PROPOSAL FOR EMPANELMENT OF CERT-IN APPROVED VENDORS FOR INFORMATION SYSTEMS (IS) AUDIT DC, DR, NDR AND COMPREHENSIVE AUDIT OF CORE BANKING PROJECT & APPLICATIONS

CIAD DEPARTMENT

HALDWANI

The Nainital Bank Limited
03rd April 2024
Proposal Reference No- **NTB/CIAD/IS/2024/03/013**

PROPOSAL No. NTB/CIAD/IS/2024/03/013

The Nainital Bank Limited
Head Office,
Seven Oaks Building,
Mallital, Nainital, Uttarakhand - 263001

Dated: 03-04-2024

The Nainital Bank Ltd. Invites Applications from eligible Cert In empaneled vendors which are valid for a period of 3 years from the last date of submission of Application date for **"**INFORMATION SYSTEMS (IS) AUDIT DC, DR, NDR AND COMPREHENSIVE AUDIT OF CORE BANKING PROJECT & APPLICATIONS**".**

Scope of Work	"EMPANELMENT OF CERT-IN APPROVED VENDORS FOR INFORMATION SYSTEMS (IS) AUDIT DC, DR, NDR AND COMPREHENSIVE AUDIT OF CORE BANKING PROJECT & APPLICATIONS"	
Application Money (Non-Refundable)	Rs. 1,000/-(Rupees One Thousand only) Plus GST	Application Money has to be deposited as DD / PO / NEFT at the time of Application submission. The NEFT should be sent on or before last date of Application submission as per account details mentioned below: Account Name -APPLICATION MONEY & EMD Account Number – 999421390000001 IFSC Code - NTBL0NAI999
Last date and time of submission of queries		06/04/2024
Last date and time of submission of Application		23/04/2024 (17:00 Hrs.)
Last date of submission of clarifications by the bank on bank's website		15/04/2024

Interested parties may view and download the Empanelment Application containing the detailed terms & conditions, from the website

https://www.nainitalbank.co.in/english/tender.aspx

1. **Document Control Sheet**

Name of Organization	THE NAINITAL BANK LIMITED
Empanelment Category (Services/Goods/works/ Empanelment)	Empanelment
Type/Form of Contract (Work/Supply/Auction/Service/Buy / Empanelment)	Empanelment
Technical Evaluation (Yes/No)	Yes
Is Multi Currency Allowed	No (Only INR)
Payment Mode (Online/Offline)	Offline / Online
Empanelment Issuance Date	03-04-2024
Last date of submission of Empanelment Application response (Closing date) **And address for submission of Application**	23-04-2024 (By 17:00 Hrs.) The Nainital Bank Ltd., Central Internal and Audit Division, 4rd Floor, Opposite Session Court, Haldwani, District Nainital Uttarakhand - 263139
Mode of Submission of Application	Application shall send the Envelope through Courier / Registered Post / Speed Post at The Nainital Bank Ltd., Central Internal Audit Division, 4th Floor, Opposite Session Court, Haldwani, District Nainital Uttarakhand - 263139 on or before 23-04-2024 (By 17:00 Hrs.) (Application Submission Date). The date of dispatch of Courier / Registered Post / Speed Post receipt should be on or before last date of Application submission. The receipt of Courier / Registered Post / Speed Post for tracking purpose should be sent on email id of Audit Department mentioned in Document Control Sheet. However, if the said Application

	Envelope sent through Courier / Registered Post / Speed Post is lost in transit or is not delivered within 3 days from revised last date of Application submission in such circumstances the Bank shall not be liable, whatsoever, due such misplacement or non-delivery of said envelope. Further, the Applicant, whose envelope is misplaced in transit or is undelivered within 3 days from the last date of Application submission cannot resubmit his Application on the pretext of misplacement or non-delivery of the Application envelope.
Contract Type (Empanelment/Tender)	Empanelment
Multiple Technical Annexure(s)	Yes
Quoting for all Technical Annexures is compulsory	Yes
Application Validity days	3 years from the last date for submission of Application
Location for Submission of Application	The Nainital Bank Limited, Central Internal and Audit Division (CIAD), 4th Floor, Opposite Session Court, Haldwani, District Nainital Uttarakhand - 263139
Validity of Contract	3 years from the date of Empanelment
Address or Communication	Mr. Deepak Sanwal The Nainital Bank Ltd., Central Internal and Audit Division (CIAD), 4th Floor, Opposite Session Court, Haldwani, District Nainital Uttarakhand – 263139 Mob. -7055101627 Email : rbia@nainitalbank.co.in

2. Executive Summary of the Project

The Nainital Bank Limited was established in the year 1922 with the objective to cater banking needs of the people of the region. Bank of Baroda, a premier nationalized bank, is managing the affairs of The Nainital Bank Limited since 1973. The Bank is having 169 branches at present

operating in five states i.e. Uttarakhand, Uttar Pradesh, Delhi, Haryana and Rajasthan. Bank's Head Office is at Nainital, Uttarakhand and -3- Regional Offices are functioning at Delhi, Dehradun and Haldwani. The Bank is running with a vision which states: "To emerge as a customer centric National Bank & become the most preferred bank for its product, services, technology, efficiency & financials."

