

# Request for Proposal

for

ICT Audit, IS Audit, VAPT & AUA/KUA Audit

of

06 SBI Sponsored RRBs

- 1 Arunachal Pradesh Rural Bank
- 2 Chhattisgarh Gramin Bank
- 3 Jharkhand Gramin Bank
- 4 Rajsthan Gramin Bank
- 5 Telangana Grameena Bank
- 6 Uttrakhand Gramin Bank



# SECTION – I

## **1. Introduction and Disclaimer**

This Request for Proposal document ("RFP") has been prepared solely to enable SBI Sponsored RRBs ("Bank") in the selection of suitable organization (Service Provider - SP) to tender for assisting the Bank in conducting ICT Audit , IS Audit and AUA / KUA Audit.

The RFP document is not a recommendation, offer or invitation to enter into a contract, agreement or other arrangement in respect of the services.

## **2. Details of Participating Banks:**

<b>SIno</b>	<b>Bank Name</b>	<b>Head Office</b>	<b>Proposed Audit Requirements</b>
1	Arunachal Pradesh Rural Bank ( <a href="https://www.aprb.bank.in/">https://www.aprb.bank.in/</a> )	Naharlagun (Arunachal Pradesh)	ICT, AUA-KUA , IS Audit & VAPT
2	Chhattisgarh Gramin Bank ( <a href="https://cgb.bank.in">https://cgb.bank.in</a> ) <b>(Nodal bank for this Common RFP )</b>	Nawa Raipur (Chhattisgarh)	ICT , AUA-KUA , IS Audit & VAPT
3	Jharkhand Gramin Bank ( <a href="https://jrgbank.bank.in/">https://jrgbank.bank.in/</a> )	Ranchi ( Jharkhand)	ICT , AUA-KUA , IS Audit & VAPT
4	Rajasthan Gramin Bank ( <a href="https://rgb.bank.in/">https://rgb.bank.in/</a> )	Camp Office : Jodhpur ( Rajasthan) Head Office: Jaipur (Rajasthan)	ICT , AUA-KUA , IS Audit & VAPT
5	Telangana Grameena Bank ( <a href="https://tgb.bank.in/">https://tgb.bank.in/</a> )	Hyderabad (Telangana)	ICT , AUA-KUA , IS Audit
6	Uttarakhand Gramin Bank ( <a href="https://ukgb.bank.in/">https://ukgb.bank.in/</a> )	Dehradun ( Uttarakhand)	ICT , AUA-KUA , IS Audit

## **3. Information Provided**

The RFP document contains statements derived from information that is believed to be reliable at the date obtained but does not purport to provide all of the information that may be necessary or desirable to enable an intending contracting party to determine whether or not to enter into a contract or arrangement with Bank in relation to the provision of services. Neither Bank nor any of its employees, agents, contractors, or advisers gives any representation or warranty, express or implied as to the accuracy or completeness of any information or statement given or made in this RFP document. Neither Bank nor any of its employees, agents, contractors, or advisers has carried out or will carry out an independent audit or verification or due diligence exercise in relation to the contents of any part of the RFP document.

## **4. For Respondent Only**

The RFP document is intended solely for the information of the party to whom it is issued ("the Recipient" or "the Respondent") and no other person or organization.

## **5. Confidentiality**

The RFP document is confidential and is not to be reproduced, transmitted, or made available by the Recipient to any other party. The RFP document is provided to the Recipient on the basis of the undertaking of confidentiality given by the Recipient to Bank. Bank may update or revise the RFP document or any part of it. The Recipient acknowledges that any such revised or amended document is received subject to the same terms and conditions as this original and subject to the same confidentiality undertaking.

The Recipient will not disclose or discuss the contents of the RFP document with any officer, employee, consultant, director, agent, or other person associated or affiliated in any way with Bank or any of its customers, suppliers, or agents without the prior written consent of Bank.

## **6. Disclaimer**

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

## **7. Costs Borne by Respondents**

All costs and expenses incurred by Recipients / Respondents in any way associated with the development, preparation, and submission of responses, including but not limited to attendance at meetings, discussions, demonstrations, etc. and providing any additional information required by Bank, will be borne entirely and exclusively by the Recipient / Respondent.

## **8. No Legal Relationship**

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

## **9. Recipient Obligation to Inform Itself**

The Recipient must conduct its own investigation and analysis regarding any information contained in the RFP document and the meaning and impact of that information.

## **10. Evaluation of Offers**

Each Recipient acknowledges and accepts that Bank may, in its absolute discretion, apply whatever criteria it deems appropriate in the selection of organizations, not limited to those selection criteria set out in this RFP document.

The RFP document will not be construed as any contract or arrangement which may result from the issue of this RFP document or any investigation or review carried out by a Recipient. The Recipient acknowledges by submitting its response to this RFP document that it has not relied on any information, representation, or warranty given in this RFP document.

### **11. Errors and Omissions**

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

### **12. Acceptance of Terms**

A Recipient will, by responding to Bank RFP, be deemed to have accepted the terms as stated above from Para 1 through Para 10.

### **13. Submission of Bids**

All submissions must be supplied to and addressed to "Bank's Evaluation Office" at:

**General Manager (Information  
Technology), Chhattisgarh Gramin  
Bank, Corporate Office, Plot No 47  
Sector-24 Nawa Raipur, Atal Nagar  
C.G - 492018**

#### **Submission will be valid if:**

Copies of the RFP are submitted before the schedule closing time by email.

Submission is not allowed by Fax transmission.

Bids are submitted in two separate files "Technical Proposal" & "Commercial Proposal".

**Commercial proposal should be password protected and the password will be shared only on the date of tender opening, when requested during live meeting.**

**Please do not share the password of Commercial proposal during submission of bids.**

#### **Only One Submission Permitted.**

Only one submission of tender by each SP will be permitted. In case of proprietorship / Partnerships / consortium, only one submission is permitted through the SP.

### **13.1 Registration of RFP**

Registration will be effected upon Bank receiving the RFP response in the above manner (Para 12). The registration must contain all documents, information, and details required by this RFP. If the submission to this RFP does not include all the information required or is incomplete or submission is through Fax mode, the RFP is liable to be rejected.

All submissions, including any Banking documents, will become the property of Bank. Recipients shall be deemed to license, and grant all rights to, Bank 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 who have registered a submission and to disclose and/or use the contents of the submission as the basis for any resulting RFP process, notwithstanding any copyright or other intellectual property right that may subsist in the submission or Banking documents.

### **13.2 Late RFP Policy**

Respondents are to provide detailed evidence to substantiate the reasons for a late RFP submission.

RFPs lodged after the deadline for lodgment of RFPs may be registered by Bank and may be considered and evaluated by the evaluation team at the absolute discretion of Bank. It should be clearly noted that Bank has no obligation to accept or act on any reason for a late submitted response to RFP. Bank has no liability to any person who lodges a late RFP for any reason whatsoever, including RFPs taken to be late only because of another condition of responding.

### **13.3. Tender Validity Period**

The bids will remain valid for a period of at least six (6) months from the date of opening the technical bids.

### **13.4. Requests for Information**

Recipients are required to direct all communications related to this RFP through the Nominated Point of Contact person i.e.

**Chief Manager (I.T.),  
Chhattisgarh Gramin Bank,  
Corporate Office, Plot No 47  
Sector-24 Nawa Raipur, Atal  
Nagar C.G - 492018  
Email – [it.ho@cgb.bank.in](mailto:it.ho@cgb.bank.in)**

All questions relating to the RFP, technical or otherwise, must be in writing only to the Nominated Point of Contact.

Bank will not answer any communication initiated by Respondents later than five business days prior to the due date for bids submission. However, Bank may in its absolute discretion seek, but under no obligation to seek, additional information or material from any Respondents after the tender closes and all such information and material provided must be taken to form part of that Respondent's response.

Respondents should invariably provide details of their email address(es) as responses to queries will only be provided to the Respondent via email.

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

Bank may in its absolute discretion engage in discussion or negotiation with any Respondent (or simultaneously with more than one Respondent) after the tender closes to improve or clarify any response.

#### **14. Notification**

Bank will notify the Respondents in writing as soon as practicable about the outcome of the RFP evaluation process, including whether the Respondent's RFP response has been accepted or rejected. Bank is not obliged to provide any reasons for any such acceptance or rejection.

#### **15. Disqualification**

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

#### **16. Process**

Selection of a successful SP will involve an 8 stages approach. The approach follows the Indian Government's Central Vigilance Commission (CVC) guidelines.

