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 Comprehensive Security Assessment of SFMS Infrastructure

1- OBJECTIVE:

The primary objective of this engagement is to identify and address vulnerabilities within The Nainital Bank's New SFMS Infrastructure, ensuring its resilience against potential cyber threats and unauthorized access. The comprehensive Security Assessment 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 SECURITY ASSESSMENT 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 17-09-2024 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. 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

Comprehensive Security Assessment should cover the application and its components including web server, app server, DB Server, Networking systems, Security devices, load balancers etc.

After the Security 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.

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- Use of outdated protocols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

➢ **VAPT Activities:** VAPT should be credential based scanning and comprehensive but not limited to the 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
- Man in the Middle attack.
- Man in the browser attack.
- Any other attack.

- **OS Hardening & Review:** OS Hardening & Review should be comprehensive but not limited to the following activities.

- Microsoft Defender Firewall
- Services
- User Accounts
- User Accounts
- Startup
- Windows Features
- Windows Updates
- Windows Defender Antivirus
- Group Policy Object (Gpo)
- Registry
- Disable Accounts
- Password Policy
- Lockout Policy
- User Account Control
- Interactive Logon
- Network Access
- Network Security
- Windows Defender Antivirus
- Windows Update

- **Firewall Hardening & Review:** Firewall Hardening & Review should be comprehensive but not limited to the following activities.

- Rulesets Review
- Application based firewall
- Stateful inspection
- Logging
- Patches and updates
- Location – DMZ
- Vulnerability assessments/ Testing
- Compliance with security policy
- Port restrictions
- File Transfers
- Mail Traffic
- ICMP (ICMP 8, 11, 3)
- IP Readdressing/IP Masquerading
- Remote access
- Zone Transfers
- Egress Filtering
- Critical servers
- Distributed firewalls
- Stealth Firewalls
- Continued availability of Firewalls

- **Thick Client Pen-testing:** Thick Client Pen-testing should be comprehensive but not limited to the following activities.

- Information Gathering
- Traffic Analysis
- Sensitive Data in Registry
- Obtaining Connection String in Memory
- CSV and SQL Injection
- Reverse Engineering
- DLL Hijacking
- Logging, Timestamps and Signing
- Memory Manipulation
- Run Time Manipulation
- Registry Permissions
- Registry Contents
- Registry Manipulation
- Decryption And De Obfuscation
- Decompile And Application Rebuild
- Public Methods
- Memory Manipulation
- Run Time Manipulation
- Registry Permissions
- Registry Contents
- Registry Manipulation
- Decryption And De Obfuscation
- Decompile And Application Rebuild
- Public Methods
- Function Exported
- File And Content Manipulation
- File Content Debugging
- Gui Testing
- Access Control and Injection-Based Vulnerabilities
- Bypass Controls by Utilizing Intended Gui Functionality
- Check Improper Error Handling
- Check Weak Input Sanitization
- Try Privilege Escalation
- Try Payment Manipulation
- File Testing
- Files Permission
- File Continuity

- **IBM MQ Hardening & Review:** Thick Client Pen-testing should be comprehensive but not limited to the following activities.

- Security updates
- Security overview
- security requirements
- Setting up security
- Identifying and authenticating users
- Authorizing access to objects
- LDAP authorization
- Confidentiality of messages
- Confidentiality for data at rest on IBM

- Data integrity of messages
- Auditing
- IBM MQ Console and REST API security
- files
- Managed File Transfer
- Securing AMQP clients
- Security
- Advanced Message Security (AMS)

➢ **Database Hardening & Review:** Thick Client Pen-testing should be comprehensive but not limited to the following activities.