3. Clarification

When deemed necessary, during the process, the Bank may seek clarifications or ask the applicant to make technical presentations on any aspect from any or all the applicant. However, that would not entitle the applicant to change or cause any change in the substance of the application submitted or price quoted.

THE NAINITAL BANK LTD. reserves the right to seek fresh set of documents or seek clarifications on the already submitted documents.

4. Evaluation of Eligibility Criteria

In this part, the application will be reviewed for determining the compliance of the general conditions of the contract and Eligibility Criteria as mentioned in the proposal. Any deviation from general conditions of the proposal and eligibility criteria will lead to rejection of the proposal.

The applicants are expected to meet all the general conditions of the contract and the eligibility criteria as mentioned below. Applicants failing to meet these criteria or not submitting requisite supporting documents / documentary evidence for supporting pre-qualification criteria are liable to be rejected summarily.

The Applicant must possess the requisite experience, strength and capabilities in providing the services necessary to meet the requirements, as described. The application must be complete in all respects and should cover the entire scope of work as stipulated in the proposal. The eligibility criteria are as follows:

S. No	Eligibility Criteria	Supporting Required	Complied (Yes/No)
1	Applicant should be Government Organization / PSU / PSE / partnership firm under Partnership Act / LLP /private or public limited company in India at least for last 5 years as on date of Application.	Documentary Proof to be attached (Certificate of Incorporation). Submit copy of PAN Card, GST Registration.	
2	Applicant must not be blacklisted / debarred by any Statutory, Regulatory or Government Authorities or Public Sector Undertakings / Banks (PSUs / PSBs) or Private Banks or Financial Institutions since last 3 FY years and	Letter of confirmation (self-certified letter as per the format given in pt. 17.1 signed by authorized official of the Applicant)	

S. No	Eligibility Criteria	Supporting Required	Complied (Yes/No)
	till date.		
3	The Applicant shall be CERT-In Empanelled organization from at least past 3 years and its current empanelment should be valid/not expired.	Cert-in Document empanelment evidence of the same to be enclosed	
4	The Applicant should have a minimum financial turnover of **INR 1.5 crore** & above. Positive net worth for each year in the last three years financial year 2020-21, 2021-2022 and 2022-23.	Audited Financial statement for the financial 2020-21,2021-2022 and 2022-23. Certified letter from the Chartered Accountant. The CA certificate in this regard should be without any riders or qualification	
5	The Applicant should have a minimum of 10 certification for pool of resources who possess qualifications such as: CISA /DISA/ CISSP / CCNA/ CISM / OSCP	Documentary Proof to be attached	
6	Vendor should have the experience of conducting audit from any five of the following core areas: 1. CBS Application Functionality audit 2. IS Audit of DC/DRC/ Near site 3. Networking audit 4. Cyber Security audit 5. Application security Audit/ Security Audit of Delivery channels. 6. Mobile Banking App Security Audit 7. API 8. VAPT	Copy of letter of assignment & certification of satisfactory completion of assignment to be submitted from respective Banks	

S. No	Eligibility Criteria	Supporting Required	Complied (Yes/No)
7	The Applicant should have performed IS Audit/ Risk Assessment in at least 2 Schedule Commercial/PSU/Private Bank/ Regional Rural Banks/ Co-Operative Bank* in India. *The Co-Operative Bank must have the following criteria as on 31.03.2023. 1-Branch Operations in at least three states in India. 2-Total Business of Rs. 1,000 crore or above in India. (Copy of proof must been closed For both Point No i and ii)	Purchase order shall be shares for same	
8	The Applicant should not be an existing Core Banking Solution provider in the Bank.	Self-declaration	

Note: Applicant must comply with all the above-mentioned criteria as specified above. Non-compliance of any of the criteria can entail rejection of the offer.

Photocopies of relevant documents / certificates duly stamp by the organization/institution should be submitted as proof in support of the claims made for each of the above-mentioned criteria and as and when the Bank decides, originals / certified copies should be shown for verification purpose. The Bank reserves the right to verify / evaluate the claims made by the applicant independently.

Any deliberate misrepresentation will entail rejection of the offer ab-initio.

