Request for Proposal

For

Information System Audit

&

Vulnerability Assessment and Penetration Testing

of

The HP State Cooperative Bank Ltd. (Scheduled Bank)

Background

The Himachal Pradesh State Cooperative Bank Ltd (HPStCB); a Scheduled Bank, is an Apex Cooperative Bank of HP State of India. HPStCB Ltd is one of the fast growing Banks in India having 218 branches and 23 extension counters spread throughout the state and one branch at Delhi. HPStCB Ltd offers a full range of financial products and services in Himachal Pradesh including deposit taking, electronic banking, term loans and commercial bill acceptances.

The Bank mainly caters to the needs of the farmers through the Cooperative Societies viz. Primary Agriculture Societies, District Federations, Tehsil Unions and Apex Coop. Societies. Apart from this, the Bank also caters to the needs of individuals and govt. employees/ companies.

The Bank is fully CBS and its Data Centre is located at ACSTI, Sangti, Summer Hill, Shimla-5. The Data Recovery Site to the Bank is presently functioning in the Data Centre of ITI Ltd, Doorvaninagar, Bangluru. The Bank intends to conduct IS Audit of its branches and Data Centre from CERT-IN empanelled qualified Auditors. The scope of work has been elaborated as under:

Conducting IS Audit of the Bank: Scope of work

1. Scope of work:-

Scope of work of IS Audit are indicative but not restricted to the following;

(A) Audit of Information Security Architecture & Implementation of Information Security Policy with specific reference to

1. Information Security Organization Structure
2. Roles and Responsibilities
3. Data Classification Policy
4. Software Policy
5. Application Security Policy
6. ATM Application Security
7. Electronic Payment System
8. Password Security Policy
9. Internet Banking Policy
10. Data Centre Security & Monitoring
11. Virus Control Policy
12. Backup Policy
13. Data Centre Policy
14. Networking Internet Security Policy
15. Hardware Policy
16. Physical Security Policy
17. Environment Security Policy
18. Incident Management Policy
19. Business Continuity and Disaster Recovery Plan

(B) IS Audit of key IT Systems and resources:- Network Management & Security Audit:

1. Network admission control
2. Hardening of systems, switches and routers
3. Patch update Management
4. Port based security controls
5. Process control for change management
6. Security incident and management
7. Access control for DMZ application
8. Content filtering for web access and data leakage
9. Net scanning-vulnerability assessment
10. Network admission control, hardening of system, switches routers, port based security control
11. Penetration testing (both internal and external)
12. Password cracking
13. Intrusion detection system testing
14. Router testing
15. Denial of Services testing
16. While doing the penetration test on server in live environment the ISA should be ensured of the system
17. Audit of Network design from security, integrity and availability point of view
18. Audit of setting of Network equipment from security and functionality point of view
19. Evaluation of Firewall policy and its implementation
20. Network of performance testing (including suggestions for increasing the performance)
21. Review of appropriateness of the network topology
22. Review of adequacy or otherwise of the hardware installed
23. Network stress/Load test
24. Network Information Security and Administration (Public Key Infrastructure, Authentication, Access control, operating system controls etc.) of Key Applications Assessment (ATM, Internet Access, Anti-Virus, E-mail, ABB, RTGS, etc.)
25. The Bank's Web-site and server

2. <u>Data Centre- CBS Operations</u>:

1. IS Audit of Data Centre operations for Core Banking System
2. Physical security a) Physical access controls; b) Environment management systems such as electrical supply, UPS, air-conditioning, fire detection and suppression, generator, etc.
3. 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 delivery channels in the case of CBS and other external ATM switches the case of the ATM system) h) Hardening of Operating System.
4. Gap analysis of CBS operations, if any.

3. Application Software- BancMate (CBS and other interfaces, if any)

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

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

1. Compliance with Bank's Disaster Recovery Plan aspects;
2. Log shipping management Review the Disaster Recovery Plan/Procedures documented for Core Banking Solution and its implementation by the prime vendor at the Data Centre and Disaster Recovery Centre.

6- IT Products:

A.) ATM Centre and Card operations and Reconciliation: IS Audit of ATM centre card operational processes with respect to

1. PIN Management
2. Card Management
3. Delivery of ATM cards/ PINs to customers
4. Hot listing of cards
5. Customer dispute resolution
6. Reconciliation within the Bank and with settlement agency/Banks
7. ATM Network Security Architecture Analysis
8. ATM functionality audit
9. ATM Switch
10. ATM Switch Reconciliation
11. Vulnerability analysis of ATM Network
12. Database controls
13. Backup & Recovery
14. Analysis of administrative procedures
15. Outsourcing arrangements
16. ATM sharing arrangements with other Bank and other agencies and compliance thereof