##### 1. Issue of Tender Notification

This RFP is made available on the Bank's website [www.cgb.bank.in](http://www.cgb.bank.in) under the **Tenders** section. It has also been sent via email to the currently **CERT-In empanelled organizations** as per the list available on the CERT-In website ([https://www.cert-in.org.in/PDF/Empanel\\_org.pdf](https://www.cert-in.org.in/PDF/Empanel_org.pdf)) on the date of issuance of the tender notification.

##### 2. Pre-bid meeting

The pre-bid meeting will be organized online (MS Teams) on the scheduled date and

time. All the queries or clarifications of the bidders shall be answered by the Bank. The reply or any further changes in the RFP shall be communicated during the meeting OR sent to the participants only. However, those who could not attend the meeting shall also be communicated the outcome of the pre-bid meeting if any material change is made.

3. Submission of Bids
4. Technical bids Evaluation
5. Commercial bids comparison
6. Negotiation with the final bidder
7. Issuance of letter of appointment (LOA)
8. Acceptance of the LoA

### **16.1. Process Timeframe**

The following is an indicative timeframe for the overall selection process. Bank reserves the right to vary this timeframe at its absolute and sole discretion should the need arise. Changes to the timeframe will be relayed to the affected Respondents during the process.

<b>Description</b>	<b>Due Date</b>
Issue Tender Notification	12-12-2025
Pre-bid meeting (online in MS Teams)	16-12-2025 at 04:30 PM
Tender Submission (last date)	20-12-2025 before 9 PM
Technical bids opening	23-12-2025 at 11.30 AM
Financial Bid Opening	23-12-2025 at 01.30 PM
Issuance of PO	29-12-2025
Acceptance of PO	31-12-2025
Submission of all reports and Deliverables	ICT Audit Report : 31-01-2026 AUA /KUA Report : 31-01-2026 IS Audit Report: 31-01-2026 VAPT Reports : 15-02-2026

\*All dates mentioned above are tentative dates and the bidder acknowledges that it cannot hold the Bank responsible for breach of any of the dates. Bank may extend deadlines without giving reasons.

\* Pre Bid Meeting Details (MS Teams)

**Meeting ID: 489 970 433 609 34**  
**Passcode: u9v2Qc3z**

# SECTION – II

## **1. Bank- The Bank**

### **Introduction**

All the participant Banks are Regional Rural Banks constituted under Regional Rural Bank Act 1976 and are sponsored by State Bank of India. All the banks are having a common Application Service Provider (ASP) , and are using shared infrastructure.

The Bank has chosen B@ncs24 of M/s. C-edge Technologies Ltd, as the Core Banking Solution and the CBS project is implemented and supported by M/s. C-edge Technologies Ltd. The bank's data Centre is at Mumbai. The D/R Data Centre is located at Bangalore.

### **Products offered**

#### **Products and services offered by the Bank**

The bank has a rich assortment of Deposits, Loans, Remittances, and other fee based products.

#### **CBS**

Bank has implemented CBS for all its branches. Bank is providing most of the digital services like online account opening, Remittances (UPI/IMPS/NEFT/RTGS), Debit Cards, AEPS, Micro ATMs, and ATM Machines

#### **Networking**

Bank has set up its own network using RF, 4G, VSATs and LL. All the sites have two network links, one is used as primary link and other one is used as secondary link. RTGS and NEFT services have been implemented through Infinite.

#### **Alternate Delivery Channels**

Banks are having ATM, AEPS, UPI, IMPS, NEFT/RTGS, Mobile Banking & Internet Banking as alternate delivery channels. (Complete List will be shared with interested bidders over email.)

#### **In-House Applications**

Bank maintains various In-House developed applications for MIS and other requirements. The applications are hosted at Bank's on premises / cloud. (List will be shared with interested bidders over email.)

# SECTION – III

## **1. Current RFP Objectives:**

### **2.1 Audit Objectives**

The Bank wishes to appoint competent SP for conducting an ICT Audit (as instructed by NABARD) , Gap Assessment of Cyber Security Framework (as per NABARD's Cyber security Framework) , AUA/KUA Audit as per UIDAI guidelines , IS Audit of its IT Security architecture and Information System resources and infrastructure with the major objectives of evaluation of internal system and control for

- Safeguarding of Information System Assets/Resources
- Maintenance of Data Integrity, Reliability and Confidentiality
- Maintenance System Effectiveness.
- Ensuring System Efficiency.

The SP will be responsible as per the scope and timelines outlined below.

### **2.2. Audit Approaches**

Information Systems Audit approach includes the following Auditing around the computer

Auditing through the computer

Auditing with the computer

Through preparation of IS audit checklists based on accepted standards and RBI/ NABARD guidelines/ circulars.

Based on the audit findings, risk assessment to be classified as Low, Medium, High, Very high and extremely high in each specific audit areas.

### **2.3 Audit Methodology**

The IS audit work will include manual procedures, computer assisted procedures and fully automated procedures, depending on the chosen audit approach.

### **2.4 Auditors:**

Audit should be carried out by CERT-In empanelled audit firms / by persons having CISA / CISSP / CISM / GIAC (SANS) qualifications with adequate experience in the audit areas given below.

### **2.5 Audit Scope:**

A description of the envisaged scope is enumerated in brief as under and in detail in Annexure - A. However, the Bank reserves its right to change the scope of the RFP considering the size and variety of the requirements and the changing business conditions. The Bank groups the entire proposed audits into following major AREAS as under -

(A) Cyber Security Audit of Network , Servers , Endpoints , IT Infrastructure , Databases , Payment System Applications , Switches & Middleware deployed by the Bank / ASP (ICT Audit)

- (B) IS Audit as per all controls referenced in NABARD's Cyber Security Framework (link), the Comprehensive Cyber Security Framework for Regional Rural Banks (RRBs) : A Graded Approach (link), Reserve Bank of India (Regional Rural Banks – Digital Banking Channels Authorization) Directions, 2025 (link) with Gap Assessment and Internal Controls Adequacy (GAICA) report , the IS Audit Guidelines issued by NABARD (link) & MeitY ([https://cgb.bank.in/tender/MeitY\\_Guidelines.pdf](https://cgb.bank.in/tender/MeitY_Guidelines.pdf)) & shall be fully addressed and covered for the both i.e. : Bank's ASP and the Bank.
- (C) IT Products (INB / MB / DISA etc.)
- (D) Onsite Vulnerability Assessment and Penetration Testing (VAPT) of public facing & In-House applications of the Bank
- (E) AUA /KUA Audit based on UIDAI's latest applicable Checklist & Audit shall follow latest UIDAI circulars, including ecosystem hardening, operator management, key rotation verification, and AUA/KUA infrastructure inspection.
- (F) Closure certificate & Closure Report (of each Audit) based on the compliance Audit/ verification/evidences/artifacts submitted by the Bank.

Based on the contents of the RFP, the selected SP shall be required to independently arrive at Audit Methodology, based on acceptable standards and best practices.

The Bank expressly stipulates that the SP's selection under this RFP is on the understanding that this RFP contains only the principal provisions for the entire audit assignment. The SP shall be required to undertake to perform all such tasks, render requisite services and make available such resources as may be required for the successful completion of the entire audit assignment at no additional cost to the Bank.

## **2.6 Audit Findings & Reports:**

Deliverables Under the Audit-the SP will deliver detailed reports as below for each bank separately signed by CISA qualified person:

The following reports are an indicative that should be covered for the area-wise auditing-

- (1) ICT Audit Report
- (2) IS Audit Report ( With Separate sections mentioning findings of visit to DC/DR & Gap Assessment as per Cyber Security Framework of NABARD & GAICA Report)
- (3) AUA / KUA Audit Report ( Based on UIDAI checklist)
- (4) Scope / Application wise VAPT reports
- (5) Recommendations for Risk Mitigation
- (6) Gap analysis and recommendation for mitigation
- (7) The check list with guidelines for the subsequent audit (hard & soft copies)

The report's findings should cover all the areas separately mentioned in the scope.

### **2.7 Duration of Audit:**

The entire audit should be completed as mentioned above.

### **2.8 Pre-Qualification Criteria**

The SP is required to meet the following minimum eligibility criteria and provide adequate documentary evidence for each of the criteria stipulated below:

- 2.8.1. The SP should be in existence for a period of at least 3 years
- 2.8.2. SP should not have been blacklisted by any Government/Bank/Regulator in last 3 years.
- 2.8.3. The SP should have a current CERT-In Empanelment and should have CISA qualified auditors.
- 2.8.4. The SP should have certified penetration testers having any one or more of the following certifications. (CEH/ OSCP/ ECSA/ CPTE/ CHFI/ LPT/ CPT/ CEPT/ GPEN/ CMWAPT)
- 2.8.5. The SP should have audited at least one Bank / Financial Institute with areas mentioned above.

