Chhattisgarh Rajya Sahakari Bank Maryadit

Expression of Interest
from CERT-In empanelled audit firms
For Information Communication Technology Audit / IS Audit, Information Security Audit, VAPT Audit, GAP Analysis Audit

EOI Reference No.: 2026/01

Issued by

Chhattisgarh Rajya Sahakari Bank Maryadit

Plot No. 74, Sector 24, Atal Nagar, Nava Raipur (C.G.) – 492002

Last date of EOI Submission: 12/01/2026
Contact: 9826579795

1. Introduction and Disclaimer

This EOI has been prepared solely to enable Chhattisgarh Rajya Sahakari Bank (Apex Bank) of Chhattisgarh State for selection of suitable organization (Service Provider – “SP” mandatory CERT-In empaneled audit firms) to respond for assisting the Bank in conducting ICT Audit / IS Audit, Information Security Audit, VAPT Audit & GAP Analysis Audit.

Chhattisgarh Rajya Sahakari Bank is managing its services under ASP Model (Outsource Model). This audit will encompass a thorough examination of Outsourced IT infrastructure, Core Banking Systems, cyber security controls, application and network security, as well as adherence to regulatory compliance standards set by RBI, NABARD, Cert-In, NPCI and any other regulators along with alignment with ISO 27001. The appointed auditor is expected to identify any gaps, propose effective mitigation measures, and confirm the resolution of previous audit findings.

2. Details of Participating Banks

S.No	Bank Name	Head Office	Proposed Audit Requirements
1	Chhattisgarh Rajya Sahakari Bank Limited.	Raipur (Chhattisgarh)	ICT Audit / IS Audit, Information Security Audit, VAPT Audit & GAP Analysis.

.

3. Submission of Bids

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

Managing Director,
Chhattisgarh Rajya Sahakari Bank Maryadit
Head Office: Sahakar Bhawan, Plot No 74,
Sector- 24, Atal Nagar, Nava Raipur, Pin-492002.

Introduction

"The participating banks are the Chhattisgarh Rajya Sahakari Bank (Apex Bank) of Chhattisgarh State, constituted under the relevant State Cooperative Societies Act and functioning as the cooperative bank in Chhattisgarh." The bank is having a common Application Service Provider (ASP), and are using shared infrastructure.

The Bank is using B@ncs24 of M/s. Tata Consultancy Service, as the Core Banking Solution and the CBS project is implemented and supported by M/s. Tata Consultancy Services. The bank's Data Centre is at Thane, Mumbai. The DR Data Centre is located at Bangalore.

Products and services offered by the Bank

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

CBS

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

Networking

Bank has outsourced the network to the same vendor for CBS and using RF, 4G, VSATs. All the sites have two network links, one is used as primary link and other one is used as secondary link.

Alternate Delivery Channels

Banks are having ATM, UPI, IMPS, NEFT/RTGS, Mobile Banking & Internet Banking as alternate delivery channels.

4. Current EOI Objectives:

4.1 Audit Objectives

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

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

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

4.2. Audit Approaches

Information Systems Audit approach includes the following Auditing around the computer

Auditing through the computer
Auditing with the computer

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

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

4.3 Audit Methodology

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

4.4 Auditors:

Audit should be carried out by CERT-In empaneled audit firms only with having CISA / CISSP / CISM / GIAC(SANS) qualified staff with adequate experience in the audit areas given in annexure-A of this EOI.

The Service Provider must have similar experience in conducting required audit for a minimum period of 4 years. The firm has their physical office in Raipur Chhattisgarh for at least one year or an experienced employee based in Chhattisgarh is required.

4.5 Audit Scope:

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

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

(B) IS Audit as per guidelines issued by NABARD (circular attached) and gap assessment as per Cyber Security Framework

(C) IT Products (INB / MB / DISA etc.)

Details of Audit Scope are given in annexure – A.

