मेघालय ग्रामीण बैंक

MEGHALAYA RURAL BANK

A joint undertaking of Govt. of India, Govt of Meghalaya & State Bank of India

Request for Proposal (RFP) for

IS Audit,

Cybersecurity Audit &

UIDAI AUA/KUA Audit

2025 – 2026

Table of Contents

SECTION – I :: Introduction and Overview

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

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

1. **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 the information that may be necessary or desirable to enable an intending contracting party to determine whether 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.

2. **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 organisation.

3. **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 based on 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.

4. **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 or omission.

5. **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.

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

7. 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.

8. 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 organisations, 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.

9. Errors and Omissions

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

10. 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.

11. Submission of Bids

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

General Manager
Meghalaya Rural Bank, Head Office
K.J.P. Assembly Conference Hall,
Central Ward, Barik, Shillong 793001
Email: ho@megrrb.in

11.1 Submission will be valid if:

a. Copies of the RFP are submitted before the schedule closing time by email. Submission is not by Fax transmission.
b. Bids are submitted in two separate files "Technical Proposal" & "Commercial Proposal"
c. “Commercial Proposal” to be password protected.
d. Only One Submission Permitted
e. 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.

11.2 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.

11.3 Late RFP Policy

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

RFPs lodged after the deadline for lodgement 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.

11.4 Validity Period

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

11.5 Requests for Information

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

General Manager (IT),
Meghalaya Rural Bank, Head Office
K.J.P. Assembly Conference Hall,
Central Ward, Barik, Shillong 793001

b. All questions relating to the RFP, technical or otherwise, must be in writing only to the Nominated Point of Contact.
c. 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.
d. Respondents should invariably provide details of their email address(es) as responses to queries will only be provided to the Respondent via email.
e. 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.
f. 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.

11.6 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.

12. Disqualification

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

13. Process

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

i. **Issue of RFP**

This RFP is made available at the Bank's web site https://meghalayaruralbank.co.in/ under tenders. And sent by e-mail/post to the current CERT-In empanelled organizations.

ii. **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.

iii. **Submission of Proposals**

iv. **Technical bids Proposals**

v. **Commercial Proposals comparison**

vi. **Negotiation with the final bidder**

vii. **Issuance of Engagement Letter**

viii. **Acceptance of the Engagement Letter**

14. Process Timeline

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.

Description	Due Date
Issue of RFP	**06-06-2025**
Pre-bid meeting (online in MS Teams)	**12-06-2025 at 04:30 PM**
Proposal Submission	**16-06-2025 before 9 PM**
Evaluation of Technical Proposals	**17-06-2025 at 11.30 AM**
Evaluation of Financial Proposals	**17-06-2025 at 3.00 PM**
Issuance of Engagement Letter	**18-06-2025**
Acceptance of Engagement Letter	**21-06-2025**
Submission of all reports and Deliverables	IS Audit Report: **21-07-2025** IS Audit Compliance Report: **21-08-2025** Cybersecurity Audit Report: **30-09-2025** Cybersecurity Audit Compliance Report: **30-10-2025** AUA /KUA Report: **31-01-2026** AUA /KUA Compliance Report: **27-02-2026**

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.

SECTION – II :: Bank Profile and IT Infrastructure

Meghalaya Rural Bank, a Regional Rural Bank constituted under Regional Rural Bank Act 1976 is sponsored by State Bank of India (SBI), currently has 89 branches, 3 regional offices, a Rural Self Employment Training Institutes (RSETI) and Head Office in Shillong.

All business units of the bank are connected via RF/4G/VSAT managed by **C-Edge Technologies Ltd** headquartered in Mumbai (and their implementing telecommunications partners viz., Airtel, Hughes & Tatanet (NELCO). Implementation of **CBS** is on **Application Service Provider (ASP) Model** wherein the **Data Center is located in Mumbai** and **Disaster Recovery (DR) site is located in Bangalore**.