### **2.9 Earnest Money Deposit**

No EMD should be deposited by the bidder.

### **2.10 Submission of Bids**

The bids shall be in two parts viz. Technical Proposal and Commercial Proposal, Both Technical and Commercial Bids shall be submitted in separate pdf files over email to [it.ho@cgb.bank.in](mailto:it.ho@cgb.bank.in) with subject "IS/ICT/AUA-KUA AUDIT 2025-26". The Commercial proposal should be password protected and the password will be shared only on the date of tender opening, when requested during live meeting. Please do not share the password during submission of bids.

The technical proposal shall be organized and submitted as per the following sequence:

Sl. No.	Items	
1.	Details of business and business background Service Profile & client profile	ANNEXURA-1

2.	Details of experience/knowledge possessed in the areas of Project Planning and management review, Resource Planning, Role and Responsibility definition, Co-ordination across multiple teams, Project risk analysis and containment.	ANNEXURE-2
3.	Details of the similar assignments executed by the bidder in the Banks	ANNEXURE-3
4.	Details of the similar assignments executed by the bidder in other than Banking industry	ANNEXURE - 4
5.	Details of lead audit certification from leading certification Bodies	ANNEXURE - 5
6.	Compliance Certificate	ANNEXURE-C
7.	Comments on the Terms & Conditions, Services and Facilities provided	ANNEXURE-D
8.	Bidder's profile with the details of past experience	ANNEXURE-E
9.	Proposed Team Profile	ANNEXURE-F1
10.	Other staff in the SP	ANNEXURE-F2

All the relevant pages of the proposals (except literatures, datasheets and brochures) are to be numbered and be signed by authorized signatory on behalf of the Bidder. The number should be a unique running serial no. across the entire document.

The Bids shall be addressed and submitted to the Banks Evaluation Office (General Manager -IT).

The bids (arranged as mentioned above) are to be submitted over email to [it.ho@cqb.bank.in](mailto:it.ho@cqb.bank.in)

It may be noted that all queries, clarifications, questions etc., relating to this RFP, technical or otherwise, must be in writing only and should be to the nominated point of contact. Bidders should provide their E-mail address in their queries without fail.

The bidder will submit an undertaking specifying that the bidder has obtained all necessary statutory and obligatory permission to carry out project works, if any.

Certification of completion or work order of similar audit of any eligible institution is to be provided to establish past experience of the auditor. Sensitive information may be masked during bid submission, but actual documents have to be produced in case the Bidder is selected, else it may lead to disqualification.

The proposal should be prepared in English. The e-mail address and phone/fax numbers of the bidder should also be indicated on the sealed cover.

**FORMATS OF BIDS:** The bidders should use the formats prescribed by the Bank in the RFP for submitting both technical and commercial bids.

## **2.11 General Terms and Conditions (Please also refer to Section - 1)**

### **2.12.1 Adherence to Terms and Conditions:**

The bidders who wish to submit responses to this RFP should note that they should abide by all the terms and conditions contained in the RFP. If the responses contain any extraneous conditions put in by the respondents, such responses may be disqualified and may not be considered for the selection process.

### **2.12.2 Other terms and conditions:**

1. Bank reserves the right to:

- (i) Reject any and all responses received in response to the RFP
- (ii) Waive or Change any formalities, irregularities, or inconsistencies in proposal format delivery
- (iii) To negotiate any aspect of proposal with any bidder and negotiate with more than one bidder at a time
- (iv) Extend the time for submission of all proposals
- (v) Select the most responsive bidder (in case no bidder satisfies the eligibility criteria in totality)
- (vi) Select the next most responsive bidder if negotiations with the bidder of choice fail to result in an agreement within a specified time frame.
- (vii) Share the information/ clarifications provided in response to RFP by any bidder, with any other bidder(s) /others, in any form.
- (viii) Cancel the RFP/Tender at any stage, without assigning any reason whatsoever.

**3. Substitution of Project Team Members:** During the assignment, the substitution of key staff identified for the assignment will not be allowed unless such substitution becomes unavoidable to overcome the undue delay or that such changes are critical to meet the obligation. In such circumstances, the SP can do so only with the concurrence of the Bank by providing other staff of same level of qualifications and expertise. If the Bank is not satisfied with the substitution, the Bank reserves the right to terminate the contract and recover whatever payments made by the Bank to the SP during the course of this assignment besides claiming an amount, equal to the contract value as liquidated damages. However, the Bank reserves the right to insist the SP to

replace any team member with another (with the qualifications and expertise as required by the Bank) during the course of assignment.

**4. Professionalism:** The SP should provide professional, objective and impartial advice at all times and hold the Bank's interest's paramount and should observe the highest standard of ethics while executing the assignment.

**5. Adherence to Standards:** The SP should adhere to laws of land and rules, regulations and guidelines prescribed by various regulatory, statutory and Government authorities

**6.** The Bank reserves the right to conduct an audit/ongoing audit of the consulting services provided by the SP.

**7.** The Bank reserves the right to ascertain information from the banks and other institutions to which the bidders have rendered their services for execution of similar projects.

#### **8. COMMERCIAL BID:**

The prices should be quoted for all areas for the services offered by the SP as per the format enclosed as Annexure - B.

It may be noted that Bank will not pay any amount/expenses / charges / fees / travelling expenses/ boarding expenses / lodging expenses / conveyance expenses/ out of pocket expenses other than the above "Agreed Professional Fee".

**9.** The bidder cannot change the Project Manager during entire period of execution of the scope unless consented in written by the Bank.

**10.** The bid should contain the resource planning proposed to be deployed for the project which includes, inter-alia, the number of personnel, skill profile of each personnel, duration etc.

**11.** The bidder is expected to quote for the prices of the services the applicable taxes as on the date of bid submission. Any upward / downward revision in the tax rates from the date of the bid submission will be to the account of the Bank.

#### **12. TERMS OF PAYMENT:**

The SP's fees will be paid in the following manner for each item which is described in the Commercial bid (Annexure - B) as per the submission of audit findings and reports as per point.no.2.6:

- 05 % of the audit charges will be paid in advance after the kick-off meeting,
- 75% upon submission of the final audit & VAPT reports,
- 15% after compliance / verification Audit,

- And the remaining 5% after closure of audit/VAPT observations & closures certificate from SP.

### **13. LIQUIDATED DAMAGES (LD):**

The Bank will impose liquidated damages, of Rs. 1,000/- (Rupees One thousand only) per week or part thereof, for delay in not adhering to the time schedules (Section-I - 16.1).

If the selected Bidder fails to complete the due performance of the contract in accordance to the specifications and conditions agreed during the final contract negotiation, the Bank reserves the right either to cancel the contract or to accept performance already made by the bidder. The Bank reserves the right to recover an amount as deemed reasonable by the Bank as Liquidated Damages for non-performance.

Both the above Liquidated Damages are independent of each other and are applicable separately and concurrently.

LD is not applicable for reasons attributable to the Bank and Force Majeure. However, it is the responsibility of the bidder to prove that the delay is attributed to the Bank and Force Majeure. The bidder shall submit the proof authenticated by the bidder and Bank's official that the delay is attributed to the Bank and Force Majeure along with the bills requesting payment.

### **14. Indemnity:**

The bidder shall indemnify Bank and keep indemnified for against any loss or damage by executing an instrument to the effect on a Non-Judicial stamp paper that Bank may sustain on account of violation of patent, trademarks etc. by the bidder.

### **15. Authorized Signatory:**

The selected bidder shall indicate the authorized signatories who can discuss and correspond with the bank, with regard to the obligations under the contract.

The selected bidder shall submit at the time of signing the contract, a certified copy of the extract of the resolution of their Board, authenticated by Bank, authorizing an official or officials of the Bank or a Power of Attorney copy to discuss, sign agreements/contracts with the Bank. The bidder shall furnish proof of signature identification for above purposes as required by the Bank.

