



Central Bank of India

LIMITED TENDER

LIMITED TENDER

Reference Number: CO:DIT:PUR:2022-23:358 dated 16.06.2022

For

*Vulnerability Assessment and Penetration Testing
of various Applications in Central Bank Of India
and It's Two RRB's*

TABLE OF CONTENTS

❖ Invitation for Limited Tender	Page 3
❖ Instructions to vendors	Page 4
❖ Terms and Conditions	Page 12
❖ Proposal Formats	Page 18
❖ Commercial Proposal Format (Bid)	Page 19

Annexures

Annexure -I Offer covering letter	Page 20
Annexure -II Details of the Vendor	Page 21
Annexure -III Details of Applications(Central Bank of India)	Page 22
Annexure -IV Details of Applications (RRBs)	Page 23
Annexure -V Details of Applications Server (RRBs)	Page 24
Annexure -VI Details of Unix servers of RRBs	Page 25
Annexure -VII Instructions to Bidders for e - tendering	Page 26

Invitation for Limited Tender:

Central Bank of India invites online commercial bids from Service providers empaneled through Tender process CO:DIT:PUR:2021-22:336, dated 25/08/2021 are only eligible to submit bid for this for Security Audit (Vulnerability Assessment and Penetration Testing) of various applications in Central bank Of India and it's Two RRB as specified in this document.

The details are given below:

Date of issue of Limited Tender	16.06.2022
Last Date and Time for submission of online commercial bid	29.06.2022 before 3.00 P.M.
Date and Time of Commercial Bid Opening	29.06.2022 at 3.30 P.M.
Mode of Bid submission : Online	URL: https://centralbank.abcpurchase.com/EPROC
Address of Communication	Assistant General Manager - Compliance, Central Bank of India, Department of Information Technology, 4 th Floor, Plot No. 26, Sector – 11, Opposite to CBD Railway Station, CBD Belapur, Navi Mumbai – 400614
Email Id:	cmitcomp@centralbank.co.in
Contact Telephone Numbers	Phone : 022 - 67123559 : 022 – 67123666
Tender Document cost	Rs.1,000/- (Rupees One Thousand only) in the form of Demand Draft issued by a Scheduled Commercial bank (except Central Bank of India) in favour of “Central Bank of India” payable at Mumbai and the DD should be submitted along with the Commercial Bid. The tender fee can also be submitted by way of NEFT in account no. 3287810289 of Central Bank of India (IFSC Code – CBIN0283154) with narration “Tender ref no “ CO: DIT: PUR:2022-23:358 dated 16.06.2022 ” in favor of “Central Bank Of India” and payable at MUMBAI
Earnest Money Deposit	Mention details of PBG submitted after empanelment
Response Type - Single Bid	Document cost + Commercial Bid

Central Bank of India (CBI) is one of the leading public sector Banks with a large network of approximately 4689+ branches / offices spread across the country. Bank also, has two sponsored Regional Rural Banks namely UBGB, UBKGB.

Bank has implemented a host of customer centric delivery channel solutions like Internet Banking, Mobile Banking, Tab Banking, UPI, SMS Alerts and various other applications (Detailed list attached as Annexure-III-VI).

The Bank as a part of implementation of robust security features across the applications intends to carry out Security Audit of these applications and Bank's Official Website (along with associated hardware & network infrastructure and equipment supporting them) through third party vendor. For the purpose, an RFP to empanel service providers was floated and eligible vendors were shortlisted. Bank invites bids from such empanelled vendors for primarily undertaking inter-alia the activities mentioned in Scope of work.

Assistant General Manager - IT

Instructions to vendors

1. Basic Requirement:

Security Audit (Vulnerability Assessment and Penetration Testing) of the Bank's Internet Banking & Mobile Banking, Official Website and other applications including applications of two RRBs (Vulnerability Assessment) as per the list attached as Annexures III to VI.

2. Scope of the Job

The scope of the job is to carry out Security Audit (Vulnerability Assessment and Penetration Testing) of Bank's Internet Banking, mobile banking System, Bank's Official Website and other applications as per the list attached as Annexure-III & VI, during the contract period along with associated hardware & network infrastructure and equipment supporting them. As such, scope will also include DR Servers. Bank reserves the right to add/delete any application during the contract period. The security audit (Vulnerability Assessment and Penetration Testing) is to be done for the period from April to September' 2022.

The scope of work will be as detailed in clause no. 1.4 of Tender document CO:DIT:PUR:2021-22:336, dated 25/08/2021 and will also include the following:

Successful bidder must ensure that during the VAPT activity, level of intrusiveness & boundaries of testing are not violated. Roles and responsibilities of bidders would be as follows but not limited to: -

1. The security assessment should use the industry standard penetration test methodologies and scanning techniques, and will focus on applications.
2. Attempting to guess passwords using password-cracking tools.
3. Attempting penetration through perceivable network equipment/addressing and other vulnerabilities.
4. Check if any Vulnerability exists in the Servers, Database, Applications, Network and Security devices in scope without disturbing operations.
5. Sniffing Data or information.
6. To check whether there is any vulnerability present in all IT assets in scope.
7. To ascertain the configuration, placement and deployment of IDS is configured for intrusion detection, suspicious activity on host are monitored and reported to server, firewall and IDS logs are generated and scrutinized.
8. Vulnerabilities of unnecessary utilities residing on Application server.
9. Unnecessary ports or services open/ running on the servers.
10. Effectiveness of Tools being used for monitoring systems and network against intrusions and attacks.
11. If any cases of unauthorized access through hacking, denial of service due to technological failure is possible.
12. The assessment should include following sections for testing:-
 - a. DMZ Zone
 - b. Remote Access
 - c. Network Security Assessment

- d. Network Security Components
 - e. VPNs
 - f. VC & VoIP Communications Network
13. Provide scheduled updates regarding the project.
14. Provide documents / diagrams detailing the project information in a timely manner.

Vulnerability Assessment

To identify, rank, and report vulnerabilities that, if exploited, may result in an intentional or unintentional compromise of a system through a variety of automated tools combined with manual verification of identified issues. VAPT should be comprehensive but not limited to following activities: -

- **Network Scanning /Surveying** : Vendor shall identify active hosts on a network, for the purpose of simulating attack and also for network security assessment with the help of suitable procedure/tools including but not limited to :-
 - a. Examine Name server responses
 - b. Review the outer wall of the network
 - c. Review tracks from the target organization
 - d. Review Information Leaks
- **Port Scanning** : To find the active ports on server port addresses on a host vendor shall perform the following but not limited to :-
 - a. Error Checking
 - b. Enumerate Systems
 - c. Enumerating Ports
 - d. Verification of Various Protocol Response
 - e. Verification of Packet Level Response
- **Port sweep** : To scan multiple hosts for a specific listening port for potential vulnerabilities.
- **System & OS Fingerprinting** : To guess the system information i.e. type and version of OS etc.
- **System Identification & Trusted System Scanning** : Vendor shall perform the SITS scanning which would include but not limited to the following :-
 - a. Match each open port to a service and protocol.
 - b. Identify server uptime to latest patch releases.
 - c. Identify the application behind the service and the patch level using banners or fingerprinting.
 - d. Verify the application to the system and the version.
 - e. Locate and identify service remapping or system redirects.
 - f. Identify the components of the listening service.
 - g. Use UDP-based service and Trojan requests to all the systems in the network.