Service Level Agreement (SLA) is in place with C-Edge Technologies Ltd inclusive of CBS, CBS Plus services & Network Management Services as below:

Core Services

- Core Banking Solution (CBS) – including serverless CBS (Java frontend) and eKYC.
- Digital Banking Solutions – Mobile Banking, Internet Banking.
- Switching Services – NFS Switch for financial and non-financial transactions.
- UPI, AEPS & IMPS – Issuer and Acquirer solutions.
- ATM Services – Terminal driving, card lifecycle management.
- NEFT/RTGS – As sub-member through SBI.
- NACH Services – Including pre-validation and mandate management.
- PFMS & Social Security Solutions – For government benefit disbursements.

Security & Compliance

- Cyber Security Operations Center (CSOC) – Continuous monitoring and threat response.
- PCI DSS & PSS Act Audits – Regular compliance audits.
- Vulnerability Assessment (VA) & Penetration Testing (PT) – Quarterly and annual respectively.
- Data Security & Confidentiality – Including Aadhaar Data Vault and customer data protection.
- Regulatory Compliance – Adherence to RBI, NABARD, and other statutory guidelines.

Reporting & Analytics

- Regulatory Reporting – Customizable and compliant with change management.
- Customer Risk Categorization – For AML and fraud detection.
- Brand Monitoring & Positive Pay Systems – For fraud prevention.

Integration & Interfaces

- API Services – For CBS and third-party integrations.
- Bulk Data Update Interfaces – For CBS.
- Passbook Printing KIOSK Interface.
- Loan Origination System (LOS) – Including PAN verification and account creation.

Infrastructure & Support

- Hosting & Hardware
- Network & Connectivity
- Disaster Recovery (DR)
- Monitoring Dashboards

In-House & Bank's Own Applications

- Bank maintains in-House developed applications for MIS and other requirements. The applications are hosted at Bank's on premises / cloud. The hosting & management of the Bank's Website have been outsourced.

SECTION – III :: Audit Objectives and Scope

1. Current RFP Objectives:

The Bank wishes to appoint competent SP for conducting the following Audits -

1.1 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

i. Safeguarding of Information System Assets/Resources
ii. Maintenance of Data Integrity, Reliability and Confidentiality
iii. Maintenance System Effectiveness.
iv. Ensuring System Efficiency.

The conduct of IS Audit will be guided by extant guidelines issued by the Bank's Regulatory bodies from time to time and an indicative list of which are reproduced below for reference:

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	Conduct of IT/Cyber Security Audit
EC No. 309/DoS-27/2024	17-12-2024	NABARD	Conduct of Vulnerability Assessment/Penetration Testing (VA/PT)

1.2 Cybersecurity Audit in line with NABARD & MEITY/CERT-IN guidelines, Gap Assessment of Cyber Security Framework (as per NABARD's Cyber security Framework),

The conduct of Cybersecurity Audit will be guided by extant guidelines issued by the Bank's Regulatory bodies from time to time and an indicative list of which are reproduced below for reference:

Circular No.	Date	Issuing Authority	Circular / Direction Heading
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	Comprehensive Cyber Security Framework for RRBs – A Graded Approach
EC No. 307/DoS-25/2024	17-12-2024	NABARD	Conduct of IT/Cyber Security Audit
EC No. 309/DoS-27/2024	17-12-2024	NABARD	Conduct of Vulnerability Assessment/Penetration Testing (VA/PT)

1.3 AUA / KUA Audit as per UIDAI guidelines.

2. Scope & Timelines

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

2.1 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.

2.2 Audit Methodology

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

2.3 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.

2.4 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 maior AREAS as under -

a. IS Audit as per extant regulatory guidelines
b. Cyber Security Audit and gap assessment as per NABARD Cyber Security Framework & MEITY/CERT-IN Guidelines
c. AUA /KUA Audit based on UIDAI's latest applicable Checklist

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

The Bank expressly stipulates that the Auditor's selection under this RFP is on the understanding that this RFP contains only the principal provisions for the entire audit assignment. The Auditor 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.