4.6 Audit Findings & Reports:

Deliverables Under the Audit-the SP will deliver detailed reports as below for each bank separately signed by CISA qualified person. **ICT/ IS Audit, Information Security Audit , GAP Analysis Audit will be conducted once in year and VAPT Audit to be conducted twice in year as per norms of NABARD.**

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

(1) ICT Audit Report / IS Audit Report & Information Security Audit Report

(2) VAPT Report and Recommendations.

(3) Gap analysis Report and recommendation for mitigation

(4) 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.

4.7 Submission of Response / Bids

The bids shall be in two parts viz. Technical Proposal and Commercial Proposal, Both Technical and Commercial Bids shall be submitted in separate envelope with subject **"ICT / IS Audit / VAPT Audit / GAP Analysis of Chhattisgarh Rajya Sahakari Bank".** Proforma of technical & Commercial proposal are given Annexure B & C of this Expression of Interest.

All the relevant pages of the proposals are to be numbered and be signed by authorized signatory on behalf of the respondent. The number should be a unique running serial no. across the entire document.

The Bids shall be addressed and submitted to the Banks Evaluation Office.

4.8 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. In this matter decision of Bank will be final and binding to all respondent of this expression of interest.

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 Service Providers at its sole discretion if the Service Provider 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. If any dispute arise in any matter decision of Bank will be final and binding in all respondent of this expression of interest. All disputes are to be subject under Raipur Jurisdiction only.

Eligibility Criteria:-

1. Eligible firms must be registered in India and possess a minimum of 4 years of direct experience in IS Audit and VAPT, specifically for banks with minimum 1 similar audit of State Cooperative Bank/ District Central Cooperative Bank in last 3 financial years.
2. Eligible firms must have valid ISACA and EC council certifications or ISO 27001 and CISA / CISSP / CISM / GIAC(SANS) certified professionals. Firms must be CERT-IN empanelled.
3. Eligible firms must have a physical office in Raipur, Chhattisgarh, for at least one year or an experienced employee based in Chhattisgarh is required. Preference will be given to firms with experience serving State Cooperative Banks/ District Central Cooperative Banks who are managing its services under ASP Model.

ANNEXURE-A

SCOPE OF AUDIT

The details provided in the scope are indicative lists but not restricted to the following. All the controls mentioned in NABARD's Cyber Security Framework (https://www.nabard.org/circularpage.aspx?cid=504&id=803) and IS Audit Guidelines issued by NABARD should be covered.

Alignment of IT strategy with Business strategy			
*	IT Governance related processes		
*	Long term IT strategy and Short term IT plans		
*	Information security governance, effectiveness of implementation of security policies and processes		
*	IT Architecture		
	-	Acquisition and Implementation of Packaged software	
		>	Requirement Identification and Analysis

		>	Product and Vendor selection criteria	
		>	Vendor selection process	
		>	Contracts	
		>	Implementation	
		>	Post Implementation Issues	
	-	Development of software - In-house and Out-sourced		
		>	Audit framework for software developed in house, if any	
		>	Software Audit process	
			o	Audit at Program level
			o	Audit at Application level
			o	Audit at Organizational level
		>	Audit framework for software outsourcing	
	-	Operating Systems Controls		
		>	Adherence to licensing requirements	
		>	Version maintenance and application of patches	
		>	Network Security	
		>	User Account Management	
		>	Logical Access Controls	
		>	System Administration	
		>	Maintenance of sensitive user accounts	
-		Application Systems and Controls		
		>	Logical Access Controls	
		>	Input Controls	
		>	Processing Controls	
		>	Output Controls	
		>	Interface Controls	
		>	Authorization Controls	
		>	Data Integrity / File Continuity controls	
		>	Review of logs and audit trails	
-		Database Controls		
		>	Physical access and protection	
		>	Referential Integrity and accuracy	
		>	Administration and Housekeeping	
-		Network Management audit		

