

**KOLHAPUR DISTRICT CENTRAL CO-OPERATIVE BANK LTD.****INFORMATION TECHNOLOGY DEPARTMENT**

HEAD OFFICE: Kolhapur District Central Co-op. Bank Ltd.,
1092, E Ward, Shahupuri, Kolhapur.
Pin – 416001

REQUEST FOR PROPOSAL (RFP)**FOR****Selection of IT System Auditor for FY 2024-2025**

REF NO.: RFP/IT/2024-25/006

PARTICULARS	DEADLINE
Availability of Bid Document at Bank's website	28/12/2024 up to 10.00 AM
Last date for receiving queries through e-mail:	03/01/2025 up to 12:30 PM
Last date of submission of the Technical and Commercial bid	13/01/2025 up to 12:30 PM
Date of opening of the Technical bid	15/01/2025 up to 1:00 PM
Bank email id for RFP related communication	manager.it@kdccbank.com

**Disclaimer**

The information contained in this scope 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 scope document and all other terms and conditions subject to which such information is provided. This scope is neither an agreement nor an offer and is only an invitation by Bank to the interested parties for submission of bids. The purpose of this RFP is to provide the bidder(s) with information to assist the formulation of their proposals. While effort has been made to include all information and requirements of the Bank with respect to the solution requested, this RFP 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 RFP 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 RFP. The Bank may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFP.



Contents

1. Introduction	4
2. Detailed Scope of Work	4
2.1. Core Banking Software Audit	4
2.2. Electronic Funds Transfer Switch Audit	5
2.3. Mobile Banking Application IMPS, UPI, Micro-ATM and BBPS Audit.....	5
2.4. DC and DR Centre Operations Audit	7
2.5. IT Setup at Head Office and Branches (Random 5 Branches recommended by Bank).....	8
2.6. Core IT Operations	8
2.7. Vulnerability Assessment and Penetration Testing (2 Audits – First Audit plus Compliance Audit) 8	
2.8. Cyber Security Controls Review	8
2.9. Deliverables.....	9
2.10. Time Frames.....	9
2.11. Compliance Verification	9
3. Eligibility Criteria	10
4. Evaluation Procedure	11
5. Introduction to the Bidders.....	11
5.1. Submission of Bid	11
5.2. Limitation of Liability.....	12
5.3. Indemnity	12
5.4. Document To be submitted with Bid	13
5.5. Force Majeure	13
5.6. Bidder's Integrity.....	13
5.7. Bidder's Obligation.....	13
5.8. Information Ownership.....	14
5.9. No Legal Relationship.....	14
5.10. Errors and Omissions	14
5.11. Acceptance of Terms.....	14
5.12. Termination for Convenience	14
6. Commercial Bid Information.....	14
7. Payment Terms and Schedule.....	15
8. Annexure - 1 - Letter for Eligibility Bid & Commercial Bid	16
9. Annexure – 2 Bidder's Information.....	17
10. Annexure – 3 Confirmation to Eligibility Criteria	18
11. Annexure – 4 Letter of Confirmation	19
12. Annexure – 5 Commercial Bid.....	20



1. Introduction

Kolhapur District Central Co-operative Bank Ltd., (KDCCB) Kolhapur is a District Co-operative bank in Western region of Maharashtra. The bank, having 191 branches and Head Office, has computerized entire operation using Core Banking Solution. KDCC has co-located both, Data Centre at Mumbai and Disaster Recovery Site at Bangalore. KDCC Bank implemented following range of customer centric and other solutions:

- Core Banking Solution from Infracore Technologies including deposits, advances, RuPay KCC etc.
- Payment & Settlement Systems like NEFT, RTGS, CTS, and NFS etc.
- HRMS, Anti-Money Laundering Solution, Asset/Liability Management.
- Delivery Channels like ATM, POS, ECOM, SMS Alerts, Mobile Banking, Micro ATMs etc.