### **16 Applicable Law and Jurisdiction of court:**

The Contract with the selected bidder shall be governed in accordance with the Laws of India for the time being enforced and will be subject to the exclusive jurisdiction of

Courts at Raipur, C.G. (with the exclusion of all other Courts)

### **17. CANCELLATION OF CONTRACT AND COMPENSATION:**

The Bank reserves the right to cancel the contract of the selected bidder and recover expenditure incurred by the Bank on the following circumstances:

- The selected bidder commits a breach of any of the terms and conditions of the bid/contract.
- The bidder goes into liquidation voluntarily or otherwise.
- An attachment is levied or continues to be levied for a period of 7 days upon effects of the bid.
- The progress regarding execution of the contract, made by the selected bidder is found to be unsatisfactory.
- If deductions on account of liquidated Damages exceeds more than 10% of the total contract price.

After the award of the contract, if the selected bidder does not perform satisfactorily or delays execution of the contract, the Bank reserves the right to get the balance contract executed by another party of its choice by giving one-month notice for the same. In this event, the selected bidder is bound to make good the additional expenditure, which the Bank may have to incur to carry out bidding process for the execution of the balance of the contract. This clause is applicable, if for any reason, the contract is cancelled.

The Bank reserves the right to recover any dues payable by the selected bidder from any amount outstanding to the credit of the selected bidder, including the pending bills and/or invoking Bank Guarantee, if any, under this contract or any other contract/order.

### **18. NON PAYMENT OF PROFESSIONAL FEES:**

If any of the items/activities as mentioned in the price bid and as mentioned in annexure G are not taken up by the Bank during the course of this assignment, the Bank will not pay the professional fees quoted by the SP in the Price Bid against such activity/item.

### **19. ASSIGNMENT:**

Neither the contract nor any rights granted under the contract may be sold, leased, assigned, or otherwise transferred, in whole or in part, by the SP, and any such attempted sale, lease, assignment or otherwise transfer shall be void and of no effect without the advance written consent of the Bank.

## **20. Subcontracting:**

The SP shall not subcontract or permit anyone other than its personnel to perform any of the work, service or other performance required of the SP under the contract without the prior written consent of the Bank.

At the sole discretion and determination of the Bank, the Bank may add any other relevant criteria for evaluating the proposals received in response to this RFP.

Bank may, at its sole discretion, decide to seek more information from the respondents in order to normalize the bids. However, respondents will be notified separately, if such normalization exercise as part of the technical evaluation is resorted to.

## **21 Commercial Bid Evaluation Criteria**

It may be noted that commercial bids will be subjected to following evaluation process.

Based on the technical evaluation criteria, only those bidders qualifying the technical requirement will be short-listed for commercial evaluation.

### **Computation Methodology for arriving at "Least Price / Least Quote"**

"Least Price / Least Quote" will be computed for all bidders who have qualified Technical Bid process. Bank deserves the right to split the various audit assignments to different SPs at its sole discretion if the SP is not able to carry out the assignment in given timeframe.

Bank reserves the right to negotiate the price with the finally short listed bidder before awarding the contract. It may be noted that Bank will not entertain any price negotiations with any other bidder, till the Least Price bidder declines to accept the offer. The Bank will apply the Technical Evaluation criteria as deemed fit for the purpose of evaluation in consultation with the Committee constituted for this purpose. The evaluation criteria as applied by the Bank will be final and binding and no SP will have the right to challenge or question the criteria applied by the Bank.

## **SECTION – IV**

## **SUPPLEMENTAL TERMS AND CONDITIONS**

### **A. Proprietary and Related Rights**

1. Bank Property: All data or information supplied by the Bank to the SP in connection with the services being provided by SP ('the Services') shall remain the property of the Bank or its licensors. All deliverables to the extent prepared by SP hereunder for delivery to the Bank ('the Deliverables') shall be the property of the Bank.

2. SP Property: In connection with performing the Services, SP may use certain data, modules, components, designs, utilities, subsets, objects, program listings, tools, models, methodologies, programs, systems, analysis frameworks, leading practices and specifications ('Technical Elements'). Certain Technical Elements were owned or developed by SP prior to, or independently from, its engagement hereunder and are the sole and exclusive property of SP and SP retains all rights thereto, as well as to all modifications, enhancements and derivative works of such Technical Elements created, developed or prepared by SP during the performance of the Services. Certain other Technical Elements consist of third party works and products that SP has acquired the rights to use. In addition, SP retains the right to use its knowledge, experience and know-how, including processes, ideas, concepts, and techniques developed in the course of performing the Services, in providing services to other clients. The Bank shall have no rights in the Technical Elements. All working papers prepared by SP in connection with the Services shall remain the property of SP.

3. Use of Deliverables and Services: The Deliverables and SP's Services (including any related recommendations and advice) are intended solely for the information and use of the Bank's management, officers, directors and employees and may not be disclosed to any other person without the prior written consent of SP (other than the Bank's external auditors, subject to their agreement that none of the Deliverables, or any portion thereof, shall be further disclosed to any other person or entity except as required by law or professional obligation and that such auditors shall in no event make any claims against SP arising out of or in connection with the Deliverables). If the Deliverables or Services (including any portion, abstract or summary thereof, whether oral or in writing) is disclosed to an unauthorized third party, Bank agrees to indemnify and hold harmless SP, its partners, employees, agents and advisors from and against all claims, causes of action, liabilities, losses, damages, costs, and expenses (including, without limitation, reasonable attorneys' fees) resulting from such disclosure.

4. Systems: Unless SP has expressly agreed to do so in writing in this Agreement, the Services do not involve identifying, addressing or correcting any errors or defects in computer systems, other devices, or components thereof ('Systems'), due to imprecise or ambiguous entry, storage, interpretation, processing or reporting of data, including dates, and SP shall have no responsibility or liability for any defect or problem arising out of or related to processing in any Systems. However, SP is liable for negligence, SP cannot damage system or cause downtime & SP must perform only safe testing during the performance of our engagement. Testing shall be non-disruptive and SP shall be liable for damages resulting from negligence or unauthorized activity.

## **B. Confidential Information**

1. Confidentiality: Except as otherwise expressly provided in the text of the engagement letter, one party receiving Confidential Information, as defined below, in connection with the provision of the Services shall not disclose such Confidential Information outside of its organization or use it for any purpose other than in connection with the Services. 'Confidential Information' means all information in which a party has rights that is not generally known to the public and that under all the circumstances should reasonably be treated as confidential or proprietary, whether or not the material is specifically marked as confidential. Notwithstanding the foregoing, Confidential Information does not include information that: (i) is, as of the time of its disclosure, or thereafter becomes, part of the public domain through a source other than the receiving party; (ii) was known to the receiving party as of the time of its disclosure; (iii) is independently developed by the receiving party without reference to the Confidential Information; or (iv) is subsequently learned from a third party not known by the receiving party to be subject to an obligation of confidentiality with respect to the information disclosed.

2. Exceptions: Nothing in this Agreement shall limit the ability of a party in possession of the Confidential Information of the other to disclose such Confidential Information, and such party shall have no liability for such disclosure, if such disclosure is: (i) required to be disclosed pursuant to law, regulation, professional responsibility, government authority, duly authorized subpoena or court order whereupon the disclosing party will provide notice to the other party prior to such disclosure; (ii) required to be disclosed to a court or other tribunal in connection with the enforcement of such party's rights under this Agreement; or (iii) is approved for disclosure by the prior written consent of the other party.

3. Survival of Restrictions: The terms of this Section B will survive the termination of this Agreement and will continue in full force and effect for a period of twelve months from the date of such termination or as otherwise required by law or regulation.

4. Conflict of Interest: Subject to confidentiality restrictions set forth herein, SP and its affiliates shall have the right to render similar services to any third parties, even if such parties are in competition with the Bank, provided that, in the event the Bank has given SP prior notice of a potential conflict, SP shall either obtain a waiver of both parties or in the absence of such waiver (which should not be unreasonably withheld or delayed), refrain from rendering similar services in a manner which would create a conflict with respect to such circumstances.

## **C. Management responsibilities**

Management of the Bank is responsible for establishing and maintaining the Bank's system of internal control. The Bank's management and the Audit Committee are responsible for the following:

- (1) Determining the scope, risk, and frequency of activities performed by SP
- (2) Evaluating the findings and results arising from the activities performed by SP

- (3) Evaluating the adequacy of the procedures performed by SP and the findings resulting from those activities, including actions by management, if any, necessary to respond to the findings and among other things, obtaining reports from SP
- (4) Ensuring that all information provided to SP is accurate and complete in all material respects contains no material omissions and is updated on a prompt and continuous basis. SP shall be entitled to rely on all information provided by and decisions and approvals of the Bank in connection with SP's work. SP will not be responsible if any information provided by the Bank is not complete, accurate or current. In addition, the Bank will also be responsible for obtaining all third-party consents and security clearances required to enable SP to access and use any third-party products necessary to our performance.