- Encryption in Motion/Transit
- Encryption at rest
- Control Access
- Database Access
- Application Access

- Row level Security
- Dynamic Data Masking
- Proactive Monitoring
- Tracking & Detecting
- Auditing tracks database events

➢ **Internal Penetration Testing**

Straight-Through Processing (STP) should focus on evaluating the security controls that protect the end-to-end automation of financial transactions. The audit should include testing for vulnerabilities in transaction data transmission, system authentication, data integrity, and authorization processes. Additionally, the auditor should assess the resilience of the STP system against threats such as unauthorized access, data breaches, and potential disruptions that could compromise the accuracy and efficiency of automated transactions. The goal is to ensure that the STP system is secure, reliable, and compliant with relevant regulatory requirements.

➢ **Compliance of Regulatory guidelines/Advisories:** Successful Bidder shall perform Security Assessment 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.

E. LIST OF APPLICATION/INFRASTRUCTURE:

Sr.	Application/Server Name		Application Type	Total Instances
1	**Structured Financial Messaging System**		**Web Application**	**1**
2	**SFMS Server – 4 CIMS – 1 CCIL – 1 CCIL/CIMS – 1**	**Switches – 3 Firewall – 3 SAN Storage – 1 Clients – 4**	**Servers, Firewall, Switch & SAN**	**18**
3	**SFMS Signer NDS-Call**		**Thick Client**	**2**
4	**SFMS CCIL**		**IBM MQ WebSphere**	**2**
5	**SFMS – 4 CCIL – 1 CIMS – 1 CCIL/CIMS – 1**		**OS Configuration Review**	**7**
6	**Firewall – 2 Switch – 3**		**Firewall & Network Configuration Review**	**5**
7	**Straight-Through Processing Transaction from CBS to SFMS**		**Network**	**1**
			Total	**37**

F. TECHNICAL DETAILS OF THE APPLICATIONS

1- Vulnerability Assessment & Penetration Testing

Sr.	Application	Site	OS/Device
1	**SFMS Primary**	DC	Windows Server
2	**SFMS Secondary**	DC	Windows Server
3	**SFMS UAT**	DC	Windows Server
4	**CCIL Primary**	DC	Windows Server
5	**CIMS Primary**	DC	Windows Server
6	**SAN Storage**	DC	Windows Server
7	**FortiGate Firewall 1**	DC	FG60F
8	**FortiGate Firewall 2**	DC	FG40F
9	**FortiGate Firewall 3**	DR	FG40F
10	**Managed Switch 1**	DC	Catalyst 1000 48port GE
11	**Managed Switch 2**	DC	Catalyst 1000 48port GE
12	**Managed Switch 3**	DR	Aruba ION 1930-24G
13	**SFMS**	DR	Windows Server
14	**CCIL/CIMS**	DR	Windows Server

2- Web Application Penetration Testing

Structured Financial Messaging System	
Application Name	**Structured Financial Messaging System**
Application Type(.exe/Web/Android/iOS)	Web Application
Languages Used	Java Script
System type	UAT
Database Server	Oracle 19.22.0.0
Web server/ Application Server	Apache Tomcat
Roles & types of privileges for the different roles. (Admin/User)	SUPER(Admin) – All permissions CHECKER - Request Verification MAKER - Request Generation
Number of login modules	2
Number of Static Pages	0
Number of Dynamic Pages	100+
Number of API Calls	0
Number of form/fields/parameter/inputs	100+
Does the application provide a file download/Upload feature (Yes/ No)	Yes

3- Thick Client Security Assessment

Thick Client Application		
Sr.	Application	Technology
1	SFMS Signer Application	**Java Application**
2	NDS Call Application	**EXE Application**

4- IBM MQ Configuration Review

IBM MQ WebSphere	
Sr.	**Application**
1	**SFMS**
2	**CIMS**

5- OS Configuration Review

Operating System		
Sr.	**Application**	**Type**
1	**SFMS**	Windows Server
2	**CIMS**	Windows Server
3	**CCIL**	Windows Server

6- Firewall & Network Configuration Review

Firewalls	
Sr.	**Application**
1	**FortiGate Firewall FG40F**
2	**FortiGate Firewall FG60F**
3	**Managed Switches**

7- Internal Penetration Testing

Straight-Through Processing (STP) should focus on evaluating the security controls that protect the end-to-end automation of financial transactions. The audit should include testing for vulnerabilities in transaction data transmission, system authentication, data integrity, and authorization processes. Additionally, the auditor should assess the resilience of the STP system against threats such as unauthorized access, data breaches, and potential disruptions that could compromise the accuracy and efficiency of automated transactions. The goal is to ensure that the STP system is secure, reliable, and compliant with relevant regulatory requirements.

