MEGHALAYA
RURAL BANK

REQUEST FOR PROPOSAL (RFP)

Selection of CERT-In Empanelled Audit Firm for Conduct of

Information System (IS) Audit,
Cyber Security Audit (inc. Gap Assessment),
Vulnerability Assessment / Penetration Testing (VA/PT)
& UIDAI AUA/KUA IS Audit

2026 – 2027

Date of Issue: 25-05-2026

Table of Contents

TIMELINES

A. Bid Schedule

The Bank reserves the right to modify the schedule at its discretion. Any change in the bid schedule shall be notified through written communication / corrigendum / addendum issued by the Bank.

SN	Event	Date / Time
1	RFP publication date	**Monday, 25-05-2026**
2	Online pre-bid meeting *(meeting link to be shared on Bank's website)*	**Monday, 01-06-2026**
3	Last date and time for bid submission	**Tuesday, 09-06-2026, up to 4:00 PM**
4	Technical Bid opening and evaluation	**Wednesday, 10-06-2026, 11:00 AM**
5	Commercial Bid opening	**Friday, 12-06-2026, 11:00 AM**, *subject to completion of Technical Bid evaluation*
6	Issuance of Engagement Letter	**Friday, 12-06-2026,** *subject to completion of Financial Bid evaluation*
7	Acceptance of Engagement Letter by selected bidder	**Monday, 15-06-2026**

A1. Bid Submission

For "**Physical Submission"**, the Technical Bid and Commercial Bid shall be submitted in separate sealed covers, clearly marked as "**A. Technical Bid**" and "**B. Commercial Bid**", at:

General Manager (I)
Meghalaya Rural Bank, Head Office
KJP Assembly Conference Centre,
Barik, Shillong – 793001, Meghalaya

For "**Electronic Submission"**, the Technical Bid and Commercial Bid shall be sent as **separate documents** to **ciso@meghalayaruralbank.bank.in**. The **Commercial Bid** shall be **password protected**. The password shall be shared in a separate email only upon intimation by the Bank at the stage of Commercial Bid opening.

B. Indicative Audit Deliverable Schedule

The timelines below are indicative and may be refined in the audit plan approved by the Bank. The auditor shall plan and execute the assignment in a manner that ensures completion of regulatory / compliance-linked deliverables with adequate buffer before applicable outer timelines.

B1. IS Audit Schedule

SN	Milestone	Indicative Timeline / Target Date
1	Kick-off	**24-06-2026** *(T + 7 working days)*
2	IS Audit activities	**25-06-2026** to **07-08-2026** *(approx. 45 days from kick-off)*
3	Submission of Draft IS Audit Report	**14-08-2026** *(within 7 days from completion of audit process)*
4	Submission of Final IS Audit Report	**28-08-2026** *(within 7 days from receipt of management response / completion of discussion)*
5	IS Audit compliance / re-verification and closure / compliance certificate	**28-09-2026** *(within one month from Final IS Audit Report, subject to Bank's mitigation evidence)*

T = Acceptance of Engagement Letter by selected bidder, i.e., 15-06-2026

B2. Cyber Security Audit, Gap Assessment and VA/PT Schedule

SN	Milestone	Indicative Timeline / Target Date
1	Kick-off & Scope Freeze	**01-09-2026 to 03-09-2026**
2	Cyber Security Audit, Gap Assessment and VA/PT activities	**04-09-2026 to 09-10-2026** *(approx. 35 days)*
3	Submission of VA/PT Report	**23-10-2026** *(within 14 days from completion of activities)*
4	Submission of Draft Cyber Security Audit Report including Gap Assessment	**30-10-2026** *(within 7 days from VA/PT Report / completion of review)*
5	Submission of Final Cyber Security Audit Report including Gap Assessment	**13-11-2026** *(within 14 days from Draft Report / management discussion)*
6	VA/PT retest / validation and closure statement	**27-11-2026** *(subject to Bank's / ASP's remediation evidence)*
7	Cyber Security Audit compliance / re-verification and closure / compliance certificate	**07-12-2026**

B3. UIDAI AUA/KUA IS Audit Schedule

SN	Milestone	Indicative Timeline / Target Date
1	Kick-off & Scope Freeze	**01-12-2026 to 03-12-2026**
2	UIDAI AUA/KUA IS Audit activities	**07-12-2026 to 20-01-2027** *(approx. 45 days from start of activities)*
3	Submission of Draft UIDAI AUA/KUA IS Audit Report	**27-01-2027** *(within 7 days from completion of audit activities)*
4	Submission of Final UIDAI AUA/KUA IS Audit Report / completed checklist / applicable certificate or statement	**03-02-2027** *(within 7 days from Draft Report / management discussion)*
5	UIDAI AUA/KUA compliance / re-verification and closure / closure status note	**26-02-2027**

SECTION I – Introduction and Overview

1.1 Introduction

The Bank invites proposals from **eligible and qualified CERT-In empanelled audit firms** to conduct Information Technology and Cyber Security related audits for the Bank.

This Request for Proposal (RFP) sets out the scope, eligibility requirements, evaluation methodology, deliverables, commercial requirements and general terms for selection of audit firm(s) to provide independent assurance on the Bank's information systems, cyber security posture, outsourced technology operations and Aadhaar-based services.

1.2 Purpose of the RFP

The purpose of this RFP is to select suitable audit firm(s) for conducting the following audit streams:

- Information Systems (IS) Audit
- Cyber Security Audit, including Cyber Security Gap Assessment
- Vulnerability Assessment and Penetration Testing (VA/PT)
- UIDAI AUA / KUA IS Audit

These audits are intended to assist the Bank in assessing the adequacy and effectiveness of its technology-related controls and in meeting supervisory, regulatory, and governance requirements.

1.3 Nature of Engagement

The audits covered under this RFP are independent assurance engagements. They are not consultancy, certification, forensic investigation, managed security service, system-design or implementation assignments.

Each audit stream has a distinct objective, scope and deliverable, as specified in the relevant sections of this RFP.

1.4 Applicable Framework

The audits shall be conducted in line with applicable directions, guidelines and requirements issued by NABARD, Reserve Bank of India (RBI), CERT-In / MeitY, UIDAI and other relevant regulatory, statutory or supervisory authorities, as applicable, and the Bank's Board-approved internal policies.

1.5 Technology Operating Model

The Bank operates its core technology environment under an **Application Service Provider (ASP) model.** The Bank retains overall accountability for governance, oversight and regulatory compliance, while certain operational and technical controls are operated by service providers under contractual arrangements.

Reliance on service-provider-operated controls shall be acceptable where appropriate assurance evidence is reviewed, and the basis of reliance is documented by the auditor.

1.6 Audit Philosophy

The audits under this RFP shall be conducted in accordance with the following principles:

- **Proportionality:** Audit scope and depth shall be commensurate with the Bank's size, complexity, and risk profile.
- **Clear Accountability:** The Bank's accountability for systems and controls is preserved, including in an outsourced environment.
- **Defined Scope:** Each audit stream is clearly delineated to avoid overlap or ambiguity.
- **Assurance-Oriented:** The audits are intended to provide independent assurance and identify gaps or weaknesses.
- **Operational Practicality:** Audit execution should be non-disruptive and aligned with normal banking operations.

1.7 Information Provided in the RFP

Information provided in this RFP and subsequent clarifications is provided in good faith to assist bidders in preparing their proposals. Bidders are expected to make their own assessment before submitting proposals.

The Bank does not warrant that the information contained in this RFP is complete or exhaustive and shall not be liable for errors or omissions.

1.8 Confidentiality

This RFP and any information provided by the Bank in connection with the RFP shall be treated as confidential and used only for the purpose of participation in the bidding process.

Sensitive information and audit artefacts shall be shared only with the selected bidder, where required, subject to execution of the applicable NDA / confidentiality agreement.

1.9 Cost of Proposal

All costs incurred by bidders in preparing and submitting proposals, including meetings, visits, presentations and clarifications, shall be borne by the bidder. The Bank shall not be liable for such costs.

1.10 Bank's Rights

The Bank reserves the right to accept or reject any or all proposals, seek clarifications, modify or cancel the RFP process, annul or re-tender the process, or not award the assignment, without assigning any reason, subject to applicable procurement norms.

1.11 Acceptance of RFP Terms

Submission of a proposal shall be deemed to constitute acceptance of the terms and conditions of this RFP, subject to the bidder's unconditional acceptance submitted in the prescribed format.

1.12 Structure of the RFP

This RFP is structured to cover the Bank's profile, regulatory framework, audit scope, deliverables, eligibility criteria, bid evaluation methodology, commercial requirements, general conditions and prescribed submission formats.

SECTION II :: Bank Profile and IT / Digital Environment

2.1 Bank Profile

2.1.1 **Meghalaya Rural Bank ("the Bank")** is a Regional Rural Bank (RRB) sponsored by State Bank of India (SBI). The Bank has its Head Office at Shillong and operates through:

- Head Office (HO) - 1
- Regional Offices (ROs) - 3
- Branches - 90

2.1.2 For the audits under this RFP, field verification shall be carried out as per the scope defined in the relevant audit sections. Under IS Audit, **10–12 branches** shall be covered through risk-based sampling.

2.2 Technology Operating Model – ASP

2.2.1 The Bank operates its core technology environment under an **Application Service Provider (ASP) model**. The Bank's ASP for the core environment is **CEdge Technologies Ltd. (CEDGE)**.

2.2.2 Under this model, core banking technology services and certain allied services are delivered / operated by the ASP under contractual and regulatory arrangements. The Bank retains overall accountability for governance, oversight and regulatory compliance.

2.2.3 Relevant ASP-related assurance artefacts required for audit execution shall be shared post-award and / or under NDA, on a need-to-know basis.

2.3 IT and Digital Environment

2.3.1 The Bank's IT and digital environment includes core banking operations, customer delivery channels, payment interfaces, Aadhaar-enabled services, public web presence and Bank-owned / in-house applications used for MIS and internal workflows.