- **Vulnerability Scanning:** Vendor shall carry out VA for entire IT assets mentioned in Annexures and addendum if added in future
- **Malware Scanning :** Vendor shall do exhaustive scanning for hostile or intrusive software, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware, and other malicious programs.
- **Spoofing :** Vendor shall assess the scope of potential spoofing attacks i.e. IP, ARP etc. and other applicable ones in the Banks' environment
- **Security Policy Review:** Vendor shall carry out the review & assessment of Security Policies already in place for firewalls installed in the organization.
- **Services Probing :** Vendor shall do the following in connection with the following:-
 - a. Web Tracks
 - b. Mail Tracks
 - c. Name Services
 - d. Visible Documents
 - e. Anti-Virus and Trojan

Service Finger Printing: The vendor shall do the following:-

- a. Examine system responses to determine operating system type and patch level.
 - b. Examine application responses to determine operating system type and patch level.
 - c. Verify the TCP sequence number prediction for each live host on the network.
 - d. Search job postings for server and application information from the target.
 - e. Search tech bulletin boards and newsgroups for server and application information from the target.
 - f. Match information gathered to system responses for more accurate results.
- **Access Control Mapping:** ACL has to be reviewed and recommended for improvement.
- **Assessment of OS Hardening:** Vendor shall carry out the assessment of OS hardening to check & explore the gap in hardening, patch management etc.
- **Denial Of Service (DOS) Attacks :** Following points may be looked for DoS attack :-
 - a. Verify that administrative accounts and system files and resources are secured properly and all access is granted with "Least Privilege".
 - b. Check the exposure restrictions of systems to non-trusted networks
 - c. Verify that baselines are established for normal system activity
 - d. Verify what procedures are in place to respond to irregular activity.
 - e. Verify the response to SIMULATED negative information (propaganda) attacks.
 - f. Test heavy server and network loads.
- **DDOS Attacks:** All the steps as mentioned for DoS attack has to be verified.
- **Authorization Testing:** Vendor shall do the authorization & authentication testing for the present AD system.

- **Lockout Testing:** To mitigate the brute force attack etc., lockout testing must be carried out.
- **Password Cracking:** To mitigate the brute force attack, cryptographic attack etc., Password cracking testing must be carried out.
- **Cookie Security:** Vendor shall review the cookie settings and recommend the best practice for making the environment secure.
- **Cookie & Web Bug Analysis :** Vendor shall review the cookie for bugs and recommend the best practice for making the environment secure
- **Containment Measure Testing:** The vendor shall perform this test also wherever applicable.
- **DMZ Network Architecture Review:** Vendor shall review the present DMZ Network Architecture and recommend for the improvement if any.
- **Server Assessment (OS Security Configuration):** Vendor shall review the present configuration of critical servers and recommend for the improvement if any.
- **Security Device Assessment:** Vendor shall review the present security devices and recommend for the improvement if any.
- **Network Device Assessment:** Vendor shall review the present network devices and recommend for the improvement if any.
- **Database Assessment:** Vendor shall review the present databases and recommend for the improvement if any.
- **Website Assessment (Process):** Vendor would do the assessment of internet facing application as mentioned in the subsequent section with and without credentials having different access levels like operator, supervisor, administrator etc. to check for vulnerabilities like privilege escalation, input validation etc.
- **Vulnerability Research & Verification :** Vendor shall conduct the research including but not limited to the following :-
 - a. Integrate the currently popular scanners, latest scanning definitions/signatures, hacking tools and exploits into the tests.
 - b. Measure the target organization against the currently popular scanning tools.
 - c. Attempt to determine vulnerability by system and application type.
 - d. Attempt to match vulnerabilities to services.
 - e. Attempt to determine application type and service by vulnerability.
 - f. Identify all vulnerabilities according to applications.
 - g. Identify all vulnerabilities according to operating systems.
 - h. Identify all vulnerabilities from similar or like systems that may also affect the target systems.
 - i. Verify all vulnerabilities found during the exploit research phase for false positives and false negatives.
 - j. Verify all positives.

In addition to the above vendor shall perform Manual Vulnerability Testing and Verification also.

- **IDS/IPS review & Fine tuning of Signatures :** Vendor shall perform the IDS /IPS review including but not limited to the following :-
 - a. IDS and features identification

- b. Placement of IDS in the network
 - c. Testing IDS configuration
 - d. Reviewing IDS logs and alerts
- **Man in the Middle attack :-** To rule out the possibilities of eavesdropping the MIMA has to be accrued out
- **Man in the browser attack :** To rule out the possibilities of eavesdropping the MIBA has to be accrued out
- **Trusted Systems Testing:** The validity of trusted system also has to be checked.
- **Directory Traversal:** Directory Traversal is a type of HTTP exploit that is used by attackers to gain unauthorized access to restricted directories and files.
- **Linux Hacking:** Vendor would assess the security risk associated with systems running on Linux platform.
- **Keyloggers:** Keyloggers are a form of spyware where computer users are unaware their actions are being tracked.
- **Rootkit:** Vendor would assess the systems to see the presence or probability of presence of rootkit.
- **Botnet:** Vendor would assess the system to see the presence of botnet.
- **Any other attacks & Scenario Analysis:** Apart from all the above mentioned line item if any activity required if felt by Bank as well as vendor has to be carried out.

Website/Web – Application Assessment

Website/Web- Application assessment should be done as per latest OWASP guidelines including but not limited to the following:-

- **SQL Injection**
- **Broken Authentication and Session Management**
- **Cross-Site Scripting (XSS)**
- **Insecure Direct Object References**
- **Security misconfiguration**
- **Insecure Cryptographic Storage**
- **Sensitive Data Exposure**
- **Missing Function Level Access Control • Cross-Site Request Forgery (CSRF)**
- **Using Known Vulnerable Components**
- **Un-validated Redirects and Forwards**
- **Failure to Restrict URL Access**
- **Insufficient Transport Layer Protection**
- **Any other attacks, which are vulnerable to the web sites and web Applications**

The vendor has to perform the following activities also, to assess the internet facing applications:-

- **Re-Engineering**
 - a. Decompose or deconstruct the binary codes, if accessible.
 - b. Determine the protocol specification of the server/client application.

- c. Guess program logic from the error/debug messages in the application outputs and program behaviour/performance.

- **Authentication**

- a. Find possible brute force password guessing access points in the applications.
- b. Find a valid login credentials with password grinding, if possible.
- c. Bypass authentication system with spoofed tokens.
- d. Bypass authentication system using Injection attacks.
- e. Bypass authentication system with replay authentication information.
- f. Determine the application logic to maintain the authentication sessions - number of (consecutive) failure logins allowed, login timeout, etc.
- g. Determine the limitations of access control in the applications - access permissions, login session duration, idle duration.
- h. Determine the transmission of authentication credentials in clear text/ encrypted/ hash form.