2.5 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-

a. IS Audit Report
b. Cybersecurity Audit Report

(Separate sections mentioning findings of visit to DC/DR)

c. VA / PT report
d. Timeline-based remediation roadmap
e. Gap analysis and recommendation for mitigation

f. The check list with guidelines for the subsequent audit (hard & soft copies) The report findings should cover all the areas separately mentioned in the scope.
g. AUA / KUA Audit Report (Based on UIDAI checklist)
h. Certification of compliance for the respective Audit(s) / findings
i. Non-compliance closure report (if applicable) for the respective Audit(s) / findings

2.6 Duration of Audit:

The entire audit should be completed as mentioned above.

2.7 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:

a. The SP should be in existence for a period of at least 3 years
b. The SP should have a current CERT-In Empanelment and should have CISA qualified auditors.
c. The SP should have audited at least one Regional Rural Bank in the past 3 years in areas mentioned as above.
d. Preference will be given to SP with experience of conducting audit in a hosting environment.

2.8 Earnest Money Deposit

No EMD should be deposited by the bidder.

2.9 Submission of Proposals

The bidders should use the formats prescribed by the Bank in the RFP for submitting both technical and commercial bids. The Proposals shall be in two parts viz. **A - Technical Proposal** and **B - Commercial Proposal.** Both Technical and Commercial Bids shall be submitted in **separate pdf files** over email to **ho@megrrb.in** with subject "**IS / Cyber Security Audit of Meghalaya Rural Bank – [Name of Firm]**". The commercial Bid should be password protected

2.9.1 The **A - Technical Proposal** shall be organized in PDF files and submitted as per the following sequence:

	Items	**Annexure**
1.	Details of business and business background Service Profile & client profile	ANNEXURE – 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 Team	ANNEXURE – F2
11.	Estimated Effort and Elapsed Time for each audit area	ANNEXURE – G1, G2

a. 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.
b. The Bids shall be addressed and submitted to the Banks Evaluation Office.
c. The bids (arranged as mentioned above) are to be submitted over email to **ho@megrrb.in**.
d. 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.
e. Bidders should provide their E-mail address in their queries without fail.
f. 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.
g. 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.

2.9.2 The **"B - Commercial Bid"** should be quoted for all areas for the services offered by the SP as per the format enclosed as **Annexure – B** in this RFP document. The following points may be noted:

i. The 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".
ii. The bidder cannot change the Project Manager during entire period of execution of the scope unless consented in written by the Bank.
iii. 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.
iv. 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.

2.10 General Terms and Conditions

(Please also refer to Section - 1)

2.11 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 Other terms and conditions

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.

2.13 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.

2.14 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.

2.15 Adherence to Standards:

The SP should adhere to laws of land and rules, regulations and guidelines prescribed by various regulatory, statutory and Government authorities

2.16 Right to Audit

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

2.17 Background Checks

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

2.18 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):

100% on completion of audit, submission of audit findings and reports as per point no 2.5

2.19 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 [14]).

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.

2.20 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.

2.21 Authorized Signatory

The selected bidder shall indicate the authorized signatories who can discuss and correspond with the bank, regarding 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.

2.22 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)

2.23 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:

a. The selected bidder commits a breach of any of the terms and conditions of the bid/contract.
b. The bidder goes into liquidation voluntarily or otherwise.
c. An attachment is levied or continues to be levied for a period of 7 days upon effects of the bid.
d. The progress regarding execution of the contract, made by the selected bidder is found to be unsatisfactory.
e. 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.

2.24 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.

2.25 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.

2.26 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.

2.27 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 deserve 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, during the performance of our engagement, we may become aware of issues with respect to your 'Systems'. These findings will be communicated to you in our individual reports.

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 to 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:

(a) Determining the scope, risk, and frequency of activities performed by SP

(b) Evaluating the findings and results arising from the activities performed by SP

(c) 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

(d) 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 for 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

   (a) 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

   (b) 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.