2.3.2 The following major channels / services are currently in operation or relevant for audit consideration, on an indicative and non-exhaustive basis:

i. branch banking through CBS;
ii. BC / CSP channel;
iii. customer onboarding / KYC channels, including eKYC / Digital KYC where applicable;
iv. ATM / card / switching services;
v. Internet Banking and Mobile Banking;
vi. digital payment channels and interfaces, including UPI / IMPS / AEPS;
vii. NEFT / RTGS through sponsor / sub-membership arrangement;
viii. Aadhaar-enabled services under UIDAI AUA/KUA operating model;
ix. other payment / collection platforms such as CTS, PFMS, NACH and DBT;
x. public website / web presence;
xi. Bank-owned / in-house MIS and workflow applications.

2.3.3 Detailed technical artefacts, asset lists, architecture details, contractual documents and sensitive operational information shall be shared only with the selected bidder, as required, subject to confidentiality requirements.

2.4 Bank-Owned / In-house Applications

2.4.1 In addition to ASP-delivered services, the Bank maintains certain **Bank-owned / in-house applications for MIS and internal requirements**. Where such applications fall within the scope defined in this RFP, the auditor may be required to conduct selective **application security review/testing** as specified in the relevant scope sections.

2.4.2 **Source code review does not apply to CBS/ASP-owned platforms** unless explicitly made available through contractual/legal arrangements.

2.5 Confidentiality of Detailed Technology Information

2.5.1 Detailed scope and service descriptions contained in the Bank's contractual arrangements with the ASP (including service catalogues, site details, operational processes, security tooling, and compliance artefacts) are **confidential** and **are not part of this public RFP**.

2.5.2 Relevant contractual and assurance artefacts required for audit execution shall be shared **post-award** and/or under **NDA** strictly on a need-to-know basis and in coordination with the ASP, as applicable.

The audits under this RFP shall be conducted in line with applicable directions, guidelines, advisories, circulars, checklists and issued by NABARD, Reserve Bank of India (RBI), CERT-In / MeitY, UIDAI and other relevant regulatory, statutory or supervisory authorities from time to time. The references below are indicative. Any update, amendment, clarification or revised requirement applicable during the period of the assignment shall also apply.

3.1 Information Systems (IS) Audit – NABARD References

The IS Audit shall be conducted in line with NABARD's IS Audit directions applicable to RRBs, including the broad guidelines, scope and checklists referenced by NABARD through circulars/reiterations.

Circular No.	Date	Issuing Authority	Circular / Direction Heading
DoS Circular No. 33/DoS-01/2015	25-02-2015	NABARD	Guidelines on Information System (IS) Audit
Circular No. 134/DoS-13/2019	21-05-2019	NABARD	Information System (IS) Audit (reiteration of 2015 guidelines; policy + annual IS audit + HO/critical branches coverage)
EC No. 193/DoS-22/2022	23-08-2022	NABARD	Information System (IS) Audit (reiteration & supervisory emphasis)

3.2 Cyber Security Audit & VA/PT - NABARD References

Cyber Security Audit, Cyber Security Gap Assessment and VA/PT shall be aligned to NABARD's Cyber Security Framework for RRBs and applicable directions on conduct of IT / Cyber Security Audit and VA/PT through CERT-In empanelled organisations.

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 (Levels; VA/PT cadence; VICS reference)
EC No. 332/DoS-55/2020	21-12-2020	NABARD	Cyber Security Framework – Reporting of Near Misses
EC No. 307/DoS-25/2024	17-12-2024	NABARD	Conduct of IT/Cyber Security Audit through CERT-In empanelled agencies; follow MeitY/CERT-In guidelines
EC No. 309/DoS-27/2024	17-12-2024	NABARD	Conduct of VA/PT by CERT-In empanelled organisations only; remediation + validation testing

Note: The **Cyber Security Gap Assessment** under this RFP shall be aligned to NABARD's Cyber Security Framework (graded approach) and informed by VA/PT outcomes.

3.2.1 While NABARD directions form the primary supervisory framework for RRBs, relevant RBI directions, guidelines and advisories relating to information technology, cyber security, outsourcing, digital payments and risk management shall also be considered, wherever applicable, including RBI guidance adopted or reiterated for RRBs through NABARD or otherwise.

3.2.2 CERT-In / MeitY References

The Cyber Security Audit and VA/PT under this RFP shall follow the applicable CERT-In / MeitY guidelines, including principles for audit planning, execution, evidence/documentation, reporting, and handling of third-party hosting/outsourced environments.

Document / Guideline	Date / Version	Issuing Authority	Purpose / Applicability
Comprehensive Cyber Security Audit Policy Guidelines	v1.0 (25-07-2025)	CERT-In	Audit planning, execution, evidence and reporting
Terms & Conditions for Empanelment of IS Auditing Organisations	v7.2	CERT-In	Empanelment obligations, confidentiality, NDA and audit data handling
Guidelines for Auditee Organisations – IT Security Auditing	v5.0	CERT-In	Auditee / auditor responsibilities, scope definition and engagement controls
Directions under Section 70B of the IT Act	28-04-2022	CERT-In	Information security practices, incident reporting, log retention and time synchronisation
Guidelines for Secure Application Design, Development, Implementation and Operations	25-01-2024	CERT-In	Application security baseline for in-scope applications

3.3 UIDAI AUA/KUA Audit

UIDAI AUA/KUA audit Shall be carried out strictly as per UIDAI's regulations/specifications and audit requirements, including the UIDAI compliance checklist issued for AUA/KUA controls.

Document / Guideline	Date / Version	Issuing Authority	Purpose / Applicability
UIDAI Compliance Checklist for certifying compliance with controls that the AUA/KUA is required to have in place	Latest applicable version	UIDAI	Checklist-based compliance assessment and certification requirement

3.4 Bank's Internal Policies

In addition to the above, the audits shall be aligned to the Bank's **Board-approved internal policies** (e.g., IS Audit Policy, IT Policy, Cyber Security Policy, Information Security Policy and other relevant governance/outsourcing risk controls), as applicable. These policies provide the Bank's internal control baseline consistent with supervisory directions.

3.5 Precedence / interpretation

In case of overlap in any instruction:

- NABARD directions shall be treated as the primary supervisory requirements for the Bank as an RRB.
- CERT-In / MeitY documents shall govern the **conduct and methodology** of Cyber Security Audit and VA/PT.
- UIDAI requirements shall govern the AUA/KUA audit

SECTION IV :: Overall Scope & Audit Approach

4.1 Scope at a Glance

4.1.1 The Bank proposes to conduct the following audits under this RFP:

i. Information Systems (IS) Audit
ii. Cyber Security Audit, including Cyber Security Framework Gap Assessment
iii. Vulnerability Assessment & Penetration Testing (VA/PT)
iv. UIDAI AUA/KUA Audit

4.1.2 Each audit stream is a **distinct engagement** with distinct objectives, scope boundaries, and deliverables, even if conducted by the same audit firm.

4.2 Governing Framework

4.2.1 The audits shall be conducted in line with the regulatory and policy framework specified in **Section III – Regulatory & Policy Framework**.

4.2.2 Nothing in this section shall be construed as limiting, diluting or modifying the requirements specified under the applicable NABARD, RBI, CERT-In / MeitY, UIDAI or Bank policy framework.

4.3 Overall Coverage

4.3.1 The audits under this RFP shall cover the following operating units / environments, as applicable to each audit stream:

i. **Head Office (HO)**
ii. **Regional Offices (ROs) – 3**
iii. **Branches – 90**, with field verification through sample selection
iv. **ASP environment / outsourced technology operations**
v. **Bank-owned / in-house applications**, where in scope

4.3.2 For IS Audit, **10–12 branches** shall be covered through risk-based sampling. A DC/DR walkthrough or virtual walkthrough may be facilitated as an assurance activity, subject to feasibility and ASP coordination.

4.4 ASP and Third-Party Reliance

4.4.1 The Bank operates its core technology environment under an ASP model. Accordingly, certain technical and operational controls may be operated by the ASP or other service providers.

4.4.2 The auditor may rely on ASP / service-provider-operated controls where appropriate assurance evidence is reviewed and the basis of reliance is documented. Direct access, walkthroughs or testing involving ASP / third-party environments shall be subject to feasibility, contractual arrangements, approvals and agreed rules of engagement.

4.5 Audit Stream Relationship

To avoid overlap and ensure clarity:

i. **IS Audit** focuses on governance, controls, process discipline, oversight of outsourced services, and onsite verification.
ii. **Cyber Security Audit** assesses cyber governance and control posture and includes the **Gap Assessment** aligned to the NABARD cyber framework.

iii. **VA/PT** provides technical findings on exploitable vulnerabilities and feeds into Cyber Security Audit conclusions and gap assessment. VA/PT is an input to cyber risk and closure verification; Cyber Security Audit does not re-perform VA/PT.

iv. **UIDAI AUA/KUA Audit** is a statutory audit based on UIDAI's checklist and reporting format, supported by evidence.

4.6 Common Audit Approach

The audit firm shall adopt a structured approach which is **non-disruptive** and aligned with normal banking operations across all audit streams:

i. **Planning and scoping** (including information request list and schedule)
ii. **Understanding environment** (Bank + ASP dependence)
iii. **Control review and verification** (as per audit stream)
iv. **Sampling and onsite verification** (branch visits under IS Audit)
v. **Technical testing** (VA/PT as per agreed scope and windows)
vi. **Observation and risk classification**
vii. **Draft reporting and management discussion**
viii. **Final reporting and submission of deliverables**
ix. **Follow-up / closure verification** (including VA/PT retest; compliance closure)

4.7 Deliverables and Reporting

The audit firm shall submit separate deliverables for each audit stream, even if conducted by the same firm. Each stream report shall include:

i. **Executive summary** (for senior management/Board)
ii. **Scope covered** (including locations visited / assets tested, as applicable)
iii. **Observations** and **risk categorisation**
iv. **Evidence references** supporting conclusions
v. **Recommendations / corrective actions**
vi. **Management responses** and **target closure timelines**

For Cyber Security Audit and UIDAI AUA/KUA Audit, where a **certificate / compliance statement** is required by guideline, the same shall be issued as per applicable format.

4.8 Compliance Timelines, Closure and Re-verification

The audit engagement under this RFP does **not** end with submission of the audit report. A closure loop shall be followed, as below:

4.8.1 **Compliance / Mitigation by the Bank**

i. Upon receipt of the final report(s), the Bank shall initiate mitigation of observations/non-compliances and record compliance status based on risk and feasibility.
ii. For **IS Audit**, NABARD expects compliance to be furnished within a stipulated timeframe of **one month from the date of issue of the IS Audit Report**.