- **Session Management**

- a. Determine the session management information - number of concurrent sessions, IP based authentication, role-based authentication, identity-based authentication, cookie usage, session ID in URL encoding string, session ID in hidden HTML field variables, etc.
- b. Guess the session ID sequence and format
- c. Determine the session ID is maintained with IP address information; check if the same session information can be retried and reused in another machine.
- d. Determine the session management limitations - bandwidth usages, file download/upload limitations, transaction limitations etc.
- e. Gather excessive information with direct URL, direct instruction, action sequence jumping and/or pages skipping.
- f. Gather sensitive information with Man-In-the-Middle attacks.
- g. Inject excess/bogus information with Session-Hijacking techniques.
- h. Replay gathered information to fool the applications.

- **Input Manipulation**

- a. Verify that input validation is happening at client or server or both end.
- b. Find the limitations of the defined variables and protocol payload - data length, data type, construct format etc.
- c. Use exceptionally long character-strings to find buffer overflows vulnerability in the applications. Concatenate commands in the input strings of the applications.
- d. Inject SQL language in the input strings of database-tiered web applications.
- e. Examine "Cross-Site Scripting" in the web applications of the system.
- f. Examine unauthorized directory/file access with path/directory traversal in the input strings of the applications.

- g. Use specific URL-encoded strings and/or Unicode-encoded strings to bypass input validation mechanisms of the applications.
- h. Execute remote commands through "Server Side Include".
- i. Manipulate the session/persistent cookies to fool or modify the logic in the server-side web applications.
- j. Manipulate the (hidden) field variable in the HTML forms to fool or modify the logic in the server-side web applications.
- k. Manipulate the "Referrer", "Host", etc. HTTP Protocol variables to fool or modify the logic in the server-side web applications.
- l. Use illogical/illegal input to test the application error-handling routines and to find useful debug/error messages from the applications.

- **Output Manipulation**

- a. Retrieve valuable information stored in the cookies
- b. Retrieve valuable information from the client application cache.
- c. Retrieve valuable information stored in the serialized objects.
- d. Retrieve valuable information stored in the temporary files and objects.
- e. Retrieve bulk information/ multiple rows from database.

- **Information Leakage**

- a. Find useful information in hidden field variables of the HTML forms and comments in the HTML documents.
- b. Find valuable information stored in the HTML source code on browser like Unencrypted View State
- c. Examine the information contained in the application banners, usage instructions, welcome messages, farewell messages, application help messages, debug/error messages, etc.

Penetration Testing

To identify ways to exploit vulnerabilities to circumvent or defeat the security features of system components through manual process that may include the use of vulnerability scanning or other automated tools, resulting in a comprehensive report.

Deliverables

Detailed technical Vulnerability Assessment and Penetration Test report should be provided which should contain:

- Executive Summary – Summarize the scope, critical findings, and the positive security aspects identified in a manner suitable for the management.
- Categorization of vulnerabilities based on risk level – The report should classify the vulnerabilities as High/Medium/Low based on the Impact and Ease of Exploitation.
- Details of the security vulnerabilities discovered during the review – The detailed findings should be brought out in the report which will cover the details in all aspects.
- Solutions for the discovered vulnerabilities – The report should contain emergency quick fix solutions and long term solutions based on industry standards.

Reports should be in -

- Soft copies with screen shots
- Hard copies – Two nos.
- Tool generated Outputs
- Soft outputs which are importable into a database, spread sheet, or GRC platform e.g. XML files, CSV files etc.
- Tracking sheet
- Metrics and Dashboards
- Power point presentation
- Vulnerabilities identified
- Exploit Reports and supporting Evidences
- Vulnerability ratings
- Threat Profile
- Test Plan
- Compliance profile covering compliance with Banks policies, legal and regulatory requirements (inclusive of RBI Guidelines on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds etc.)

3. Eligibility Criteria of Vendors:

Service providers empaneled through Tender process CO:DIT:PUR:2021-22:336, dated 25/08/2021 are only eligible to submit bid for this Limited Tender.

4. Terms and Conditions

Central Bank of India invites the Vendor's attention to the terms and conditions elaborated in Tender no. CO:DIT:PUR:2021-22:336, dated 25/08/2021 and following terms and conditions which underline this Limited Tender and which provide a statement of understanding between the interested parties.

4.1 Single Bid System

Mode of Bid submission : Online	URL: https://centralbank.abcpocure.com/EPROC
Response Type - Single Bid	Document cost + Commercial Bid

4.2 Date of Submission

The last date of online bid submission is as per details furnished in Table of contents on Page no:3 of this document.

4.3 Liabilities of Bank

This LIMITED TENDER is not an offer by Bank, but an invitation for Vendor responses. No contractual obligation on behalf of Bank whatsoever shall arise from the LIMITED TENDER process unless and until a formal contract is signed and executed by duly authorized officials of Bank and the Vendor(s).

4.4 Proposal Process Management

Bank reserves the right to accept or reject any and all proposals, to revise the LIMITED TENDER, to request one or more re-submissions or clarifications from one or more Vendors, or to cancel the process in part or whole. No Vendor is obligated to respond to or to continue to respond to the LIMITED TENDER. Additionally, Bank reserves the right to alter the requirements, in part or whole, during the LIMITED TENDER process, and without re-issuing the LIMITED TENDER. Each party shall be entirely responsible for its own costs and expenses that are incurred while participating in the LIMITED TENDER and contract negotiation processes.

4.5 Date of Bid Expiration

Proposals must be valid for a minimum of 30 days from the proposal date. Responses must clearly state the validity of the bid and its explicit expiration date.

4.6 Bidder Indication of Authorization to Bid

Responses submitted by a Vendor to this LIMITED TENDER, represent a firm offer to contract on the terms and conditions described in the Vendor's response. The proposal must be signed by an official authorized to commit the bidder to the terms and conditions of the proposal. Vendor must clearly identify the full title and authorization of the designated official and provide a statement of bid commitment with the accompanying signature of the official and submit the copy of power of attorney / authority letter authorizing the signatory to sign the bid.

4.7 LIMITED TENDER Ownership

The LIMITED TENDER and all supporting documentation/templates are the sole property of Central Bank of India and should NOT be redistributed, either in full or in part thereof, without the prior written consent of Bank. Violation of this would be a breach of trust and may, inter-alia cause the Vendor to be irrevocably disqualified. The aforementioned material must be returned to Bank when submitting the Vendor proposal, or upon request. In case the Vendor is not interested in responding to the LIMITED TENDER, the LIMITED TENDER documents and any appendices must be returned to Bank immediately.

4.8 Proposal Ownership

The proposal and all supporting documentation submitted by the Vendor shall become the property of Central Bank of India unless the Vendor specifically requests, in writing, that the proposal and documentation be returned or destroyed.

4.9 Bid Pricing Information

By submitting a signed bid, the Vendor certifies that:

The Vendor has arrived at the prices in its bid without agreement with any other bidder of this LIMITED TENDER for the purpose of restricting competition. The prices in the bid have not been disclosed and will not be disclosed to any other bidder of this LIMITED TENDER. No attempt by the Vendor to induce any other bidder to submit or not to submit a bid for restricting competition has occurred.

4.10 Bidder Status

Each Vendor must indicate whether or not they have any actual or potential conflict of interest related to contracting services with Central Bank of India.