7. Internet/Mobile Banking:

1. To Assess Flaws in Web hosting Software i.e. Security of web server and e Design of the Applications
2. Attempting to guess passwords using password-cracking tools
3. Search for back door traps in the software
4. Attempting to overload the systems using Distributed Denial of Services (DDOS) and Denial of Services (DOS) attacks
5. Attempting penetration through perceivable network equipment/addressing and other vulnerabilities
6. Check Vulnerabilities like IP Spoofing, Buffer Overflows, session hijacks, account spoofing, Frame Spoofing, Caching of web pages, Cross site scripting, Cookie handling, injection flaws
7. Check system of penetration testing and its effectiveness
8. Sniffing
9. 128-bit SSL Certificate & PKI verification
10. Whether solution architecture provides 24X7 availability to customer. If all servers are configured to synchronize time with Central NTP server.
11. To Check whether date and time stamp are appearing correctly on all reports
12. To check whether servers are updated with latest security patches. Remote server Management Software used, Web logic server is up to date, IOS version in Router is vulnerable one.
13. Confirm Rule base in Firewall are configured properly
14. To ascertain IDS is configured for instruction detection, suspicious activity on host are monitored and reported to server, firewall and IDS logs are generated and scrutinized. IP routing is disabled.
15. For changing system parameters whether Maker-Checker concept is followed.
16. Logical Access Controls Techniques viz. Passwords, Smart Cards or Other Biometric Technologies.
17. Proxy Server is issued between Internet and proxy systems.
18. Vulnerabilities of unnecessary utilities residing on Application server.
19. Computer Access, messages are logged and security violations reported and acted upon.
20. Effectiveness of Tools being used for monitoring systems and network against intrusions and attacks.
21. Proper infrastructure and schedule for back up is fixed, testing of back-up data done to ensure readability.
22. Legal issues.
23. Electronic Record is authenticated by Asymmetric Cryptosystem and hash function.
24. Secrecy and confidentiality of Customer preserved.
25. If any cases of unauthorized transfer through hacking, denial of service due to Technological failure is brought.
26. Regulatory and Supervisory issues.
27. Any other items relevant in the case of security.
28. All the guidelines issued by RBI and CERT-IN form time to time relating to Internet Banking Application and Bank's Official Website/Web hosting Software should be adhered to.

8. Apart from above, the auditors shall

1. Check for gaps in controls for Data Loss Prevention Strategy and Anti phishing strategy.
2. Check for gap analysis of Inventory Management of Business IT Asset.
3. Auditors shall check IT Architecture / framework for security compliance.

4. Check for gap in cyber intrusion plan and preventing access to unauthorised software.
5. Check for gaps in environmental controls, network management and security.
6. Check for gaps in secure configuration, anti-virus and patch management and user access control and management.
7. Check for gaps in Backup and restoration management, data leak and prevention strategy.

SCOPE OF WORK (VAPT)

Security and compliance Audit

1. CBS Application Assessment (all layer) should be done as per latest CERT -IN guidelines including but not limited to the following:
   - SQL Injection
   - Broken Authentication and Session Management
   - 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

2. THE AUDITOR shall perform security audit of the DC as per the Guidelines issued by the CERT-In/ Miety Govt. of India, and provide recommendations to the Bank so as to ensure integrity, confidentiality and availability of information and resources.
3. THE AUDITOR shall conduct the vulnerability assessment & penetration testing on the identified components and share the results with the bank in the form of a report and certificate which may be shared with regulators.
4. THE AUDITOR would review the policy of granting access to the HPSCB DC / network.
5. THE AUDITOR would one time conduct vulnerability and penetration testing.
6. THE AUDITOR Audit will also include the following:
   a. Vulnerability Assessment
   b. Penetration Testing
   c. Network Management Review (If any)
   d. Helpdesk Management Review
   e. HPSCB DC Administration Review (if any)
   f. Network Security Audit

g. Software vulnerability (If any)
h. Audit of Web, Application and DB Server.

Review of IT infrastructure from the point of view of Information/Cyber Security

THE AUDITOR shall:

1. Review of the Current Security Architecture and Security Technology of the organization.
2. Review best practices for server's OS, Web application, Database, Security Devices, Network Devices, Desktops, Laptops, Mobile devices etc.
3. Would identify network and design architectural weaknesses in term of security, performance, scalability, etc.
4. Review of Information / Cyber Security Incident management system.
5. Prepare Information / Cyber Security Risk Assessment Metrics.
6. Shall provide recommendations to increase the effectiveness of the security controls.

THE AUDITOR Deliverables (IS Audit and VAPT)

1. Audit Framework Design
2. Security and Compliance Audit Report
3. Vulnerability assessment and penetration testing. The final Report with Summary should include: Identification of vulnerabilities, Evaluation of potential risks, Prioritization of risks as per CERT-IN guidelines.

Price

The CERT-IN empanelled agencies shall quote the price for conducting IS Audit in attached Annexure-A. Applicable taxes are required to be quoted in the designated column. The rates will be applicable for a period of three years.

Period of validity

The rate quoted shall be valid for a period of three years.

Submission of Bids/quotes

The quotes/bids should be submitted in sealed envelope on the address given below:

General Manager (Banking)
The HP State Cooperative Bank Ltd.