4.8.2 **Re-verification by Auditor**

i. The auditor shall re-verify closure based on evidence submitted by the Bank and/or retesting where applicable.
ii. For **VA/PT**, after remediation, **validation testing shall be conducted** to ensure vulnerabilities have been effectively addressed and no new vulnerabilities introduced.

4.8.3 **Closure / Compliance Certificate -** After satisfactory re-verification, the auditor shall issue a **closure / compliance certificate** (stream-wise) confirming closure status and listing any residual open items with reasons.

4.9 Governance Review: ACB / Board Oversight

Audit reports and closure status shall be placed before the appropriate governance forums of the Bank, including the Audit Committee of the Board / Board of Directors, wherever applicable under regulatory or internal governance requirements.

4.10 Confidentiality, Data Handling and Information Sharing

The selected auditor shall maintain confidentiality of all information received or accessed during the assignment. Sensitive information, ASP-related artefacts and technical details shall be shared post-award and / or under NDA on a need-to-know basis.

4.11 Scope Exclusions

Unless specifically stated elsewhere in this RFP, the following are not part of scope:

i. Continuous SOC operations or managed security operations
ii. Certification audits (ISO, etc.)
iii. Red-team / adversarial simulations / stress testing
iv. Routine forensic investigations (incident-triggered only and not included in this RFP)
v. Deep technical re-audit of ASP DC/DR infrastructure beyond assurance walkthroughs
vi. Source code review of CBS / ASP-owned platforms (unless expressly made available under legal/contractual arrangements)

4.12 Level and Proportionality

The Bank's cyber control expectations are aligned to the **RRB graded cyber security framework** and the Bank's current risk/exposure profile. Audit depth and effort shall be **proportionate**, focused on assurance, and designed to meet supervisory expectations without over-engineering.

SECTION V :: Scope of Work – Information Systems (IS) Audit

5.1 Objective

The objective of the Information Systems (IS) Audit is to provide independent assurance on the adequacy and effectiveness of the Bank's **IT governance, IT operations, information systems security controls, and oversight mechanisms**, including controls operating in an **outsourced/ASP model** and their implementation at operating units.

The IS Audit is conducted as an annual assurance activity and is planned such that the IS Audit output is available for consideration prior to statutory audit, as per supervisory expectations.

5.2 Coverage Units

The IS Audit shall cover the following units:

i. **Head Office (HO)** – Full coverage
ii. **Regional Offices (ROs)** – Full coverage (3 ROs)
iii. **Branches** – **10 to 12 branches** through risk-based sampling for onsite verification
iv. **ASP environment (C-EDGE)** – through Bank's oversight controls and assurance evidence review

5.3 Scope of Review

The IS Audit scope shall include, but not be limited to, the following areas (as applicable to the Bank's environment and operating model):

5.3.1 **IT Governance & Management Oversight**

i. **IT governance** structure, roles and responsibilities, committee oversight and reporting
ii. **Policy framework** (IT Policy / Information Security Policy / Cyber Security Policy / IS Audit Policy etc) and compliance monitoring
iii. **IT risk management** and reporting mechanisms
iv. **Oversight on technology service delivery** and **vendor/third-party management** at Bank level

5.3.2 **Outsourcing / ASP Governance**

The Bank operates under an ASP model. Accordingly, the IS Audit shall include review of the Bank's governance and oversight over ASP-delivered services, including:

i. **Bank's Oversight Mechanisms**
    a. Monitoring and review mechanisms at Bank level (service review meetings, escalation mechanism, issue tracking)
    b. Evidence of follow-up actions taken by the Bank on major issues/incidents/deficiencies
    c. Governance of access provisioning, approvals and controls exercised by the Bank (where applicable)
ii. **Review of ASP Artefacts (for Bank assurance)**

The auditor shall review relevant assurance artefacts available with the Bank (or provided to the Bank through the ASP under confidentiality arrangements), such as:

    a. **DR drill evidence and outcomes**, including gaps observed and actions taken
    b. **VA/PT reports and closure/validation evidence** relevant to Bank-facing assets/services

c. **Cyber security audit / IS audit / compliance assurance** reports and certificates shared with the Bank for the ASP-hosted environment (where available)
d. Evidence of Bank's tracking and closure of observations arising from such assurance artefacts

Principle of reliance: Reliance on ASP-operated controls is acceptable where the auditor reviews appropriate assurance evidence and documents the basis of such reliance in the audit records and report.

5.3.3 **Access Management & Segregation of Duties**

i. User access provisioning/de-provisioning and maker–checker controls
ii. Privileged access governance for Bank users
iii. Periodic user access review processes and exception handling
iv. Password/credential discipline and access governance

5.3.4 **IT Operations & Change Management (Bank-side governance)**

i. IT operations processes (operational checklists, monitoring, exception handling)
ii. Backup governance and restoration readiness (evidence-based)
iii. Change management governance (request/approval/implementation/rollback controls) at Bank control points
iv. Patch/update governance (policy-level and evidence-based review)

5.3.5 **Information Security Controls**

i. Bank-side information security controls and governance (as applicable)
ii. Logging/monitoring practices available at Bank level, including oversight of outsourced monitoring
iii. Incident management discipline and escalation (Bank-side process and evidence)

5.3.6 **Business Continuity / DR Oversight**

i. Review of BCP/DR governance and responsibilities
ii. Review of DR drill evidence/outcomes made available to the Bank and follow-up action status
iii. Coordination mechanisms with the ASP for continuity readiness

DC/DR walkthrough/visit: A DC/DR walkthrough/visit (physical or virtual) may be facilitated as an assurance activity subject to feasibility and coordination with the ASP. This is not intended as a deep technical re-audit of ASP DC/DR infrastructure.

5.3.7 **Branch-Level Implementation (Onsite Verification)**

Branch visits shall validate practical implementation of controls, including:

i. Physical security of IT assets and records
ii. User practices (credential discipline, device handling, controlled access)
iii. Maker–checker discipline in practice
iv. Handling of sensitive data (including Aadhaar-related handling where applicable)
v. BC/CSP operational oversight at branch level (where relevant)
vi. Awareness of incident reporting/escalation procedures

5.4 Audit Execution Approach

5.4.1 IS Audit shall be conducted through a mix of:

i. Document review and control verification
ii. Interviews with relevant stakeholders
iii. Evidence-based sampling
iv. Onsite verification at HO/ROs and selected branches

5.4.2 The auditor shall document:

i. locations visited,
ii. records examined,
iii. samples checked, and
iv. evidence references supporting each observation.

5.5 Deliverables

The auditor shall submit the following deliverables for IS Audit:

5.5.1 **IS Audit Report (Final)**

i. Executive summary
ii. Scope covered (HO/ROs, branch sample, walkthroughs as applicable)
iii. Observations with risk categorisation and evidence references
iv. Recommendations/corrective actions (practical and implementable)
v. Management responses and target closure timelines

5.5.2 **Branch Visit Observation Summary** - Consolidated branch-level observations and common themes

5.5.3 **ASP Assurance Review Note**

i. Summary of assurance artefacts reviewed (e.g., DR drills, VA/PT closure evidence, audit/certification artefacts made available)
ii. Key observations relevant to Bank assurance and oversight

5.5.4 **DC/DR Walkthrough Note -** Assurance observations and evidence reviewed

5.6 Compliance Timeline, Re-verification and Closure Certificate

IS Audit engagement includes a closure loop:

i. Submission of **IS Audit Report** by the auditor.
ii. **Compliance / mitigation** by the Bank: NABARD expects IS Audit reports to be placed before governance forums and compliance to be furnished within a stipulated timeframe of **one month from the date of issue of the IS Audit Report**.
iii. **Re-verification by auditor**: The auditor shall **verify closure** based on evidence submitted by the Bank.
iv. **IS Audit Closure / Compliance Certificate**: Upon satisfactory verification, the auditor shall issue an **IS Audit closure/compliance certificate** listing closed items and any pending items with reasons.

SECTION VI :: Scope of Work – Cyber Security Audit (Including Gap Assessment)

6.1 Objective

6.1.1 The objective of the Cyber Security Audit is to provide independent assurance on the Bank's **cyber security governance, control posture, cyber risk management and preparedness.**

6.1.2 The audit shall include a **Cyber Security Framework Gap Assessment** aligned to the applicable NABARD cyber security framework for RRBs and shall be conducted in line with applicable CERT-In / MeitY requirements. The audit approach shall also consider relevant RBI cyber security guidance applicable to banks, as adopted or applicable to RRBs.

6.1.3 This audit is an assurance engagement. It is not a certification audit, red-team exercise, routine forensic investigation, or a consultancy/system redesign assignment.

6.2 Coverage Units (Locations / Offices)

The Cyber Security Audit shall cover:

i. **Head Office (HO)**
ii. **Regional Offices (Three ROs)**
iii. **Branches:** branch-level cyber hygiene and governance inputs shall be leveraged from IS Audit branch visits (to avoid duplication). Additional branch verification shall be undertaken only if required.
iv. **Bank-owned / in-scope applications, channels and interfaces**, where relevant to cyber governance and control posture.
v. **ASP environment (C-EDGE):** assessment through evidence-based reliance and review of assurance artefacts, consistent with the applicable guidelines for third-party hosting/outsourcing

6.3 Scope of Review

6.3.1 **Cyber Security Governance & Oversight**

The auditor shall review:

i. cyber security governance structure, roles and responsibilities;
ii. cyber security policy framework and review mechanism;
iii. cyber risk identification, assessment, treatment and reporting;
iv. cyber security committee / management oversight and escalation;
v. reporting discipline for cyber incidents and near misses;
vi. oversight of cyber risks arising from ASP / third-party arrangements.

6.3.2 **Awareness, Hygiene and User-Level Controls**

The auditor shall review:

i. user awareness and cyber hygiene initiatives;
ii. anti-phishing awareness and reporting mechanisms;
iii. incident reporting and escalation awareness;
iv. endpoint / user practice hygiene at a governance and sample-verification level;
v. branch-level cyber hygiene inputs, where available from IS Audit visits.