F. 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 CRGB.
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 Bank shall indemnify and hold harmless EY 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 publicise 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:
    a. SP, the Bank and others participating in this engagement may correspond or convey documentation via Internet e-mail unless the Bank expressly requests otherwise,
    b. no party has control over the performance, reliability, availability, or security of Internet e-mail, and
    c. 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.

G. 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.

1. **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.

2. **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 : Audit Scope

A. IS AUDIT SCOPE

All the controls mentioned in the latest NABARD Circulars on IS Audit should be covered.

Circular No.	Date	Issuing Authority	Circular / Direction Heading
Circular No 33/DoS-01/2015	25-Feb-2015	NABARD	Introduction of Information System (IS) Audit
Circular No 134/DoS-13/2019	21-May-2019	NABARD	Information System (IS) Audit
EC No 193/DoS-22/2022	23-Aug-2022	NABARD	Information System (IS) Audit
EC No. 307/DoS-25/2024	17-Dec-2024	NABARD	Conduct of IT/Cyber Security Audit
EC No. 309/DoS-27/2024	17-Dec-2024	NABARD	Conduct of Vulnerability Assessment/Penetration Testing (VA/PT) by CERTIn Empanelled Auditors

The scope provided in this document is an indicative guideline but not restricted to the following:

1. IT Governance and Strategy

i. Evaluate the alignment of IT strategy with business goals.
ii. Review IT policies, procedures, and governance structure.
iii. Assess roles and responsibilities of IT Steering Committee and Board oversight.

2. Information Security Management

i. Review of the Information Security Policy and its implementation.
ii. Assess access control mechanisms (logical and physical).
iii. Evaluate password policies, user account management, and privilege access.
iv. Review antivirus, anti-malware, and endpoint protection systems.
v. Assess security incident management and response.

3. Core Banking and Application Controls

i. Evaluate application-level controls (input, processing, output, interface, authorization).
ii. Review change management and version control.
iii. Assess data integrity and audit trail review.
iv. Conduct pre- and post-implementation reviews of new applications.

4. IT Infrastructure and Network Security

i. Review server and workstation configuration and patch management.
ii. Assess firewall, router, and switch configurations.
iii. Evaluate network segmentation and intrusion detection/prevention systems.
iv. Review wireless network security.

5. Database and Operating System Controls

i. Review database access and administration controls.
ii. Assess backup and recovery procedures.
iii. Evaluate patch management and vulnerability assessment.
iv. Review logs and audit trails.

6. **Cybersecurity and Emerging Threats**
   i. Review cybersecurity framework and incident response readiness.
   ii. Assess compliance with CERT-In guidelines and audit by empanelled agencies.

7. **Disaster Recovery and Business Continuity**
   i. Review BCP/DRP documentation and testing.
   ii. Assess Recovery Time Objective (RTO) and Recovery Point Objective (RPO).
   iii. Evaluate availability of alternate processing sites (hot/cold/warm).
   iv. Review data backup frequency, storage, and restoration testing.

8. **IT Operations and Service Management**
   i. Review IT helpdesk and incident management.
   ii. Assess capacity planning and performance monitoring.
   iii. Evaluate vendor and third-party service management.
   iv. Review SLAs and compliance.

9. **Audit of Delivery Channels**
   i. Review internet banking, mobile banking, ATM, POS, UPI systems.
   ii. Assess security of digital banking platforms.
   iii. Evaluate authentication mechanisms (2FA, biometrics, OTP).
   iv. Review transaction logs and exception reports.

10. **Compliance and Regulatory Reporting**
   i. Assess adherence to RBI/NABARD IT and Cybersecurity guidelines.
   ii. Review compliance with IT Act, 2000 and amendments.
   iii. Evaluate audit trails and compliance logs.

11. **Human Resource and Training**
   i. Review segregation of duties, job rotation, and background checks.
   ii. Assess cybersecurity awareness and training programs.

12. **Third-Party and Outsourcing Risk**
   i. Review vendor risk management and SLA reviews.
   ii. Assess third-party hosted applications and APIs.