#### **D. Relationship of Parties**

1. Independent Contractor: Nothing herein contained will be construed to imply a joint venture, partnership, Principal-agent relationship or co-employment or joint employment between the Bank and SP. SP, in furnishing services to the Bank hereunder, is acting only as an independent contractor. SP does not undertake by this Agreement or otherwise to perform any obligation of the Bank, whether regulatory or contractual, or to assume any responsibility for the Bank's business or operations. The parties agree that, to the fullest extent permitted by applicable law; SP has not, and is not, assuming any duty or obligation that the Bank may owe to its customers or any other person.

2. Concerning Employees: Personnel supplied by either party will be deemed employees of such party and will not for any purpose be considered employees or agents of the other party. Except as may otherwise be provided in this Agreement, each party shall be solely responsible for the supervision, daily direction, and control of its employees and payment of their salaries (including withholding of appropriate payroll taxes), workers' compensation, disability benefits, and the like.

#### **E. Testing Services**

1. If the Services include testing, penetration, intrusion or analysis of the Bank's information systems or enterprise whether by using intrusive or passive techniques and software tools (Testing Services'), the provisions of this Section E shall apply and the Bank hereby consents to SP performing the Testing Services.

2. If the testing services involve third party SPs, the Bank shall obtain all necessary consents of third party SPs. This consent shall be in the form attached to this letter.

3. The Bank understands that Testing Services may result in disruptions of and/or damage to Client's or third party's information systems and the information and data contained therein, including but not limited to denial of access to a legitimate system user, automatic shutdown of information systems caused by intrusion detection software or hardware, or failure of the information system. The Bank is solely responsible for understanding the testing steps that will be performed as part of the

Testing Services and for arranging alternative means of operation should such disruptions or failures occur and for all damage caused by the Testing Services. SP shall have no responsibility or liability for, and the Bank shall have no recourse against, SP or its partners, employees, agents or consultants for any damages as a result of such Testing Services.

4. The Bank shall have no recourse against, and shall bring no claim (in the nature of contribution or otherwise) against, SP, its subcontractors or their respective partners, officers, directors, agents, consultants and employees with respect to (i) any third-party claim (from all causes of action of any kind, including contract, tort or otherwise) against the Bank or its subsidiaries or affiliates related to or arising out of the Testing Services provided hereunder, or (ii) any losses, liabilities, damages or expenses (including attorneys' fees and expenses) incurred by the Bank or its subsidiaries or affiliates as a result of any such third-party claim. In addition, the Bank shall indemnify and hold harmless SP, its subcontractors and their respective partners, officers, directors, agents, consultants and employees ("SP Indemnitees") from and against (i) all claims and causes of action of any kind, including contract, tort or otherwise, by any third party related to or arising out of the Testing Services provided hereunder, and (ii) any losses, liabilities, damages and expenses (including, but not limited to, reasonable attorneys' fees and expenses incurred by the SP Indemnitees in any action or proceeding between an SP Indemnitee and any third party or otherwise) that are incurred by the SP Indemnitees as a result of any such claims or causes of action. The Bank shall reimburse the SP Indemnitees for such Indemnified Costs as they are incurred by the SP Indemnitees. The Bank's subsidiaries and affiliates are deemed a third party as that term is used in this section E.

#### **E. Other Provisions**

1. Applicable Law; Severability: This Agreement shall be governed by the laws of the Union of India. If any portion of this Agreement is held to be void, invalid, or otherwise unenforceable, in whole or part, the remaining portions of this Agreement shall remain in effect.

2. Assignment: Neither this Agreement, nor any rights or obligations here under, may be assigned, in whole or in part, by either party without the prior written permission of the other party; provided that, upon written notice to the other, either party may assign this Agreement to a corporation or legal entity that acquires substantially all of or a controlling interest in that party ("Change of Control"), and SP may assign this Agreement to any member or affiliated firm of CGB.

3. Entire Agreement; Applicable Law: This Agreement constitutes the entire agreement between the parties with respect to the subject matter hereof and supersedes all agreements and understandings between the Bank and SP with respect to the subject matter hereof made prior to the date of this Agreement. Each of the Bank and SP confirms that it has the right, power and authority to execute and deliver this Agreement and that it will be enforceable in accordance with its terms.

4. Term: The term of this Agreement shall commence on the date of the Engagement Letter ("Effective Date of contract") and shall continue up to the completion of the engagement ("Term") until terminated by either party through prior notice.

5. Transition After Termination: Upon the termination of this Agreement, SP shall, subject to the timely payment to it of all amounts owed hereunder, and the payment during the period of transition of its fees at its then-applicable hourly rate and its expenses, cooperate with the Bank in the orderly transition of its responsibilities to its successor, whether that be personnel employed by the Bank or an entity retained by the Bank for such purpose. In connection with such transition, SP will (a) continue to provide services contemplated hereunder for a reasonable period of time and, should the Bank desire, provide such services in coordination with the successor; and (b) make its personnel available at times mutually agreeable to discuss its work and transition issues with the Bank and the successor.

6. Non-Solicitation of Personnel: The Bank shall not solicit for employment or hire any SP employee who is involved in the performance of this Agreement during the term of this Agreement and for a period of twelve months following its termination except as may be agreed to in writing by both parties. In case the Bank does so, it will have to pay SP a sum equivalent to twelve months Cost to Bank of such employee.

7. Indemnity and Hold Harmless: The SP (Successful bidder) shall indemnify and hold harmless to Bank and its personnel and subcontractors (collectively, the 'Indemnified Parties') from and against any loss, cost, damage and expense. (including but not limited to attorneys' fees) incurred by any Indemnified Party relating to any claims arising out of or in any way relating to the Services or this agreement. This provision shall survive the termination of this agreement for any reason.

8. Changes and Delays: Changes in the type or extent of the services requested by the Bank or that are required for any other reason including any change in applicable law, professional standards or schedule delays or other events beyond a party's reasonable control (collectively, 'Unexpected Events'), may require fee and / or date of performance revisions to be agreed upon by both parties. If either party's performance is delayed or suspended as a result of Unexpected Events, and without its fault or negligence, then the period during which the services are to be performed shall be extended to the extent of such delay and neither party shall incur any liability to the other party as a result of such delay or suspension.

9. Conflict and survival: In the event if any conflict, ambiguity or inconsistency between this Annexure, the main engagement letter and any other document to which this Annexure 1 may be annexed or which may be annexed to this Annexure 1, including any terms and conditions on the Bank's purchase orders or otherwise, the terms and conditions of this Annexure 1 shall govern. The provisions of this Agreement that give the parties rights beyond termination of this Agreement will survive any termination of this Agreement.

10. Use of SP's name: Except as may be expressly permitted by this Agreement, the Bank shall not use or publicize SP's name, trademark, service mark or logo in

connection with the Services, without the prior written consent of SP, which may be subject to certain conditions, in SP's discretion.

11. Internet e-mail: The Bank acknowledges that: (i) SP, the Bank and others participating in this engagement may correspond or convey documentation via Internet e-mail unless the Bank expressly requests otherwise, (ii) no party has control over the performance, reliability, availability, or security of Internet e-mail, and (iii) SP shall not be liable for any loss, damage, expense, harm or inconvenience resulting from the loss, delay, interception, corruption, or alteration of any Internet e-mail due to any reason beyond SP's reasonable control.

## **DISPUTE RESOLUTION PROCEDURES**

The following procedures shall be used to resolve any controversy or claim ('dispute') as provided in our engagement letter to which this annexed. If any of these provisions are determined to be invalid or unenforceable, the remaining provisions shall remain in effect and binding on the parties to the fullest extent permitted by law.

### **Mediation**

A dispute shall be submitted to mediation by written notice to the other party or parties. The mediator shall be selected by agreement of the parties and any mediator so designated must be acceptable to all parties.

If the parties cannot agree on a mediator, a mediator shall be designated by the Indian Council of Arbitration (ICA') at the request of a party. Any mediator so designated must be acceptable to all parties. The mediation shall be conducted as specified by the mediator and agreed upon by the parties. The parties agree to discuss their differences in good faith and to attempt, with facilitation by the mediator, to reach an amicable resolution of the dispute. The mediation shall be treated as a settlement discussion and therefore shall be confidential. The mediator may not testify for either party in any later proceeding relating to the dispute. No recording or transcript shall be made of the mediation proceedings.

Each party shall bear its own costs in the mediation. The fees and expenses of the mediator shall be shared equally by the parties.

