Sealed Quotation for conducting Vulnerability Assessment and Penetration Testing & Application Security Testing of Bank's Website, Reconciliation Application, Complaint Module and their Infrastructure

1- OBJECTIVE:

The primary objective of this engagement is to identify and address vulnerabilities within The Nainital Bank's Website, Reconciliation Application, Complaint Module and their infrastructure, 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 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 VAPT & 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. SCOPE OF WORK: ANNEXURE I

C. Last Date of Submission of Quotation:

The last date for submission of sealed Quotation (through courier / by hand) is **11-Oct-2023** at below address-

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

D. COMMERCIAL FORMAT: Annexure II

E. FREQUENCY: The frequency for conducting VAPT & APPSEC would be one time. However, the Bank at its own discretion can change the frequency.

F. 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

Vulnerability Assessment and Penetration Testing & AppSec should cover the application and its components including web server, app server, DB Server, Networking systems, Security devices, load balancers etc.

After the VAPT & AppSec assessment and submission of the report to the Bank, Bank may at its discretion request in writing for Compliance verification on closure of observations.

VAPT Activities: VAPT should be credential based scanning and comprehensive but not limited to following activities.
- Network Scanning
- Port Scanning
- System Identification & Trusted System Scanning
- Vulnerability Scanning
- Malware Scanning
- Spoofing
- Scenario Analysis
- Application Security Testing & Code Review
- OS Fingerprinting
- Service Fingerprinting
- Access Control Mapping
- Denial of Service (DOS) Attacks
- DDOS Attacks
- Authorization Testing
- Lockout Testing
- Password Cracking
- Cookie Security
- Functional validations
- Containment Measure Testing
- War Dialing
- DMZ Network Architecture Review
- Firewall Rule Base Review
- Server Assessment (OS Security Configuration)
- Security Device Assessment
- Network Device Assessment
- Database Assessment
- Website Assessment (Process)
- Vulnerability Research & Verification
- IDS/IPS review & Fine tuning of Signatures

THE NAINITAL BANK LTD.

- Man in the Middle attack
- Man in the browser attack
- Any other attack.

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

- Injection
- Broken Authentication and Session Management
- Cross-Site Scripting (XSS)
- Insecure Direct Object References
- Security misconfiguration
- Insecure Cryptographic Storage
- Sensitive Data Exposure
- Failure to Restrict URL Access
- Missing Function Level Access Control
- Cross-Site Request Forgery (CSRF)
- Using Known Vulnerable Components
- Un-validated Redirects and Forwards
- Insufficient Transport Layer Protection
- Any other attack which are vulnerable to the web sites and web

Compliance of Regulatory guidelines/Advisories: Successful Bidder shall perform VAPT & APPSEC and also 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.

List of Application:

Sr. No	Name of the Application	Purpose of the Application
1	Bank Website	Nainital Bank Website - nainitalbank.co.in
2	i-recon	Reconciliation Application
3	Complaint Module	Module designed for Complaints lodging

Technical Details of the Applications

1- Bank's Website

CONFIGURATION FOR WEBSITE	
Website name	www.nainitalbank.co.in
Server IP	192.168.70.153
Website configuration path	D:\ftp site\nainital bank\data
System type	64 bit operating system
MS SQL Server	Windows server 2019 standard
IIS server	Internet information service (IIS) 10 Internet information service (IIS) 6.0 manager
Application Server with Version	Internet information service 10 Application server management
Front-end Tool	Asp.net

THE NAINITAL BANK LTD.

Back-end Database	Microsoft SQL Server 2016
Authorization no. of roles & types of privileges for the different roles.	Admin checker Admin maker
Content management module (CMS) (If yes, then which?)	YES
Number of forms & input fields	2
Number of dynamic pages	6
Number of static pages	188
No. of login modules	3
Does the application provide a file download feature (Yes/ No)	Yes

2- i-recon

CONFIGURATION FOR i-recon		
PARAMETER	**DESCRIPTION**	
Application	Reconcile	Reconcile
Role	Application Server	Database Server
Hostname	noinprrecapp01	noinprrecdb01
Environment	UAT	UAT
APP/DB	App	DB
Operating System	Oracle Linux Server 8.5	Oracle Linux Server 8.5
Database	NA	Oracle 19c EE 19.18.0
Location	DC	DC
Management IP for MITS	198.18.4.243	198.18.4.149
Management IP	172.23.100.7	172.23.100.78
Production IP	172.23.98.40	172.23.99.45

THE NAINITAL BANK LTD.

- **ADDITIONAL DETAILS OF I-RECON**

Web Application Name & URL (If possible dummy username/ password)	https://172.23.98.40:9891/UPIRECON_BETA
Application Server withVersion	Tomcat (8.5.83)
Front-end Tool	Java
Back-end Database	Oracle 19c
Authorization no. of roles &types of privileges for the different roles.	2 (Admin & User)
Content management module (CMS) (If yes, then which?)	No
Number of forms & input fields	4
Number of dynamic pages	1
Number of static pages	12
No. of login modules	4
Does the application provide a file download feature (Yes/ No)	Yes

THE NAINITAL BANK LTD.