5. Details of Scope of Work

The overall scope of Information Systems Audit and Comprehensive Audit of CBS Project & Other Applications will largely include the following:

- The Auditors shall understand the current IT Setup/ processes involved in the Bank and the industry prevailing standards and Regulatory guidelines.
- Audit of IT Governance, Policy, Procedures, Standard Practices & other regulatory requirements.
- IS Audit shall cover entire gamut of computerized function including electronic delivery channels such as Internet Banking, Debit Cards, UPI, IMPS, RTGS/ NEFT, Financial Inclusion Mobile Banking etc., robustness of different function, such as application

system and subsystems, architecture, infrastructure, network, network hygiene, Logical Security & access control, input, Change Management, User Management and Password Policies being followed, processing and output controls, procedures, data integrity/ efficiency and effectiveness in implementation of Bank's Information/ IT Security Policy & procedures. This shall include any other new addition/ upgradation in hardware, software, business application, new deliverables, change in architecture/ information systems audit and Security Audit during the contract period at Data Centre, DR site and Near-DR, Treasury Department.

Locations for Audit:

Location of audit will be Noida, Mumbai, Delhi, Haldwani & Nainital. Site/ locations of Outsourced vendors will be provided separately to interested/ selected Applicant.

Prior to starting the groundwork on the audit, the successful Applicant shall provide Audit plan and procedure for Information Systems audit and Comprehensive Audit of CBS project & Other Applications. Detailed test cases and plans for the items as per scope of the audit.

Selected vendor has to submit the details of tool(s) to be used for VA/ PT including name of the tool. Selected vendor has to submit the copy of license of the tool to be used for VA/ PT.

IS Audit should include following: -

- Bank's policies & procedures related to IT, Information Security, Cyber Security, BCP etc.
- Evaluating adequacy of operating processes and internal controls
- Determining effectiveness of planning and oversight of IT activities
- Identifying areas with deficient internal controls, recommend corrective actions to address deficiencies and follow-up, to ensure that the management effectively implements the required actions
- Determining adequacy of enterprise-wide compliance efforts, related to IT policies and internal control procedures
- Proper planning for business continuity and disaster recovery measures. Independent audit of BCP Plan and corresponding test results by the bank. Review of BCP & Verify the BCP/DR arrangements/policy in place includes procedures to be followed in case of cyber risks- Business Continuity Management, Identification of critical business. Assurance from Service providers of critical operations for having BCP in place with testing performed on periodic basis, maintaining and testing business continuity and recovery

plans by Banks and service providers, participation in drills conducted by RBI for Banks using RTGS/NEFT

- Study of CBS and other applications for adequacy of input, processing and output controls and conduct various test to verify existence and effectiveness of the controls.
- Controls over automated processing/updating of records review or check of critical calculation such as interest rates, levying of various charges etc. review of the functioning of automated scheduled task, batch process, output reports design, reports distribution etc.
- Auditing, both at client side and server side, including sufficiency and accuracy of event logging, SQL Prompt Command, usage, database level logging etc.
- Adherence to application security and cyber security related controls.
- Review of DR Drills of critical applications of the bank as per BCP.
- Adherence to API Security Controls.
- System Audit Report for Data Localization (SAR Audit).
- Review of Cyber Security Framework for the Bank.
- Verify the Cyber Security Policy of the Bank w.r.t. the framework and strategy to check cyber threats depending on the level of complexity of business and acceptable levels of risks and the measures to address/reduce the said risks.
- Vendor risk assessment.
- Annual Maintenance Contract.
- Anti-Virus status etc.
- Reconciliation process of ATM, UPI, RTGS & NEFT, Mobile Banking and other digital channel transaction etc.
- Detailed audit delivery channels and related processes like ATM, internet banking, mobile banking, card-based processes: Debit Card operation &Card Management, ATM/POS Dispute Management.
- 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.
- Verify the detective and corrective measures/steps in place to address various types of cyber threats / system procedure in services offered by the Bank – NEFT/RTGS/IMPS//debit cards, etc.

- Vendor's NDA and contractual agreement review.
- Database Control Review- Physical access and protection, Referential Integrity and accuracy, Administration and Housekeeping.
- IT Operations control review- Application Security covering access control, Customer Education and awareness for adaptation of security measures, Use of SSL and updated certification in website, informing client of various attacks like phishing, Capacity Management, Service Continuity and availability management, Securing of confidential data with proper storage, Media disposal, Backups and Restoration.
- Network Control Review- All areas of network, including wide area network, local area network, data center management, security architecture, shall fall under the purview of IS Audit.
- Incident management and Response.
- IT inventory Management.
- Review of IT processes.
- RTGS/ NEFT operation and control

Project Scope:

1) **Application Audit:** Complete review of applications and security audit of all major applications including Finacle 10.x application and Delivery Channels i.e., Internet Banking, Debit Cards, UPI, IMPS, RTGS/ NEFT, Financial Inclusion etc. (Approximate 30 applications)

   - **Top 10 OWASP Vulnerabilities:** Compliance review of top 10 OWASP (Open Web Application Security Project) vulnerabilities, especially for public facing applications. Internet Banking, IMPS, Corporate Website, Financial Inclusion etc. Web-application security and other related security practices are to be observed.