4.11 Confidentiality

This document contains information confidential and proprietary to Central Bank of India. Additionally, the Vendor will be exposed by virtue of the contracted activities to internal business information of Bank, affiliates, and/or business partners. Disclosure of receipt of any part of the aforementioned information to parties not directly involved in providing the services requested could result in the disqualification of the Vendor, pre-mature termination of the contract, or legal action against the Vendor for breach of trust.

No news release, public announcement, or any other reference to this LIMITED TENDER or any program there under shall be made without written consent from Bank. Reproduction of this LIMITED TENDER, without prior written consent of Bank, by photographic, electronic, or other means is strictly prohibited.

4.12 Bid Security

Performance Bank guarantee submitted after empanelment through Tender no. CO:DIT:PUR:2021-22:336 will constitute bid security for this LIMITED TENDER and will be dealt with as per the terms and conditions mentioned the RFP.

4.13 Disclaimer

The Bank and/or its officers, employees disown all liabilities or claims arising out of any loss or damage, whether foreseeable or not, suffered by any person acting on or refraining from acting because of any information including statements, information, forecasts, estimates or projections contained in this document or conduct ancillary to it whether or not the loss or

damage arises in connection with any omission, negligence, default, lack of care or misrepresentation on the part of Bank and/or any of its officers, employees.

The short-listed vendor should execute (a) a Service Level Agreement, which would include all the services and terms and conditions of the services to be extended as detailed herein and as may be prescribed by the Bank and (b) Non-disclosure Agreement.

4.14 Right to Reject

Central Bank of India reserves the right to reject any or all proposals received in response to the LIMITED TENDER without assigning any reasons thereof.

Waive or modify any formalities, irregularities, or inconsistencies in proposal format delivery. Reserve the right to discuss any specific aspect/s of the proposal with any bidder and negotiate with more than one bidder at a time.

Accept/reject any counter proposal or addendum submitted by the bidder. Extend time for submission of all proposals.

Select the next most responsive vendor in the event of negotiations with the L1 vendor fail to result in an agreement within a specified time frame.

Share the information/ clarifications provided in response to LIMITED TENDER by any vendor, to any other vendor(s) /others.

4.15 Other General Conditions:

All responses received after the due date/time would be considered late and would not be accepted.

All responses should be in English Language. All responses by the vendors to this LIMITED TENDER document shall be binding on such vendors for a period of 120 days after the opening of the commercial bid.

All responses including commercial bid would be deemed to be irrevocable offers/proposals from the vendors and may if accepted by the bank form part of the final contract between the bank and the selected vendor.

Any commercial bid, submitted cannot be withdrawn /modified after the last date for submission of the bids unless specifically permitted by the bank.

The vendor is requested to quote in Indian Rupees (INR). Bids in currencies other than INR would not be considered.

Bank reserve the absolute right to reject the offer if it is not in accordance with its requirements and no further correspondence, whatsoever, will be entertained by the Bank in the matter.

The prices quoted by the vendor shall include all costs except taxes. The price payable to the vendor shall be inclusive of carrying out any modifications changes/upgrades to the software or equipment that is required to be used in order to carry out the specified assignments.

In case of any variation (upward or downward) in Government levies, taxes, GST, cess, excise etc. up to the date of invoice, the benefit or burden of the same shall be passed on or adjusted to

the bank. If the vendor makes any conditional or vague offers, without conforming to these guidelines, the bank will treat the prices quoted as in conformity with these guidelines and proceed accordingly. Local entry taxes or octroi whichever is applicable, if any, will be paid by the bank on production of relative payment receipts/documents. Necessary documentary evidence should be produced for having paid the customs/excise duty, sales tax, if applicable, and/or other applicable levies.

The project will be deemed complete only when the vendor with the satisfaction of the bank completes all the assignments contracted by the bank and all deliverables are provided.

Any additional or different terms and conditions proposed by the vendor would be rejected unless expressly assented to in writing by the bank.

All terms and conditions, payments schedules, time frame for completion of assignments as per this LIMITED TENDER will remain unchanged unless explicitly communicated by the Bank in writing to the vendor. The bank shall not be responsible for any judgments made by the vendor with respect to any aspect of the assignment.

All disputes and differences of any kind whatsoever, arising out of or in connection with this Offer or in the discharge of any obligation arising under this Offer (whether during the course of execution of the order or after completion and whether before or after termination, abandonment or breach of the Agreement) shall be resolved amicably. In case of failure to resolve the disputes and differences amicably the matter may be referred to a sole arbitrator mutually agreed upon after issue of at least 30 days' notice in writing to the other party clearly setting out there in the specific disputes. In the event of absence of consensus about the single arbitrator, the dispute may be referred to joint arbitrators, one to be nominated by each party, and the said arbitrators shall appoint a presiding arbitrator. The provisions of the Indian Arbitration and Conciliation Act, 1996, shall govern the arbitration. The venue of the arbitration shall be Mumbai jurisdiction only.

4.16 Payment Terms

The Vendor must accept the payment terms proposed by the Bank. The financial bid submitted by the vendor must be in conformity with the payment terms proposed by the bank. Any deviation from the proposed payment terms would not be accepted.

The bank shall have the right to withhold any payment due to the vendor, in case of delays or defaults on the part of the vendor. Such withholding of payment shall not amount to a default on the part of the bank.

The payment terms need to be read in conjunction with the price bid:

Payment will be made for each quarterly assignment as per the terms given below:-

- 1. 70% Fees for a quarter shall be paid after submission of the final report for VAPT exercise.**
- 2. 30% Fees for the quarter shall be paid on finalization and submission of closure report.**

Further, Vendor has to submit separate Invoice for Central Bank of India on Mumbai and two separate invoices for each RRB at their respective states as per payment ratio for each RRB provided by bank to L1 Vendor at the time of issuing purchase order.

4.17. Project Completion Time

Detailed and realistic Project Plan, Management and Implementation schedule should be provided. Approximate maximum time for completion of audit will be **Four (4) weeks (for each quarterly audit) from the date of the assignment.**

Further, vendor has to submit closure report/certificate within two weeks' time after submission of compliance report by the Bank.

Please note that scanning activity of various machines must be carried out after banking business or in night in consultation with respective team. Vendor has to certify that there will be no impact of smooth functioning of banking transactions due to various activities carried for VAPT.

4.18 Penalty Clause

The vendor must strictly adhere to the schedules for completing the assignments. Failure to meet these delivery dates, unless it is due to reasons entirely attributable to the bank, may constitute a material breach of the vendor's performance. In the event that the Bank is forced to cancel an awarded contract (related to this LIMITED TENDER) due to the vendor's inability to meet the established delivery dates, the bank may take suitable penal actions as deemed fit including invoking the PBG.

All deliverables including reports need to be submitted within 15 days from the actual deliverable date / completion of the activity. Bank will impose penalty on concerned Vendor for nonperformance of the contractual obligation in time schedule/ during currency of the contract. Penalty will be imposed on delay in submitting the necessary reports or non-performance of the contractual obligation as per time schedule @2.5% of order value per month or part thereof subject to maximum 10% of order value.