KDCC Bank plans to carry out following Information Systems (IS) Audit by outsourcing IS Audit FY 2024-25 comprising of –

- Core Banking Software Audit
- Electronic Fund Transfer Switch Audit
- Mobile Banking IMPS, UPI, Micro-ATM and BBPS Audit
- DC and DR Centre Operations Audit
- IT Setup at Head Office and five Branches recommended by Bank
- Core IT Operations
- Vulnerability Assessment and Penetration Testing. The same will be conducted based on the change in Application software version.
- Cyber Security Controls Review

2. Detailed Scope of Work

Bank is inviting bids to shortlist the auditor to conduct Information System audit for FY 2024-25 as per the scope mentioned below:

2.1. Core Banking Software Audit

I. 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.

II. 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.

- 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.
- x. All statutory /MIS reports.
- xi. Overall CBS operational review.

2.2. Electronic Funds Transfer Switch Audit (Pertaining to NFS-OSG Guidelines V2.3 or latest)

Audit report of ATM Switch Vendor services – ATM Switching, ATM / POS / ECOM / other devices configuration, Carding, PIN Printing, and Implementation of compliance of NPCI Operating Circulars, Reconciliation, Chargeback and Dispute Management. Audit report should be based on PCI-DSS standard guidelines.

- i. PIN Management
- ii. Card Management
- iii. Delivery of ATM cards/ PINs to customers
- iv. Hot listing of cards
- v. Customer dispute resolution
- vi. Reconciliation within the Bank and with settlement agency/Banks
- vii. ATM Network Security Architecture Analysis
- viii. ATM functionality audit,
- ix. ATM Switch,
- x. Micro ATM service (Transaction Flow, Application, Devices, Reconciliation, Security, MIS)
- xi. ATM Switch Reconciliation,
- xii. Vulnerability analysis of ATM Network,
- xiii. Database controls,
- xiv. Backup & Recovery,
- xv. Analysis of administrative procedures,
- xvi. Outsourcing arrangements,
- xvii. ATM sharing arrangements with other Banks/RuPay and other agencies and compliance thereof.

2.3. Mobile Banking Application IMPS, UPI, Micro-ATM and BBPS Audit

Mobile Banking Application, Micro-ATM Application security audit based on Open Web Application



Security Project (OWASP) guidelines with POC Screenshots. Information security related issues in Mobile Banking Department operations such as – customer applications, providing user account and PIN to customer, customer requests / compliant handling, integration with Bill Payment channel vendors (if bill payment is integrated with MB), IMPS/UPI/BBPS reconciliation, customer chargeback / dispute management, NPCI settlement posting in CBS, NPCI Operating Circulars compliance verification (including NPCI Compliance Form). Analysis of network 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, 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.

2.4. DC and DR Centre Operations Audit

I. Physical security

- a. Physical access controls
- b. Environment management systems such as electrical supply, UPS, air-conditioning, fire detection and suppression, generator, etc.

II. Operating System (OS)

- a. Set up and maintenance of operating system parameters
- b. Updating of OS Patches
- c. OS Change Management Procedures
- d. Use of root and other sensitive passwords
- e. Use of sensitive system software utilities
- f. 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)
- g. Hardening of Operating System.

III. IS Audit of DR Site with respect to

- a. Compliance with Bank's Disaster Recovery Plan aspects
- b. Log shipping management
- c. Electronic delivery channels support

IV. DBMS and data security

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

- a. Secure use of Oracle DB and MS-SQL
- b. Control procedures for changes to the parameter files
- c. Logical access controls
- d. Control procedures for sensitive database passwords
- e. Control procedures for purging of Data Files
- f. Procedures for data backup, restoration, recovery and readability of backed up data.

Location	- Head Office at Kolhapur,
Data Centre at	- ESDS Software Solution Ltd., 202 B Wing, Central Rd N, Gavate Wadi, MIDC Industrial Area, Airoli, Navi Mumbai, Maharashtra 400708



Disaster Recovery site - ESDS Software Solution Ltd.,
New STPI Building, 76 & 77 Hosur Road,
Electronic city phase-1, Bengaluru – 560 100

ATM Vendor DC Site – Infracore Technologies Ltd., Mumbai.