   - **VAPT (Vulnerability Assessment & Penetration Testing):** VA (Vulnerability Assessment) of all major applications including Finacle Core & Delivery Channels and Penetration Testing of public facing applications viz. Internet Banking, IMPS, Bank Website, Financial Inclusion etc.

   - **Penetration Testing (PT)** of public facing applications viz. Internet Banking, Bank's Website etc.

   - Security Operations Centre (SOC)

2) DC/ DRC/ NDR Audit: Thorough Audit of Bank's Data Centre (DC) and near Site at Noida, Disaster Recovery Centre (DRC) at Mumbai. Audit of Disaster Recovery and Business Continuity Plans for adequacy and conformance of BCP. Audit of effectiveness of Anti-virus system. Audit shall include but not limited to Access control system Fire / flooding / water leakage / gas leakage etc., Handling of movement of man /material in /out of DC / DRC, Air-conditioning of DC/ DRC, Electrical supply to DC/ DRC, Raw power/ UPS, Surveillance system of DC/ DRC, Redundancy of power level, UPS capacity at DC, DRC, Physical & environmental controls at DC & DRC, Assets safeguarding and Incident handling procedures.

3) Network / Cyber Security Audit: -Network Infrastructure and Security Audit of entire Network infrastructure. The identified vendor will conduct Vulnerability Assessment (VA) of network infrastructure components to identify services in use and potential vulnerabilities present

Configuration Audit: - Configuration audit of various devices, especially for network & network security devices. Every router/ Switches/ firewall at DC, DRC should be checked

4) **Audit of ATM Project: -** Security audit of ATM switch hosted in the switch vendor's Data Centre, Debit/ ATM card related operations.

5) **Outsourcing Audit: -** Covering audit of Information System, functional and operational aspects Outsourcing activities as per Guidelines of RBI. Outsourced activities/ vendors of CBS, Finacle e-Banking, Finacle Treasury, Finacle Alert Services, ATM Switch, Financial Inclusion (FI), Debit Cards and other outsourced activities.

6) EOD Process: EOD Process of Finacle 10.x to be audited.

7) API- All payment system: API- Covering audit of Information System, functional and operational aspects Outsourcing activities as per Guidelines of RBI/NPCI.

Purpose of the audit:

To ensure the Core Banking System (Finacle 10 X):

- To meet business requirements
- Operates appropriately and assists the user in performing their roles efficiently and effectively.
- Ensure IT assets safeguards against threats & hazards and ensure data accuracy, integrity and protection.

- Application meets the industry best practices securities standards
- Find the bottlenecks in application which may lead to frauds.
- Find the bottlenecks in Core Banking System to protect against threats & hazards.
- To ascertain whether the processes as desired by the Bank and controls implemented function as intended in normal and also in exceptional circumstances.
- To understand flexibility, strengths and weaknesses of the Core Banking System as implemented and constraints.
- To ensure appropriate testing of various controls including input, process and output controls which would result in greater comfort & enable the Bank's management to place reliance on the new solution/ initiatives being deployed
- Audit of Data Centre & Disaster Recovery, Network infrastructure & management co security and its compliance with industry best security standards & practices.

The Scope of work is broadly as under:

Sr No	Business Area		Major Aspects to be covered
1	Information System	Management Control	To ensure proper controls are in place in the area of System development, data management, security management, operations management and quality assurance management. Industry Best Practices are observed wherever possible.
2	Information System	Information Security	Security features including user management. Evaluation of controls prescribed by Bank's Information Security Policy and Business Continuity Policy
3	Information System	Application controls	- Evaluation of system documentation and user manuals and interface with menus, submenus and reports - Evaluation of safeguarding of assets, data integrity, efficiency and effectiveness of the system - Special emphasis on Sufficiency / accuracy of all types of reports, Backups and recovery procedures, Audit trails, Version control, patch management, rollover, Setting of various parameters, Generation of exception reports and their coverage - Evaluation of existence and effectiveness of the controls, input, communications, processing, database
4	Information System	System Generated Transactions	Evaluate the Correctness, Completeness, Confidentiality Integrity & Availability of System Generated Entries, GL etc.
5	Information System	SLA	Compliance with Service Level Agreement (SLA) for Core Banking System. To ensure Monitoring of Service Level Agreements being done by the vendors and the Bank
6	Information System	Bulk Transaction Posting Utilities	Correctness, Completeness, Confidentiality, Integrity, Availability of transactions posted through bulk transaction posting utilities e.g., Trickle Feed Utility etc.
7	Information System	Change Management	• Evaluation of the Procedures adopted by the bank for the Business Process Re-engineering and controls thereof with a special emphasis on the processes reengineered since 14/02/2021 Gap Analysis for the Processes Reengineered • Evaluation of Change management process