4.19 Force Majeure

The vendor shall not be liable for forfeiture of its performance security, liquidated damages or termination for default, if any to the extent that its delay 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 explicitly beyond the control of the vendor and not involving the vendor's fault or negligence and not foreseeable. Such events may include, Acts of God or of public enemy, acts of Government of India in their sovereign capacity and acts of war.

If a Force Majeure situation arises, the vendor shall promptly notify the Bank in writing of such conditions and the cause thereof within fifteen calendar days. Unless otherwise directed by the Bank in writing, the vendor shall continue to perform his 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.

In such a case the time for performance shall be extended by a period (s) not less than duration of such delay. If the duration of delay continues beyond a period of three months, the Bank and the vendor shall hold performance in an endeavor to find a solution to the problem.

Notwithstanding the above, the decision of the Bank shall be final and binding on the Vendor.

4.20 Acceptance of Terms and Conditions:

The vendors participating in the LIMITED TENDER process should give an Acceptance Certificate for all the points mentioned through 1 to 4.23. Otherwise their offers are liable to be rejected.

4.21 Performance Guarantee

The Performance Bank Guarantee submitted by successful bidder for empanelment would be treated as performance security for VAPT engagement through this LIMITED TENDER.

4.22 Responsibilities of the auditor

The Auditor shall ensure that:

1. The auditing is carried out strictly in accordance with the terms and conditions stipulated in the audit assignment contract as well as general expectations of the auditee from an auditor.
2. All applicable codes of conduct and auditing standards are adhered to with due professional care.
3. Will use audit tools that are licensed and not the trial versions. Auditor should disclose the details of the any automated tool used for accomplishing the audit process. The auditor must have the valid license of the said automated tool(s).
4. Plan of action of audit & compliance audit and deliverables for each should be specified for every quarter along with any reconciled plan of action for future.
5. Vulnerability Assessment and Penetration Testing is to be conducted preferably after business hours or such that peak hours for customer service are avoided.
6. Actual details of various production and UAT servers will be shared with L1 bidder at the time of audit.
7. VAPT exercise covers all the customizations done during the quarter and do not hamper normal working of the applications.

4.23 Quality of Audit

The selected vendor will ensure that the audit assignments are carried out in accordance with applicable guidelines and standards as mentioned in this document and terms and conditions specified by the CERT-IN, Department of Information Technology, and Ministry of Information Technology- Government of India.

Proposal Formats:

5. Acceptance Letter to be given by the Vendor

To
Central Bank of India,
Central Office,
Mumbai.

Dear Sir,

REG: Acceptance of the Terms and Conditions and Confirmation of the Offer.

The details submitted in the format-5 : “**COMMERCIAL BID – LIMITED TENDER FOR SECURITY AUDIT (VULNERABILITY ASSESSMENT AND PENETRATION TESTING) OF APPLICATIONS LISTED IN ANNEXURE-III - VI**” are true and correct to the best of our knowledge and if it is proved otherwise at any stage of execution of the contract, Central bank of India has the right to summarily reject the proposal and disqualify us from the process.

We hereby acknowledge and confirm having accepted all terms and conditions of the LIMITED TENDER, and Bank can at its absolute discretion apply whatever criteria it deems appropriate, not just limiting to those criteria set out in the LIMITED TENDER and related documents, in short listing of vendors for providing Audit services.

We also acknowledge the information that this response of our Company for the Bank's LIMITED TENDER process is valid for a period of 180 Days, for the selection purpose, from the date of expiry of the last date for submission for response to LIMITED TENDER and related enclosures.

We also confirm that we have noted the contents of the LIMITED TENDER including various documents forming part of it and have ensured that there is no deviation in submitting our offer in response to the tender. The Bank will have the option to disqualify us in case of any such deviations.

We also confirm that we will abide by the Terms & Conditions mentioned in the Tender no. CO:DIT:PUR:2021-22:336 and section-3 of this LIMITED TENDER and also abide by the scope detailed in Tender no. CO:DIT:PUR:2021-22:336 and Scope mentioned in section - 2 as given in the LIMITED TENDER Document in full and without any deviation.

Place:

Date:

Seal & Signature of the Vendor

6. COMMERCIAL BID:

(To be submitted as per this format only)

This bill of material must be attached in commercial offer. The vendor can also mention any other component(s) that are required for their solution implementation. The vendor must take care in filling price information in the commercial version, to ensure that there are no typographical or arithmetic errors. All fields must be filled up correctly.

Consolidated, all-inclusive fee for the total project of IT auditing as specified in the Request for Proposal should be mentioned.

SECURITY AUDIT (VULNERABILITY ASSESSMENT AND PENETRATION TESTING) OF APPLICATIONS LISTED IN ANNEXURE-III - VI

S. No.	Description	Fees in Rs.
1.	<p>The total fees for the IT auditing project to be paid (For Central Bank Of India) VAPT.(ANNEXURE-III-IV)</p> <ul style="list-style-type: none">• The consolidated fees offered against each of the specified components in the commercial proposal is all-inclusive amount and no other charges, whatsoever, is payable by the Bank for whatsoever reason.• The fees quoted should be exclusive all taxes, duties, levies, GST or any other costs.• The Bank would not make any payments in respect of other charges/reimbursement of expenses like traveling, boarding & lodging, conveyance, etc., for visits to the Bank's office/branches during the tenure of IT auditing. All discussions, meetings and presentations with the Bank will be carried out at CBS Department for the purpose of IT auditing relating to this LIMITED TENDER.• Bank will deduct the tax at source, if any, as per the prevailing laws.	
2.	<p>The total fees for the IT auditing project to be paid (For Two Regional Rural Banks sponsored by Central Bank Of India) (ANNEXURE-V-VI) VA only no PT for all two RRB as there is no web facing application</p> <ul style="list-style-type: none">• The consolidated fees offered against each of the specified components in the commercial proposal is all-inclusive amount and no other charges, whatsoever, is payable by the Bank for whatsoever reason.• The fees quoted should be exclusive all taxes, duties, levies, GST or any other costs.• The Bank would not make any payments in respect of other charges/reimbursement of expenses like traveling, boarding & lodging, conveyance, etc., for visits to the Bank's office/branches during the tenure of IT auditing. All discussions, meetings and presentations with the Bank will be carried out at CBS Department for the purpose of IT auditing relating to this LIMITED TENDER.• Bank will deduct the tax at source, if any, as per the prevailing laws.	
	Total Cost of Ownership (TCO) (1 + 2) (in figures)	
	Total cost of ownership (in words) Rupees _____	

Annexure -I

Offer covering letter

Date:_____2022

To:

Having examined the documents including all annexures the receipt of which is hereby duly acknowledged, we, the undersigned, offer to supply and deliver _____ (Description of Services) in conformity with the said documents in accordance with the Schedule of Prices attached in the offer and made part of this LIMITED TENDER.

If our offer is accepted, we undertake to commence activity within_____ (Number) days and to complete Audit as per the scope of work within _____ (Number) days calculated from the date of receipt of your Notification of Award/Letter of Intent.

We agree to abide by this offer till 30 days from the date of opening of bid and our offer shall remain binding upon us and may be accepted by the Bank any time before the expiration of that period.