### **Arbitration**

If a dispute has not been resolved within 90 days after the written notice beginning the mediation process (or a longer period, if the parties agree to extend the mediation), the mediation shall terminate and the dispute shall be settled by arbitration. The arbitration will be conducted in accordance with the procedures in this document and the Rules of the Indian Council of Arbitration ('Rules') as in effect on the date of the engagement letter, or such other rules and procedures as the parties may designate by mutual agreement. In the event of a conflict, the provisions of this document will control.

The arbitration will be conducted before a panel of three arbitrators appointed as per the Rules of the Indian Council of Arbitration ('Rules'). Any issue concerning the extent to which any dispute is subject to arbitration, or concerning the applicability, interpretation, or enforceability of these procedures, including any contention that all or part of these procedures are invalid or unenforceable, shall be governed by the currently applicable Indian Arbitration & Conciliation Act and resolved by the arbitrators. No potential arbitrator shall be appointed unless he or she has agreed in writing to abide and be bound by these procedures.

The arbitration body shall have no power to award non-monetary or equitable relief of any sort. It shall also have no power to award (a) damages inconsistent with any applicable agreement between the parties or (b) Punitive damages or any other damages not measured by the prevailing party's actual damages; and the parties expressly waive their right to obtain such damages in arbitration or in any other forum. In no event, even if any other portion of these provisions is held to be invalid or unenforceable, shall the arbitration panel have power to make an award or impose a remedy that could not be made or imposed by a court deciding the matter in the same jurisdiction.

Discovery shall be permitted in connection with the arbitration only to the extent, if any, expressly authorized by the arbitration panel upon a showing of substantial need by the party seeking discovery.

All aspects of the arbitration shall be treated as confidential. The parties and the arbitration panel may disclose the existence, content or results of the arbitration only as provided in the Indian Arbitration & Conciliation Act. Before making any such disclosure, a party shall give written notice to all other parties and shall afford such parties a reasonable opportunity to protect their interests.

The result of the arbitration will be binding on the parties, and judgment on the arbitration award may be entered in any court having jurisdiction in India.

## ANNEXURE-A

### SCOPE OF AUDIT

The scope of work outlined herein is indicative and not exhaustive. All controls referenced in NABARD's Cyber Security Framework ([link](#)), the Comprehensive Cyber Security Framework for Regional Rural Banks (RRBs) : A Graded Approach ([link](#)), Reserve Bank of India (Regional Rural Banks – Digital Banking Channels Authorization) Directions, 2025 ([link](#)) with GAICA Report and the IS Audit Guidelines issued by NABARD ([link](#)) & MeitY ([https://cgb.bank.in/tender/MeitY\\_Guidelines.pdf](https://cgb.bank.in/tender/MeitY_Guidelines.pdf)) shall be fully addressed and covered for both the Bank's ASP and the Bank. The AUA /KUA Audit shall be conducted based on UIDAI's latest applicable Checklist including ecosystem hardening, operator management, key rotation verification, and AUA/KUA infrastructure inspection.

The details provided in the below scope are indicative lists but not restricted to the following.

#### Alignment of IT strategy with Business strategy

- \* IT Governance related processes
- \* Long term IT strategy and Short term IT plans
- \* Information security governance, effectiveness of implementation of security policies and processes
- \* IT Architecture
  - Acquisition and Implementation of Packaged software
    - > Requirement Identification and Analysis
    - > Product and Vendor selection criteria
    - > Vendor selection process
    - > Contracts
    - > Implementation
    - > Post Implementation Issues
  - Development of software - In-house and Out-sourced
    - > Audit framework for software developed in house, if any
    - > Software Audit process
      - o Audit at Program level
      - o Audit at Application level
      - o Audit at Organizational level
    - > Audit framework for software outsourcing

- Operating Systems Controls
  - > Adherence to licensing requirements
  - > Version maintenance and application of patches
  - > Network Security
  - > User Account Management including Active Directory & Group Policy
  - > Logical Access Controls
  - > System Administration
  - > Maintenance of sensitive user accounts
- Application Systems and Controls
  - > Logical Access Controls
  - > Input Controls
  - > Processing Controls
  - > Output Controls
  - > Interface Controls
  - > Authorization Controls
  - > Data Integrity / File Continuity controls
  - > Review of logs and audit trails
- Database Controls
  - > Physical access and protection
  - > Referential Integrity and accuracy
  - > Administration and Housekeeping
- Network Management audit
  - > Process
  - > Risk acceptance (deviation)
  - > Authentication
  - > Passwords
  - > Personal Identification Numbers ('PINS')
  - > Dynamic password
  - > Public key Infrastructure ('PKI')
  - > Biometrics authentication
  - > Access Control
  - > Cryptography

- > Network Information Security
- > E-mail and Voicemail rules and requirements
- > Information security administration
- > Microcomputer / PC security including OS Hardening
- > Audit trails
- > Violation logging management
- > Information storage and retrieval
- > Penetration testing
- Physical and environmental security
- Maintenance
  - > Change Request Management
    - o Software developed in-house
  - > Version Control
  - > Software procured from outside vendors
  - > Software trouble-shooting
    - o Helpdesk
  - > File / Data reorganization
  - > Backup and recovery
    - o Software
    - o Data
    - o Purging of data
  - > Hardware maintenance , CCTV Infra & CCTV retention review
  - > Training
- Internet Banking
  - > Information systems security framework
  - > Web server
  - > Logs of activity
  - > De-militarized zone and firewall
  - > Security reviews of all servers used for Internet Banking
  - > Database and Systems Administration
  - > Operational activities
  - > Application Control reviews for internet banking application

- > Application security , review of e-Bank Guarantee (e-BG) system (if any )
- > Digital Payment Security Controls for Internet Banking as mentioned in RBI Master Direction on Digital Payment Security Controls. (Link : [https://www.rbi.org.in/Scripts/BS\\_ViewMasDirections.aspx?id=12032](https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12032)) & as per Reserve Bank of India (Regional Rural Banks – Digital Banking Channels Authorization) Directions, 2025 (link : <https://rbidocs.rbi.org.in/rdocs/notification/PDFs/384MD.pdf>)
- Privacy and Data Protection
  - > Controls established for data conversion process
  - > Information classification based on criticality and sensitivity to business operations
  - > Fraud prevention and Security standards
  - > Isolation and confidentiality in maintaining of Bank’s customer information, documents, records by banks
  - > Procedures for identification of owners
  - > Procedures of erasing, shredding of documents and media containing sensitive information after the period of usage.
  - > Media control within the premises
- Business Continuity Management
  - > Top Management guidance and support on BCP
  - > The BCP methodology covering the following :
    - o Identification of critical business
    - o Owned and shared resources with supporting function
    - o Risk assessment on the basis of Business Impact Analysis ('BIA')
    - o Formulation of Recovery Time Objective ('RTO') and Identification of Recovery Point Objective ('RPO')
    - o Minimizing immediate damage and losses
    - o Restoring of critical business functions, including customer-facing systems and payment settlement systems
    - o Establishing management succession and emergency powers
  - > Addressing of HR issues and training aspects
  - > Providing for the safety and wellbeing of people at branch or location at the time of disaster
  - > Assurance from Service providers of critical operations for having BCP in place with testing performed on periodic basis.
  - > Independent Audit and review of the BCP and test result
  - > Participation in drills conducted by RBI for Banks using RTGS/NDS / CFMS

- > Maintaining of robust framework for documenting, maintaining and testing business continuity and recovery plans by Banks and service providers
- Asset Management
  - > Records of assets mapped to owners
  - > For PCI covered data, the following should be implemented :
    - o Proper usage policies for use of critical employee facing technologies
    - o Maintenance of Inventory logs for media
  - > Restriction of access to assets through acceptable usage policies, explicit management approval, authentication use of technology, access control list covering list of employees and devices, labeling of devices, list of approved company products, automatic session disconnection of remote devices after prolong inactivity
  - > Review of duties of employees having access to asset on regular basis.
- Human Resources
  - > Recruitment policy and procedures for staff
  - > Formal organization chart and defined job description prepared and reviewed regularly
  - > Proper segregation of duties maintained and reviewed regularly
  - > Prevention of unauthorized access of former employees
  - > Close supervision of staff in sensitive position
  - > People on notice period moved in non-sensitive role
  - > Dismissed staff to be removed from premises on immediate effect
- IT Financial Control
  - > Comprehensive outsourcing policy
  - > Coverage of confidentiality clause and clear assignment of liability for loss resulting from information security lapse in the vendor contract
  - > Periodic review of financial and operational condition of service provider with emphasis to performance standards, confidentiality and security, business continuity preparedness
  - > Contract clauses for vendor to allow RBI or personnel authorized by RBI access relevant information / records within reasonable frame of time.
- IT Operations
  - > Application Security covering access control