6.3.3 **Asset, Exposure and Third-Party Cyber Risk Governance**

The auditor shall review:

i. identification of critical systems, applications, channels and cyber-relevant assets from the Bank's perspective;
ii. cyber risk treatment for internet-facing and customer-facing channels;
iii. third-party / outsourced cyber risk governance;
iv. oversight arrangements for ASP and other technology service providers;
v. tracking of material cyber risks, exceptions and remediation actions.

This review shall be governance and evidence-based and shall not be treated as a full technical asset discovery or attack surface enumeration exercise.

6.3.4 **Network and Infrastructure Security Governance**

The auditor shall review governance and control evidence relating to:

i. perimeter / firewall rule review discipline;
ii. network segmentation / boundary control governance;
iii. DMZ / internet-facing exposure governance, where applicable;
iv. remote access governance, including VPN / controlled access approvals and review;
v. secure configuration baseline and exception management;
vi. patch governance and closure tracking.

6.3.5 **Security Operations, Logging and Monitoring**

The auditor shall review:

i. security monitoring and logging governance;
ii. availability of audit / incident evidence;
iii. incident detection, escalation and response discipline;
iv. outsourced monitoring oversight, where applicable;
v. log retention, time synchronisation and evidence production capability;
vi. linkage between monitoring outputs, incident response and governance reporting.

6.3.6 **Vulnerability and Patch Management Governance**

The auditor shall review:

i. vulnerability identification, tracking and prioritisation process;
ii. linkage between VA/PT findings and remediation actions;
iii. patch management governance and closure evidence;
iv. treatment of recurring, delayed or high-risk vulnerabilities;
v. residual risk treatment and exception approval, where applicable.

6.3.7 **Identity, Access and Privileged Access Governance**

The auditor shall review cyber-critical access governance, including:

i. privileged access governance for Bank users;
ii. periodic access review for cyber-sensitive systems;
iii. segregation of duties for cyber-sensitive functions;
iv. exception handling and approval controls;
v. evidence of access governance over outsourced or ASP-operated environments, where available.

6.3.8 **Data Protection / DLP Governance**

i. Where applicable, the auditor shall review governance of controls relating to prevention of data leakage through users, endpoints, channels, workflows and third-party arrangements.

ii. The review shall focus on policy, control design, monitoring, exception handling and evidence availability, rather than product-specific configuration unless such review is expressly in scope.

6.3.9 **Application Security Governance**

i. Application security shall be covered from a cyber control and governance perspective for in-scope Bank-owned / Bank-managed applications, web portals, mobile applications, APIs and security-critical source code modules, where applicable.

ii. The auditor shall review governance and evidence relating to:
   (a) secure development / change governance;
   (b) authentication and authorisation controls;
   (c) session management and input validation controls;
   (d) sensitive data handling;
   (e) logging and error handling;
   (f) remediation tracking of application security findings.

iii. Technical testing of web applications, mobile applications, APIs or source code modules shall be handled under the VA/PT stream where applicable. Cyber Security Audit shall consider the results of such testing for cyber risk conclusions and gap assessment.

6.3.10 **VA/PT Integration**

VA/PT is a separate audit stream under this RFP. The Cyber Security Audit shall:

i. review material VA/PT findings relevant to Bank-owned / Bank-exposed assets and in-scope applications;

ii. consider remediation progress, validation / retest outcomes and residual open vulnerabilities;

iii. reflect material technical risks in the cyber security conclusions and gap assessment;

iv. identify recurring or systemic issues emerging from VA/PT results.

The Cyber Security Audit shall not re-perform VA/PT.

6.3.11 **ASP-operated Cyber Controls**

For ASP-operated or third party operated cyber controls, the auditor shall review relevant assurance evidence made available to the Bank, including, where available:

i. cyber security audit / compliance assurance reports;

ii. VA/PT reports and closure / validation evidence;

iii. DR drill outcomes relevant to cyber resilience;

iv. incident notification / coordination evidence;

v. Bank's tracking and follow-up of ASP-related cyber observations.

Reliance on ASP-operated controls shall be acceptable where appropriate assurance evidence is reviewed and the basis of reliance is documented by the auditor.

6.4 Cyber Security Framework Gap Assessment

The auditor shall perform a Cyber Security Framework Gap Assessment aligned to NABARD's graded framework for RRBs, proportionate to the Bank's size, operating model, cyber maturity and risk profile, focusing on:

i. Control gaps relevant to the Bank's level and operating model
ii. Oversight gaps for outsourced/third-party cyber controls
iii. Gaps arising from VA/PT or other assurance findings;
iv. Practical, prioritised corrective actions
v. Residual open risks, where applicable.

6.5 **Audit Execution Approach**

The Cyber Security Audit shall be conducted through:

i. Document and evidence review
ii. Interviews/discussions with relevant stakeholders
iii. Sampling and verification appropriate to the audit stream
iv. Review of assurance artefacts for outsourced controls
v. Correlation with VA/PT findings and closure evidence
vi. Evidence and documentation shall support conclusions and recommendations, consistent with CERT-In audit guidance.

6.6 Deliverables

The auditor shall submit the following deliverables:

i. **Cyber Security Audit Report**
   (a) Executive summary
   (b) Scope covered
   (c) Observations with risk classification and evidence references
   (d) NABARD-aligned cyber framework gap assessment summary (VICS implicit)
   (e) Application security observations (web/mobile/API/code modules) where in scope
   (f) Practical recommendations and corrective actions
   (g) Management responses and target closure timelines

ii. **ASP Cyber Assurance Review Note (as applicable)**
   (a) Summary of cyber-related assurance artefacts reviewed
   (b) Key observations relevant to Bank oversight and residual risk

iii. **Cyber Security Audit Compliance & Closure Certificate**
   Issued after re-verification, listing closed items and pending items with reasons

6.7 Compliance, Re-verification and Closure Certificate

Cybersecurity Audit engagement includes a closure loop:

i. Submission of Cyber Security **Audit Report** by the auditor.
ii. **Compliance/mitigation** by the Bank based on severity and feasibility.
iii. **Re-verification** by auditor based on evidence submitted by the Bank and VA/PT retest/validation outputs where applicable.
iv. **Cyber Security Audit Compliance & Closure Certificate** to be issued upon satisfactory verification, listing closed and pending items with reasons.

SECTION VII – Scope of Work – Vulnerability Assessment & Penetration Testing (VA/PT)

7.1 Objective

7.1.1 The objective of Vulnerability Assessment and Penetration Testing (VA/PT) is to identify technical vulnerabilities and exploitable weaknesses in the Bank's in-scope systems, applications, interfaces and exposed technology assets, and to provide practical remediation guidance.

7.1.2 VA/PT shall be conducted by a **CERT-In empanelled audit firm** and shall follow applicable MeitY/CERT-In guidelines and relevant RBI / NABARD supervisory expectations on vulnerability assessment and penetration testing.

7.1.3 The VA/PT output shall be used for:

i. prioritising remediation;
ii. validating closure after remediation;
iii. supporting Cyber Security Audit conclusions; and
iv. informing the Cyber Security Framework Gap Assessment.

7.1.4 VA/PT is a technical assurance activity. It is not a red-team exercise, denial-of-service test, forensic investigation, or continuous monitoring service.

7.2 Scope Boundaries in ASP Model

7.2.1 The Bank operates under an ASP model through **C-EDGE**. Accordingly, VA/PT shall be scoped with clear distinction between:

i. Bank-owned / Bank-managed assets,
ii. Bank-exposed assets,
iii. ASP-owned / ASP-operated assets,
iv. third-party hosted or managed services.

7.2.2 For Bank-owned or Bank-managed assets, the selected auditor may conduct VA/PT directly within the agreed scope and testing windows.

7.2.3 For ASP-owned or ASP-operated assets, including applications, mobile apps, APIs or infrastructure components under ASP control, VA/PT shall be handled through one or both of the following approaches:

i. **Review of ASP assurance evidence**, including relevant VA/PT reports, closure evidence and validation / retest reports made available to the Bank; and/or
ii. **Direct VA/PT by the selected auditor**, only where contractually and operationally feasible, with prior coordination with the ASP and under agreed Rules of Engagement.

7.3 In-Scope Target Areas

The VA/PT scope shall include the following, where such systems / applications / interfaces exist and are identified as in scope.

7.3.1 **Internet-facing assets**

i. Bank website and public web presence.
ii. Internet-facing portals.
iii. Internet-facing services, exposed interfaces and endpoints.
iv. External attack surface relevant to Bank operations.

7.3.2 **Web portals and Bank-owned / in-house applications**

i. Bank-owned web portals.

ii. MIS portals and internal applications exposed through web interfaces.
iii. Bank-owned applications hosted on Bank-controlled or Bank-approved environments.
iv. Application-level security testing of in-scope applications.

7.3.3 **Mobile applications**

i. Mobile application VA/PT shall be conducted **where mobile applications are in use**.
ii. Where the mobile application is **Bank-owned** or **Bank-managed**, VA/PT shall be conducted directly by the selected CERT-In empanelled auditor.
iii. Where the mobile application is **ASP-owned / ASP-operated**, the auditor shall **review** ASP VA/PT reports, closure evidence and validation results relevant to the Bank. Direct VA/PT may be conducted only where permitted and coordinated through the Bank and ASP under agreed Rules of Engagement.

7.3.4 **APIs**

i. APIs shall be covered where they exist and are identified as in scope.
ii. The review may include API exposure, authentication, authorisation, input validation, error handling, data leakage risk, logging and abuse protection, as applicable.

7.3.5 **Network / perimeter exposure**

VA/PT shall include review of externally exposed network / perimeter posture relevant to the Bank, such as:

i. exposed ports and services,
ii. perimeter exposure,
iii. externally reachable interfaces,
iv. misconfigurations visible from the permitted testing scope.
v. This shall not be treated as a device-by-device internal configuration audit.

7.3.6 **Source code review – security critical modules**

i. Where source code is available and the application is within scope, the auditor shall conduct focused source code review of **security-critical modules** only.
ii. The review shall focus on security-relevant risks such as:
    i. authentication,
    ii. authorisation,
    iii. session management,
    iv. input validation,
    v. sensitive data handling,
    vi. insecure cryptographic usage,
    vii. error handling,
    viii. logging weaknesses.
iii. This shall not be treated as full functional code review, performance review, or application redesign.
iv. Application security testing and source code review shall be guided, where applicable, by CERT-In's Guidelines for Secure Application Design, Development, Implementation & Operations.