No. 1, Bank Building, Head Office
The Mall Shimla-171001

Only one bid/quote per service provider will be permitted.

Acceptance of terms

A recipient will be deem to have accepted the terms of this document. The auditing firm should be in the CERT-IN list of empanelled vendors. The envelope containing the bid should be sealed and should be marked **'Bid for IS Audit 2022'.**

Process time frame

The following is the time frame for overall selection process:

Description	**Due date**
Issue bid notification	15.06.2022
Bid submission	30.06.2022 till 11.00 AM
Bid opening	30.06.2022 at 2.30 PM

Duration of Audit

The entire audit should be completed within 20 days from the date of receipt of letter of empanelment.

Payment

The payment shall be made on production of bill after IS audit of the branches or Data Centre is completed and report of the same is submitted to Head Office of the Bank. No advance payment shall be made.

Indemnity

The bidder shall indemnify bank and keep indemnified against any loss or damage by executing as instrument to the effect on Non-Judicial Stamp paper that bank may sustain on account of violation of trade mark, data leak, theft etc. by the bidder.

Bid evolution criteria

Only commercial bids will be evaluated. The service provider quoting lowest rate will be awarded the work. Bank reserve the right to split the various assignments to different service provider if they quote the same rates. However, the bank shall have the right to negotiate the price with the lowest bidder before awarding the work. It may be noted that bank will not entertain any price negotiation with any other bidder till the least price bidder declines to accept the offer.

Confidentiality

Except as otherwise expressly provided in the text of engagement letter, one party receiving confidential information in connection with the provision of the services shall not disclose such confidential information outside of its organization or use it for any purpose other than in connection with the services. Confidential information means all information in which a party has rights that is not generally known to the public and that under all the circumstances should reasonably to be treated as confidential or proprietary, whether or not material is specially marked as confidential. Notwithstanding the foregoing, confidential information does not include the information that (i) is, as of the time of its disclosure, or thereafter becomes, part of the public domain through a source other than the receiving party (ii) was known to the receiving party as of the time of its disclosure (iii) is independently developed by the receiving party without reference to the confidential information or (iv) is subsequently learned from a third party not known by the receiving party to be subject to an obligation of confidentiality with respect to the information disclosed.

Agreement

Selected bidder shall sign an agreement with the Bank immediately on the award of the work.

Disputes

Disputes concerning the interpretation or validity shall be decided by arbitrator. The executing agency shall have to become "B" Class nominal member of the bank. Both the parties shall endeavor to resolve any problem or variance resulting from interpretations of application of this contract in the spirit of cooperation and mutual interpretation. In the event of any dispute arising out or relating to this, the same shall be referred to Arbitration under Section 72,73 of the HP State Cooperative Societies Act, 1968 (Act 3 of 1969) to Registrar, Cooperative Societies, HP and his decision will be final and binding on the parties.

Other terms and conditions

- The IS Auditor(s) empanelled shall furnish all type of certificates or declaration, if demanded by statutory/ regulatory agencies, of the period of audit to the Bank on demand.
- Roadmap for conducting Audit as per the scope should be submitted by the bidders.
- The IS auditor(s) shall conduct gap analysis vis-à-vis IS Policy framed by the bank and current best practices during the course of IS audit of the Data Centre and the branches.
- The VAPT of all branches through remote access from any of our locations shall be conducted. Audit of processes/best practices may be checked in a sample of branches located near our HO i.e. at Shimla.
- There is possibility of rolling over of DR Site into main Data Centre of the Bank or vice versa. Hence, rates should be quoted keeping in view of that situation.
- The Agencies intending to participate for quoting rates shall have the option to visit our branches, Data Centre or Data Recovery Site.
- The auditor(s) empanelled by the Bank shall mandatorily provide a copy of registration and proof of empanelment validity date with CERT-IN.

- The bid is competitive Bid evaluation criteria are to be defined by the Bank.
- And Bank will be the final authority for evaluation and no clarification will be provided to bidder for evaluation and selection process. Sub-Contracting is not allowed without prior permission from the Bank. If permitted, the selected bidder should notify the Bank, in writing, of all subcontracts awarded under the Contract & subcontractors shall comply with the provisions of bidding document and/ or CERT-IN/ Miety Govt. of India guidelines. Bank may reject any bid without assigning any reason and bank's decision will be final and binding on all matter relating to bidding process.
- Payment will be made after submission of original bill by THE AUDITOR after submitting the report to the Bank.
- The bidder will submit Document for CERT-IN empanelment which is valid on the day of submission of bid.
- The selected Auditor shall not outsource any component of scope of work to any other vendor/company without prior written approval of the Bank.

-000-

Annexure-A

Bid format

Comprehensive IS Audit covering above mentioned scope of work.

Name of company/ Firm	Nature of work	Fees (A)	Taxes (B)	Total (A+B)
	Comprehensive IS Audit			
	VAPT			
	Total			

Note: L-1 shall be decided based on total rates quoted for comprehensive IS Audit and VAPT.