ATM Vendor DR Site – Trimax, Bengaluru, Karnataka

Mobile Banking DC Site – Sify, Airoli, Navi Mumbai

Mobile Banking DR Site – Trimax, Bengaluru, Karnataka

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

2.5. IT Setup at Head Office and Branches (Random 5 Branches recommended by Bank)

- 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
- X. IT/ Cyber Security Governance - Policies, Procedures, Business Continuity Plan, Disaster recovery Plan etc.
- XI. IT Outsourcing/ Third party/ Vendor management- Service Level Agreements (SLA), Non-Disclosure Agreements (NDA), Risk management, Business Continuity, Audit, Compliance monitoring etc.

2.6. Core IT Operations

- I. Application security controls, Change Management, IT operation management, Incident/Problem Management, Internal & External Interfaces, Bulk Transaction Posting, System Generated Transactions, Reports generation, Access Controls, Assets and Infrastructure security.
- II. Regulatory Compliances, Data protection.

2.7. Vulnerability Assessment and Penetration Testing (2 Audits – First Audit plus Compliance Audit)

- I. CBS Application
- II. Allied Applications
- III. Mobile Banking Application
- IV. DC Application
- V. CBS internal URL
- VI. Mail Application
- VII. Micro-ATM Application VII. ATM Switch
- VIII. UPI CBS Application
- IX. IMPS CBS Application
- X. BBPS CBS Application
- XI. All Critical IT Assets (Including Servers, Storage, SAN Switches, Routers, Firewalls, Manageable Switches, Sample Branch Network Devices etc.)
- XII. External Application-Website



2.8. Cyber Security Controls Review

Architecture, Network, Server and Endpoint security, Cyber Security Incident and Fraud Management, Overall Risk Management, VAPT review, Patching, Hardening, Encryption, and Training & Awareness etc.

2.9. Deliverables

Sr.no.	Audit area	Report (with Risk based categorization of observations)
1.	Complete scope	Executive summary
2.	Software audit	Detailed audit report of Core Banking Software and Mobile Banking Software
3.	DC and DR Centre Operations	Detailed audit report
4.	IT Setup at Head office and branches	Detailed audit report of each location. Each branch shall have separate audit report.
5.	Core IT Operations	Detailed audit report
6.	VA & PT	Detailed audit report
7.	Cyber Security Controls Review	Detailed audit report
8.	Audit observations	Audit observations should be classified as – a. High Risk b. Medium Risk c. Low Risk
9.	Audit Report	A draft report shall be discussed with concerned KDCC 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.

2.10. Time Frames

Sr.no.	Scope of Work	Timeline
1	Phase I: Information System Audit	30 days
2	Phase II: Submission of draft report and acceptance of final report	15 days
	Total	45 days

2.11. Compliance Verification

- Bank shall submit the compliance measures (implemented and to be implemented with timeline) to the auditor by 30 days from submission of final reports.
- For implemented compliance measures, one round of compliance verification audit shall be carried out by the auditor regarding following areas –
 - Core Banking Software audit (pt.2.1)
 - Electronic Funds Transfer Switch (pt.2.2)
 - Mobile Banking Application and IMPS (pt.2.3)
 - Data Centre Operations (pt.2.4)
 - IT setup at Head Office and Branches (pt.2.5)
 - Core IT Operations(pt.2.6)
 - Vulnerability Assessment and Penetration Testing(pt.2.7)
 - Cyber Security Controls Review(pt.2.8)



3. 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	Bidder should have Existence in at least 3 years and carrying out Information Systems Audit services.	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 (2021-2022, 2022-2023 and 2023-2024).	Audited Balance Sheet and Profit and Loss Account Statement for last three years.
4	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
5	The Bidder should be CERT-In empaneled vendor having expertise in carrying out Information Security Audits	Substantial Proof for CERT-In empaneled should be attached.
6	The bidder should have experience of conducting similar scope as proposed by KDCC. A minimum of 3 audit projects having scope of audit (all inclusive) as – a. Vulnerability Assessment and Penetration Testing (VAPT) b. IS Audit c. Cyber Security audit/assessment in banking environment where banks have their own data center. d. Data Center Operation Audit e. IT Setup at HO/Branches (5 identified branches) f. Application Software Audit: I. Core Banking software II. Allied Applications III. ATM Switch and Allied Solutions IV. Mobile Banking Application, Micro-ATM, BBPS, IMPS and UPI	Credentials from clients in form of purchase orders / contract / credential letters etc.