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

- **Location of the Audit**

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

Sr.	Application/Server Name	Location for Performing Audit
1	**Structured Financial Messaging System**	Information Security Cell The Nainital Bank Limited Railway Bazar, Haldwani, District Nainital, Uttarakhand India-263139 **OR** The Nainital Bank Limited 4th Floor, UPRNN Building C-20 / 1A / 7 Sector 62, Noida Uttar Pradesh - 201309 Ph: -120-2401083
2	**SFMS Server – 4** **CIMS – 1** **CCIL – 1** **CCIL/CIMS – 1** **Switches – 3** **Firewall – 3** **SAN Storage – 1**	
3	**SFMS Signer** **NDS-Call**	
4	**SFMS** **CCIL**	
5	**SFMS – 4** **CCIL – 1** **CIMS – 1** **CCIL/CIMS – 1**	
6	**Firewall – 2** **Switch – 3**	
7	**Straight-Through Processing Transaction from CBS to SFMS**	

G. GENERAL TERMS & CONDITIONS

- **Security Assessment Schedule:** Vendor has to undertake Security Assessment 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 Security Assessment 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 Security Assessment activity.
- Security Assessment 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 Security Assessment 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 security assessment along with recommendations should be immediately brought to the notice of Bank without waiting for the completion of security assessment. 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 security assessment 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 Draft report of the Security Assessment findings should be submitted to the Bank for Management comment within 15 days of the start of audit.

d. Submission of Final Reports

- The Service Provider should submit the final report of security assessment findings as per the report format mentioned in deliverables. All the security assessment 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 security assessment Report as mentioned in the Scope and acceptance of the audit findings.

- **Deliverables**

The deliverables for Security Assessment 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 Security Assessment Report followed by final report.
- Compliance verification

The Security Assessment Report should contain the following: -

- Identification of Auditee (Address & contact information)
- Dates and Locations of security assessment
- 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 Security Assessment Report should comprise the following sub reports: -

- **Security Assessment 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.
- **Security Assessment Report – Core Findings along with Risk Analysis:** The vendor should submit a report bringing out the core findings of the security assessment conducted for network devices, security devices, servers, and websites.
- **Security Assessment Report – Detailed Findings/Checklists:** The detailed findings of the security assessment 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 security assessment 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.

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

Final security assessment report has to be submitted within -15- days of issuance of the initial Draft report after considering the Management comments on the Draft report.

Annexure II- Commercial
(Excluding applicable taxes)

Sr.	Service Type	Name of Application		Total Instances	Commercials (Price) per instance	Commercials (Price) Total Instances
1	Web Application Penetration Testing (Grey-Box)	Structured Financial Messaging System Web Application		1		
2	Vulnerability Assessment & Penetration Testing	SFMS Server – 4 CIMS – 1 CCIL – 1 CCIL/CIMS – 1	Switches – 3 Firewall – 3 SAN Storage – 1 Clients – 4	18		
3	Thick Client Security Assessment	SFMS Signer	NDS-Call	2		
4	IBM MQ Configuration Review	SFMS	CCIL	2		
5	OS Configuration Review	SFMS – 4 CCIL – 1	CIMS – 1 CCIL & CIMS – 1	7		
6	Database Configuration Review	SFMS – 1		1		
7	Firewall & Network Configuration Review	Firewalls – 2	Switches – 2	5		
8	Internal Penetration Testing	Straight-Through Processing Transaction from CBS to SFMS		1		
Total Instances				37		
Grand- Total						
Cost shall include all Travelling, Lodging and other expenses.						

NOTE- *Based upon the frequency, Bank at its discretion can conduct the Security Assessment 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.*