The Nainital Bank Limited
Information Security Cell, Railway Bazar, Haldwani, 263139
Ph.: 05946-251550 E-Mail: ciso.office@nainitalbank.co.in

Sealed Quotation for conducting Cyber Security Risk Posture Assessment The Nainital Bank Limited

A. OBJECTIVE: The primary objective of this engagement is to identify and address vulnerabilities within The Nainital Bank's Mobile Application, ensuring its resilience against potential cyber threats and unauthorized access. The comprehensive VAPT and Application Security Assessment will help in identifying security gaps, weaknesses, and potential entry points for malicious actors.

ELIGIBILITY CRITERIA

Sr	Eligibility Criteria	Support Documents to be submitted
1	The vendor should be Company/Firm/ Organization registered in India	Certificate of Incorporation & Commencement of Business (whichever applicable) should be submitted
2	The vendor should have a valid CERT-In empanelment.	Cert-in empanelment document.
3	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
4	Vendor Should have conducted Cyber Security Risk Posture Audit for at least two Banks in last 4 years (other than cooperative banks)	Copy of purchase order and Client certificate.
5	Vendor should have at least 4 years' 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.

Last Date of Submission of Quotation:
The last date for submission of sealed Quotation (through courier / by hand) is 05-June-2025 at below address-

Chief Information Security Officer
Information Security Cell
The Nainital Bank Limited
Railway Bazar, Haldwani,
District Nainital, Uttarakhand-263139

For any clarifications, please contact **Mr. Pankaj Adhikari** at +91 9456108588.

B. COMMERCIAL FORMAT: Annexure II

C. FREQUENCY: The frequency for conducting Cyber Security Risk Posture Audit would be one time. However, the Bank at its own discretion can change the frequency.

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.

ANNEXURE I - SCOPE OF WORK

The selected Bidder post the process would support NTB as per the scope defined in the"Scope of Work" section below-

Activity Location Address - NTB office, located at Haldwani & Nainital.

The Audit Scope should be as per Cyber Security Audit Baseline Requirements from CERT-In (Publication NSCS-46-16 Rev 1.0).

High-Level Scope for Cyber Security Risk Posture Assessment Project comprising of the followingareas focusing on the People, Process, Product, Technology and Partners supporting the Cyber Security Program at NTB, it includes but is not limited to –

Detailed Assessment, Gap Analysis, and Recommendations for the following security areas -

1. **Review of the Cyber Security Governance, Cyber Risk Management, and Cyber Security Compliance mechanisms**
   - **a.** Cyber Security Governance Structure that aligns with the global best practices and standards such as ISO 27001, NIST framework, and ITGC framework.
   - **b.** Cyber Security Risk Assessment Methodology, Procedures, Practices, and Corresponding Mitigation techniques employed including frequency of risk assessment, and comparison against global best practices.
   - **c.** Compliance status against global standards and compliance requirements from the regulatory perspective including data privacy standards and frameworks.

2. **Asset Management**
   - **a.** Review of information asset management policy, procedure, and processes including information asset lifecycle management practices (including software/ license management) based on the NIST CSF framework and ISO 27001 standard.
   - **b.** Assess existing information asset inventory tools, practices, information asset version updates, patch updates, and other update practices and processes.

3. **Access Management**
   - **a.** Review of access management policy, procedure, and processes including user access lifecycle management practices based on the NIST CSF framework and ISO 27001 standards.
   - **b.** Assess existing user and privileged access review processes and practices
   - **c.** Evaluate privileged access management tools, practices, and processes with leading industry practices.

4. **Vulnerability Management**
   - **a.** Review of vulnerability management policy, procedures, processes, and sample reports (last two quarters) in line with the NIST CSF framework and ISO 27001 standard requirements.
   - **b.** Evaluate vulnerability assessment tools and practices based on designed processes and leading industry standards.

5. **Patch Management**
   - **a.** Review the patch management policy, procedures, and processes including patch testing and approval processes.
   - **b.** In line with the NIST CSF framework, ISO 27001 standards, and leading industry practices.
   - **c.** Assess the patch management practices and timelines between the issuance of patches from vendors to the application of patches

6. **Secure Configuration Management**
   - **a.** Review the secure configuration management policy, procedure, and processes in line with NIST CSF and ISO 27001 standard requirements.
   - **b.** Review the secure configuration/hardening guidelines for the information assets/ security solution.