Please note –

1. The bidder who does not fulfil 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. Proof of Certification of Professionals (CA / CISA / CISSP / CEH / Other) should be valid and must have company seal of submitting organization.
3. All the proofs attached should have company seal and self-attested by authorized signatory.



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. Introduction to the Bidders

5.1. Submission of Bid

- i. Bidders are required to submit the Eligibility Bid cum Technical Bid and Commercial bid in physical form as per the submission timeline. The Language of Bid should be in English.
- ii. The bidder will take care of submitting the Bid properly filed so that the papers are not loose. The Bids, which are not sealed as indicated above, may be liable for rejection.
- iii. The tender not submitted in the prescribed format or incomplete in any aspect is liable for rejection. The Bank is not responsible for non-receipt of bid within the specified date and time due to any reason including postal delays or Holidays.
- iv. The Eligibility cum Technical Bid will be submitted in separate envelope marked as “**Eligibility Bid for Selection of IT System Auditor for FY 2024-2025**” and commercial bid will be put in a separate envelope marked as “**Commercial Bid for Selection of IT System Auditor for FY 2024-2025**”. Both bid put together in an outer envelope marked as “**RFP response for Selection of IT System Auditor for FY 2024-2025**”.
- v. In addition to the above marking, each envelope must be super-scribed with the following information:
 - a. RFP Reference Number.
 - b. Name and Address of Bidder.
 - c. All the inner and outer envelopes shall be addressed to the Bank at the address given below:

**The Chief Executive Officer,
Kolhapur District Central Co-operative
Bank Ltd. Head Office: 1092, E Ward,
Shahupuri,
Kolhapur. Pin-
416001 0231-
2531641 to
2531650**
- vi. **Soft Copy** : The Eligibility Bid shall be submitted in separate PDF marked as Eligibility Bid for Selection of IT System Auditor for FY 2024-2025 and commercial bid shall be in a separate password protected PDF file marked as “Commercial Bid for Selection of IT System Auditor for FY 2024-2025”. Both bid put together in zip folder as “RFP response for Selection of IT System Auditor for FY 2024-2025”. The commercial bid should be password protected and the password of the Commercial Bid file should be shared in separate mail only after KDCC Bank’s request email. If the commercial bid submitted by the bidder without password along with the technical bid, then the bidder will be considered as disqualified.

vii. Bid Security - Earnest Money Deposit (EMD)

The bidder shall furnish as part of its bid, bid security of INR 1,00,000/- (Rupees One Lacs



Only) in the form of RTGS/NEFT only (A/c no. : 000113032000001, IFSC : IBKL0463KDC, A/c Name: - Kolhapur District Central Cooperative Bank Ltd, Branch:: Head Office). Bidder are requested to submit the UTR/fund transfer details with the technical bid response. Otherwise the bid response will be rejected by bank).

The bid security submitted by the bidder shall be forfeited if:

- a) The bidder withdraws the bid within the bid validity period; or
- b) The bidder fails to accept the "Letter of Award" within the given stipulated time; or
- c) The bidder violates any of the provisions of the terms and conditions of this bid document.

The bid security will be refunded to:

- a) The unsuccessful bidder(s), only after acceptance of the "Letter of Award" by the successful bidder and the EMD will be refunded.

viii. Cost of Bid - Rs. 5,000/- + Rs. 900/- (GST) = Rs. 5,900/- (Five Thousand Nine Hundred Only) in form of NEFT. Bidder should submit the cost of bid through NEFT (A/c no.: 000113032000001, IFSC: IBKL0463KDC, A/c Name: - Kolhapur District Central Cooperative Bank Ltd, Branch: Head Office) with the eligibility cum technical bid. If any bid response found without any bid document cost, then the bid will be rejected by the bank.

ix. Telex, Cable, Facsimile or Hard Copy Bids will not be accepted.

5.2. Limitation of Liability

The aggregate liability of the vendor in connection with this Agreement, the services provided by the bidder for the specific scope of work document, regardless of the form or nature of the action giving rise to such liability (whether in contract, tort or otherwise) and including any and all liability shall be the actual limited to the extent of the total contract value.

5.3. Indemnity

The bidder shall, at its own cost and expenses, defend and indemnify the bank against all third-party claims including those of the infringement of intellectual property rights, including patent, trademark, copyright, trade secret or industrial design rights, arising from the performance of the contract.

