**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 Source Code Review & Web Application Penetration Testing Mobile Banking Admin Portal

## 1- OBJECTIVE:

The primary objective of this engagement is to identify and address vulnerabilities within The Nainital Bank's Mobile Banking Admin Portal (Web based Application) & Mobile Application's Source Code Review, 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.

## A. 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 and active 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 SCR & APPSEC 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. |

## B. Last Date of Submission of Quotation:

**The last date for submission of sealed Quotation (through courier/by hand) is 31-08-2024 at below address-**

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

## C. COMMERCIAL FORMAT: Annexure II

**D. FREQUENCY:** The frequency for conducting SCR & APPSEC during the time frame of one year would be as follows:

| Sr. | Description | Tentative Instances (Frequency) |
|---|---|---|
| 1 | SCR | 4 |
| 2 | WAPT | 4 |

***Note:***

- ***However, the Bank at its own discretion can change the frequency as the mobile banking application will have multiple rounds of development phases.***
- ***The count of instances will be established by the first scheduled audit of every service.***

**F. RIGHT TO REJECT:** The 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

AppSec & Source Code Review should cover the application and its components including web server, app server, DB Server, Networking systems, Security devices, load balancers etc.
After the AppSec & Source Code Review assessment and submission of the report to the Bank, the Bank may at its discretion request in writing for Compliance verification on closure of observations.

- **SCR Activities:** VAPT should be credential based scanning and comprehensive but not limited to the following activities.

| | |
|---|---|
| • Input Validation<br>• Output Encoding<br>• Authentication & Password Management<br>• Session Management<br>• Access Control<br>• Cryptographic Practices<br>• Error Handling & Logging<br>• Data Protection<br>• Communication Security<br>• System Configuration<br>• Database Security<br>• File Management | • User Management<br>• Authorization<br>• Encryption & Cryptography<br>• Exception Handling<br>• Reducing the attack surface<br>• Information Gathering<br>• Configuration<br>• Secure Transmission<br>• Data Validation<br>• Application Output<br>• Log Management<br>• Memory Management |

- **Application Assessment:** Mobile banking assessment should be done as per latest OWASP-MASVS, OWASP-ASVS and other relevant OWASP-MAST standards & guidelines including but not limited to the following:

| | |
|---|---|
| • Horizontal privilege escalation<br>• Vertical privilege escalation<br>• Insecure direct object references<br>• Missing function level access control<br>• Weak encryption algorithms<br>• Insecure key management<br>• Use of outdated protocols<br>• Lack of data integrity protection<br>• Default passwords or settings that are not changed<br>• Unsecured ports or services<br>• Misconfigured firewalls or access controls<br>• Inadequate logging and monitoring settings<br>• Weak or easily guessable passwords<br>• Lack of two-factor authentication<br>• Improper session management<br>• Insufficient user validation<br>• Inadequate or incomplete event logging<br>• Failure to detect or respond to security incidents<br>• Lack of monitoring for abnormal or suspicious activity<br>• Inadequate incident response procedures | • SQL injection<br>• Cross-site scripting (XSS)<br>• Command injection<br>• LDAP injection<br>• Lack of input validation<br>• Poorly designed authentication mechanisms<br>• Inadequate error handling<br>• Insecure communication channels<br>• Use of outdated operating systems or libraries<br>• Unpatched software vulnerabilities<br>• Use of unsupported software versions<br>• Failure to perform regular vulnerability scans or updates<br>• Malware or viruses<br>• Data tampering or manipulation<br>• Lack of data backup and recovery procedures<br>• Insufficient data validation and verification<br>• Bypassing firewall or access controls<br>• Accessing internal systems or resources<br>• Exploiting server-side vulnerabilities<br>• Accessing sensitive data or functionality |

- **Compliance of Regulatory guidelines/Advisories:** Successful Bidder shall perform SCR & APPSEC and ensure that regulatory guidelines issued by various bodies such as Cert-In, NCIIPC, RBI-CSITE, NPCI, OWASP-MASVS, OWASP-ASVS and other relevant OWASP standards & guidelines etc. are followed.