Conduct secure configuration reviews for critical information assets (2 of each network device/server/database) based on NIST/SANS/ CIS benchmarks and leading industry standards.

c. Review processes of configuration benchmarks based on threat intelligence.
d. Assess the configuration benchmarks and automation processes for benchmarking.
e. Evaluate the effectiveness of third-party secure configuration review report.

7. Control Management

a. Risk Driven Control Management practices and processes against global best practices and standards
b. Control processes, tools
   i. Data Center & DR Security Controls, Endpoint Security, Server Security, AD/DNS/DHCP, VPN Security, Wi-Fi Security, MFA, Perimeter Security Controlsetc.- For each we look at Documentation, Configuration, Approval, Provisioning and De-Provisioning Process, Exception Management. For AD we could perform a tool-based assessment.
   ii. API security Controls – Documentation
   iii. Encryption and Data Security.
   iv. DC/DR Security controls and Related Processes
   v. Control Reviews and Hardening processes

8. Incident Response (IR) Processes and Procedures Review:

a. Incident Response management tools, processes, and practices
b. Incident Response policy and plan
c. Cyber crisis management plan
d. Effective periodic drills for cyber crisis management plan and incident response

9. Ransomware Preparedness

a. Assess ransomware detection and mitigation tools, playbooks, practices, and processes with industry-leading practices.
b. Review the backup systems' efficacy and security processes.
c. Review backup recovery processes, practices, and periodic DR drills reports.
d. Review of Ransomware Threat Intelligence Practices

10. Third-party risk assessment

a. Review of third-party provider security policy and process
b. Evaluate the current vendor management processes in line with the drafted policy and ensure that it encompasses all NTB business units.
c. Prioritize third- parties based on services provided (e.g. criticality or risk assessment results).
d. Conduct third-party security risk assessment.

11. Cyber Security Awareness and Skilling Practices

a. Review the cyber security training and awareness policy, procedures, processes, etc., in line with the NIST CSF, ISO 27001 standard, and leading industry standards.
b. Review the human resource security policy, procedure, processes, and practices. Evaluate the security practices and implementation to meet the securityrequirements.
c. Assess the cyber security training processes for new joiners and ongoing training as per the defined periodicity for cyber security awareness

12. Cyber Security Projects Management and Information Reporting process review.

13. Design of Business Continuity and Disaster Recovery (DR)

a. Design BCM framework, policy, and procedure for IT
b. Support in designing the Business Impact Analysis template and conducting Business Impact Analysis for critical applications.

14. Detailed review of the IT Infrastructure including network devices & application capacity/performance monitoring processes

a. Authentication, Access Control, and Remote Access Practices and Processes
b. User Access Management and Identity Control Governance Processes

15. **Review the Physical & Environmental Security Controls policy, procedures, and processes in line with NIST, ISO, and leading security standards.**

16. **Secure Network Architecture Review:**
    a. Analyze the design principles adopted for ensuring Confidentiality, Integrity and Availability (CIA)
    b. Review the definition and segregation of the network into security zones such as the gateway zone (DMZ), the primary zone, the end user zone, etc. and the application of the 'Defense-in-Depth' principles
    c. Obtain an understanding of the current IT infrastructure, security, architecture and the control environment compared with similar environments/ solutions and payment environments.
    d. Review the availability/placement of key security components such as Firewall, WAF, Anti-DDOS etc.
    e. Review and assess the resilience, availability of disaster recovery setup.
    f. Review security elements of the enterprise network architecture design.
    g. Identify potential security weaknesses within the architecture.
    h. Review of network redundancy and failback mechanism.
    i. Assess the impact of security weaknesses and provide recommendations for improvement

17. **Email security assessment**
    a. Review the email security policies, rules, and security configurations.

18. **Conduct Active Directory security review:**
    a. Assess Active Directory implementation and management security design effectiveness.
    b. Assist in identifying, analyzing, and documenting security loopholes/weaknesses.
    c. Review of AD group policy (entire set of policies implemented from security standpoint)
    d. Provide an independent assessment of the operating effectiveness of the security controls.

Approximate IT Infra and Appsdetails	Counts
Internal Ips	
External Ips	
Number of applications in scope.	
Number of vendors in scope	
IT User count	
Number of user locations	

Departments in scope:

- Systems Audit
- Information Security
- Project Management
- Corporate Centre - Human Resource Team, IT Infrastructure Support Team, Finance, Legal and Accounts Teams, Admin Team, Procurement Team, Business team, Loyalty.