8	Information System	Interfaces- Internal & External	Review process and controls over interface of Finacle 10.x application, including validation of interface files and handling of rejections, with the other applications
9	Information System	Core Banking System Control Reports generation	Identify module wise modifications required to achieve the above.
10	Information System	Disaster Recovery Plan	• Ascertain Disaster Recovery Plan, its adequacy, components, awareness, related provisions in software, testing, training needs, recovery alternative and suggest changes/ modifications, if any. • Evaluation and review of Recovery Time Objective (RTO), RPO (Recovery Point Objective)
11	Information System	Review of hardware and software to suggest measures, if any, for better control	• Maintenance, monitoring, effective and efficient usage of resources Access to Operating System (OS), Version control, OS security and compliance with essential and desired functionality for Transaction Processing and its support in areas of RDBMS. • Terms and conditions specified in Annual Maintenance Contracts of Hardware and Software to safeguard Bank's interest • Evaluation of Minimum Base Line Security documents and their implementation. • Evaluation of exceptions and their conformity to business requirements.
12	Information System	Audit of other areas	Procedures/ guidelines w.r.t practice as regards generation/ maintenance of records, access control and methods adopted for checking and verification of accounting procedure and control. Any other area/ aspect relevant to the assignment with mutual understanding
13	Information System	Manual Interventions	In addition, the auditor will be required to verify 1. The risk that is posed by the manual interventions that are allowed in all the applications. This will be examined for the need to keep this and restrict it or the need to eliminate it. This decision will be conveyed by the auditor based on the critical nature of the manual control and availability of the system control to manage. 2. Possibility of any wrong figures/ misrepresentation or misstatement in financial statement due to system generated entries 3. Auditor shall suggest any modification or addition to the existing report structure or

			addition of any report(s) to highlight major exception for better management control 4. The auditor is also expected to verify the correctness of any auto reconciliation process in the Core Banking System 5. The auditor shall also evaluate the System adopted by the Bank to verify the Background, competency and trustworthiness of vendor employees
14	Information System	IS Audit Controls	ISACA IS Auditing Guidance
15	Information System	Comprehensive Cyber Security Framework	Review of Comprehensive Cyber Security Framework
16	Information System	Cyber Security controls for Third party ATM Switch Application Service Providers	Compliance review of controls mentioned in the RBI circular DoS.CO/CSITE/BC.4084/31.01.015/2019-20 regarding "Cyber Security controls for Third party ATM Switch Application Service Providers" dated December 31, 2019. [as per applicability]
17	Information System	User review	User review for CBS, Net banking, and other critical application

The Applicant will be responsible for the proposed Information Systems audit and Comprehensive Audit of Finacle 10.x & other applications to meet the scope and objectives of the Tender and all addendum & corrigendum issued thereafter. The Bank assumes no responsibility for assumptions made by the Applicant. In the event the proposal of the Applicant fails to meet the scope and objectives of the Tender and addendums, the Applicant will have to upgrade, modify or replace the strategy of services at no additional cost to the Bank.

The Bank intends the vendor appointed under the Tender shall have single point responsibility for fulfilling all obligations and providing all deliverables and services required for successful information systems audit and Comprehensive Audit of Finacle 10.x & other applications.

The selected empaneled applicant will be required to provide the services of professionals for auditing information systems audit and comprehensive audit of Finacle 10.x project & other applications. Name of few applications is given below:

S. No	**Business Application**
1	Finacle Core Banking Solution
2	Finacle e-banking Solution
3	Finacle Treasury

4	Finacle Alert System
5	Anti-Money Laundering (AML)
6	GST Module- Income Expenditure
7	ADF/MIS
8	NPA Module/Crismac
9	CTS-Inward/Outward (DEM)
10	ALM / FTP
11	Data Archival
12	C-KYC
13	PFMS
14	NACH
15	Switch Services for CMS- EFT, UPI, IMPS, PoS
16	Loan Origination System (LOS)
17	Early Warning System (EWS)
18	NEFT/ RTGS with SFMS (STP) 24x7
19	PF Application (Stand Alone)
20	Bank's Website
21	Customer Complain Module
22	FI Application
23	Board PAC
24	HRM/Salary Module
25	Kiosk
26	Mobile Banking
27	Recon Application
28	HO Module - Asset & Inventory Like

6. General Aspects in Scope

The Bank intends to appoint a Cert-In approved vendor/auditor for conducting Information Systems Audit and Comprehensive Audit of Finacle 10.x project & Other Applications to ensure completeness, accuracy, consistency, integrity, stability & smooth transition of data from the source system to the target system Finacle 10.x (and other solutions).

The Applicant has to provide the detailed project plan with deployment of number of resources, deployment schedule, software/ tools used, hardware etc. Bank shall not provide any hardware or software other than PCs with basic configuration/ OS (Windows). It shall be the sole discretion of the Bank and the vendor shall not have any rights to claim the availability of PCs. Regarding hardware provided by the Bank, any installation of software/ tool or any change in the configuration should have prior approval from the Bank.