	>	Process	
	>	Risk acceptance (deviation)	
	>	Authentication	
	>	Passwords	
	>	Personal Identification Numbers ('PINS')	
	>	Dynamic password	
	>	Public key Infrastructure ('PKI')	
	>	Biometrics authentication	
	>	Access Control	
	>	Cryptography	
	>	Network Information Security	
	>	E-mail and Voicemail rules and requirements	
	>	Information security administration	
	>	Microcomputer / PC security	
	>	Audit trails	
	>	Violation logging management	
	>	Information storage and retrieval	
	>	Penetration testing	
-	Physical and environmental security		
-	Maintenance		
	>	Change Request Management	
		o	Software developed in-house
	>	Version Control	
	>	Software procured from outside vendors	
	>	Software trouble-shooting	
		o	Helpdesk
	>	File / Data reorganization	
	>	Backup and recovery	
		o	Software
		o	Data
		o	Purging of data
	>	Hardware maintenance	
	>	Training	
-	Internet Banking		

	>	Information systems security framework	
	>	Web server	
	>	Logs of activity	
	>	De-militarized zone and firewall	
	>	Security reviews of all servers used for Internet Banking	
	>	Database and Systems Administration	
	>	Operational activities	
	>	Application Control reviews for internet banking application	
	>	Application security	
-	Privacy and Data Protection		
	>	Controls established for data conversion process	
	>	Information classification based on criticality and sensitivity to business operations	
	>	Fraud prevention and Security standards	
	>	Isolation and confidentiality in maintaining of Bank’s customer information, documents, records by banks	
	>	Procedures for identification of owners	
	>	Procedures of erasing, shredding of documents and media containing sensitive information after the period of usage.	
	>	Media control within the premises	
-	Business Continuity Management		
	>	Top Management guidance and support on BCP	
	>	The BCP methodology covering the following :	
		o	Identification of critical business
		o	Owned and shared resources with supporting function
		o	Risk assessment on the basis of Business Impact Analysis ('BIA')
		o	Formulation of Recovery Time Objective ('RTO') and Identification of Recovery Point Objective ('RPO')
		o	Minimising immediate damage and losses
		o	Restoring of critical business functions, including customer-facing systems and payment settlement systems
		o	Establishing management succession and emergency powers
	>	Addressing of HR issues and training aspects	
	>	Providing for the safety and wellbeing of people at branch or location at the time of disaster	
	>	Assurance from Service providers of critical operations for having BCP in place with testing performed on periodic basis.	

	>	Independent Audit and review of the BCP and test result	
	>	Participation in drills conducted by RBI for Banks using RTGS / NDS / CFMS services	
	>	Maintaining of robust framework for documenting, maintaining and testing business continuity and recovery plans by Banks and service providers	
-	Asset Management		
	>	Records of assets mapped to owners	
	>	For PCI covered data, the following should be implemented :	
		o	Proper usage policies for use of critical employee facing technologies
		o	Maintenance of Inventory logs for media
	>	Restriction of access to assets through acceptable usage policies, explicit management approval, authentication use of technology, access control list covering list of employees and devices, labelling of devices, list of approved company products, automatic session disconnection of remote devices after prolong inactivity	
	>	Review of duties of employees having access to asset on regular basis.	
-	IT Financial Control		
	>	Comprehensive outsourcing policy	
	>	Coverage of confidentiality clause and clear assignment of liability for loss resulting from information security lapse in the vendor contract	
	>	Periodic review of financial and operational condition of service provider with emphasis to performance standards, confidentiality and security, business continuity preparedness	
	>	Contract clauses for vendor to allow RBI or personnel authorized by RBI access relevant information / records within reasonable frame of time.	
-	IT Operations		
	>	Application Security covering access control	
	>	Business Relationship Management	
		o	Customer Education and awareness for adaptation of security measures
		o	Mechanism for informing banks for deceptive domains, suspicious emails
		o	Trade marking and monitoring of domain names to help prevent entity for registering in deceptively similar names
		o	Use of SSL and updated certification in website
		o	Informing client of various attacks like phishing
	>	Capacity Management	
	>	Service Continuity and availability management	