Cyber Security Risk Posture Audit: Vendor has to undertake Cyber Security Risk Posture Audit in scheduled manner as described below:

- Conduct Cyber Security Risk Posture Audit as per the scope, Evaluation & Submission of Preliminary Reports of findings and discussions on the finding.
- Submission of Final Report.

1. **Conduct Cyber Security Risk Posture Audit as per the scope defined in annexure I without disturbing operations**
    a. The Bank will call upon the successful Bidder/Vendor, on placement of the order, to carry out demonstration and/or walkthrough, and/or presentation and demonstration of all or specific aspects of the Cyber Security Risk Posture Audit activity.
    b. Cyber Security Risk Posture Audit to be provided 5 working days prior to the start of activity along with the team member details with technical qualification and experience. A dedicated Project Manager shall be nominated, who will be the single point of contact for Cyber Security Risk Posture Audit Activity for Nainital Bank.

c. Consultant shall have a walkthrough meeting with the concerned application team and under the process flow and architecture of the application including its modules, interfaces and user roles.
d. Consultant shall raise the prerequisites with the Bank's team and shall start the work on fulfilment of prerequisites.
e. Execute Vulnerability Assessment and Penetration testing of Bank's IT Infrastructure and Applications as per the scope on the written permission of the Bank and in the presence of Bank's Officials.
f. In case of compliance verification, verifying the observations for closure of findings.

2. Detailing the Security Gaps
a. Detailing the System setup used, and the tests conducted in assessment.
b. Critical vulnerabilities observed during Cyber Security Risk Posture Audit along with recommendations should be immediately brought to the notice of Bank without waiting for the completion of Cyber Security Risk Posture Audit. On closure of critical vulnerability, verification of closure shall have to be performed.
c. Analysis of the findings and Document the security gaps i.e. vulnerability, security flaws, loopholes, threats, etc. observed during the course of the Cyber Security Risk Posture Audit activity as per the scope of work.
d. Document recommendations and solutions for addressing these security gaps and categorize the identified security gaps based on their criticality.
e. Chart a roadmap for the Bank to ensure compliance and address these security gaps.

3. Addressing the Security Gaps
a. Recommend Actionable fixes for systems vulnerabilities in design or otherwise for application systems and network infrastructure. If recommendations for Risk Mitigation /Removal could not be implemented as suggested, alternate solutions to be provided.
b. Suggest changes/modifications in the Security Policies implemented along with Security Architecture including Network and Applications of the Bank to address the same.
c. The Draft report of the Cyber Security Risk Posture Audit findings should be submitted to the Bank for Management comment within 15 days of start of audit.

4. Submission of Final Reports
a. The Service Provider should submit the final report of Cyber Security Risk Posture Audit findings as per the report format mentioned in Deliverables. All the Cyber Security Risk Posture Audits submitted should be signed by technically qualified persons and he/she should take ownership of document, and he/she is responsible and accountable for the document/report submitted to the Bank.
b. The final report has to be submitted within -1- months of submission of the initial draft report.
c. Service provider will also submit the Executive Summary Report of the Bank's Internet facing environment.

5. Acceptance of the Report
a. The Report shall be accepted on complying with the formats of Cyber Security Risk Posture Audit as mentioned in the Scope and acceptance of the audit findings.

6. Deliverables:
a. The deliverables for Cyber Security Risk Posture Audit activity are as follows:
i. Execution of Vulnerability Assessment and Penetration Testing and Application Security Testing for the identified network devices, security devices, servers, applications, websites, interfaces (part of application) etc. as per the Scope mentioned in this scope and Analysis of the findings and guidance for resolution of the same
ii. Verification of closure of critical vulnerability.
iii. Perform compliance verification of closure of findings.
iv. Draft Cyber Security Risk Posture Audit followed by final report.
v. Compliance verification

b. The Cyber Security Risk Posture Audit should contain the following: -
i. Identification of Auditee (Address & contact information)
ii. Dates and Locations of Cyber Security Risk Posture Audit
iii. Terms of reference
iv. Standards followed including confirmation of testing as per International Best practices and OWASP Web/Mobile application security guidelines.