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

We understand that the Bank is not bound to accept the lowest or any offer the Bank may receive.

Dated this ____ day of _____2022

Signature: _____

(in the Capacity of:) _____

Duly authorized to sign the offer for and on behalf of

Annexure-II

Details of the Vendor

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

Sno	Item	Details
1.	Name of Company	
2.	Mailing Address	
3.	Telephone and Fax numbers	
4.	Constitution of the Company	
5.	Name and designation of the person authorized to make commitments to the Central Bank Of India	
6.	Email Address	
7.	Sales Tax Number	
8.	Income Tax Number	
9.	GSTN No.	

Annexure - III

* Bank reserves the right to add/delete any application for VA/PT during the contract period.

LIST OF INTERNET FACING APPLICATIONS OF CENTRAL BANK OF INDIA FOR VAPT				
S.No.	Application	Department	Application	
			VA	PT
1	HRMS	ADMIN	Y	Y
2	Biometric Authentication System	ADMIN	Y	
3	IBM Integration Bus (FTM)	ADC / DLC		Y
4	Mobile Banking System	ADC / DLC	Y	Y
5	KIOSK	ADC / DLC	Y	
6	UPI	ADC / DLC		Y
7	Tab Banking	ADC / DLC		Y
8	Mobile App- Performatrix	IN-HOUSE		Y
9	Core Banking Solutions (B@ancs24)	CBS	Y	
10	Help desk-CA	DC	Y	
11	Internet Banking System	ADC / DLC	Y	Y
12	ASBA	ADC / DLC	Y	
13	m-PASSBOOK	ADC / DLC	Y	Y
14	Mobile APP - SMA/NPA tracker	ADC / DLC	Y	Y
15	DP Secure Software for Demat	ADC / DLC	Y	
16	CPPS	ADMIN	Y	
17	e-TDS	ADMIN	Y	
18	AML (AmLock)	ADMIN	Y	
19	Document Management System	ADMIN	Y	Y
20	Off Site Monitoring	DRC	Y	
21	Financial Inclusion – Aadhar Vault	FI	Y	Y
22	Trade Finance - FX24	FOREX	Y	
23	E MAIL	NETWORK	Y	Y
24	RTGS	ADMIN	Y	
25	NEFT	ADMIN	Y	
26	E-Treasury	ADMIN	Y	
27	SWIFT	ADMIN	Y	
28	SAS Risk Management (IRMS)	RMD	Y	
29	LENDSAFE	IDA	Y	Y
30	Credit Rating System	RMD	Y	
31	CTS	CBS REMITTANCE	Y	
32	Call Centre	ADMIN	Y	
33	Finnacle (RRBs)	FI	Y	
34	SDR	IDA		Y
35	ATM Switch	ADC / DLC	Y	
36	Privilege Identity Management (PIM)	ISD	Y	
37	CSOC	ISD	Y	
38	Bank's Website	TB & DP	Y	Y
39	BBPS	TB & DP	Y	Y
40	SFTP	DC		Y
41	BOARD PAC	ADMIN	Y	
42	CCIL – CROMS, NDSCALL, NDSOM, FXCLEAR	ADMIN	Y	
43	DARS	DC	Y	
44	DIGITAL RIGHTS MANAGEMENT	ISD	Y	
45	SASIS	ADMIN	Y	
46	Cyber Security Solution	ISD	Y	
47	EFRMS	RMD	Y	
48	SAS Market Risk	RMD	Y	
49	E Learning – CentSwadhey	SPBT	Y	Y
50	Digital Rights Management	TB & DP	Y	Y
51	Staff Circulars	IN-House	Y	Y
52	PFMS	ADC / DLC	Y	Y
53	Mobile Device Management	ISD	Y	Y

Annexure –IV

SERVERS OF CENTRAL BANK FOR VA

SN	Servers	Qty	SN	Servers	Qty
1	ADHOC REPORTS	1	39	GST	8
2	ALL-IN-1	3	40	GST (No Owner)	2
3	APMOSYS	1	41	HDV	4
4	APPNOMICS	1	42	HRMS	14
5	ASBA	7	43	IDA	2
6	ATM	4	44	IDBI	20
7	AUDIT	10	45	INB	9
8	AUDIT(biomtric)	4	46	IRMS	6
9	BIOMETRIC	2	47	KIOSK	5
10	BoardPAC	7	48	MMS helpdesk	35
11	CA - EMS	10	49	MOB-APP	10
12	CA - HD	8	50	M-PB	9
13	CA - HRMS	2	51	NOC	22
14	CA - ITCM	37	52	OMS	3
15	CA - SS	2	53	PSO	6
16	CA - UAT	6	54	RAM TOOL	7
17	CA - UIM	12	55	RMD	41
18	CA-HRMS	2	56	RTGS	11
19	cbsnethelp	1	57	SAM Sir	4
20	CIMS	4	58	SCANPLUS	9
21	CKYC	7	59	SDR	4
22	CLASS	8	60	SDR-IDA	35
23	DATA-ARC	12	61	SEBI	2
24	DBA	23	62	SOC	83
25	DC Bank	5	63	SPBT	4
26	DEMAT	4	64	SUN	23
27	DEVLOPMENT	13	65	swift	3
28	DLC	23	66	TCS	1
29	DMS	10	67	TCSCONFIG	2
30	DR Team	2	68	Transaction Banking	1
31	ETDS	7	69	TXN Banking (Digital Signage)	2
32	FE	19	70	VC Helpdesk	4
33	FI	3	71	VKYC	7
34	FI- CBoI	15	72	V-SOFT	1
35	FI-RRB	13	73	WINDOWS	118
36	FOREX	2			
37	FX	2			
38	GBM	2			

Annexure –V

* Bank reserves the right to add/delete any application during the contract period.

SN	WINDOWS APPLICATION SERVERS OF RRB FOR VA
1	Universal Discovery
2	Asset Manager
3	Accelerate Endpoint Manager
4	Application Performance Monitor
5	Operations Manager i
6	EMS Data base server
7	Service Manager WEB
8	Network Node Manager
9	Platform Service Controller
10	IIS FTP Server
11	Symantec End point Manager
12	Active Directory
13	Symantec Application's Database Server
14	HP-Data Flow Probe
15	Active Directory
16	ALM APPLICATION
17	Symantec Antivirus Database Server
18	McAfee Applications Database Server
19	McAfee DAM
20	McAfee ePolicy Orchestrator
21	Vmware Vsphere Update Manager
22	Blue coat Reporter
23	ALM APPLICATION
24	Arcos PIM Application
25	Arcos PIM Database Server
26	Arcos PIM Database Server
26	Dell Storage Manager
27	McAfee NSM
28	HP-Service Manager
29	GST Server
30	EDC messaging
31	Net vault Backup
32	V center Server
33	FTP SERVER
34	NEFT SERVER
35	RTGS SERVER
36	BLUE coat Director
37	OPS Director
38	UNI Management
39	VMware vRealize Operations Server
40	ESXI Host Servers

Annexure – VI

UNIX SERVERS OF RRBs FOR VA

SN	Servers for each of the two RRB
1	RRB DB server
2	RRB APP server
3	RRB Failover
4	CSIS DB server
5	GBM DB server
6	Web Server
7	RRB1 MIS
8	OS backup Server
9	Virtual IO Server
10	AML Database
11	AML Database
12	AML APP
13	AML APP

Annexure – VII

INSTRUCTIONS TO BIDDERS FOR e - TENDERING

The Bidders participating through e-Tendering for the first time, for Central Bank of India will have to complete the Online Registration Process on the portal. All the bidders interested in participating in the online e-Tendering process are required to procure Class II or Class III Digital e-Token having -2- certificates inside it, one for Signing/Verification purpose and another for Encryption/Decryption purpose. The tender should be prepared & submitted online using the bidder's authorized individual's (Individual certificate is allowed for proprietorship firms) Digital e-Token. If any assistance is required regarding e-Tendering (registration / upload / download/ Bid Preparation / Bid Submission), please contact on the support numbers given in the support details in 10.2 below.