13. **Reporting and Follow-up**
   i. Ensure timely submission of IS Audit Reports to Top Management.
   ii. Track compliance and closure of audit observations.

B. Cybersecurity Audit Scope

All the controls mentioned in the latest NABARD Circulars on Cyber Security should be covered. The audit shall also be aligned RBI and MeitY/CERT-In/CERT-In guidelines.

The scope provided in this document includes governance, risk assessment, network security, application security, data protection, and additional controls for outsourced data centers, ASP model hosting and is an indicative guideline but not restricted to the following:

Circular No.	Date	Issuing Authority	Circular / Direction Heading
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	Comprehensive Cyber Security Framework for RRBs – A Graded Approach
EC No. 307/DoS-25/2024	17-12-2024	NABARD	Conduct of IT/Cyber Security Audit
EC No. 309/DoS-27/2024	17-12-2024	NABARD	Conduct of Vulnerability Assessment/Penetration Testing (VA/PT) by CERTIn Empanelled Auditors

1. Governance & Policy Review

i. Review of the Cybersecurity Policy (separate from IT/IS policy).
ii. Assessment of Board oversight and cyber risk governance.
iii. Evaluation of cybersecurity roles and responsibilities.

2. Risk Assessment & Asset Inventory

i. Identification and classification of critical IT assets.
ii. Review of risk assessment methodology.
iii. Validation of asset inventory and data flow diagrams.

3. Network & Infrastructure Security

i. Review of network architecture, segmentation, and firewall rules.
ii. Assessment of router/switch configurations and access controls.
iii. Evaluation of remote access policies and VPN configurations.

4. Vulnerability Assessment & Penetration Testing (VAPT)

i. External and internal VAPT of servers, endpoints, and applications.
ii. Testing of internet/mobile banking platforms.
iii. Review of patch management and remediation processes.

5. Application Security

i. Source code review (if applicable) or black-box testing.
ii. Testing of APIs, web portals, and mobile apps.
iii. Evaluation of input validation, authentication, and session management.

6. **Endpoint & Server Security**
   i. Review of antivirus/EDR solutions.
   ii. Assessment of server hardening and endpoint protection.
   iii. Validation of USB/device control policies.

7. **User Access Management**
   i. Review of user provisioning/de-provisioning.
   ii. Assessment of privileged access controls.
   iii. Validation of multi-factor authentication (MFA).

8. **Security Operations & Monitoring**
   i. Review of Security Operations Center (SOC) or outsourced monitoring.
   ii. Evaluation of SIEM logs, alerts, and incident response.
   iii. Testing of incident detection and escalation procedures.

9. **Data Protection & Backup**
   i. Review of data encryption (at rest and in transit).
   ii. Assessment of data loss prevention (DLP) controls.
   iii. Validation of backup and disaster recovery mechanisms.

10. **Compliance & Reporting**
   i. Review of compliance with:
      a. NABARD Circulars
      b. RBI Cybersecurity Framework
      c. CERT-In guidelines
   ii. Validation of audit trails and reporting to CSITE Cell.

11. **Employee Awareness & Training**
   i. Review of cybersecurity training programs.
   ii. Assessment of phishing simulation exercises (if any).
   iii. Evaluation of incident reporting culture.

12. **Additional Controls (Aligned with MeitY/CERT-In & CERT-In Guidelines)**
   i. Critical Information Infrastructure (CII) Protection:
      a. Identify systems that may qualify as CII under the IT Act, 2000.
      b. Ensure access control, redundancy, and resilience for such systems.
      c. Implement real-time monitoring and incident response.
   ii. CERT-In Compliance:
      a. Validate:
         - Incident reporting timelines
         - Log retention
         - Secure log storage and tamper-proofing.
   iii. Data Localization & Sovereignty:
      a. Ensure critical data (e.g., financial, personal) is stored and processed within India.
      b. Validate cloud service providers for compliance with MeitY/CERT-In cloud guidelines.
   iv. Supply Chain Risk Management: Assess third-party vendors and service providers for Security posture, Data handling practices, Contractual clauses for cybersecurity
   v. Secure Configuration & Hardening: Validate baseline configurations for Servers, Network devices, Endpoints. Ensure CIS Benchmarks or equivalent standards are followed.