7.4 Testing Approach and Rules of Engagement

7.4.1 VA/PT shall be conducted in a controlled and non-disruptive manner.

7.4.2 Before commencement of testing, the auditor shall agree with the Bank on:

i. final list of in-scope assets,
ii. testing windows,
iii. test accounts, if required,
iv. source IPs / tools / access requirements, where applicable,
v. coordination requirements with ASP or third parties,
vi. escalation contacts,
vii. restrictions and exclusions.

7.4.3 The auditor shall not conduct denial-of-service, destructive, disruptive or unauthorised testing.

7.4.4 Critical vulnerabilities or exposures that may materially impact the Bank shall be promptly brought to the notice of designated Bank officials, without waiting for the final report.

7.4.5 Testing shall be evidence based and findings shall be reproducible to the extent practicable.

7.5 Severity Classification

7.5.1 All VA/PT findings shall be classified into severity categories – **Critical, High, Medium, Low**

7.5.2 Severity classification shall be based on technical impact, exploitability, exposure, likelihood and potential business / regulatory impact.

7.5.3 Where applicable, the auditor may also provide CVSS score or equivalent supporting metric. However, the severity category shall be clearly stated in all reports.

7.6 Remediation and Validation Testing

7.6.1 The Bank shall initiate remediation of reported vulnerabilities based on severity and feasibility.

7.6.2 After remediation, the auditor shall conduct validation testing / retesting to confirm whether the reported vulnerabilities have been addressed.

7.6.3 The retesting shall be limited to vulnerabilities reported in the original VA/PT report, unless otherwise agreed.

7.6.4 The validation report shall clearly state:

i. vulnerabilities closed,
ii. vulnerabilities partially closed,
iii. vulnerabilities not closed,
iv. any residual risk,
v. any new vulnerability introduced during remediation, if identified.

7.7 Deliverables

The auditor shall submit the following deliverables for the VA/PT

7.7.1 **VA/PT Plan / Rules of Engagement -** This shall include:

i. in-scope assets,
ii. testing approach,
iii. testing windows,
iv. exclusions,
v. contact matrix,
vi. dependencies on Bank / ASP / third parties.

7.7.2 **VA/PT Report -** The final VA/PT report shall include:

i. executive summary,
ii. scope covered,
iii. methodology followed,
iv. assets / applications tested,
v. vulnerabilities identified,
vi. severity classification as Critical / High / Medium / Low,
vii. evidence / proof of concept, where appropriate,
viii. impact,
ix. remediation recommendations,
x. management response / target closure date.

7.7.3 **Retest / Validation Report -** The retest / validation report shall include:

i. status of each reported vulnerability,
ii. evidence of closure,
iii. residual open items,
iv. reasons for non-closure, if any,
v. recommendations for pending items.

7.7.4 **VA/PT Compliance & Closure Certificate**

Upon satisfactory validation, the auditor shall issue a stream-wise **VA/PT Compliance & Closure Certificate** / closure statement confirming the closure status of vulnerabilities and listing any pending items with reasons.

7.8 Integration with Cyber Security Audit

7.8.1 VA/PT is a separate audit stream under this RFP. However, VA/PT findings shall be used as technical inputs for Cyber Security Audit and Cyber Security Framework Gap Assessment.

7.8.2 The Cyber Security Audit shall consider material VA/PT findings, remediation progress, retest / validation outcomes, residual open vulnerabilities and recurring or systemic issues.

7.8.3 This integration is intended to ensure that VA/PT contributes to the Bank's overall cyber risk assessment and supervisory gap assessment.

SECTION VIII – Scope of Work – UIDAI AUA/KUA IS Audit

8.1 Objective

8.1.1 The objective of the **UIDAI AUA/KUA IS Audit** is to provide independent assurance on the Bank's compliance with applicable UIDAI requirements for Aadhaar Authentication User Agency (AUA) and KYC User Agency (KUA) operations.

8.1.2 The audit shall be conducted as a **checklist-based and evidence-backed compliance audit** in accordance with UIDAI-prescribed requirements, formats and compliance checklist.

8.1.3 The UIDAI-prescribed checklist / certificate / statement, wherever applicable, shall remain the **primary compliance artefact**.

8.1.4 The UIDAI AUA/KUA IS Audit is not intended to be a general cyber security audit, VA/PT exercise, forensic investigation, or consultancy assignment.

8.2 Regulatory Basis

8.2.1 The UIDAI AUA/KUA IS Audit shall be conducted in accordance with applicable UIDAI regulations, specifications, circulars, audit requirements and compliance checklist applicable to AUA/KUA entities.

8.2.2 The primary audit reference shall be the **UIDAI Compliance Checklist for certifying compliance with controls that the AUA/KUA is required to have in place**, or any updated / revised checklist applicable at the time of audit.

8.2.3 Where UIDAI prescribes a specific checklist, certificate, declaration, statement or reporting format, the auditor shall use the applicable UIDAI-prescribed format.

8.3 Coverage and Operating Model

8.3.1 The Bank is directly operating as AUA/KUA. Accordingly, the UIDAI AUA/KUA IS Audit shall assess controls applicable to the Bank as AUA/KUA.

8.3.2 The audit shall cover Aadhaar authentication / eKYC related processes, Aadhaar data handling controls, access control, logging, audit trails, incident / exception handling and oversight of technology service providers, as applicable under UIDAI requirements.

8.3.3 Where UIDAI-relevant controls are operated by the ASP / technology service provider, the auditor shall review relevant assurance evidence made available and document the basis of reliance.

8.3.4 BC/CSP-related aspects shall be considered only as part of Aadhaar operations wherever Aadhaar authentication / eKYC / Aadhaar-enabled services are performed through such channels. A separate BC/CSP audit is not intended under this section.

8.4 Scope of Work – UIDAI Checklist Based

8.4.1 The detailed scope of the UIDAI AUA/KUA IS Audit shall be governed by the UIDAI-prescribed compliance checklist and applicable UIDAI directions. The areas listed below are indicative and shall not limit, dilute or substitute the UIDAI checklist.

8.4.2 The auditor shall review, as applicable:

i. governance and UIDAI compliance ownership;
ii. AUA/KUA roles, contact points and coordination with UIDAI;
iii. Aadhaar authentication / eKYC process controls;
iv. consent and customer communication controls;

v. Aadhaar data handling, storage, masking, retention and protection controls;
vi. access control and user lifecycle controls;
vii. logging, monitoring and audit trail requirements;
viii. incident, exception and breach handling processes;
ix. ASP / technology service provider assurance evidence relevant to Aadhaar operations.

8.4.3 Where technical controls such as Aadhaar vault, encryption, HSM, secure transmission, APIs, logging or related controls are operated by the ASP / technology service provider, the auditor shall review assurance evidence available with the Bank and document the basis of reliance.

8.5 Audit Execution Approach

8.5.1 The UIDAI AUA/KUA IS Audit shall be conducted through:

i. review of UIDAI-prescribed checklist and applicable requirements;
ii. document and evidence review;
iii. discussions with relevant Bank officials;
iv. review of ASP / technology provider assurance evidence where relevant;
v. sample-based verification of Aadhaar-related processes, where applicable;
vi. preparation of auditor observations and management comments in the required format.

8.5.2 The auditor shall ensure that conclusions are evidence-backed and aligned to UIDAI checklist requirements.

8.6 Deliverables

The auditor shall submit the following deliverables for the UIDAI AUA/KUA IS Audit:

8.6.1 **UIDAI AUA/KUA IS Audit Report**

The report shall include:

i. executive summary;
ii. scope covered;
iii. compliance status;
iv. key observations / non-compliances;
v. evidence references;
vi. management responses;
vii. corrective actions and target closure timelines.

8.6.2 **Completed UIDAI Compliance Checklist**

The auditor shall submit the completed UIDAI checklist in the prescribed format, including:

i. compliance status;
ii. auditor observations;
iii. management comments;
iv. evidence references, wherever applicable.

The completed UIDAI checklist shall remain the primary checklist-based compliance artefact for this audit.

8.6.3 **UIDAI-prescribed Compliance Certificate / Statement**

i. Where UIDAI requires a specific certificate, statement, declaration or checklist output, the auditor shall issue the same strictly in the applicable UIDAI-prescribed format.

ii. Nothing in this RFP shall be construed as modifying or replacing any UIDAI-prescribed certificate, statement, declaration, checklist or reporting format.

8.6.4 **UIDAI AUA/KUA IS Audit Compliance & Closure Certificate / Closure Status Note**

i. After re-verification of observations / non-compliances, the auditor shall issue a **UIDAI AUA/KUA IS Audit Compliance & Closure Certificate / Closure Status Note**

ii. This document shall be limited to post-audit closure status and shall include:

(a) observations closed;

(b) observations pending closure;

(c) reasons for pending status;

(d) residual risk / pending action, wherever applicable.

iii. This document shall not replace, override or modify any UIDAI-prescribed checklist, certificate, statement or declaration. It shall only evidence the closure status of audit observations after re-verification for the Bank's internal governance, audit tracking and compliance monitoring.

8.7 Compliance, Re-verification and Closure

8.7.1 The UIDAI AUA/KUA IS Audit shall include a closure loop.

i. The auditor shall submit the UIDAI AUA/KUA IS Audit Report, completed UIDAI checklist and UIDAI-prescribed certificate / statement, wherever applicable.

ii. The Bank shall initiate corrective action for observations / non-compliances.

iii. The auditor shall re-verify closure based on evidence submitted by the Bank and/or evidence made available through ASP / technology provider, as applicable.

iv. Upon satisfactory verification, the auditor shall issue the UIDAI AUA/KUA IS Audit Compliance & Closure Certificate / Closure Status Note.

8.7.2 Where any observation remains open, the closure certificate / closure status note shall clearly indicate pending items and reasons.

8.7.3 The closure certificate / closure status note is intended only for the Bank's internal governance, audit tracking and closure monitoring, and shall remain consistent with UIDAI-prescribed reporting requirements.