The bidder shall expeditiously meet any such claims and shall have full rights to defend itself therefrom. If the bank is required to pay compensation to a third party resulting from such infringement etc., the bidder will bear all expenses including legal fees.

Bank will give notice to the bidder of any such claim and shall provide reasonable assistance to the Bidder in disposing of the claim.

The bidder shall also be liable to indemnify the bank, at its own cost and expenses, against all losses/damages, which bank may suffer on account of violation by the bidder of any or all applicable national/ international trade laws. This liability shall not ensue if such losses/damages are caused due to gross negligence or willful misconduct by the bank or its employees.



5.4. Document To be submitted with Bid.

The Bidders shall submit the following documents along with Bid in PDF file.

Sr.No.	Particulars	Annexure / Document
1	Letter of Eligibility Bid & Commercial Bid	Annexure – 1
2	Bidder's Information	Annexure – 2
3	Confirmation to Eligibility Criteria	Annexure – 3
4	Letter of Confirmation	Annexure – 4
5	Bidder's proposed methodology/approach for providing services to the Bank with respect to the scope of work	
6	Commercial Bill of Material (To be provided in a separate envelope)	Annexure 5 - Commercial BOM

5.5. Force Majeure

The bidder shall not be liable for forfeiture of its performance security, liquidated damages or termination for default, if any to the extent that it's delays in performance or other failure to perform its obligations under the contract is the result of an event of Force Majeure.

For purposes of this Clause, "Force Majeure" means an event beyond the control of the bidder and not involving the bidder's fault or negligence and not foreseeable. Such events may include, but are not restricted to, acts of the Bank in its sovereign capacity, wars or revolutions, fires, floods, epidemics, quarantine restrictions.

If a Force Majeure situation arises, the bidder shall promptly notify the Bank in writing of such condition and the cause thereof within fifteen calendar days. Unless otherwise directed by the Bank in writing, the bidder shall continue to perform its obligations under the Contract as far as is reasonably practical and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event.

5.6. Bidder's Integrity

The bidder is responsible for and obliged to conduct all contracted activities in accordance with the contract using state of the art methods and economic principles and exercising all means available to achieve the performance specified in the contract.

5.7. Bidder's Obligation

The bidder is obliged to work closely with the Bank's staff, act within its own authority and abide by directives issued by the Bank and implementation activities.

The bidder is responsible for managing the activities of its personnel or its representatives and will hold itself responsible for any misdemeanors. The bidder is under obligation to provide consultancy services as per the contract.

The bidder will treat as confidential all data and information about the Bank, obtained in the execution of their responsibilities, in strict confidence and will not reveal such information to any other party without the prior written approval of the Bank.



5.8. Information Ownership

All information processed, stored, or transmitted by Vendor equipment belongs to the Bank. By having the responsibility to maintain the equipment, the vendor does not acquire implicit access rights to the information or rights to distribute the information. The vendor understands the civil, criminal, or administrative penalties may for failure or protect information appropriately.

5.9. No Legal Relationship

No binding legal relationship will exist between any of the Respondents and KDCC until execution of a contractual agreement.

5.10. Errors and Omissions

Each Recipient should notify KDCC of any error, omission, or discrepancy found in this RFP document.

5.11. Acceptance of Terms

A recipient will, by responding to KDCC for RFP, be deemed to have accepted the terms of the Introduction and Disclaimer. If the submission does not include all the information required or is incomplete, the proposal is liable to be rejected.

All submissions, including any accompanying documents, will become the property of KDCC. Recipients shall be deemed to license, and grant all rights to KDCC to reproduce the whole or any portion of their submission for the purpose of evaluation, to disclose the contents of the submission to other Recipients 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.

5.12. Termination for Convenience

The Bank, by written notice sent to the bidder, may terminate the Contract with a notice of 15 days, in whole or in part, at any time for its convenience. The notice of termination shall specify that termination is for the Bank's convenience, the extent to which performance of work under the Contract is terminated and the date upon which such termination becomes effective.

6. Commercial Bid Information

The L1 bidder shall be evaluated on the base of the Composite rate of both the above items.