- > Business Relationship Management
  - o Customer Education and awareness for adaptation of security measures
  - o Mechanism for informing banks for deceptive domains, suspicious emails
  - o Trade marking and monitoring of domain names to help prevent entity for registering in deceptively similar names
  - o Use of SSL and updated certification in website
  - o Informing client of various attacks like phishing
- > Capacity Management
- > Service Continuity and availability management
  - o Consistency in handling and storing of information in accordance to its classification
  - o Securing of confidential data with proper storage
  - o Media disposal
  - o Infrastructure for backup and recovery
  - o Regular backups for essential business information and software
  - o Continuation of voice mail and telephone services as part of business contingency and disaster recovery plans
  - o Adequate insurance maintained to cover the cost of replacement of IT resources in event of disaster
  - o Avoidance of single point failure through contingency planning
- > Service Level Management
- Project Management
  - > Information System Acquisition, Development and Maintenance
    - o Sponsorship of senior management for development projects
    - o New system or changes to current systems should be adequately specified, programmed, tested, documented prior to transfer in the live environment
    - o Scrambling of sensitive data prior to use for testing purpose
  - > Release Management
    - o Access to computer environment and data based on job roles and responsibilities
    - o Proper segregation of duties to be maintained while granting access in the following environment -
      - Live

- Test
  - Development
  - Segregation of development, test and operating environments for software
- > Record Management
  - Record processes and controls
    - Policies for media handling, disposal and transit
    - Periodic review of Authorization levels and distribution lists
    - Procedures of handling, storage and disposal of information and media
    - Storage of media backups
    - Protection of records from loss, destruction and falsification in accordance to statutory, regulatory, contractual and business requirement
- > Technology Licensing
  - Periodic review of software licenses
  - Legal and regulatory requirement of Importing or exporting of software
- > IT outsourcing related controls
- > Detailed audit of delivery channels and related processes like ATM, internet banking, mobile banking, phone banking, and card based processes as mentioned in RBI Master Direction on Digital Payment Security Controls. (Link : [https://www.rbi.org.in/Scripts/BS\\_ViewMasDirections.aspx?id=12032](https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12032)) & as per Reserve Bank of India (Regional Rural Banks – Digital Banking Channels Authorization) Directions, 2025 (link : <https://rbidocs.rbi.org.in/rdocs/notification/PDFs/384MD.pdf>)
- > Data center operations and processes , access review  
Review relating to requirements of card networks (for example, PIN security review)
- > Other Aspects including but not limited to below mentioned points
  - Secrecy and confidentiality of Customer preserved.
  - If any cases of unauthorized transfer through hacking, denial of service due to Technological failure is brought.
  - Regulatory and Supervisory issues.
  - Any other items relevant in the case of security.
  - All the guidelines issued by RBI, NABARD , UIDAI , MeitY & CERT-IN from time to time relating to Internet Banking Application, Mobile Banking Application & Bank’s public facing

applications (including Bank's Official Website/Web hosting Software) should be adhered to.

### **Vulnerability Assessment and Penetration Testing (VAPT) :**

The VAPT shall include application, server, and network layer assessments as per OWASP Top 10, SANS, and CERT-In guidelines and the use of CERT-In–approved tools and frameworks are mandatory. VAPT activities shall be comprehensive and conducted onsite (Bank premises / Bank HO), and shall include, but not be limited to, the following activities for the application and related infrastructure under audit:

- Network Scanning
- Port Scanning
- System Identification & Trusted System Scanning
- Vulnerability Scanning
- Spoofing
- Scenario Analysis
- Application Security Testing
- OS Fingerprinting
- Service Fingerprinting
- Access Control Mapping
- Denial Of Service (DOS) Attacks
- DDOS Attacks (Non-Disruptive Only/ simulation)
- Authorization Testing
- Lockout Testing
- Password Cracking
- Cookie Security
- Functional validations
- Containment Measure Testing
- War Dialing
- DMZ Network Architecture Review
- Server Assessment (OS Security Configuration)
- Security Device Assessment
- Network Device Assessment
- Configuration Review of network & security devices
- Database Assessment
- Website Assessment (Process)
- Vulnerability Research & Verification
- IDS/IPS review & Fine tuning of Signatures
- Man in the Middle attack
- Man in the browser attack
- Any other attacks
- Compliance of Regulatory guidelines/Advisories: Successful Bidder shall perform VAPT and also ensure that regulatory guidelines issued by various bodies such as MeitY , Cert-In, NCIIPC, RBI-CSITE, NABARD-CSITE, NPCI etc. are followed.

### **VAPT of Website/Web/Mobile:**

Website, web application, and mobile application assessments shall be conducted onsite as per the latest OWASP MASVS, OWASP ASVS, and other relevant OWASP standards and guidelines, including but not limited to the following:

- Injection
- Broken Authentication and Session Management
- Cross-Site Scripting (XSS)
- Insecure Direct Object References
- Security misconfiguration
- Insecure Cryptographic Storage
- Sensitive Data Exposure
- Failure to Restrict URL Access
- Missing Function Level Access Control
- Cross-Site Request Forgery (CSRF)
- Using Known Vulnerable Components
- Un-validated Redirects and Forwards
- Insufficient Transport Layer Protection
- VAPT of APIs (API OwaspTop10) within web applications / mobile applications
- VAPT of Cloud based application (Bank Website & Email (Outlook))
- Any other attacks, which are vulnerable to the web sites and web application

VAPT reports shall have:

- Submission of detailed technical reports with severity classification and remediation steps.
- Detailing the Security Gaps , scoring mythology & CVVS
- Detailing the System setup used and the tests conducted in assessment.
- Critical vulnerabilities observed during VAPT along with recommendations should be immediately brought to the notice of Bank without waiting for the completion of VAPT.
- On closure of critical vulnerability, verification of closure shall have to be performed.
- Analysis of the findings and Document the security gaps i.e. vulnerability, security flaws, loopholes, threats, etc. observed during the course of the VAPT activity as per the scope of work.
- Document recommendations and solutions for addressing these security gaps and categorize the identified security gaps based on their criticality.
- Chart a roadmap for the Bank to ensure compliance and address these security gaps.
- Recommend Actionable fixes for systems vulnerabilities in design or otherwise for application systems and network infrastructure. If recommendations for Risk Mitigation /Removal could not be implemented as suggested, alternate solutions to be provided.
- Suggest changes/modifications in the Security Policies implemented along with Security Architecture including Network and Applications of the Bank to address the same.

**ANNEXURE-B**

&lt;&lt;On Letter Head of the Audit Firm&gt;&gt;

Date: \_\_\_\_\_

**Financial Bid for ICT, IS, VAPT and UIDAI AUA/KUA Audit for SBI Sponsored RRBs**

With reference to the invitation for quotation from Chhattisgarh Gramin Bank for conduction of ICT Audit, IS Audit and UIDAI AUA/KUA Audit for SBI Sponsored RRBs vide their e-mails, the **quotations per Bank** are furnished here under.

<b>Sno</b>	<b>Audit Description</b>	<b>Commercials excluding GST per Bank (in Rs.)</b>
1	ICT Audit including Audit of C- Edge premises & DC and DR	
2	IS Audit – Head Office and one Regional Business Office	
3	IS Audit – 4 Branches	
4	UIDAI AUA/KUA Audit	
5	VAPT of per Web Application /websites	
6	VAPT of per Mobile application	
7	VAPT of Bank's Network & Infrastructure	
<b>Total Cost</b>		

**We note the following:-**

1. Based on Total Cost only L-1 vendor will be finalized.
2. The proposed audit requirements are mentioned on Page 3 of the RFP; however, the participating bank shall have the right to opt out or issue a work order for any of the audits/VAPT specified in the RFP, as applicable or required, to the L-1 vendor at the rates quoted for the specific audit.
3. In case of any Bank wants to conduct IS Audit at additional locations (either branches or back offices) then the respective Bank will pay (Amount quoted for IS Audit in Item No.3)/4 for each extra location.
4. No other charges will be paid by the Banks. The quotations are all inclusive i.e Audit Fee, Boarding, Lodging, Transport etc. Travel expenses will be borne by the auditor. Bank will not entertain any other cost of any kind except GST.
5. 10% of the audit charges will be paid in advance after the kick-off meeting, 75% upon submission of the final audit & VAPT reports, 10% after compliance / verification Audit, and the remaining 5% after closure of audit/VAPT observations & closures certificate.
6. Only Vehicle for commuting from Head Office / IT Centre of respective Bank to other Audit locations will be made available by Bank.

