Auditor will review the operating system configuration and perform a preliminary assessment of its controls at DC, DRC. The review of the operating system will address:

- Operating System Installation

- Operating Systems Access controls
- Privilege Management
- Domain Account Policies
- Built In Accounts
- User Accounts Properties
- Groups
- Domain Administration
- Directory and File Security
- Back up & Recovery
- Set up and maintenance of operating system parameters;
- Updating of OS Patches;
- OS Change Management Procedures;
- Use of root and other sensitive passwords;
- Use of sensitive system software utilities;
- Interfaces with external applications (such as other electronic channels in the case of CBS and other external ATM switches such as NPCI in the case of the ATM system);
- Hardening of Operating System.

II. IS Audit of DR Site with respect to

1. Compliance with Bank's Disaster Recovery Plan aspects
2. Log shipping management
3. Electronic delivery channels support

III. DBMS and data security

Database configuration audit based on security configuration guideline released by OEM for database product version implemented by the Bank.

1. Secure use of SQL;
2. Control procedures for changes to the parameter files;
3. Logical access controls;
4. Control procedures for sensitive database passwords;
5. Control procedures for purging of Data Files;
6. Procedures for data backup, restoration, recovery and readability of backed up data.
7. Segregation of duties of database administrators
8. Password policies
9. User maintenance process
10. User access privileges
11. Authorization profiles
12. Database security functionality
13. Backup & Restore procedures
14. Archival & Purge Procedures
15. Backup security
16. Check the database for optimal performance
17. Monitoring the health of the database.
18. Synchronization between DC and DRC databases

Location - PDCC Bank, Head Office, Pune.

Data Centre at - **Pune District Central Co-operative Bank Ltd.**
Head Office: 4 B, B.J.Road,
Pune – 411001

DR Location at - PAI Data Center, Amravati, Andhra Pradesh.

Auditee – Bank IT Team and respective vendor representatives shall be available at HO for audit.

3.5 IT Setup at Head Office and Branches (Random on sample basis)

I. Maintenance of network connectivity to head office and branches
II. CBS application user management
III. IT Support to branches from IT department and vendors
IV. Anti-malware control
V. Physical security
VI. Information security awareness of users
VII. ATM management
VIII. Environmental controls for IT
IX. Business continuity arrangement at head office and branches

3.6 Scope of Migration Audit

Bank was migrated to new Core Banking Solution. Auditor shall verify following aspects as part of data migration audit –

I. Review data migration process adopted by the Vendor & Bank
II. Verify whether all the required data (Masters, Transactions, Meta Data etc.) has been migrated by the Bank from OMNI Enterprise Core Banking Solution version 2.0 & 3.0 to Trust Core Banking Solution
III. Report the observed discrepancies in the migrated data.
IV. 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.
V. The bidder is expected to study all the necessary documentation pertaining to data migration carried out by CBS Vendor.
VI. Validate migrated data: The bidder is expected to verify the integrity and correctness of the source data reconciled and uploaded into the System, identify the gaps in the data migration and provide a 'Migration audit report' stating the gaps identified in the data migration audit.

VII. 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.

3.7 Cyber Security Assessment.

NABARD guidelines issued on "***Cyber Security Frameworks' vide their EC No. 32/Dos-07/2020, Ref No. NB.DoS.Pol.HO/3182/j-1/2019-2020*** " dated 06.02.2020.

3.8 Deliverables

Pre Audit – Prior to starting the groundwork on the audit, the successful bidder shall provide Audit plan and procedure for Information System Audit AND VULNERABILITY ASSESSMENT AND PENETRATION TESTING (VAPT), Cyber Security Audit of Data Centre, Critical Applications, IT Processes etc. of the Bank. Detailed test cases and plans for the items as per scope of audit.

Vendor will involve the bank's staff during audit. All the audit reports/deliverables during and the end of audit will be property of the bank.

All reports should be submitted in soft as well as hard copy.

All Checklist and – used during the audit should be provided to the Bank.

Sr.no.	Audit area	Report (with Risk based categorization of observations)
1.	Complete scope	Executive summary
2.	Cyber security Assessment and migration audit,VAPT	Detailed report on discrepancies observed in assessment.
3.	Software audit	Detailed audit report of Core Banking Software and Mobile Banking, Internet Banking Software
4.	DC and DR (Current Collocation) Centre Operations	Detailed audit report
5.	IT Setup at Head office and branches	Detailed audit report of each location. Each branch shall have separate audit report.
6.	Audit observations	Audit observations should be classified as – a. High Risk b. Medium Risk c. Low Risk
7.	Audit Report	Draft report shall be discussed with concerned PDCC

		officer before submission of final report.

The audit firm may also submit specific suggestions/ recommendations based on the best industry practices. These suggestions may be part of report or submitted separately.

3.9 Time Frames

The bidder has to adhere to the following time lines

Stages	Particular	Period
Stage 1	Commencement of Audit work after acceptance assignment letter / contract	One week
Stage 2	Submission of audit plan, procedure and as per scope of work Stage	Two weeks
Stage 3	Submission of Interim report-after Stage 2	Three weeks
Stage 4	Submission of Final report after Stage 3	Four weeks
Stage 5	Submission of final compliance review report – after Stage 4	Four weeks

3.10 Compliance Verification

- Bank shall submit the compliance measures (implemented and to be implemented with timeline) to the auditor by 15 days from submission of final reports.
- For implemented compliance measures, one round of compliance verification audit shall be carried out by the auditor.

4 Evaluation Procedure

1. Eligibility Evaluation
2. Post eligibility evaluation commercial bid will be opened for all the eligible bidders and declare the **LOWEST COMMERCIAL PRICE** quoted bidder as the **WINER and award letter issued to the Firm/Company.** Bank may negotiate with the Lowest commercial quoted by the bidder before issuing award letter.

5 Commercial Bid

Commercial Bid Format [to be provided in a separate password protected PDF file named as "Commercial Bid for Selection of IT System Auditor for 2022-2023"].

Other than applicable taxes, PDCC will neither provide nor reimburse expenditure towards any type of accommodation, travel ticket, airfares, train fares, halting expenses, transport, lodging, boarding etc.

Sr.no.	Particular	Audit fees	Applicable Tax rate	Total Fees (in Figures and Words)
1.	Information System Audit for FY 2022-23: I. Core Banking Software II. Mobile Banking and Internet Banking Data Centre Operation			
2.	IT Setup at HO / Branches (2 identified branches)			
3.	Migration Audit			
4.	Cyber Security Assessment			
Total				

Commercial for Non TCO Items

Sr.No.	Particular	Audit Fees	Applicable Tax rate	Total Fees (in Figure and Words)
1	Vulnerability Assessment and Penetration Testing on rate contract basis applicable for 5 years. The same will be conducted based on the change in Application software version			
Total				

Annexure – I

CV of Core Audit Team Member

(Ref: - RFQ _____dated_____for IS Audit)
(To be furnished on a separate sheet for each Team member)

Name of Staff	
Date of Birth	
Professional Qualifications/ Certifications	
Services in the firm from	

Previous employment record	Organization	From	To
Activities carried out			
Details of key assignments handled in the past three years			
Organization	Month and year	Details of assignment carried out	