- Terms:
1. The quoted price is valid for next 180 days.
 2. Taxes are extra at actuals.
 3. If any changes in taxes during the project tenure the same will be borne by the bank.

For commercial, the bidder requires to refer the Annexure 5- Commercial Bid.



7. Payment Terms and Schedule

The commercial bid submitted by the Bidder must be in conformity with the payment terms proposed. Any deviation from the proposed payment terms would not be accepted. In case of delays or defaults on the part of the Bidder, the Bank shall have the right to withhold payment of the effected product and/or service due to the Bidder or withhold the payment of the disputed amount. Such withholding of payment shall not amount to a default on the part of the Bank. KDCC will release payment within 30 days of receipt of Invoice and along with all other required documents for all undisputed cases. In case of any disputed amount, the payment will be released within 15 days of resolution of the dispute. The scope of work is divided in different areas and the payment would be linked to delivery, acceptance and signoff by the respective Bank official of each area as explained below with reference to the **Annexure - 5 – “Commercial Bid”**. The bidder shall raise any invoices only after signing off for the related deliverables/Services. The currency or currencies in which payments shall be made to the supplier/ selected bidder under this Contract shall be Indian Rupees (INR) only. Taxes, as applicable, will be deducted/ paid as per the prevalent rules and regulations.

I. The payment terms will be as follows:

A) IS Audit -

- 1) 40% on submission of draft report of IS Audit.
- 2) 50% on submission of Final IS Audit report and acceptance report by Bank.
- 3) 10% on submission of IS Audit compliance certificate to Bank.

B) VA & PT Audit -

- 1) 40% on submission of first VA & PT Audit report.
- 2) 50% on submission of compliance report of first VA & PT Audit and submission of second VA & PT Audit report
- 3) 10% on submission of second VA & PT Audit compliance report.

II. Other Terms & Conditions

- a) The audit will conduct IS Audit as per the RBI & other guidelines.
- b) Taxes: GST Tax extra as applicable. Bank will deduct TDS at prevailing rates.
- c) You will enter into agreement with the Bank for conducting audit.
- d) You will sign NDA with the Bank.
- e) The detail scope of work, time frames, deliverables, and payment terms will be mentioned in the agreement in consultation with the Bank.
- f) You will submit detail audit plan before commencement of audit and finalize the same in consultation with the Bank.
- g) Bank will neither provide for reimburse expenditure towards any type of accommodation, travel ticket, airfares, Train fares, halting expenses, transport, lodging, boarding etc.



8. Annexure - 1 - Letter for Eligibility Bid & Commercial Bid

Ref: RFP/IT/2024-25/006, dated 28/12/2024

To,

The Chief Executive Officer
Kolhapur District Central Co-operative Bank
Ltd. Head Office: 1092, E Ward, Shahupuri.
Kolhapur, Pin – 416001

Bid response to Information Systems Audit [IS Audit] – FY 2024-25 Request for Proposal (RFP)

Having examined the BID (Ref: RFP/IT/2024-25/006, dated 28/12/2024) including all annexure, the receipt of which is hereby duly acknowledged, we, the undersigned, offer to deliver services in conformity with the said RFP and in accordance with our proposal and total cost indicated in the Commercial Bid and made part of this bid.

We undertake, if our bid is accepted, to deliver services and complete the project in accordance with the scheduled timelines.

We agree to abide by this bid for the period of 180 days from the date fixed for Technical bid opening and it shall remain binding upon us and may be accepted at any time before the expiration of that period.

Until a formal contract is prepared and executed, this bid, together with the bank's written acceptance thereof and bank's notification of award, shall constitute a binding Contract between us.

We undertake that, in competing for (and, if the award is made to us, in executing) the contract, we will strictly observe the laws against fraud and corruption in force in India namely "Prevention of Corruption Act 1988".

We understand that the bank is not bound to accept the lowest or any bid the bank may receive.

Place:

Dated: this day of 202 .