Authorized Signature \_\_\_\_\_

Name \_\_\_\_\_

Designation \_\_\_\_\_

## ANNEXURE – C

(On bidder's official letter head)  
Compliance Certificate

Date:

To,

**General Manager (Information Technology),  
Chhattisgarh Gramin Bank, Corporate Office,  
Plot No 47 Sector-24 Nawa Raipur, Atal Nagar C.G - 492018**

Dear Sir,

Ref: -

- 1) Having examined the Tender Documents including all annexures, the receipt of which is hereby duly acknowledged, we, the undersigned offer to conduct the above audits.
- 2) If our Bid is accepted, we undertake to complete the project within the scheduled time lines.
- 3) We confirm that this offer is valid for six months from the last date for submission of Tender Documents to the Bank.
- 4) This Bid, together with your written acceptance thereof and your notification of award, shall constitute a binding Contract between us.
- 5) We undertake that in competing for and if the award is made to us, in executing the subject Contract, we will strictly observe the laws against fraud and corruption in for in India namely "Prevention of Corruption Act 1988".
- 6) We agree that the Bank is not bound to accept the lowest or any Bid that the Bank may receive.
- 7) We have never been barred/black-listed by any regulatory / statutory authority.
- 8) No legal case of any default / blacklisting should have ever been filed by any regulator on the firm.
- 9) Enclose all annexures (1 to 9, D, E, F1, F2, G1, G2, and G3)

Signed Dated

Seal & Signature of the Bidder

## ANNEXURE - D

### Comments on the Terms & Conditions, Services and Facilities provided:

Please provide your comments on the Terms & conditions in this section. You are requested to categorize your comments under appropriate headings such as those pertaining to the Scope of work, Approach, Work plan, Personnel schedule, Terms & Conditions etc. You are also requested to provide a reference of the page number, state the clarification point and the comment/ suggestion/ deviation that you propose as shown below.

Sr. No.	Page #	Section / Point #	Clarification point as stated in the tender document	Comment / Suggestion / Deviation
1.				
2.				

## ANNEXURE-E

### Bidder's profile with the details of past experience:

Sl. No.	Particulars	Details furnished by the bidder
1.	Name of the bidder	
2.	Year of establishment and constitution Certified copy of Registration or "Partnership Deed" or " Certificate of Incorporation" should be submitted as the case may be.	
3.	Location of Registered office /Corporate office and address	
4.	Mailing address of the bidder	
5.	Names and designations of the persons authorized to make commitments to the Bank	
6.	Telephone and fax numbers of contact persons	
7.	E-mail addresses of contact persons	
8.	Details of business and business background Service Profile & client profile	Enclose as Annexure-1
9.	Details of experience/knowledge possessed in the areas of Project Planning and management review, Resource Planning, Role and Responsibility definition, Co-ordination across multiple teams, Project risk analysis and containment.	Enclose as Annexure-2
10	Details of the similar assignments executed by the bidder in the Enclose as (Name of the Bank, time taken for execution of the Assignment, total fees received and documentary proofs from are to be furnished).  The Auditee's completion certificate with the details of area, duration, fees paid and completed on. This is mandatory document to evaluate the pre-qualification Criteria and technical evaluation.	Enclose as Annexure-3
11.	Details of the similar assignments executed by the bidder in other than Banking industry (Name of the Organization, time taken for execution of the assignment, total fees received and documentary proofs are to be furnished).  The Auditee's completion certificate with the details of area, duration, fees paid and completed on. This is mandatory document to evaluate the pre-qualification Criteria and technical evaluation.	Enclose as Annexure-4

12.	Names of team members identified for this assignment and their professional qualifications and experience/expertise Details of similar assignments handled by the said team members Documentary proofs for all the assertions are to be enclosed.	<b>As per annexure F1</b>
13.	Details of other professional in the organization	<b>As per annexure F2</b>
14.	Details of lead audit certification from leading certification bodies	Enclose as Annexure - 7
15.	Effort estimate and elapsed time are to be furnished in annexure G-	<b>As per annexure G1, G2, G3,</b> (Annexures G1, G2, and G3 pertain to SP / bidder submission and are to be prepared in the format prescribed by SP / Bidder)
16.	Details of inputs, infrastructure requirements required by the bidder to execute this assignment	<b>Enclose as Annexure - 8</b>
17.	Details of the bidder's proposed methodology/approach for providing services to the Bank with specific reference to the scope of work.	<b>Enclose as Annexure - 9</b>
18.	Details of deliverables the bidder proposes with specific reference to the scope of work .	Enclose as Annexure - 10

**Declaration:**

1. We confirm that we will abide by all the terms and conditions contained in the RFP.
2. We hereby unconditionally accept that Bank can at its absolute discretion apply whatever criteria it deems appropriate, not just limiting to those criteria set out in the RFP, in short listing of bidders.
3. All the details mentioned by us are true and correct and if Bank observes any misrepresentation of facts on any matter at any stage, Bank has the absolute right to reject the proposal and disqualify us from the selection process.
4. We confirm that this response, for the purpose of short-listing, is valid for a period of six months, from the date of expiry of the last date for submission of response to RFP.
5. We confirm that we have noted the contents of the RFP and have ensured that there is no deviation in filing our response to the RFP and that the Bank will have the right to disqualify us in case of any such deviations.

Place:

Date:

Seal & Signature of the bidder

**ANNEXURE-F**

**Proposed Team Profile**

Documentary proofs are to be enclosed to substantiate the claims made.

<b>Member No. M1 M2 etc.</b>	<b>Name of proposed Auditor</b>	<b>Professional Qualification</b>	<b>Certifications/ Accreditations</b>	<b>(Mention if he has worked in Banks earlier) In terms of years and areas of expertise</b>	<b>IT Expertise in terms of years and areas of expertise</b>	<b>Number of similar assignments involved in Banks in India</b>

**This form will consist two parts**

**ANNEXURE-F1 Proposed Team Profile**

**ANNEXURE-F2 Other staff in the SP**

**ANNEXURE-G**

Estimated Effort and Elapsed Time for each audit area (Annexure - G1 for ISP, Annexure - G2 for NMS, etc.)

Sl. No.	Activities for Scope of Work	Elapsed time	Effort in Man days	Member who will be deployed (M1/2..)	Annexure-A Ref.no.	Tools used	Deliverables
---------	------------------------------	--------------	--------------------	--------------------------------------	--------------------	------------	--------------

The above audit shall be completed with a total \_\_\_\_\_ man days.

The above activities can be started from \_\_\_\_\_ to \_\_\_\_\_.

if the Bank issues LoA on \_\_/\_\_/202\_\_.

**ANNEXURE-G1**

**ANNEXURE-G2**

**ANNEXURE-G3**

Place:

Date:

Seal and Signature of Bidder:

## Reference Documents:

The relevant guidelines issued by RBI, NABARD, CERT-In, etc., can be accessed through their respective official websites. Bidders are advised to refer to the latest versions of these documents to ensure compliance with all applicable regulatory and audit requirements.

The documents mentioned below are for reference only, and the scope of the audit is not limited to these. For the complete scope of the audit, please refer to the relevant section of this RFP document.

Circular No.	Date	Issuing Authority	Circular / Direction Heading
Circular No 33/DoS-01/2015	25-02-2015	NABARD	Introduction of Information System (IS) Audit
Circular No 134/DoS-13/2019	21-05-2019	NABARD	Information System (IS) Audit
EC No 193/DoS-22/2022	23-08-2022	NABARD	Information System (IS) Audit
EC No. 307/DoS-25/2024	17-12-2024	NABARD	<a href="#">Conduct of IT/Cyber Security Audit</a>
EC No. 309/DoS-27/2024	17-12-2024	NABARD	Conduct of Vulnerability Assessment/Penetration Testing (VA/PT)
Circular No.51/DoS-17/2018	16-03-2018	NABARD	Cyber Security Framework in Banks
EC No. 33/DoS-08/2020	06-02-2020	NABARD	<a href="#">Comprehensive Cyber Security Framework for RRBs – A Graded Approach</a>
RBI/DOR/2025-26/384 DOR.RAUG.AUT.REC.307/ 24.01.041/2025-26	28-11-2025	RBI	<a href="#">Regional Rural Banks – Digital Banking Channels Authorization) Directions, 2025</a>

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