In brief, the expectations from the Applicant will be–

1. Understand the business requirements of application, which will allow the Applicant's team to refer to the business requirements specification and explore the application-under-test (AUT). Attach these requirements to (or auto-generate) Audit cases, establishing a traceable link to the corresponding requirement definition.
2. Applicant should submit document mentioning methodology of Auditing Strategy to identify various functional modules, tools deployed, business operational environment, execution setup, timelines and acceptance criteria.
3. Applicant should be able to calculate the effort needed to spend on auditing each requirement, based on the requirement's level of business risk and available resources.
4. The Applicant should also take care of the entire defect life cycle from initial problem detection through fixing the defect and verifying the fix. Therefore, no defect is overlooked or closed before it has been addressed.
5. Applicant shall provide graphs and reports that will help analyze application readiness at any point in the Auditing process. Provide graphs and reports using information about requirements coverage, planning progress, run schedules or defect statistics. Bank can make informed decisions on whether an application is ready to go live.
6. Applicant needs to prepare Audit strategy document listing the resources to be deployed, the roles and responsibilities of the Bank's team members, the execution methodology, reporting methodology, documentation deliverable.
7. Review the Audit results with the Bank. Report the results of the Audit and make recommendations to the authorities that it should be accepted.
8. The Applicant is expected to use best in class industry proven safeguards that prevents the misuse of information and appropriately protect the confidentiality, integrity and availability of information systems. Follow industry standards during the whole SDLC Process.
9. Applicant should sign the Service Level Agreement (SLA) based services and SLA tracking system for maintaining operational workflow.
10. Time, being an essential feature of the contract, the selected Applicant is expected to successfully complete the Audit and submit all reports as prescribed by Bank within 12 months from the date of acceptance of Purchase Order.
11. Final Compliance Report should be comprehensive to enable the bank to refer to any details at a future date in case of faults/errors or maintenance/upgradation.
12. In case any Applicant quotes open-source software for any requirement given in the Tender, then it is mandatory for the Applicant to quote rightful subscription and support charges to ensure compliance with the service levels defined in the Tender. The Applicant shall take into consideration future takeover/ merger/ acquisition/ amalgamation of the open-source software to/ by other company. The Applicant should

give an undertaking stating the continuation of support of the open-source software used if any.

13. The Applicant shall also ensure that the software does not and shall not contain any computer code or any other procedures, routines or mechanisms to:
    a. Disrupt, disable, harm or impair in any way the software (or other applications installed on the system the software is installed or interacts with) orderly operation based on the elapsing of a period of time, exceeding an authorized number of copies, advancement to a particular date or other numeral (sometimes referred to as "time bombs", "time locks", or "drop dead" devices.
    b. Cause the software to damage or corrupt any of the Banks' or its clients' data, storage media, programs, equipment or communications, or otherwise interfere with the Banks operations, or
    c. Permit the Applicant and/or its personnel and/or its licensors and/or any other third party, to access the software (or any other software or Banks computer systems) to cause such disruption, disablement, harm, impairment, damage or corruption (sometimes referred to as "traps", "access codes" or "trap door" devices).

    The scope of work shared above is only indicative and non-exhaustive. The bank and successful Applicant will prepare an exhaustive list of work to be conducted during the audit

7. Bank's Right to Vary Scope of Contract at the time of Award

The Bank may at any time, by a written order given to the Applicant, make changes to the scope of the Contract as specified.

8. Bank's Right to Accept Any Application and to Reject Any or All Applications

The Bank reserves the right to accept any Application and reject all Applications at any time prior to award of contract, without thereby incurring any liability to the affected Applicant or Applicants or any obligation to inform the affected Applicant or Applicants of the grounds for the Bank's action.

9. Notification of Award

The Bank will notify the successful Applicant in writing that its application has been accepted.

The successful Applicant shall execute the Non-Disclosure Agreement & Undertaking and return it within 15 days of allotment.

10. Proposal Related Condition

The Applicant should confirm unconditional acceptance of full responsibility of completion of job and for executing the 'Scope of Work' of this proposal. This confirmation should be

submitted as part of the Eligibility and Application form. The Applicant shall also be the sole point of contact for all purposes of the empanelment.

The Applicant should not be involved in any major litigation/arbitration that may have an impact of affecting or compromising the delivery of services as required under this contract. If at any stage of Tendering process or during the currency of the Contract, any suppression / falsification of such information is brought to the knowledge of the Bank, the Bank shall have the right to reject the Application or terminate the contract, as the case may be, without any compensation to the Applicant and claim damages before the court of law, resulting from such rejection/termination as the case may be.

General Conditions of Contract and Service Levels Agreement.