.....
.....Signature) (In the Capacity of)

Duly authorized to sign bid for and on behalf of



9. Annexure – 2 Bidder’s Information

Name of the Bidder	
Constitution & Year of Establishment	
Registered Office/Corporate office Address	
Mailing Address	
Name and designations of the persons authorized to make commitments to the Bank	
Telephone Fax e-mail	
Name & Addresses of Directors/Promoters	
Details of Organization Structure	
Gross annual turnover of the bidder. (Amount in INR Crore) 2021-22: 2022-23: 2023-24:	
Net Profit of the bidder: (Amount in INR Crore) 2021-22: 2022-23: 2023-24:	



10. Annexure – 3 Confirmation to 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	Bidder should have Existence in at least 3 years and carrying out Information Systems Audit services.	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 (2021-2022, 2022-2023 and 2023-2024)	Audited Balance Sheet and Profit and Loss Account Statement for last three years.
4	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
5	The Bidder should be CERT-In empaneled vendor having expertise in carrying out Information Security Audits	Substantial Proof for CERT-In empaneled should be attached.
6	The bidder should have experience of conducting similar scope as proposed by KDCC. A minimum of 3 audit projects having scope of audit (all inclusive) as – <ul style="list-style-type: none"> a. Vulnerability Assessment and Penetration Testing (VAPT) b. IS Audit c. Cyber Security audit/assessment in banking environment where banks have their own data center. d. Data Center Operation Audit e. IT Setup at HO/Branches (5 identified branches) f. Application Software Audit: <ul style="list-style-type: none"> I. Core Banking software II. Allied Applications III. ATM Switch and Allied Solutions IV. Mobile Banking Application, Micro-ATM, BBPS, IMPS and UPI 	Credentials from clients in form of purchase orders / contract / credential letters etc.



11. Annexure – 4 Letter of Confirmation

Ref: RFP/IT/2024-25/006, dated 28/12/2024

Date:

To,

The CEO,
Kolhapur District Central Co-operative Bank Ltd.
Head Office: 1092, E Ward, Shahupuri.
Kolhapur, Pin – 416001.

Dear Sir,

We confirm having submitted the Bid and annexures in accordance with the said RFP. The details submitted by us are true and correct to the best of our knowledge and if it is proved otherwise at any stage of execution of the contract, Kolhapur District Central Co-operative Bank has the right to summarily reject the proposal and disqualify us from the process.

We confirm that we will abide by the conditions mentioned in the Tender Document (RFP and annexure) in full or in accordance with the deviations in “Terms & Conditions” accepted by the bank.

We hereby confirming you that we will complete all the scope of work in the defined timeline mentioned in the RFP.

We, hereby acknowledge and confirm, having accepted that the Bank can at its absolute discretion, apply whatever criteria is deemed appropriate, not just limiting to those criteria set out in the RFP and related documents, in short listing of bidders.

We shall observe confidentiality of all the information passed on to us in course of the tendering process and shall not use the information for any other purpose than the current tender.

We also confirm that we have not been blacklisted by any Govt. Department/ PSU/PSE or Banks or otherwise not involved in any such incident with any concern whatsoever, where the job undertaken/performed and conduct has been questioned by any authority, which may lead to legal action.

Place:

Date:

SEAL

(Authorized Signatory)



12. Annexure – 5 Commercial Bid

Commercial Bid Format [to be provided in a separate envelope named as “Commercial Bid for Selection of IT System Auditor for FY 2024-2025”, also in a separate password protected PDF file marked as “Commercial Bid for Selection of IT System Auditor for FY 2024-2025”].

Other than applicable taxes, KDCC 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
1.	Information System Audit for FY 2024-25: a. Core Banking Software audit b. Electronic Funds Transfer Switch c. Mobile Banking Application and IMPS d. Data Centre Operations e. Core IT Operations f. Cyber Security Controls Review	
2.	IT Setup at HO / Branches (5 identified branches)	
3.	VA & PT Audit (2 Audits – VA & PT Audit plus Compliance Audit)	
Total :-		
In words:		

Commercial for Non TCO Items :

Sr.No.	Particular	Audit Fees
1	Sub AUA/ Sub KUA Annual IS Audit as per UIDAI checklist Ver.1.0 issued in April 2024. Timeline : 01 Week	
In words:		

Notes on Non TCO items

1. The Non TCO items cost will not be part of the TCO
2. KDCC Bank having rights to negotiate with the Non TCO items cost (if any proposed by the bidders)