SECTION IX :: Bid Submission, Eligibility, Evaluation and Timelines

9.1 Eligibility and Evaluation Principle

9.1.1 The Bank shall follow a **two-bid evaluation process** comprising:

i. Technical Bid

ii. Commercial Bid

9.1.2 Only bidders meeting all mandatory eligibility criteria shall be considered technically qualified. Commercial bids of only technically qualified bidders shall be opened.

9.1.3 Selection shall be based on the **lowest total evaluated commercial quote (L1)** for the complete scope of work covering all audit streams under this RFP, namely:

i. Information Systems (IS) Audit

ii. Cyber Security Audit including Gap Assessment

iii. Vulnerability Assessment & Penetration Testing (VA/PT)

iv. UIDAI AUA/KUA IS Audit

9.1.4 All eligibility criteria specified in this section are mandatory unless expressly stated otherwise.

9.1.5 The bidder shall submit responses strictly in the formats prescribed in the **Annexures**. The prescribed formats are intended to ensure uniformity of responses and facilitate objective evaluation.

9.2 Minimum Eligibility Criteria

The bidder shall satisfy all minimum eligibility criteria listed below. Failure to meet any mandatory criterion, or failure to submit acceptable documentary evidence against any mandatory criterion, shall render the bid technically non-responsive.

SN	Eligibility Criterion	Minimum Requirement	Response Format / Evidence
1	**CERT-In Empanelment**	Bidder must be a CERT-In empanelled Information Security Auditing Organisation as on bid submission date and must remain empanelled during the engagement period.	**Annexure B** and **Annexure G.5**; attach CERT-In empanelment proof / current listing reference
2	**Legal Constitution**	Bidder must be a legally constituted entity permitted to undertake audit / assurance services.	**Annexure B**; attach registration / incorporation documents
3	**Minimum Existence**	Bidder must have been in operation for at least **3 years** as on bid submission date.	**Annexure B**; attach proof of establishment / incorporation / registration
4	**Financial Turnover**	Bidder must have **average annual turnover** of at least **₹75 lakh** during the latest three audited financial years available as on the bid submission date.	**Annexure B**; attach audited financial statements and / or CA certificate
5	**Banking / Financial Sector Experience**	Bidder must have completed at least **2 similar technology audit engagements** in banking / financial sector aligned to RBI / NABARD regulatory framework during the last **3 years**.	**Annexure C.1**; attach work orders / completion certificates / client confirmations / anonymised evidence
6	**RRB (ASP Model) Experience**	Bidder must have completed **at least one engagement** involving an **RRB** operating	**Annexure C.2**; attach work order / completion certificate / scope

SN	Eligibility Criterion	Minimum Requirement	Response Format / Evidence
		under an **Application Service Provider (ASP) model**, within the last **3 years**.	evidence / anonymised evidence
7	**UIDAI AUA/KUA IS Audit Experience**	Bidder must have completed at least **1 UIDAI AUA/KUA IS Audit / Aadhaar ecosystem compliance audit / UIDAI checklist-based audit engagement**.	**Annexure C.3**; attach work order / completion certificate / client confirmation / anonymised evidence
8	**Qualified Audit Team**	Bidder must propose named resources meeting minimum team requirements specified in this RFP.	**Annexure D**; attach CVs and certification proof
9	**No Blacklisting / Debarment**	Bidder must **not be blacklisted / debarred** by any Government department, regulatory authority (including RBI / NABARD), statutory authority, public sector bank, financial institution, CERT-In, UIDAI or NABARD-supervised entity.	**Annexure G.2**
10	**Confidentiality and Conflict of Interest**	Bidder must accept **confidentiality, NDA and conflict-of-interest** requirements.	**Annexure G.3**
11	**No Subcontracting**	Bidder must undertake that the assignment shall be executed through its own personnel and shall not be subcontracted.	**Annexure G.4**
12	**Acceptance of RFP Terms**	Bidder must submit unconditional acceptance of all RFP terms and conditions.	**Annexure G.1**

9.3 Submission of Bids

9.3.1 The proposal shall be submitted in two separate parts:

i. **Technical Bid**

ii. **Commercial Bid**

9.3.2 Bids may be submitted either:

i. **electronically by email** to the following email address – **ciso@meghalayaruralbank.bank.in** or

ii. **physically in separate sealed covers** to the address below

General Manager (I)
Meghalaya Rural Bank, Head Office
KJP Assembly Conference Centre,
Barik, Shillong – 793001, Meghalaya

9.3.3 The **Technical Bid** shall contain **all Annexures and supporting documents** required under this RFP and shall not contain any commercial information.

9.3.4 The **Commercial Bid** shall be submitted separately in **Annexure F – Commercial Bid Format**. Where submitted electronically, the Commercial Bid shall be **password protected**, and the password shall be shared only upon request by the Bank at the stage of Commercial Bid opening. Where submitted physically, the Commercial Bid shall be submitted in a **separate sealed cover** clearly marked as "Commercial Bid".

9.3.5 Bidders are advised to ensure consistency and completeness of submission. In the event of **multiple submissions** by the same bidder through different modes, the Bank may, at

its discretion, seek written confirmation from the bidder as to the version to be treated as final; failing such confirmation, the Bank may treat the latest complete submission received within the prescribed time as the final bid.

9.3.6 Bids received after the prescribed date and time, bids not submitted in the prescribed format, or bids in which the Technical Bid contains commercial information may be treated as non-responsive.

9.4 Bid Validity

The bid shall remain valid for a period of 180 days from the last date of bid submission.

9.5 Bid and Eligibility Conditions

9.5.1 All mandatory eligibility credentials shall be in the **name of the bidder** submitting the bid. Credentials of group companies, affiliates, associates, subcontractors, proposed consultants or third parties shall not be considered for satisfying mandatory eligibility criteria.

9.5.2 The **Bank may seek clarifications** during evaluation. Such clarifications shall be limited to explanation, confirmation or validation of documents already submitted with the bid. Clarifications shall not be used to submit new eligibility documents, cure failure to meet mandatory eligibility criteria, substitute bidder credentials, replace experience documents, introduce new team credentials, or modify the Commercial Bid.

9.5.3 The selected bidder shall execute the assignment through its **own qualified personnel**. Subcontracting, outsourcing, assignment or transfer of the audit assignment, in whole or in part, shall not be permitted.

9.5.4 The bidder shall deploy the **named team proposed** in the Technical Bid. Replacement of key team members after award shall not be permitted except in unavoidable circumstances and only with prior written approval of the Bank. Any approved replacement shall possess equal or better qualifications and experience than the originally proposed resource.

9.5.5 The bidder shall submit unconditional acceptance of the RFP terms. Bids containing material deviation, conditional acceptance or conditional pricing may be rejected.

9.6 Minimum Team Requirements

9.6.1 The proposed team shall collectively demonstrate capability to perform all audit streams under this RFP. The bidder shall provide named resources for the following roles in **Annexure D – Proposed Team Profile and Role Mapping**.

i. **Engagement Lead / Audit Lead** – experienced in IS / cyber security audit of banks or financial institutions and possessing at least one relevant professional qualification such as CISA, DISA, CISSP, CISM or ISO 27001 Lead Auditor.

ii. **IS Audit / Cyber Security Audit Resource** – experienced in IS Audit, Cyber Security Audit, control review, gap assessment and evidence-based reporting.

iii. **VA/PT Specialist** – experienced in VA/PT of web applications, APIs, mobile applications where applicable, internet-facing assets and network / perimeter exposure.

iv. **Application Security Resource** – experienced in web application security, mobile application security, API security and source code review of security-critical modules.

v. **UIDAI AUA/KUA IS Audit Resource** – experienced in UIDAI AUA/KUA IS Audit, Aadhaar ecosystem compliance audit or UIDAI checklist-based assessment.

9.6.2 Generic statements such as "qualified resources will be deployed" shall not be sufficient unless supported by named profiles and documentary evidence in **Annexure D**.

9.7 Evaluation Methodology – Two Bid Model

The Bank shall follow a two-bid evaluation process as under:

Stage 1 – Technical Bid Evaluation

Stage 2 – Commercial Bid Evaluation and Award

Stage 1 – Technical Bid Evaluation

i. The Bank shall evaluate the Technical Bid to determine whether the bidder meets the mandatory eligibility and technical requirements specified in this RFP.

ii. The Technical Bid evaluation shall include verification of:
   (a) submission of the bid within the prescribed date and time;
   (b) completeness of required Annexures and declarations;
   (c) valid CERT-In empanelment proof;
   (d) compliance with Minimum Eligibility Criteria under Section 9.2;
   (e) supporting documents submitted against the prescribed Annexures;
   (f) proposed team credentials and role mapping;
   (g) proposed audit approach, work plan and effort estimate;
   (h) absence of commercial information in the Technical Bid.

iii. A bidder shall be treated as technically qualified only if all mandatory eligibility requirements are met.

iv. There shall be **no Earnest Money Deposit (EMD)** for this RFP.

Stage 2 – Commercial Bid Evaluation and Award

i. Commercial bids of only technically qualified bidders shall be opened.

ii. Commercial evaluation shall be based on the **total evaluated cost for all audit streams taken together**, and not on stream-wise lowest rates.

iii. The bidder with the lowest total evaluated commercial quote for the complete scope shall be considered **L1**, subject to:
   (a) arithmetic correctness;
   (b) compliance with **Annexure F – Commercial Bid Format**;
   (c) absence of conditional pricing;
   (d) Bank's right to seek clarifications.

iv. Stream-wise lowest rates shall not be used for award determination.

v. The Bank may issue work order / letter of award to the successful bidder after completion of evaluation and approval by the competent authority.

vi. The Bank reserves the right to accept or reject any bid, cancel the RFP process, seek clarifications, annul or re-tender the process, or not award the assignment to any bidder, without assigning any reason, subject to applicable procurement norms.

9.8 No Negotiation:

There shall be no negotiation with bidders after opening of Commercial Bids, except where permitted under applicable procurement norms and with approval of the competent authority.

9.9 Anti-canvassing / anti-lobbying

Any form of canvassing, lobbying or attempt to influence the evaluation process may result in rejection of the bid.