Quality: Material/solution not conforming to given specifications will be rejected & it will be replaced by the vendor, free of cost. The material/solution must be as per the detailed specifications listed out in Tender document and shall be as per standard engineering practice, relevant IS/ Imitational code of practice, and shall be as per the Specifications as mentioned in Proposal.

Statutory Laws: Vendor shall bide by all applicable rules and regulations regarding taxes, duties, labor etc., which are in force and from time to time enforced by the Government of India, also registration, labor laws, payments, ESIC, PF, insurance etc. Vendor shall coordinate for all these matters with concerned authorities directly.

Confidential Information: All information exchanged between the parties will be confidential. If the implementation project requires disclosure of, or receipt of, confidential information, such disclosure or receipt will be made with mutual agreement and may be with a separately executed MoU / Non-Disclosure agreement with Vendor by the Bank.

Extra Deviated Items: Any extra item like variation in quantity, deviated item should be executed only after getting the appropriate approvals with written confirmation, from the bank. At the time of submitting the invoice, all the documentary evidence of appropriate approvals for Extra / deviated Items / Variation in Quantities should be attached. Payments will not be made without scrutiny of aforesaid approvals.

Force Majeure: Bank shall not be responsible for delays or non-performance of any or all obligations, contained in this proposal or agreement thereafter, caused by war, revolution, insurrection, civil commotion, riots, mobilizations, strikes, blockade, acts of God, Plague, epidemics or pandemics, fire, flood, obstructions of navigation by ice of Port of dispatch, acts of government or public enemy or any other event beyond the control of the bank, which directly, materially and adversely affect the performance of any or all such obligations. However, the applicant shall continue to perform its obligations as contained in this proposal thereafter.

Arbitration: The Bank and the Applicant shall make every effort to resolve amicably, by direct negotiation between the respective Designated Officials of the Bank and the Applicant, any disagreement or dispute arising between them under or in connection with the Tender and or contract thereafter.

If the designated official of the Bank and the Applicant are unable to resolve the dispute within -30- days from the commencement of such informal negotiations, they shall immediately escalate the dispute to their Senior Authorized Person.

If within -30- days from the commencement of such negotiations between the Senior Authorized Person designated by the Applicant and Bank, are unable to resolve their dispute amicably, in such case the dispute shall be settled finally by arbitration in Nainital, Uttarakhand, India under and in accordance with the provisions of the Arbitration and Conciliation Act, 1996 or any statutory modification or re-enactment thereof. The right to appoint arbitrator shall lie with the bank only.

Jurisdiction: The Jurisdiction for all disputes will be in the city of Nainital (Uttarakhand), India.

Safety: All the safety codes and the preventive measure for this type of work shall be strictly followed. In case of any mishap which causes injury, disability or death of any personnel and staff either on site or offsite during or after the duration of the project due to negligence of the staff of the vendor, shall be sole responsibility of vendor, this shall not be responsibility of Bank in any case. No Claims in this regard shall be paid by Bank.

11. Prices

Prices quoted must be firm and shall not be subject to any upward revision on any account whatsoever throughout the period of contract. However, if there is any increase/decrease in taxes/ duties due to any reason whatsoever, after Notification of Award, the same shall be passed on to The Nainital Bank Ltd.

12. Payment Terms and Schedule

The payment would be disbursed on completion of each milestone as mentioned in table below. The milestone-based pay-out percentages are defined in the table below:

Milestone	Deliverables	% pay-out
1	Submission of all Final Draft Report	20%
2	Completion of all Final Audit Reports as finalized by Bank.	30%
3	Submission of final compliance report	50%

The Vendor's request(s) for payment shall be made to "The Nainital Bank Ltd." in writing (Invoice) accompanied by Service Level Requirements compliance reports for which payment is being claimed.

All the payments to the Vendor shall be subject to the report of satisfactory accomplishment of the concerned task. Penalties, if any, on account of liquidated damages and non-compliance of Service Level Requirements, shall be deducted from the invoice value. Payments will be released only on satisfactory acceptance of the deliverables for each Task.

All Payments shall be made in Indian Rupees Only and shall be released by the Bank against the

invoices raised by Applicant within 30 calendar days given all the relevant documents are submitted timely and are complete in all reference.

Note:

- All payments will be made through electronic mode only.
- Payments should be subject to deductions of any amount for which the Applicant is liable under the tender conditions. Further, all payments shall be made subject to deduction of TDS (Tax deduction at Source) as per the applicable Income-Tax Act.
- No advance payment will be made.

13. Service Level Agreement & Targets

The selected vendor has to sign a detailed SLA before the issuance of Purchase Order. The SLA will be prepared jointly by the Bank & the selected vendor and will be based on

- The scope of the application and any amendment done in the application before submission of the Application.
- The solution offered by the vendor in response to the Application.
- The SLA will be binding on the vendor for the entire period of term of contract.
- The Penalty clause shall be defined in SLA.