		o	Consistency in handling and storing of information in accordance to its classification	
		o	Securing of confidential data with proper storage	
		o	Media disposal	
		o	Infrastructure for backup and recovery	
		o	Regular backups for essential business information and software	
		o	Continuation of voice mail and telephone services as part of business contingency and disaster recovery plans	
		o	Adequate insurance maintained to cover the cost of replacement of IT resources in event of disaster	
		o	Avoidance of single point failure through contingency planning	
	>	Service Level Management		
-	Project Management			
	>	Information System Acquisition, Development and Maintenance		
		o	Sponsorship of senior management for development projects	
		o	New system or changes to current systems should be adequately specified, programmed, tested, documented prior to transfer in the live environment	
		o	Scrambling of sensitive data prior to use for testing purpose	
	>	Release Management		
		o	Access to computer environment and data based on job roles and responsibilities	
		o	Proper segregation of duties to be maintained while granting access in the following environment -	
			--	Live
			--	Test
			--	Development
		o	Segregation of development, test and operating environments for software	
	>	Record Management		
		o	Record processes and controls	
			--	Policies for media handling, disposal and transit
			--	Periodic review of Authorization levels and distribution lists
			--	Procedures of handling, storage and disposal of information and media
			--	Storage of media backups

			--	Protection of records from loss, destruction and falsification in accordance to statutory, regulatory, contractual and business requirement
	>	Technology Licensing		
		o	Periodic review of software licenses	
		o	Legal and regulatory requirement of Importing or exporting of software	
	>	IT outsourcing related controls		
	>	Detailed audit delivery channels and related processes like ATM, internet banking, mobile banking, phone banking, card based processes		
	>	Data centre operations and processes Review relating to requirements of card networks (for example, PIN security review)		
	>	Other Aspects including but not limited to below mentioned points		
		1. Secrecy and confidentiality of Customer preserved. 2. If any cases of unauthorized transfer through hacking, denial of service due to Technological failure is brought. 3. Regulatory and Supervisory issues. 4. Any other items relevant in the case of security. 5. All the guidelines issued by RBI and CERT-IN from time to time relating to Internet Banking Application and Bank's Official Website/Web hosting Software should be adhered to. 6. The SP shall assist in addressing any query raised by NABARD / RBI or any other Authority arising from the report prepared and submitted by SP.		

(On bidder's / Respondent official
letter head) Compliance
Certificate

Date:

To,
Managing Director,
Chhattisgarh Rajya Sahakari Bank Maryadit
Head Office: Plot No 74, Sahkar Bhavan, Sector-24, Nava Raipur, Atal Nagar, Pin-492002.

Dear Sir,

Ref: -

1) Having examined the EOI Documents including all annexures, the receipt of which is hereby duly acknowledged, we, the undersigned offer to conduct the above audits.

2) If our Bid is accepted, we undertake to complete the project within the scheduled time lines.

3) We 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".

4) We agree that the Bank is not bound to accept the lowest or any Bid that the Bank may receive.

5) We have never been barred/black-listed by any regulatory / statutory authority.

6) No legal case of any default / blacklisting should have ever been filed by any regulator on the firm.

8) Enclose all annexures

Date: Seal & Signature of the bidder

ANNEXURE-B

Bidder's / Respondent profile with the details of past experience:

Sl. No	Particulars	Details furnished by the Bidder/ Respondent
1.	Name of the bidder / Respondent	
2.	Year of establishment and constitution Certified copy of Registration or "Partnership Deed" or " Certificate of Incorporation" should be submitted as the case may be.	
3.	Location of Registered office /Corporate office and address & Other offices	
4.	Mailing address	
5.	Names and designations of the persons authorized to make commitments to the Bank	
6.	Telephone and fax numbers of contact persons	
7.	E-mail addresses of contact persons	
8.	Details of business and business background Service Profile & client profile	Enclose as Annexure-1
9.	Details of experience/knowledge possessed in concern areas	Enclose as Annexure-2
10	Details of the similar assignments executed by the bidder (Name of the Bank, time taken for execution of the Assignment, total fees received and documentary proofs from are to be furnished).	Enclose as Annexure-3
11.	Details of the similar assignments executed by the bidder in other than Banking industry (Name of the Organization, time taken for execution of the assignment, total fees received and documentary proofs are to be furnished).	Enclose as Annexure-4
12.	Names of team members identified for this assignment and their professional qualifications and experience/expertise Details of similar assignments handled by the said team members Documentary proofs for all the assertions are to be enclosed.	Enclose as Annexure-5
13.	Details of other professional in the organization	Enclose as Annexure-6
14.	Details of lead audit certification from leading certification bodies	Enclose as Annexure-7
15.	Effort estimate and elapsed time are to be furnished.	Enclose as Annexure-8