9.10 Timeline and Sequencing

9.10.1 The assignment timeline shall be reckoned from the date of work order / kick-off.

9.10.2 The bidder shall provide its proposed audit approach, work plan, resource deployment, effort estimate and indicative timeline in **Annexure E – Audit Approach, Work Plan and Effort Estimate**.

9.10.3 The key dates and milestones are set out in the **Bid Schedule**, and the indicative audit deliverable timelines are set out in the **Indicative Audit Deliverable Schedule**, both forming part of this RFP. The selected bidder shall align its detailed audit plan accordingly, subject to approval by the Bank.

9.10.4 Commencement and adherence to timelines shall be material to the engagement. Failure to attend the kick-off, submit the agreed audit plan, commence audit activities, provide timely responses, or achieve the approved milestones may be treated as failure to perform, particularly where such delay may affect the Bank's regulatory, supervisory, statutory audit, UIDAI compliance or governance timelines.

9.11 Bank's Right to Modify Timelines

i. The Bank may modify the schedule based on operational requirements, availability of evidence, regulatory urgency, branch availability, ASP coordination or administrative reasons.

ii. The bidder shall plan resources accordingly. Reasonable schedule adjustments by the Bank shall not be treated as change in scope unless such modification materially alters the agreed work.

9.12 Governing Law and Jurisdiction

This RFP and the resulting engagement shall be governed by the laws of India and subject to the jurisdiction of courts at Shillong, Meghalaya.

9.13 Pre-bid Queries (Online)

9.13.1 The Bank may conduct an online pre-bid meeting on the date and time specified in the RFP / notice. Bidders may raise queries during the meeting. The Bank may, at its discretion, respond during the meeting or issue written clarification / corrigendum / addendum. The Bank shall not be obligated to respond to every query. Verbal discussions shall not modify the RFP unless confirmed in writing by the Bank. Participation in the meeting, raising of queries, or pendency of any clarification shall not entitle any bidder to seek extension, suspension or deferment of the RFP process. **Any written clarification / corrigendum / addendum issued by the Bank shall form part of the RFP.**

9.13.2 All written communications / clarifications relating to this RFP shall be addressed to the designated Bank email address (ciso@meghalayaruralbank.bank.in) specified for bid submission, unless otherwise notified by the Bank.

SECTION X :: Payment Terms and General Conditions

10.1 Payment Terms

10.1.1 Payment shall be made against accepted deliverables as under:

Milestone	Payment
Submission and acceptance of all final stream-wise audit reports / checklists / certificates, as applicable	70%
Completion of all re-verification / retesting and submission of applicable stream-wise closure certificates / closure notes	30%

10.1.2 No stream-wise, partial or interim payment shall be payable. Payment shall be subject to satisfactory submission and acceptance of deliverables by the Bank.

10.2 Taxes and Invoicing

Applicable GST shall be paid as per the Commercial Bid and applicable law. Invoices shall be raised only after completion and acceptance of the relevant payment milestone. **Statutory deductions**, if applicable, shall be made as per law.

10.3 No Additional Charges

The quoted amount shall include all costs required to complete the assignment, including fees, travel, onsite visits, reporting, re-verification, retesting and applicable closure certificates / notes. No additional charges shall be payable unless specifically accepted by the Bank in writing.

10.4 Ownership, Confidentiality and Performance

10.4.1 All reports, checklists, certificates, closure notes and other deliverables submitted under this assignment shall be the property of the Bank.

10.4.2 The selected bidder shall maintain confidentiality of all information received or accessed during the assignment and shall execute the NDA / Confidentiality Agreement prescribed in **Annexure H – Draft NDA / Confidentiality Agreement** before receiving sensitive information / artefacts.

10.4.3 The selected bidder shall adhere to the agreed audit plan and timelines. Any claim of delay due to dependency on the Bank, ASP or technology service provider shall be valid only if documented, promptly escalated, and accepted by the Bank.

10.5 Withholding / Termination

10.5.1 The Bank may withhold payment for incomplete, delayed, defective or materially non-compliant deliverables until deficiencies are rectified.

10.5.2 The Bank may terminate the engagement, cancel the award, or take such other action as permitted under applicable procurement norms in case of material breach of the RFP / contract terms, breach of confidentiality, loss / suspension of CERT-In empanelment, subcontracting, failure to commence work, persistent delay, non-responsiveness, or failure to perform in accordance with the agreed timelines.

10.5.3 Where delay or non-performance may expose the Bank to regulatory, supervisory, statutory audit, UIDAI compliance or governance risk, the Bank may take immediate remedial action, subject to applicable procurement norms.

ANNEXURE A – TECHNICAL BID CHECKLIST
(To be submitted as part of the Technical Bid)

The bidder shall complete the checklist below and indicate the page number / file reference for each submitted document.

SN	Document / Annexure	Submitted (Yes/No/NA)	Pg No. / File Reference
1	Covering Letter / Bid Submission Letter		
2	**Annexure B –** Bidder Profile, Legal Details, CERT-In Empanelment and Financial Details		
3	Supporting documents for Annexure B		
4	**Annexure C –** Experience Credentials		
5	Supporting documents for Annexure C		
6	**Annexure D** – Proposed Team Profile and Role Mapping		
7	Supporting documents for Annexure D		
8	**Annexure E –** Audit Approach, Work Plan and Effort Estimate		
9	Annexure G – Declarations and Undertakings		
10	Signed acceptance / undertaking to execute **Annexure H – Draft NDA / Confidentiality Agreement**, if selected and required by the Bank		
11	Any other document required under the RFP		

Commercial Bid Separation

SN	Confirmation	Response (Yes / No)
1	The Technical Bid does not contain any commercial information.	
2	The Commercial Bid has been submitted separately in **Annexure F** – Commercial Bid Format.	

Bidder Confirmation:
The bidder confirms that the Technical Bid does not contain any commercial information and that all applicable documents have been submitted as per the RFP requirements.

Particular	Details
Name of Bidder	:
Authorised Signatory	:
Designation	:
Date	:
Place	:
Signature and Seal	:

ANNEXURE B – BIDDER PROFILE, LEGAL DETAILS, CERT-IN EMPANELMENT AND FINANCIAL DETAILS

(To be submitted as part of the Technical Bid)

B1. Bidder Details

SN	Particulars	Details to be Filled by Bidder
1	Name of Bidder	
2	Legal Constitution	Company / LLP / Partnership / Proprietorship / Other
3	Date of Incorporation / Registration	
4	Registered Office Address	
5	Correspondence Address	
6	PAN	
7	GSTIN	
8	Name of Authorised Signatory	
9	Designation of Authorised Signatory	
10	Contact Number	
11	Email ID	
12	CERT-In Empanelment Reference / Certificate No. / Listing Reference	
13	CERT-In Empanelment Validity	
14	Number of years in operation as on bid submission date	

B2. Financial details for the latest three audited financial years available as on date

Financial Year	Annual Turnover ₹	Supporting Document Reference / Page No.
FY 202___-2____		
FY 202___-2____		
FY 202___-2____		
Average Annual Turnover		

Documents to be Attached

The bidder shall attach the following documents, as applicable:

i. Certificate of incorporation / registration / partnership deed / LLP registration.
ii. PAN copy and GST registration copy
iii. CERT-In empanelment proof / current CERT-In listing reference.
iv. Audited financial statements and / or CA certificate for the latest three audited financial years available as on bid submission date.

Bidder Confirmation

The bidder confirms that the above information is true and correct, and that the bidder meets the relevant eligibility requirements specified in the RFP.

Particular	Details
Name of Bidder	:
Authorised Signatory	:
Designation	:
Date	:
Place	:
Signature and Seal	:

ANNEXURE C – EXPERIENCE CREDENTIALS

(To be submitted as part of the Technical Bid)

The bidder shall provide experience details as required under Section 9.2 of the RFP. **Supporting Evidence:** For each engagement listed under **C.1, C.2 and C.3**, the bidder shall attach supporting evidence such as work order / engagement letter, completion certificate / client confirmation, scope extract, or anonymised evidence where confidentiality restrictions apply.

C.1 Banking / Financial Sector Technology Audit Experience

Minimum requirement: At least **2 similar technology audit engagements** in banking / financial sector during the last **3 years**.

SN	Client / Institution Name	Sector	Nature of Assignment	Period of Assignment	Scope Covered	Supporting Document Reference / Page No.
1		Bank / Financial Institution	IS Audit / Cyber Audit / VA/PT / Other			
2		Bank / Financial Institution	IS Audit / Cyber Audit / VA/PT / Other			
3		Bank / Financial Institution	IS Audit / Cyber Audit / VA/PT / Other			

C.2 RRB (ASP Model) Experience

Minimum requirement: Bidder must have completed **at least one engagement** involving an **RRB** operating under an **Application Service Provider (ASP) model**, within the last **3 years**.

SN	Client / Institution Name	Institution Type	Nature of Assignment	Period of Assignment	ASP / Outsourced Technology Context	Supporting Document Reference / Page No.
1		RRB / StCB / DCCB / Bank / Financial Institution	IS Audit / Cyber Audit / VA/PT / Other			
2		RRB / StCB / DCCB / Bank / Financial Institution	IS Audit / Cyber Audit / VA/PT / Other			

ANNEXURE C – EXPERIENCE CREDENTIALS *(continued)*

(To be submitted as part of the Technical Bid)

C.3 UIDAI AUA/KUA IS Audit Experience

Minimum requirement: At least **1 UIDAI AUA/KUA IS Audit / Aadhaar ecosystem compliance audit / UIDAI checklist-based audit engagement**.

SN	Client / Institution Name	Nature of Assignment	Period of Assignment	Scope / Checklist Basis	Supporting Document Reference / Page No.
1		UIDAI AUA/KUA IS Audit / Aadhaar Compliance Audit / UIDAI Checklist-based Audit			
2		UIDAI AUA/KUA IS Audit / Aadhaar Compliance Audit / UIDAI Checklist-based Audit			

Bidder Confirmation

The bidder confirms that the experience details furnished above are true and correct and relate to engagements completed by the bidder in its own name.

Particular	Details
Name of Bidder	:
Authorised Signatory	:
Designation	:
Date	:
Place	:
Signature and Seal	:

ANNEXURE D – PROPOSED TEAM PROFILE AND ROLE MAPPING

(To be submitted as part of the Technical Bid)

The bidder shall provide details of named resources proposed for the assignment. Generic statements such as "qualified resources will be deployed" shall not be sufficient.