14. Revelation of Prices

Prices in any form or by any reason before opening the Commercial Application should not be revealed, failing which the offer shall be liable to be rejected.

15. Terms and Conditions of Applicants

Printed terms and conditions of the Applicants will not be considered as forming part of their Applications. The terms and conditions mentioned the Application will solely prevail.

16. Consortium

Consortium is not allowed

17.1 Declaration for Non-Blacklisting

UNDERTAKING FOR NON- BLACKLISTED

To be provided on letter head of the Applicant's Company

To,
The Chief Operating Officer,
The Nainital Bank Limited,
Head Office - Mallital, Nainital-263001 (Uttarakhand)

Madam/Dear Sir,

Reg.: Proposal Reference No: NTB/CIAD/IS/2024/03/013

We M/s _____, a company incorporated under the companies act, 1956/2013 with its headquarters at _____, do hereby confirm that we have not been blacklisted/ debarred by the Statutory, Regulatory or Government Authorities or Public Sector Undertakings (PSUs / PSBs) or Private Banks or Financial Institutions in India during last 3 years.

This declaration is being submitted and limited to, in response to the tender reference mentioned in this document

Thanking You,

Yours faithfully,

Signature of Authorized Signatory

Name of Signatory:

Designation:

Seal of Company

17.2 Undertaking of Information Security

(This letter should be on the letterhead of the applicants duly signed by an authorized signatory on Information security as per regulatory requirement)

To,
The Chief Operating Officer,
The Nainital Bank Limited,
Head Office - Mallital, Nainital-263001 (Uttarakhand)

Madam/Sir,

Reg.: Proposal Reference No: NTB/CIAD/IS/2024/03/013

We hereby undertake that the proposed hardware / software to be used for Audit will be free of malware, free of any obvious bugs and free of any covert channels in the code (of the version of the application being delivered as well as any subsequent versions/modifications done)

Dated this……..by …….2025

Yours faithfully,

Authorized Signatory

Name:

Designation:

Applicant’s Corporate Name

Address

Email and Phone #

17.3 Undertaking by the Applicant

To be provided on letter head of the Applicant's Company

To,
The Chief Operating Officer,
The Nainital Bank Limited,
Head Office - Mallital, Nainital-263001 (Uttarakhand)

Madam/Sir,

Reg.: Proposal Reference No: NTB/CIAD/IS/2024/03/013

It is certified that the information furnished here in and as per the document submitted is true and accurate and nothing has been concealed or tampered with. We have gone through all the conditions of Application and are liable to any punitive action for furnishing false information / documents. Dated this _____ day of _____ 2025.

Yours faithfully,

Authorized Signatory

Name:

Designation:

Applicant's Corporate Name

Address

Email and Phone #

17.4 Undertaking for No Deviation

To be provided on letter head of the Applicant's Company

To,
The Chief Operating Officer,
The Nainital Bank Limited,
Head Office - Mallital, Nainital-263001 (Uttarakhand)

Madam/Sir,

Reg.: Proposal Reference No: NTB/CIAD/IS/2024/03/013

Further to our proposal dated ……, in response to the Request for Proposal Ref. No NTB/CIAD/IS/2024/03/013 hereinafter referred to as "Empanelled" issued by Bank, we hereby covenant, warrant and confirm as follows:

We hereby agree to comply with all the terms and conditions / stipulations as contained in the Tender and the related addendums and other documents including the changes made to the original tender documents if any, issued by the Bank. The Bank is not bound by any other extraneous matters or deviations, even if mentioned by us elsewhere either in our proposal or any subsequent deviations sought by us, whether orally or in writing, and the Bank's decision not to accept any such extraneous conditions and deviations will be final and binding on us.

Yours faithfully,

Authorized Signatory

Name:

Designation:

Applicant's Corporate Name

Address

Email and Phone #

17.5 NEFT Details

To be provided on letter head of the Applicant's Company

To,
The Chief Operating Officer,
The Nainital Bank Limited,
Head Office - Mallital, Nainital-263001 (Uttarakhand)

Madam/Sir,

Reg.: Proposal Reference No: NTB/CIAD/IS/2024/03/013

Further to our proposal dated ……, in response to the Request for Proposal Ref. No NTB/CIAD/IS/2024/03/013 hereinafter referred to as "Empanelled" issued by Bank, we herewith submit the NEFT details for sending Application Money pertaining to this Proposal.

(Submit Separate details of each NEFT)

1. Account Number of Sender - Please mention the account name from which NEFT is sent pertaining to Application Money.
2. Date – Date of sending NEFT.
3. Bank Name – Name of Bank from which NEFT sent.
4. Transaction Number - Transaction / UTR number generated after sending the NEFT
5. Amount (In Rs.) – Amount of NEFT sent.

Yours faithfully,

Authorized Signatory

Name:

Designation:

Applicant's Corporate Name

Address