Registration Process for Bidders

- a) Open the URL: <https://centralbank.abcpurchase.com/EPROC/>
- b) On Right hand side, Click and save the Manual "**Bidder Manual for Bidders to participate on e-tender**"
- c) Register yourself with all the required details properly.
- d) TRAINING: Agency appointed by the Bank will provide user manual and demo / training for the prospective bidders
- e) LOG IN NAME & PASSWORD: Each Bidder / Bidder will be assigned a Unique User Name & Password by the agency appointed by the Bank. The Bidders are requested to change the Password and edit the information in the Registration Page after the receipt of initial Password from the agency appointed by the Bank.

GENERAL TERMS & CONDITIONS: Bidders are required to read the "Terms and Conditions" section of the portal (of the agency concerned, using the Login IDs and passwords given to them.

Bid Submission Mode.	https://centralbank.abcpurchase.com/EPROC/ Through e-tendering portal (Class II or Class III Digital Certificate with both Signing & Encryption is required for tender participation)
Support person and phone number for e-tender service provider for any help in accessing the website and uploading the tender documents or any other related queries.	e-Procurement Technologies Limited Technical Support Team Mr. Sujith Nair : 079 68136857 [sujith@eptl.in] Ms. Geeta : 079 90334460 [geeta@auctiontiger.net] Ms.Khushboo : 09510813528 [khushboo.mehta@eptl.in] Ms. Pooja : 09328931942 [pooja.shah@eptl.in] Ms. Komal : 07904407997 [komal.d@eptl.in] Mr Nandan Valera : 9081000427 [nandan.v@eptl.in] Ms Vrusha Soni : 9904407997 [vrusha@eptl.in] Mobile Numbers: +91-9904407997 9081000427

Note: please note Support team will be contacting through email and whenever required through phone call as well. Depending on nature of assistance support team will contact on the priority basis. It will be very convenient for bidder to schedule their online demo in advance with support team to avoid last minute rush.

- f) All bids made from the Login ID given to the bidder will be deemed to have been made by the bidder.
- g) BIDS PLACED BY BIDDER: The bid of the bidder will be taken to be an offer to sell. Bids once made by the bidder cannot be cancelled. The bidder is bound to sell the material as mentioned above at the price that they bid.

Preparation & Submission of Bids

The Bids shall have to be prepared and subsequently submitted online only. Bids not submitted "ON LINE" shall be summarily rejected. No other form of submission shall be permitted.

Do's and Don'ts for Bidder

- a) Registration process for new Bidder's should be completed at the earliest
- b) The e-Procurement portal is open for upload of documents with immediate effect Hence Bidders are advised to start the process of upload of bid documents well in advance.
- c) Bidder has to prepare for submission of their bid documents online well in advance as
- d) The upload process of soft copy of the bid documents requires encryption (large files take longer time to encrypt) and upload of these files to e-procurement portal depends upon bidder's infrastructure and connectivity.
- e) To avoid last minute rush for upload bidder is required to start the upload for all the documents required for online submission of bid one week in advance.
- f) Bidder to initiate few documents uploads during the start of the RFP submission and help required for uploading the documents / understanding the system should be taken up with e-procurement bidder well in advance.
- g) Bidder should not raise request for extension of time on the last day of submission due to non-submission of their Bids on time as Bank will not be in a position to provide any support at the last minute as the portal is managed by e-procurement service provider.
- h) Bidder should not raise request for offline submission or late submission since only online e-Procurement submission is accepted.
- i) Part submission of bids by the Bidder's will not be processed and will be rejected.

Terms & Conditions of Online Submission

- a. Bank has decided to determine L1 through bids submitted on Bank's E-Tendering website <https://centralbank.abcprocure.com/EPROC>. Bidders shall bear the cost of registration on the Bank's e-tendering portal. Rules for web portal access are as follows:
- b. Bidder should be in possession of CLASS II or CLASS III-Digital Certificate in the name of company/bidder with capability of signing and encryption for participating in the e-tender. Bidders are advised to verify their digital

certificates with the service provider at least two days before due date of submission and confirm back to Bank.

- c. Bidders at their own responsibility are advised to conduct a mock drill by coordinating with the e-tender service provider before the submission of the technical bids.
- d. E-Tendering will be conducted on a specific web portal as detailed in (schedule of bidding process) of this RFP meant for this purpose with the help of the Service Provider identified by the Bank as detailed in (schedule of bidding process) of this RFP.
- e. Bidders will be participating in E-Tendering event from their own office / place of their choice. Internet connectivity /browser settings and other paraphernalia requirements shall have to be ensured by Bidder themselves.
- f. In the event of failure of their internet connectivity (due to any reason whatsoever it may be) the service provider or Bank is not responsible.
- g. In order to ward-off such contingent situation, Bidders are advised to make all the necessary arrangements / alternatives such as back -up power supply, connectivity whatever required so that they are able to circumvent such situation and still be able to participate in the E-Tendering Auction successfully.
- h. However, the bidders are requested to not to wait till the last moment to quote their bids to avoid any such complex situations.
- i. Failure of power at the premises of bidders during the E-Tendering cannot be the cause for not participating in the E-Tendering.
- j. On account of this, the time for the E-Tendering cannot be extended and BANK is not responsible for such eventualities.
- k. Bank and / or Service Provider will not have any liability to Bidders for any interruption or delay in access to site of E-Tendering irrespective of the cause.
- l. Bank's e-tendering website will not allow any bids to be submitted after the deadline for submission of bids. In the event of the specified date and time for the submission of bids, being declared a holiday for the Bank, e-tendering website will receive the bids up to the appointed time on the next working day. Extension / advancement of submission date and time will be at the sole discretion of the Bank.
- m. During the submission of bid, if any bidder faces technical issues and is unable to submit the bid, in such case the Bank reserves its right at its sole discretion but is not obliged to grant extension for bid submission by verifying the merits of the case and after checking necessary details from Service provider.
- n. Utmost care has been taken to reduce discrepancy between the information contained in e-tendering portal and this tender document. However, in event of any such discrepancy, the terms and conditions contained in this tender document shall take precedence.
- o. Bidders are suggested to attach all eligibility criteria documents with the Annexures in the technical bid.