vi. Secure Software Development Lifecycle (SSDLC): Review policies for Code review, Static/Dynamic Application Security Testing (SAST/DAST), DevSecOps integration
vii. Business Continuity & Disaster Recovery (BC/DR): Review BCP/DR plans for cyber incidents. Validate DR drills and data recovery capabilities.
viii. Cybersecurity Awareness & Phishing Simulations: Conduct employee training and mock phishing campaigns. Evaluate incident reporting behavior and response readiness.

13. Outsourced Data Center & ASP Model Hosting

i. Third-Party Risk Management: Review of Service Level Agreements (SLAs) and Master Service Agreements (MSAs) with the ASP and data center provider.
ii. Assessment of vendor security posture, including:
   a. Certifications (e.g., ISO 27001, PCI-DSS)
   b. Background checks
   c. Incident response capabilities

iii. Data Center Security (Outsourced):
   a. Physical and environmental controls: Access control systems, Surveillance (CCTV), Fire suppression, power backup
   b. Logical security: Network segmentation, Intrusion detection/prevention systems (IDS/IPS), Patch and vulnerability management

iv. ASP Model Controls:
   a. Review of CBS application hosting environment:
      - Data encryption (at rest and in transit)
      - Application-level access controls
   b. Backup and disaster recovery mechanisms
   c. Evaluate change management and release processes for CBS updates.
   d. Data Ownership & Sovereignty: Ensure data ownership clauses are clearly defined in contracts. Validate that data is stored within India, per MeitY/CERT-In and RBI guidelines.
   e. Audit Rights & Compliance: Confirm that the bank retains the right to audit the ASP and data center.
   f. Ensure the ASP complies with:
      - RBI outsourcing guidelines
      - NABARD cybersecurity framework
      - CERT-In incident reporting norms
   g. Business Continuity & Incident Response:
      - Review of joint incident response plans between the bank and ASP.
      - Validate BCP/DR drills involving both the bank and the service provider.

14. Vulnerability Index for Cyber Security (VICS) – Gap Assessment

A Gap Assessment is a critical part of the cybersecurity audit and VICS process. This shall involve:

i. Baseline Evaluation: Compare current controls against NABARD Level 2 requirements, MeitY/CERT-In/CERT-In guidelines, and RBI Cybersecurity Framework.
ii. Control Mapping: Identify which controls are fully implemented, partially implemented, or not implemented.
iii. Risk Grading: Use VICS scoring to assign a risk grade (e.g., Low, Medium, High). Prioritize gaps based on impact and likelihood.

iv. Remediation Planning: Develop a Corrective Action Plan (CAP) with timelines. Assist the bank in assigning responsibilities and track progress.

C. UIDAI AUA / KUA AUDIT SCOPE

Information Systems (IS) Audit of the operations and systems as per latest Compliance checklist issued by Unique Identification Authority of India (UIDAI) for certifying compliance with controls supported by latest artefacts (aged <6 months) along with non- compliance closure report (in case of any non-compliance) and a Self-Assessment Checklist.

Any instructions issued by UIDAI during or prior to commencement of Audit pertaining to this Audit shall form part of the scope.

ANNEXURE - B :: "B-Commercial" Bid Format

<<On Letter Head of the Audit Firm>>

Date: ___/____/_____

To,

The General Manager (Ops)
Meghalaya Rural Bank – Head Office
KJP Assembly Conference Hall, Barik
Shillong – 793001, Meghalaya

Madam / Sir,

"B – Commercial" Bid for Information Security (IS), Cyber Security and UIDAI AUA/KUA Audit of Meghalaya Rural Bank

With reference to the Request for Proposals (RFP) for conduct of Information Security (IS), Cyber Security and UIDAI AUA/KUA Audit of Meghalaya Rural Bank the commercials are furnished as here under:

SN	Audit Description	Commercials excluding GST (in ₹.)
1	**IS Audit** (HO, RO, Data Center / DR Site, CBS/ASP environment, Digital channels & 10% of Branches)	₹
2	**Cyber Security Audit** (HO, RO, Data Center / DR Site, CBS/ASP environment, Digital channels, Payment Systems, Network Perimeter & Endpoints, Third-Party Interfaces, Security Operations, VA / PT & 10% of Branches)	₹
4	**UIDAI AUA/KUA Audit**	₹
	Total Cost	₹

In words, Rupees _____only

We note the following:

1. Based on Total Cost only L-1 vendor will be finalised.
2. Proposed audit requirements have been mentioned in Page no 2 of RFP, whereas the Bank would have right to opt / provide work order for any of the audit work specified out of the 3 audits mentioned in RFP with L-1 vendor on the rates quoted for that specific audit.
3. No other charges will be paid by the Bank. The quotations are all inclusive i.e Audit Fee, Boarding, Lodging, Transport etc. Bank will not entertain any other cost of any kind except GST.
4. 25% of Audit charges will be paid as advance after Kick-off meeting and 75% will be paid after submission of Final Audit Reports.

Authorised Signature _____

Name _____

Designation _____

ANNEXURE – C :: Compliance Certificate

<<On Letter Head of the Audit Firm>>

Date: ___/____/_____

To,

The General Manager (Ops)
Meghalaya Rural Bank – Head Office
KJP Assembly Conference Hall, Barik
Shillong – 793001, Meghalaya

Madam / Sir,

Compliance Certificate for Information Security (IS), Cyber Security and UIDAI AUA/KUA Audit of Meghalaya Rural Bank

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 timelines**.
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. No legal case of any default / blacklisting should have ever been filed by any regulator on the firm.
8. Enclosed are all **Annexures** (**1 to 5, D, E, F1, F2, G1, G2, ..**)

Authorised Signature _____

Name _____

Designation _____

ANNEXURE – D :: Comments

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 points as stated in the tender document	Comment / Suggestion / Deviation
1.				
2.				
3.				

ANNEXURE – E :: Bidder profile

Bidder's profile with the details of experience:

SN	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.	
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	Enclosed 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.	Enclosed 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.	Enclosed as Annexure-3
11	Details of the similar assignments executed by the bidder in other than Banking industry (Name of the Organisation, 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.	Enclosed 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.	As per annexure F1
13	Details of other professionals in the organization	As per annexure F2
14	Details of lead audit certification from leading certification bodies	Enclosed as Annexure - 7
15	Effort estimate and elapsed time are to be furnished in annexure G	As per annexure G1, G2, G3,
16	Details of inputs, infrastructure requirements required by the bidder to execute this assignment	Enclosed as Annexure - 8
17	Details of the bidder's proposed methodology/approach for providing services to the Bank with specific reference to the scope of work.	Enclosed as Annexure - 9
18	Details of deliverables the bidder proposes with specific reference to the scope of work.	Enclosed 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.

Authorised Signature _____ (Seal)

Name _____

Designation _____

ANNEXURE – F :: Team Profile

Proposed Team Profile

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

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

This form will consist of two parts:

ANNEXURE F1 - Proposed Team Profile

ANNEXURE F2 - Other staff in the SP

Authorised Signature _____ (Seal)

Name _____

Designation _____

ANNEXURE – G :: Effort & Time Estimate

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

SN	Activities for Scope of Work	Elapsed time	Effort in Man days	Member who will be deployed (M1/M2 ..)	Annexure-A Ref.no.	Tools used	Deliverables

The above audit shall be completed within a total _____man day.

The above activities can be started from ___/___/_____to ___/___/_____

if the Bank issues Letter of Acceptance (LoA) on ___/___/_____

This form will consist of multiple parts:

ANNEXURE - G1
ANNEXURE - G2
ANNEXURE - G3

Authorised Signature _____ (Seal)

Name _____

Designation _____

******** End of Document ********