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

➢ **List of Application/Infrastructure:**

| Sr. No. | Name of the Application/Service | Purpose of the Application |
|---|---|---|
| 1 | Source Code Review | Mobile Banking Android Application |
| 2 | Mobile Banking Admin Portal | Mobile Banking Admin Panel |

➢ **Technical Details of the Applications**

**1- Source Code Review**

| Mobile Banking Application Code Review | |
|---|---|
| **Android** | Primary APK Code |

**2- Mobile Banking Admin Portal**

| Mobile Banking Admin Portal | |
|---|---|
| **Application Name** | Nainital Admin-Portal |
| **Application Type(.exe/Web/Android/iOS)** | Web Application |
| **Languages Used** | Java, JavaScript, HQL, SQL, HTML |
| **System type** | UAT |
| **Database Server** | Oracle |
| **Web server/ Application Server** | Web logic |
| **Roles & types of privileges for the different roles. (Admin/User)** | SUPER(Admin) – All permissions<br>CHECKER - Request Verification<br>MAKER - Request Generation |
| **Number of login modules** | 1 |
| **Number of Static Pages** | 1 |
| **Number of Dynamic Pages** | 30+ |
| **Number of API Calls** | 2 |
| **Number of form/fields/parameter/inputs** | 100+ |
| **Does the application provide a file download/Upload feature (Yes/ No)** | Yes |

**3- Servers**

| Server Details | | | | |
|---|---|---|---|---|
| **Sr. No** | **Application** | **Environment** | **Role** | **Operating System** |
| **1.** | Web Server | UAT | APP | Oracle Linux |
| **2.** | App Server | UAT | WEB | Oracle Linux |
| **3.** | DB | UAT | DB | Oracle Linux |

**Note:** ***Further Technical Details will be shared to the successful bidder beforehand initiation of the Security Audit.***



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

➢ **Location of the Audit**

The applications covered under the scope are hosted in below mentioned locations.

| Name of the Application | Location of Hardware | Location for Performing Audit |
|---|---|---|
| **Source Code Review** | Infrasoft Technologies Limited 7th Floor, Building 09, Gigaplex, Airoli West, Navi Mumbai-400708, Maharashtra, India | 7th Floor, Building No 9, Gigaplex IT Park, Mindspace Airoli West, MSEB Staff Colony, TTC Industrial Area, Airoli, Navi Mumbai, Maharashtra 400708 |
| **Mobile Banking Admin Portal** | Remote (VPN Access will be provided by the Bank) | Remote (VPN Access will be provided by the Bank) |

➢ **SCR & AppSec Schedule:** Vendor has to undertake VAPT & Application Security testing in scheduled manner as described below:

- Conduct VAPT and Application Security testing as per the scope, Evaluation & Submission of Preliminary Reports of findings and discussions on the finding.
- Submission of Final Report.

**a. Conduct SCR & AppSec as per the scope defined in annexure I without disturbing operations.**

- The Bank will call upon the successful Bidder/Vendor, on placement of the order, to conduct demonstration and/or walkthrough, and/or presentation and demonstration of all or specific aspects of the SCR & AppSec activity.
- SCR & AppSec schedule to be provided five 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 SCR & AppSec Activity for Nainital Bank.
- 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.
- Consultant shall raise the prerequisites with the Bank's team and shall start the work on fulfilment of prerequisites.
- 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.
- In case of compliance verification, verifying the observations for closure of findings.

**b. Detailing the Security Gaps**

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

**c. Addressing the Security Gaps**

- 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, alternative solutions to be provided.
- Suggest changes/modifications in the Security Policies implemented along with Security Architecture including Network and Applications of the Bank to address the same.