Guidelines to Contractors on the operations of Electronic Tendering System of Central Bank of India

Pre-requisites to participate in the Tenders

Registration of Bidders on Electronic Tendering System on Portal of CBI: The Bidders Non Registered in Central Bank of India and interested in participating in the e-Tendering process of CBI shall be required to enroll on the Electronic Tendering System. To enroll Bidder has to generate User ID and password on the “[https://centralbank.abcprocure.com /EPROC](https://centralbank.abcprocure.com/EPROC)”

Registration of New Bidders:

<https://centralbank.abcprocure.com/EPROC/bidderregistration>

The Bidders may obtain the necessary information on the process of Enrollment either from Helpdesk Support Team: 079-68136815, 9879996111 or may download User Manual from Electronic Tendering System for CBI. i.e. <https://centralbank.abcprocure.com/EPROC>

Preparation of Bid & Guidelines of Digital Certificate

The Bid Data that is prepared online is required to be encrypted and the hash value of the Bid Data is required to be signed electronically using a Digital Certificate (Class – II or Class – III). This is required to maintain the security of the Bid Data and also to establish the identity of the Bidder transacting on the System. This Digital Certificate should be having Two Pair (1. Sign Verification 2. Encryption/ Decryption)

The Digital Certificates are issued by an approved Certifying Authority authorized by the Controller of Certifying Authorities of Government of India through their Authorized Representatives upon receipt of documents required to obtain a Digital Certificate.

Bid data / information for a particular Tender may be submitted only using the Digital Certificate.

Certificate which is used to encrypt the data / information and Signing Digital Certificate to sign the hash value during the Online Submission of Tender stage. In case, during the process of preparing and submitting a Bid for a particular Tender, the Bidder loses his / her Digital Signature Certificate (i.e. due to virus attack, hardware problem, operating system problem); he / she may not be able to submit the Bid online. Hence, the Users are advised to store his / her Digital Certificate securely and if possible, keep a backup at safe place under adequate security to be used in case of need.

In case of online tendering, if the Digital Certificate issued to an Authorized User of a Partnership Firm is used for signing and submitting a bid, it will be considered equivalent to a no objection certificate / power of attorney to that User to submit the bid on behalf of the Partnership Firm. The Partnership Firm has to authorize a specific individual via an authorization certificate signed by a partner of the firm (and in case the applicant is a partner, another partner in the same firm is required to authorize) to use the digital certificate as per Indian Information Technology Act, 2000 and subsequent amendment.

Unless the Digital Certificate is revoked, it will be assumed to represent adequate authority of the Authorized User to bid on behalf of the Firm for the Tenders processed on the Electronic Tender Management System of Central Bank of India as per Indian Information Technology Act, 2000 and subsequent amendment. The Digital Signature of this Authorized User will be binding on the Firm. It shall be the responsibility of Partners of the Firm to inform the Certifying Authority or Sub

Certifying Authority, if the Authorized User changes, and apply for a fresh Digital Signature Certificate. The procedure for application of a Digital Signature Certificate will remain the same for the new Authorized User.

The same procedure holds true for the Authorized Users in a Private / Public Limited Company. In this case, the Authorization Certificate will have to be signed by the Director of the Company or the Reporting Authority of the Applicant.

The bidder should Ensure while procuring new digital certificate that they procure a pair of certificates (two certificates) one for the purpose of Digital Signature, Non-Repudiation and another for Key Encryption.

Recommended Hardware and Internet Connectivity

To operate on the Electronic Tendering System, the Bidder are recommended to use Computer System with at least 1 GB of RAM and broadband connectivity with minimum 512 kbps bandwidth. However, Computer Systems with latest i3 / i5 Intel Processors and 3G connection is recommended for better performance.

Operating System Requirement: Windows 7 and above Browser Requirement (Compulsory): Internet Explorer Version 9 (32 bit) and above and System Access with Administrator Rights.

Toolbar / Add on / Pop up blocker

Users should ensure that there is no software installed on the computers which are to be used for using the website that might interfere with the normal operation of their Internet browser. Users have to ensure that they do not use any pop-up blockers, such as those provided by Internet Explorer and complementary software, like for example the Google tool bar. This might, in certain cases depending on users' settings, prevent the access of the EAS application.

Online viewing of Detailed Notice Inviting Tenders

The Bidders can view the Detailed Tender Notice along with the Time Schedule (Key Dates) for all the Live Tenders released by CBI on the home page of CBI e-Tendering Portal on <https://centralbank.abcpocure.com/EPROC>

Download of Tender Documents:

The Pre-qualification / Main Bidding Documents are available for free downloading. However, to participate in the online tender, the bidder must purchase the bidding documents via Demand Draft mode by filling the cost of tender form fee.

Online Submission of Tender

Submission of Bids will be preceded by Online Submission of Tender with digitally signed Bid Hashes (Seals) within the Tender Time Schedule (Key dates) published in the Detailed Notice Inviting Tender. The Bid Data is to be prepared in the templates provided by the Tendering Authority of CBI. The templates may be either form based, extensible tables and / or unloadable documents. In the form based type of templates and extensible table type of templates, the Bidders are required to enter the data and encrypt the data/documents using the Digital Certificate / Encryption Tool.

In case Unloadable document type of templates, the Bidders are required to select the relevant document / compressed file (containing multiple documents) already uploaded in the briefcase.

Notes:

- a) The Bidders upload a single documents unloadable option.
- b) The Bid hash values are digitally signed using valid class – II or Class – III Digital Certificate issued any Certifying Authority. The Bidders are required to obtain Digital Certificate in advance.
- c) The bidder may modify bids before the deadline for Online Submission of Tender as per Time Schedule mentioned in the Tender documents.
- d) This stage will be applicable during both. Pre-bid / Pre-qualification and Financial Bidding Processes.

The documents submitted by bidders must be encrypted using document encryption tool which available for download under Download section on:

<https://centralbank.abcprocure.com/EPROC>

Steps to encrypt and upload a document:

- Select Action: Encryption -> Tender ID: (enter desired tender ID) -> Envelope: (Technical / Price Bid) -> Add File: (Select desired document to be encrypted) -> Save File(s) to: (select desired location for encrypted file to save).
- After successful encryption, format of encrypted file will change to .enc which is required to be uploaded by bidders.
- After encryption bidders are required to upload document as per the mandatory list mentioned in the envelope i.e. Technical / Commercial.

Note: Bank and e-Procurement Technologies Limited shall not be liable & responsible in any manner whatsoever for my/our failure to access & bid on the e-tender platform due to loss of internet connectivity, electricity failure, virus attack, problems with the PC, any other unforeseen circumstances etc. before or during the event. Bidders are advised to ensure system availability and prepare their bid well before

time to avoid last minute rush. Bidder can fix a call with support team members in case guidance is required by calling on numbers mentioned in 10.2 above.

Bidders need to take extra care while mentioning tender ID, entering incorrect ID will not allow Bank to decrypt document.

Closure of Bidding:

After the expiry of the cut- off time of Online Submission of Tender stage to be completed by the Bidders has lapsed, the Tender will be closed by the Tendering Authority.

Online Final Confirmation:

After submitting all the documents bidders need to click on “Final Submission” tab. System will give pop up “You have successfully completed your submission” that assures submission completion.

*****END OF DOCUMENT*****