v. Summary of audit findings including identification tests, tools used, and results of tests performed (like vulnerability assessment, penetration testing, application security assessment, website assessment, etc.)
    1. Tools used and methodology employed
    2. Positive security aspects identified
    3. List of vulnerabilities identified
    4. Description of vulnerability
    5. Risk rating or severity of vulnerability
    6. Category of Risk: Very High (Critical) / High / Medium / Low
    7. Test cases used for assessing the vulnerabilities
    8. Illustration of the test cases
    9. Applicable screenshots.

vi. Analysis of vulnerabilities and issues of concern

vii. Recommendations for corrective action

viii. Personnel involved in the audit

The Service Provider may further provide any other required information as per the approach adopted by them and which they feel is relevant to the audit process. All the gaps, deficiencies, vulnerabilities observed shall be thoroughly discussed with respective bank officials before finalization of the report.

The Cyber Security Risk Posture Audit should comprise the following sub reports: -

Cyber Security Risk Posture Audit – Executive Summary: The vendor should submit a report to summarize the Scope, Approach, Findings and recommendations, in a manner suitable for senior management. Vendor will also detail the positive findings (No Gap found) for various tests conducted.

Cyber Security Risk Posture Audit – Core Findings along with Risk Analysis: The vendor should submit a report bringing out the core findings of the Cyber Security Risk Posture Audit conducted for network devices, security devices, servers and websites.

Cyber Security Risk Posture Audit – Detailed Findings/Checklists: The detailed findings of the Cyber Security Risk Posture Audit would be brought out in this report which will cover in details all aspects viz. identification of vulnerabilities/threats in the systems (specific to equipment's/resources indicating name and IP address of the equipment with Office and Department name), identifications of threat sources, identification of Risk, Identification of inherent weaknesses, Servers/Resources affected with IP Addresses etc. Report should classify the observations into Critical /Non-Critical category and asses the category of Risk Implication as Very High (Critical) /High/Medium/Low Risk based on the impact. The various checklist formats, designed and used for conducting the Cyber Security Risk Posture Audit activity as per the scope, should also be included in the report separately for Servers (different for different OS), application, Network equipment's, security equipment's etc., so that they provide minimum domain wise baseline security standard /practices to achieve a reasonably secure IT environment for technologies deployed by the Bank. The Reports should be substantiated with the help of snap shots/evidence /documents etc. from where the observations were made.

Cyber Security Risk Posture Audit – In Depth Analysis of findings /Corrective Measures & Recommendations along with Risk Analysis: - The findings of the entire Cyber Security Risk Posture Audit Process should be critically analyzed and controls should be suggested as corrective /preventive measures for strengthening / safeguarding the IT assets of the Bank against existing and future threats in the short /long term. Report should contain suggestions/recommendations for improvement in the systems wherever required. If recommendations for Risk Mitigation /Removal could not be implemented as suggested, alternate solutions to be provided. Also, if the formal procedures are not in place for any activity, evaluate the process & the associated risks and give recommendations for improvement as per the best practices. Separate reports should be provided for common infrastructure assets and Applications.

Documentation Format

- All documents will be handed over in soft copy format.
- Soft copies of all the documents properly encrypted in MS Word /MS Excel /PDF format also to be submitted in
- Soft copies along with the hard copies.
- All documents shall be in plain English.

Project Timelines:

The vendor shall furnish a schedule of assessment within -7- days of issuance of Purchase order. Cyber Security Risk Posture Audit has to be mutually agreed by both the parties. In certain situations, Bank may be required to defer the scheduled activity due to non-availability of the production environment for Cyber Security Risk Posture Audit for whatever may be the reason. In such a situation, Cyber Security Risk Posture Audit activity has to be deferred however the same has to be within the overall contract validity period.

Final Cyber Security Risk Posture Audit has to be submitted within -1- months of issuance of the initial Draft report after considering the Management comments on the Draft report.

ANNEXURE II- COMMERCIAL

(Excluding applicable taxes)

Sr. No	Name of the Audit	Commercials (Price) per instance
1	Cyber Security Risk Posture Assessment	
	Grand- Total	
Cost shall include all Travelling, Lodging and other expenses.		

NOTE-

Price: **(should be Exclusive of Taxes)** ***(Price should include Travelling, Lodging and other expenses)***

****Selection Criteria –**

The Vendor should be qualified in all technical aspects required for the banking security standards.

The least accumulative Total of all received quotations will be considered as L1.