3- Complaint Module

CONFIGURATION DETAILS OF COMPLAINT MODULE	
Software name	Nainital Bank Complaint Portal
HOST IP	172.24.0.10
Software configuration path	C:\Users\NTB2157\Desktop\Complaint_Portal\NBL_Complaint_Service-master\P_068 E-Complaints(EasyBank)
Windows edition	Windows server 2019 standard
MS SQL Server	MySQL 8.0 November 2022 Copyright (c) Oracle Corporation Standard Edition (64- bit) on Windows Server 2019 Standard 10.0 <X64> (Build 17763:)
IIS server	Internet information service (IIS) 10
	Internet information service (IIS) 6.0 manager
Web Application Name & URL (If possible dummy username/ password)	Nainital Bank Complaint Portal (http://172.24.0.10:8085/home)
Operating System Details(i.e. Windows Server 2012)	Window Server 2019(Standard)
Application Server with Version	Tomcat (8.5.83)
Front-end Tool	Java , JSP
Back-end Database	Oracle MySQL
Authorization no. of roles & types of privileges for the different roles.	1 Admin & Multi User(Managed by Admin)
Content management module (CMS) (If yes, then which?)	No
Number of forms & input fields	6
Number of dynamic pages	1
Number of static pages	16
No. of login modules	6
Does the application provide a file download feature (Yes/ No)	No

THE NAINITAL BANK LTD.

Locations covered: The applications covered under the scope are hosted in below mentioned locations. Please note that – "No remote logins and/or remote desktop sessions shall be provided for Bank's location".

Name of the Application	Location of Hardware	Location for Performing Audit
Bank's Website	Netmagic Solutions Pvt. Ltd. A-14, Sector 62, Gautam Buddha Nagar, Noida UP	Netmagic Solutions Pvt. Ltd. A-14, Sector 62, Gautam Buddha Nagar, Noida UP
i-recon	Sify Technologies Ltd., B7, Sector 132, Noida Expressway, UP	DIT, The Nainital Bank Ltd., Railway Bazar, Haldwani
Complaint Module	Sify Technologies Ltd., Reliable Plaza, K-10 Thane, Belapur Road, Navi Mumbai-400710	DIT, The Nainital Bank Ltd., Railway Bazar, Haldwani

VAPT & 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 VAPT & 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 carry out demonstration and/or walkthrough, and/or presentation and demonstration of all or specific aspects of the VAPT & Appsec activity.
- VAPT & Appsec schedule 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 VAPT & 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 pre requisites with the Bank's team and shall start the work on fulfilment of pre requisites.
- 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.

THE NAINITAL BANK LTD.

b. **Detailing the Security Gaps**
- Detailing the System setup used and the tests conducted in assessment.
- Critical vulnerabilities observed during VAPT & APPSEC along with recommendations should be immediately brought to the notice of Bank without waiting for the completion of VAPT & 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 VAPT & 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, alternate 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 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 VAPT & APPSEC findings as per the report format mentioned in Deliverables. All the VAPT & APPSEC reports 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.
- The final report has to be submitted within -1- months of submission of the initial draft report.
- 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 VAPT & APPSEC Report as mentioned in the Scope and acceptance of the audit findings.

Deliverables:

The deliverables for VAPT & Appsec activity are as follows: -

- Execution of Vulnerability Assessment and Penetration Testing and Application Security Testing for the identified network devices, security

THE NAINITAL BANK LTD.

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 VAPT & Appsec Report followed by final report.
- Compliance verification

The VAPT & APPSEC Report should contain the following: -

- Identification of Auditee (Address & contact information)
- Dates and Locations of VAPT & 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, vulnerabilities observed shall be thoroughly discussed with respective bank officials before finalization of the report.

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

VAPT & 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.

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

VAPT & APPSEC Report – Detailed Findings/Checklists: The detailed findings of the VAPT & 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 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 VAPT & 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/evidences /documents etc. from where the observations were made.

VAPT & APPSEC Report – In Depth Analysis of findings /Corrective Measures & Recommendations along with Risk Analysis: - The findings of the entire VAPT & 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, 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. VAPT & APPSEC schedule 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 VAPT & APPSEC for whatever may be the reason. In such a situation, VAPT & APPSEC activity has to be deferred however the same has to be within the overall contract validity period.

Final VAPT & 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 LTD.

Annexure II- Commercial
(Excluding applicable taxes)

Sr. No	Name of the Application	Purpose of the Application	Commercials(Price) per instance for VA conduction
1	Bank Website	Nainital Bank Website www.nainitalbank.co.in	
2	i-recon	Reconciliation Tool	
3	Complaint Module	Module designed for Complaints lodging	
Cost shall include all Travelling, Lodging and other expenses.			

Sr. No	Name of the Application	Purpose of the Application	Commercials (Price) per instance for PT conduction
1	Bank Website	Nainital Bank Website www.nainitalbank.co.in	
2	i-recon	Reconciliation Tool	
3	Complaint Module	Module designed for Complaints lodging	
Cost shall include all Travelling, Lodging and other expenses.			

Sr. No	Name of the Application	Purpose of the Application	Commercials (Price) per instance for Appsec conduction
1	Bank Website	Nainital Bank Website www.nainitalbank.co.in	
2	i-recon	Reconciliation Tool	
3	Complaint Module	Module designed for Complaints lodging	
Cost shall include all Travelling, Lodging and other expenses.			

NOTE- Based upon the frequency, Bank at its discretion can conduct the VAPT & APPSEC of any/all application as per the commercials mentioned above in respective category.

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

THE NAINITAL BANK LTD.