Declaration:

1. We confirm that we will abide by all the terms and conditions.

2. 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.

Date: Seal & Signature of the bidder

<<On Letter Head of the Audit Firm>>

Annexure - C

Financial Bid for ICT / IS Audit, Information Security Audit, VAPT Audit & GAP Analysis for Apex Bank Chhattisgarh of Chhattisgarh.

With reference to the invitation for conduction of ICT Audit / IS Audit, Information Security Audit, VAPT Audit & GAP Audit for Chhattisgarh Rajya Sahakari Bank. (Apex Bank) of Chhattisgarh State, the **Quotations per Bank** are furnished here under.

S. No.	Audit Description	Commercials excluding GST Per Bank (in Rs.)
1	ICT Audit / IS Audit & Information Security Audit – Head Office with number of 18 Branches (To be conducted once in Year)	
2	VAPT Audit – Head Office with 18 Branches. (To be conducted Twice in Year)	
3	GAP Audit including Audit of C-edge/TCS premises, DC and DR & Head Office as per Nabard/ RBI/Cert-In guidelines. (To be conducted once in Year)	
Total Cost		

Authorised Signature:-

Name :-

Designation :-

ANNEXURE- 1.

Business & Client Profile

Section	Details
1.Name of the Organization	
2. Year of Establishment	
3. Legal Structure	
4. Company Registration Number	
5. GST Registration Number	
6. PAN Number	
7. Registered Office Address	
8. Contact Details	
9. Key Personnel	
10. Number of Employees	
11. Certifications (if any)	
12. Brief Business Overview	

Service Profile

Service Category	Description	Target Market/Industry	Years of Experience	Geographical Coverage

Client Profile

Client Name	Industry	Type of Service Provided	Duration of Engagement	Location

Annexure 2

Details of Experience/Knowledge in Concern Areas

Sr. No.	Area of Expertise / Concern Area	Details of Experience	No. of Projects Handled	Certifications/Tools Used	Remarks
1	Network Security Audit				
2	Application Security Testing				
3	IT Infrastructure Audit				
4	Cloud Security Assessment				
5	Compliance & Regulatory Audits				

Annexure 3

Details of Similar Assignments Executed in Banking Industry

Sr. No.	Name of the Bank/Client	Scope of Assignment	Time Taken for Execution	Documentary Proof Enclosed (Yes/No)	Remarks
1					
2					
3					

Annexure 4

Details of Similar Assignments Executed in Non-Banking Industry

Sr. No.	Name of the Organisation	Industry Sector	Scope of Assignment	Time Taken for Execution	Documentary Proof Enclosed (Yes/No)	Remarks
1						
2						
3						

Annexure 5
Proposed Team Profile

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

Member No.	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 ofyears and areas of expertise	Number

Annexure 6
Details of Other Professionals in the Organization

Sr. No.	Name	Designation	Qualification	Area of Expertise	Years of Experience	Certifications (if any)	Role in ICT Audit Assignments
1							
2							

Annexure 7
Details of Lead Audit Certifications from Leading Certification Bodies

Sr. No.	Name of Auditor	Certification Title	Issuing Body	Certificate ID / Number	Date of Certification	Valid Until	Area of Specialization	Remarks
1								
2								

ANNEXURE- 8

Estimated Effort and Elapsed Time for each audit area

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

The above audit shall be completed with a total_______________man days.

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