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

**The Draft report of the VAPT and AppSec findings should be submitted to the Bank for Management comment within 15 days of start of audit.**

**d. Submission of Final Reports**

- The Service Provider should submit the final report of SCR & APPSEC findings as per the report format mentioned in Deliverables. All the SCR & APPSEC reports submitted should be signed by technically qualified people and he/she should take ownership of the document and he/she is responsible and accountable for the document/report submitted to the Bank.
- The final report has to be submitted within -1- months of submission of the initial draft report.
- The service provider will also submit the Executive Summary Report of the Bank's Internet facing environment.

**e. Acceptance of the Report**

- The Report shall be accepted on complying with the formats of SCR & APPSEC Report as mentioned in the Scope and acceptance of the audit findings.

➢ **Deliverables**

The deliverables for SCR & AppSec activity are as follows: -

- 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.
- Verification of closure of critical vulnerability.
- Perform compliance verification of closure of findings.
- Draft SCR & AppSec Report followed by final report.
- Compliance verification

**The SCR & APPSEC Report should contain the following: -**

- Identification of Auditee (Address & contact information)
- Dates and Locations of SCR & APPSEC
- Terms of reference
- Standards followed including confirmation of testing as per International Best practices and OWASP Web/Mobile application security guidelines.
- 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.)
    - Tools used and methodology employed
    - Positive security aspects identified
    - List of vulnerabilities identified
    - Description of vulnerability
    - Risk rating or severity of vulnerability
    - Category of Risk: Very High (Critical) / High / Medium / Low
    - Test cases used for assessing the vulnerabilities
    - Illustration of the test cases
    - Applicable screenshots.
- Analysis of vulnerabilities and issues of concern
- Recommendations for corrective action
- 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, and vulnerabilities observed shall be thoroughly discussed with respective bank officials before finalization of the report.

**The SCR & APPSEC Report should comprise the following sub reports: -**



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

- **SCR & APPSEC Report – 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.
- **SCR & APPSEC Report – Core Findings along with Risk Analysis:** The vendor should submit a report bringing out the core findings of the SCR & APPSEC conducted for network devices, security devices, servers, and websites.

- **SCR & APPSEC Report – Detailed Findings/Checklists:** The detailed findings of the SCR & APPSEC 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 assess 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 SCR & APPSEC 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.

- **SCR & APPSEC Report – In Depth Analysis of findings /Corrective Measures & Recommendations along with Risk Analysis: -** The findings of the entire SCR & APPSEC 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, alternative 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. SCR & APPSEC schedule has to be mutually agreed by both the parties. In certain situations, the Bank may be required to defer the scheduled activity due to the non-availability of the production environment for SCR & APPSEC for whatever may be the reason. In such a situation, SCR & APPSEC activity has to be deferred however the same has to be within the overall contract validity period.

  Final SCR & APPSEC report has to be submitted within -1- months of issuance of the initial Draft report after considering the Management comments on the Draft report.



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

**Annexure II- Commercial**
**(Excluding applicable taxes)**

| Sr. No | Name of the Application | Purpose of the Application | Commercials (Price) per instance for SCR conduction |
|---|---|---|---|
| 1 | Mobile Banking APK Source Code Review | Mobile Banking Android Application Source Code | |
| | | **Sub-Total** | |

| Sr. No | Name of the Application | Purpose of the Application | Commercials (Price) per instance for AppSec conduction |
|---|---|---|---|
| 1 | Mobile Banking Admin Portal WAPT | Mobile Banking Admin Panel | |
| | | **Sub-Total** | |
| | | **Grand- Total** | |
| **Cost shall include all Travelling, Lodging and other expenses.** | | | |

**NOTE-** ***Based upon the frequency, Bank at its discretion can conduct the SCR & APPSEC of any/all application as per the commercials mentioned above in respective category. Invoices will be raised for per instance completed.***

*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 in all received quotations will be considered as L1.***



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