SN	Name of Resource	Proposed Role	Audit Stream(s) Mapped	Key Qualification / Certification	Relevant Experience	Supporting Document Reference / Page No.
1		Engagement Lead / Audit Lead	IS Audit / Cyber Security Audit / VA/PT / UIDAI AUA/KUA IS Audit			
2		IS Audit / Cyber Security Audit Resource	IS Audit / Cyber Security Audit			
3		VA/PT Specialist	VA/PT / Application Security			
4		Application Security Resource	Web / Mobile / API / Source Code Review			
5		UIDAI AUA/KUA IS Audit Resource	UIDAI AUA/KUA IS Audit			

(Additional rows may be inserted by the bidder, if required.)

Documents to be Attached

The bidder shall attach supporting documents such as:

1. Brief CV / profile of each proposed resource.
2. Copies of relevant certifications.
3. Evidence of relevant experience, wherever available / applicable.

Bidder Confirmation

The bidder confirms that the resources listed above are proposed for the assignment and that the bidder shall deploy named resources as per the RFP requirements.

Particular	Details
Name of Bidder	:
Authorised Signatory	:
Designation	:
Date	:
Place	:
Signature and Seal	:

ANNEXURE E – AUDIT APPROACH, WORK PLAN AND EFFORT ESTIMATE

(To be submitted as part of the Technical Bid)

The bidder shall provide a brief audit approach, work plan and effort estimate for completing the scope under this RFP.
The proposed work plan and timeline shall be indicative. The final audit schedule shall be agreed with / approved by the Bank after award.
Additional rows may be inserted by the bidder, if required.

E.1 Audit Approach Summary

SN	Audit Stream	Proposed Approach / Methodology	Key Dependencies / Assumptions
1	IS Audit		
2	Cyber Security Audit including Gap Assessment		
3	VA/PT including Retest / Validation		
4	UIDAI AUA/KUA IS Audit		

E.2 Work Plan and Indicative Timeline

SN	Activity	Proposed Timeline / Week	Remarks
1	Kick-off meeting and Information Request List		
2	Document review and understanding of Bank / ASP environment		
3	IS Audit fieldwork including HO / RO / branch visits		
4	Cyber Security Audit and Gap Assessment		
5	VA/PT testing as per agreed Rules of Engagement		
6	UIDAI AUA/KUA IS Audit		
7	Submission of draft reports		
8	Management discussion and response incorporation		
9	Submission of final reports		
10	Re-verification / retesting and closure certificates / closure notes		

E.3 Resource Deployment / Effort Estimate

SN	Role	Audit Stream(s) Supported	Estimated Effort / Man-days	Remarks
1	Engagement Lead / Audit Lead			
2	IS Audit / Cyber Security Audit Resource			
3	VA/PT Specialist			
4	Application Security Resource			
5	UIDAI AUA/KUA IS Audit Resource			

(cont....)

ANNEXURE E – AUDIT APPROACH, WORK PLAN AND EFFORT ESTIMATE *(Continued)*

(To be submitted as part of the Technical Bid)

E.4 Branch Visit Plan

SN	Proposed Coverage	No. of Units / Visits	Remarks
1	Head Office		
2	Regional Offices		
3	Branches for IS Audit onsite verification, subject to Bank's approval		
4	DC/DR walkthrough		

Bidder Confirmation

The bidder confirms that the proposed work plan and effort estimate are sufficient to complete the scope defined in the RFP and that the final audit schedule shall be mutually agreed with the Bank after award.

Particular	Details
Name of Bidder	:
Authorised Signatory	:
Designation	:
Date	:
Place	:
Signature and Seal	:

ANNEXURE F – COMMERCIAL BID FORMAT

(To be submitted as part of the Commercial Bid only)

The bidder shall submit the Commercial Bid strictly in the format below. The Commercial Bid shall not be included in the Technical Bid.

F.1 Commercial Quote

SN	Audit Stream / Activity	Amount excluding GST (₹)	GST (₹)	Total Amount including GST (₹)
1	Information Systems (IS) Audit			
2	Cyber Security Audit including Gap Assessment			
3	VA/PT, including retest / validation			
4	UIDAI AUA/KUA IS Audit			
	Grand Total			

Grand Total excluding GST (in words) – Rupees_____

F.2 Commercial Bid Conditions

i. The quoted fee shall be inclusive of all activities required to complete the assignment, including planning, fieldwork / testing, reporting, management discussions, compliance evidence review, re-verification / retesting and issuance of applicable stream-wise closure certificates / closure notes.

ii. GST shall be shown separately and paid as applicable.

iii. **Commercial evaluation** shall be based on the **Grand Total excluding GST**, with GST payable extra as applicable.

iv. A nil / zero quote or commercially unrealistic quote may be treated as non-responsive at the Bank's discretion.

v. No additional charges shall be payable unless specifically accepted by the Bank in writing.

vi. Conditional pricing, assumptions affecting price or deviation from this format may render the Commercial Bid non-responsive.

F.3 Bidder Confirmation

The bidder confirms that the commercial quote above is for the complete scope of work under the RFP and includes all deliverables, re-verification / retesting obligations, and applicable stream-wise closure certificates / closure notes required under the RFP.

Particular	Details
Name of Bidder	:
Authorised Signatory	:
Designation	:
Date	:
Place	:
Signature and Seal	:

ANNEXURE G – DECLARATIONS AND UNDERTAKINGS

(To be submitted as part of the Technical Bid)

The bidder shall confirm the declarations and undertakings below as part of the Technical Bid.

G.1 Compliance Certificate / Unconditional Acceptance

i. The bidder confirms that it has read and understood the RFP, including all Sections and Annexures, and unconditionally accepts the terms, conditions, scope, deliverables, eligibility requirements, evaluation methodology, confidentiality requirements, no-subcontracting condition, re-verification / closure requirements and commercial bid requirements specified in the RFP.

ii. The bidder further confirms that the Technical Bid does not contain any commercial information and that the information and documents submitted are true, complete and correct to the best of its knowledge.

G.2 Non-Blacklisting / Non-Debarment Declaration

i. The bidder declares that it has not been blacklisted, debarred or restrained from participating in tenders / assignments by any Government department, regulatory authority, statutory authority, public sector bank, financial institution, CERT-In, UIDAI or NABARD-supervised entity.

ii. The bidder undertakes to immediately inform the Bank if any such blacklisting, debarment, restraint, regulatory action or disqualification arises during bid evaluation or during the engagement period, if awarded.

G.3 Confidentiality and Conflict of Interest Declaration

i. The bidder undertakes to maintain confidentiality of all information, documents, records, audit evidence, system information, reports, logs, artefacts and any other information received from or accessed in relation to the Bank.

ii. The bidder confirms that it shall use such information only for the RFP / audit assignment, shall execute the NDA / Confidentiality Agreement prescribed in **Annexure H – Draft NDA / Confidentiality Agreement**, if selected, and does not have any conflict of interest affecting its independence, objectivity or ability to perform the assignment.

iii. The bidder shall immediately inform the Bank if any actual, potential or perceived conflict of interest arises during bid evaluation or during the engagement period.

G.4 No Subcontracting Undertaking

i. The bidder undertakes that the audit assignment shall be executed through its own qualified personnel proposed for the engagement.

ii. The bidder shall not subcontract, outsource, assign or transfer the audit assignment, in whole or in part, to any other entity, firm, individual, consultant or third party.

ANNEXURE G – DECLARATIONS AND UNDERTAKINGS *(continued)*

(To be submitted as part of the Technical Bid)

G.5 Continued CERT-In Empanelment Undertaking

i. The bidder confirms that it is a CERT-In empanelled Information Security Auditing Organisation as on the date of submission of the bid and has submitted valid proof of CERT-In empanelment / current CERT-In listing reference as part of the Technical Bid.

ii. The bidder undertakes to remain CERT-In empanelled during the engagement period and shall immediately inform the Bank if its CERT-In empanelment is suspended, withdrawn, expired, cancelled or otherwise ceases to remain valid during bid evaluation or engagement period.

Bidder Confirmation

The bidder confirms that the declarations and undertakings furnished above are true and correct and are binding on the bidder. The bidder understands that any false statement, misrepresentation, suppression of material information or breach of the above declarations may result in rejection of the bid and / or cancellation of award, if already made.

Particular	Details
Name of Bidder	:
Authorised Signatory	:
Designation	:
Date	:
Place	:
Signature and Seal	:

ANNEXURE H – DRAFT NDA / CONFIDENTIALITY AGREEMENT

(To be executed by the selected bidder before receipt of sensitive information / artefacts)

The selected bidder shall execute a Non-Disclosure Agreement / Confidentiality Agreement with the Bank before receiving any sensitive information, audit artefacts, system details, ASP-related documents, logs, reports, credentials, evidence, configurations, architecture documents, VA/PT scope details, UIDAI-related artefacts or any other confidential information.

The NDA shall be based on the **CERT-In Model Non-Disclosure Agreement between CERT-In empanelled Auditor and Auditee**, with suitable Bank-specific particulars inserted.

For the purpose of execution:

Particular	Details
Auditee	Meghalaya Rural Bank
Auditor	Selected Bidder / Audit Firm
Purpose	Conduct of IS Audit, Cyber Security Audit including Gap Assessment, VA/PT and UIDAI AUA/KUA IS Audit
Governing Law	Laws of India
Jurisdiction / Venue	Shillong, Meghalaya, unless otherwise decided by the Bank
Term	As specified at the time of execution / engagement
Confidentiality Survival	As per NDA terms

The selected bidder shall comply with all confidentiality, secure handling, need-to-know access, data protection, return / destruction, non-disclosure and audit-related data handling obligations under the executed NDA.

The Bank may require execution of the NDA before sharing any confidential or sensitive information, including information relating to the Bank's ASP / technology service provider environment.

Bidder Acknowledgement

The bidder confirms that, if selected, it shall execute the NDA / Confidentiality Agreement in the format prescribed by the Bank before receiving sensitive information or commencing activities requiring access to confidential artefacts.

Particular	Details
Name of Bidder	:
Authorised Signatory	:
Designation	:
Date	:
Place	:
Signature and Seal	: