Madam/ Dear Sir

Sub: Sealed quotation for conducting Audit of FI application, Infrastructure hostage at third party Data Center & DR

Nainital Bank Limited is having a hosted Data Center at Mumbai & DR at Nasik for FI application.

This quotation inquiry seeks to engage a Service Provider who has the capability and experience for Conducting Information Audit of DC & DR/ / Application Audit/ Functional Security audit and to make appropriate recommendations, as covered under the Scope of Work.

Process Timeframe

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

Description	Due Date
Issue quotation Notification	16.02.2021
Last date of receiving written request for clarifications	20.02.2021
Email ID for clarifications	ciad@nainitalbank.co.in
SPOC from Bank	**Manoj Dwivedi, Manager IS Audit**
SPOC Mobile No	7055101509,9058637751
SPOC Email ID	ciad@nainitalbank.co.in
Mode for submission of quotation	Sealed Quotation
Last date for submission	**01.03.2021**
Address	Central Internal Audit Division THE NAINITAL BANK LIMITED 4th Floor, UPRNN Building C-20 / 1A / 7 Sector 62, Noida Uttar Pradesh – 201309 Ph:-120-2401083
Duration of Audit	Within 15 Days from the date of PO
Submission of Draft report	Within 20 days from the date of PO
Submission of Final Report	Within 1 Month from the date of PO
Compliance Audit	Within 2 Month from the date of Submission of Final Report

Audit Methodology

The IS audit work will include manual procedures, computer assisted procedures and fully automated procedures.

1- For System audit of all Infrastructure installed in DC & DR including Network infra auditor have to visit Banks's DC & DR.

2- For application auditor can visit at Bank's Noida/ Delhi/ Head Office

Auditors:

Audit should be carried out by CERT-In empaneled audit firm by persons having CISA /CISSP/ CISM / GIAC (SANS) qualifications with adequate experience in the audit areas related to Information AUDIT/ VAPT/Application Audit.

A. ELIGIBILITY CRITERIA

Sr. No	Eligibility Criteria	Support Documents to be submitted
	The vendor should be Company/Firm/ Organization registered in India	Certificate of Incorporation & Commencement of Business (whichever applicable) should be submitted
	The vendor should have a valid CERT-In empanelment.	Cert-in empanelment document.
	The SP should have a pool of resources who possess qualifications such as :CISA/ CISSP/ CCNA/ CISM/ GIAC(SANS)	Detail required to share
	The vendor should have audited Information Audit/ VAPT of CBS Infra, Net banking/ Application Audit/ Functional Security audit at least any two scheduled commercial banks other than Nainital Bank having not less than 500 branches in India.	Copy of relevant certificate/ purchase order and Client certificate.
	The vendor should not be banned/blacklisted/ debarred by any Bank/PSU/GOI Department/Indian Financial Institute	An undertaking letter to be enclosed by vendor
	Vendor should have at least 4 year experience in offering Information Security Services such as Security assessment, defining security policies procedures & baselines, Risk Assessment, security Consulting assignments to clients in India.	Copy of relevant certificate/ purchase order and Client certificate.

B. AUDIT SCOPE: ANNEXURE I

C. COMMERCIAL FORMAT: Annexure II

D. RIGHT TO REJECT: Bank reserves the absolute and unconditional right to reject the response to this inquiry if it is not in accordance with its requirements and no further correspondence will be entertained by the Bank in the matter.

E. Last Date of Submission of Quotation:

The last date for submission the sealed quotation is of password protected is 01.03.2021 at mentioned.

Annexure I- Audit Scope

A description of the envisaged scope is enumerated in brief as under:

A- SCOPE OF WORK for Audit of FI application, Infrastructure hostage at third party Data Center

1. **Physical and Environmental Security-**
   a) Physical access controls;
   b) Environment management systems such as electrical supply, UPS, air conditioning, fire detection and suppression, generator, etc.
2. **Operating System (OS)**
   a. Set up and maintenance of operating system parameters;
   b. Updating of OS Patches;
   c. OS Change Management Procedures;
   d. Use of root and other sensitive passwords;
   e. Use of sensitive system software utilities;
   f. Interfaces with external applications (such as CBS);
   g. Hardening of Operating System.
3. **Application software – FI application**
   a. Authorization Control such as concept of maker checker, exceptions, overriding exceptions, and error conditions.
   b. Authentication mechanism.
   c. User Management & Password Management
   d. Parameter Maintenance
   e. Access rights;
   f. Access logs/ Audit Trail generation;
   g. Change management procedures including procedures for testing;
   h. Documentation of change management;
   i. Documentation of Data Centre Operations.
4. **DBMS and Data Security Control**
   a. Secure use of SQL;
   b. Control procedures for changes to the parameter files;
   c. Logical access controls;
   d. Control procedures for sensitive database passwords;
   e. Control procedures for purging of Data Files;
   f. Procedures for data backup, restoration, recovery and readability of backed up data.
5. **Disaster Recovery Site** - BCP: IS Audit of DR Site with respect to
   a) Compliance with Bank's Disaster Recovery Plan aspects
   b) Log shipping management
6. **CIA and Access Management:**
   a) Maintenance of Data Integrity, Reliability and Confidentiality
   b) Safeguarding of Information System Assets/Resources
7. **Agreement Review:**
   a) Vendor's NDA and contractual agreement review
   b) SLA
8. **Network Management, Network Segmentation & Security Audit**
   a. Network Architect Diagram
   b. *Network admission control*
   c. *Hardening of routers*
   d. *Patch update Management*
   e. *Port based security controls*
   f. *Process control for change management*
   g. *security incident and management*
   h. *access control for DMZ application*

i. *VAPT with manual configuration review.*
j. *VPN review – end to end encryption*

9. **Storage of Payment System Data**: System providers are required to store the entire data relating to payment systems operated by them in a system only in India.
10. **Application & Functional audit:**
    a) Customer On-boarding (Aadhar and non-Aadhar)
    b) Financial Transactions (Cash Deposit Cash Withdrawal) with AEPS and Rupay Card
    c) Business Correspondent Management
11. **Data Center Compliances and Standards**

B- **Location:** DC- Mumbai & DR – Nasik; For application auditor can visit at Bank's Noida/ Delhi/ Head Office
C- **Infrastructure: Server-** 02 No DC & 02 No DR, Firewall
D- **Operating System:** Windows 2012
E- **Database:** MS SQL 2012

Annexure II-Commercial

Sr. No	Description	Price (Exclusive Tax) **{Prices includes Travelling, Lodging and other expenses}**
A	Audit of FI application, Infrastructure hostage at third party Data Center	