



The Kangra Central Cooperative Bank Ltd
Dharamshala
H.P. 176 215

RFP Notice Number KCCB/VAPT/ISD/2022/01

Request for Proposal

Vulnerability Assessment and Penetration Testing
(VAPT)

Document Cost Rs 5,000/-

IMPORTANT DATES AND CONTACT INFORMATION

Sr. No	Description	Schedule
1	Date of commencement of Bidding Process (Posting of Advertisement of Tender on Bank's Web Site and print media)	10.12.2022
2	Last date and time for receipt of written queries for clarification from bidders	16.12.2022 upto 5:00PM (only through email id: isd@kccb.in)
3	Last Date and Time for Bid Submission	27.12.2022 upto 01:00 PM
4	Date and Time of Technical Bid Opening	27.12.2022 at 3:00 PM
5	Name, Address and email for Communications	The Kangra Central Cooperative Bank Ltd. IS Division, HO Dharamsala, Distt Kangra HP. 176215. email: isd@kccb.in
6	Place for Technical Bid Openings	The Kangra Central Cooperative Bank Ltd. HO Dharamsala, Distt Kangra HP. 176215.

RFP TERMINOLOGY

DEFINITIONS - Throughout this RFP, unless inconsistent with the subject matter or context:

- **The Bank:** The Kangra Central Cooperative Bank Limited, Dharamshala H.P. 176 215.
- **Bidder/Service Provider/Audit Firm** – A CERT-IN empanelled eligible entity/firm submitting a Proposal/Bid in response to this RFP.
- **Supplier/Audit Firm** – Selected Bidder/Audit Firm under this RFP.
- **Bank/Purchaser/KCCB** – Refer to the “Bank”, “KCCB” and “Purchaser” shall be determined in context and may mean without limitation “*The Kangra Central Cooperative Bank Ltd*”.
- **Proposal/Bid** – The Bidder’s written reply or submission in response to this RFP.
- **RFP** – The request for proposal (this document) in its entirety, inclusive of any addenda that may be issued by the Bank.
- **Services/Work/VAPT** – “Services” or “Work” or “VAPT” means all services, scope of work and deliverables to be provided by a Bidder as described in the RFP and include VAPT and other obligation of the Supplier covered under the RFP.
- **ITB** – Mean Instructions To the Bidder.
- **CERT-IN** – Indian Computer Emergency Response Team.

TABLE OF CONTENT

Para No	Particulars	Page #
1	NOTICE INVITING TENDER	6
2	THE MAIN OBJECTIVE OF THIS RFP	6
3	SCOPE OF WORK	6
4	INSTRUCTIONS TO BIDDERS	9
4.1	Schedule of Tender	9
4.2	Procedure for Submission of Bids	9
4.2.1	Tender Fee & Earnest Money Deposit	10
4.2.2	Technical Bid	11
4.2.3	Commercial Bid	11
4.2.4	Copy of Technical Bid	11
4.2.5	Copy of Commercial Bid	11
4.3	Cost Incurred with tendering	11
4.4	Amendment in Tender Document	11
4.5	Language of Bids	12
4.6	Bid currency	12
4.7	Validity	12
4.8	Modification and Withdrawal	12
4.9	Bid Evaluation Process	12
5	BIDDER'S QUALIFICATIONS	13
5.1	General Criteria	13
5.2	Specific Criteria	13
6	TERMS & CONDITIONS OF THE TENDER	14
6.1	General Conditions	14
6.2	Completion Period	16
6.3	Responsibilities of the Bidder	16
6.4	Responsibilities of the Bank	16
6.5	Delivery and Payment Terms	16
6.6	Earnest Money	17
6.7	Penalties	17
6.8	Performance Guarantee	17
6.9	Termination	17
6.10	Indemnity	18
6.11	Confidentiality	18
6.12	Compliance to laws in India	18
6.13	Limitation of Liability	18
6.14	Force Majeure During the Pendency	18
6.15	Arbitration	18

6.16	Applicable Laws & Jurisdiction of Courts	19
------	--	----

ANNEXURES

1	Bid Covering letter Proforma	20
2	Proforma Technical Bid	22
3	Proforma Commercial Bid	24
4	Details of Servers, Networking Equipment's etc	25
5	Non-Disclosure Agreement	26
6	VAPT Agreement	29

1. NOTICE INVITING TENDER

The Kangra Central Co-Operative Bank Limited, Dharamshala is a DCCB currently operating in five districts of Himachal Pradesh viz Kangra, Hamirpur, Una, Kullu and Lahaul & Spiti with its head office at Dharamshala and a network of 18 Zonal Offices, 216 Branches and 12 Extension Counters. The Bank has its Data Center at Dharamshala and Disaster Recovery Site at Bengaluru. The Bank is a direct member of National Financial Switch since 2014. The Bank is fully computerized and networked in order to achieve the effective and efficient customer services and back-office operations.

The Kangra Central Cooperative Bank Ltd (KCCB) intends to select CERT-IN (Indian Computer Emergency Response Team) empanelled auditors for undertaking the process of Vulnerability Assessment and Penetration Testing (VAPT). The objective of the assessment will be to determine the effectiveness of the security of organization's infrastructure and its ability to withstand an intrusion attempt. The security assessment should use the industry standard penetration test methodologies (like OSSTMM, ISSAF etc.) and scanning techniques and will focus on applications. The application tests should cover but not limited to OWASP Top 10 attacks.

Hence bank invites technically complete and commercially competitive proposals from CERT-IN empanelled IS auditors.

2. THE MAIN OBJECTIVE OF THIS RFP:

The main objective of this RFP will be as follows:

- i. To have an external examination of the IT Security to ward off risks in the IT **Domain by arranging a VAPT through a professional agency.**
- ii. To comply with RBI Circular no: DCBR.BPD.(PCB/RCB) Cir. No. 6/19.51.026/2015-16,dated November 05, 2015.
- iii. To determine effectiveness of planning and oversight of IT activities in the bank.
- iv. To evaluate adequacy of operating processes and internal controls.
- v. To identify the areas with deficient internal controls, recommend corrective action to address deficiencies and follow-up, to ensure that the management effectively implements the required actions.

3. SCOPE OF WORK:

The Vendor would be required to provide services broadly in following categories:

- Planning & Technical Assessment
- Execution
- Interim Reporting and Post execution activities.
- Retesting
- Final Report Submission

- 3.1. The scope of the activity can be enhanced and/or repeated as per requirements of Bank. Initially Bank proposes VAPT to be conducted for IT assets in Data Center, Disaster Recovery Center & Branch Offices but subsequently, intends to repeat the activity one or more times within a year. The selected vendor will have to conduct audit/ s according to the periodicity fixed by the bank, from time to time, at the accepted price, during the period of one years from the date of acceptance of purchase order. At present the periodicity is 'half yearly'. The dates and duration of each audit to be conducted shall be fixed on mutual agreement.
- 3.2. Vulnerability Assessment and Penetration Testing should cover the Bank's Information System Infrastructure which includes Networking systems, Security devices, Servers, Databases, Applications Systems accessible through WAN, LAN as well as with public IP's, websites maintained at Bank's premises Data Centre. This will include identifying existing threats if any and suggest remedial solutions

and recommendations of the same to mitigate all identified risks, with the objective of enhancing the security of Information Systems. VAPT should include:

- 3.2.1. Attempting to guess passwords using password-cracking tools.
- 3.2.2. Search for back door traps in the programs.
- 3.2.3. Malware scanning, OS finger printing, war dialing, Man in middle attack and Man in the browser attack.
- 3.2.4. Port scanning of the servers, network devices and security devices/applications.
- 3.2.5. Network traffic observation for important and confidential information like username, password flowing in clear text.
- 3.2.6. Comprehensive scanning of all IP address ranges in use to determine vulnerabilities that may exist in network devices & servers and to audit all responses to determine if any risks exist.
- 3.2.7. Check for the known vulnerabilities in the Operating Systems and applications like Browser, E-Mail, Web Server, Web Application Server and FTP etc.
- 3.2.8. Check for unnecessary services/ applications running on network devices/ servers/ workstations.
- 3.2.9. Unauthorized access into the network and extent of such access possible.
- 3.2.10. Unauthorized modifications to the network and the traffic flowing over network.
- 3.2.11. Review of specific controls against Web Defacing and uploading of Trojan/ Virus/ Malware/ Spyware etc. on various servers and further spread of the same to clients/connected machines.
- 3.2.12. Attempt to overload the System using Distributed Denial of Service (DDoS) & Denial of Service (DoS) attacks.
- 3.2.13. Check if commonly known holes in the software, especially the browser and the e-mail software exist.
- 3.2.14. The penetration testing may also be carried out by engaging outside experts (often called 'Ethical Hackers').
- 3.2.15. Checking for the other common vulnerabilities like IP Spoofing, Buffer overflows, Session hijacks, Account spoofing, Frame spoofing, Caching of web pages, Cross-site scripting, Cookie handling etc.
- 3.2.16. Control over network access points.
- 3.2.17. Possibility of traffic route poisoning.
- 3.2.18. Test for directory Traversal.
- 3.2.19. Test for insecure services such as SNMP.
- 3.2.20. Check for vulnerabilities based on version of device/server.
- 3.2.21. Test for SQL, XSS and other web application related vulnerabilities.
- 3.2.22. Check for weak encryption.
- 3.2.23. Check for SMTP related vulnerabilities.

- 3.2.24. Check for strong authentication scheme.
- 3.2.25. Test for sample and default applications/pages.
- 3.2.26. Check for DNS related vulnerabilities.
- 3.2.27. Test for information disclosure.
- 3.2.28. Remote code execution.
- 3.2.29. Weak SSL Certificate and Ciphers.
- 3.2.30. Missing patches and versions.
- 3.2.31. Check if vulnerability exist in the Servers, Database, Application, Network and security device in scope without disturbing operations.
- 3.2.32. If any change in “Scope of Work” is necessitated for the subsequent audits, the Bank has the right to change the same
- 3.2.33. VAPT should cover all Servers and Networking equipments at Data Centre, DR Site and other locations, the details of which are given in ANNEXURE - IV
- 3.2.34. Locations covered in VAPT are Dharamshala and Bengaluru and other centres, if any, mentioned in ANNEXURE - IV.
- 3.2.35. During the course of conduct of the audit, if the bank desires, the successful bidder shall conduct the audit in the presence of the Bank’s IT/ IS Audit officials nominated by the Bank and shall familiarize them with the audit processes/ applications/ tools with explanations, discussions, materials and hands-on training to the satisfaction of the Bank.
- 3.2.36. Further The KCCB expects an authenticated type but non-destructive vulnerability assessment to be carried out. Bidder should be able to cover a broad range of systems like Operating system (Windows, Red Hat Linux etc.), Databases (MySQL, Oracle etc.), Web servers (Apache Tomcat, IIS etc.), Network devices (Routers, Switches, Gateway, Proxy etc.), Security devices (Firewall, IDSs, IPSs etc.).

- 3.3. **ASSESSMENT OF OS HARDENING:** Bidder shall carry out the assessment of OS hardening to check & explore the gap in hardening, patch management etc.

The scope defined above is however illustrative and not exhaustive. Bidders are expected to update and include additional relevant items in these activities to conform to global best practices and currently available knowledge base. The scope may also undergo changes/updates due to implementation of new products, projects, configuration requirements, business needs, legal and regulatory requirements etc. At present the available applications/products for VAPT are CBS, ATM Switch, Internet Banking, IMPS, Mobile Banking and various NPCI Products.

Penetration testing should be according to prevailing RBI Guidelines, IT Act and other applicable regulations in India.

4. INSTRUCTIONS TO BIDDERS

The Bidder is expected to have read and examined all the instructions, forms, terms and Scope of Work in the Tender Document with full understanding of its implications. Failure to furnish all information

required in the Tender Document or submission of a bid not substantially responsive to the Tender Document in every respect will be at the Bidder's risk and may result in outright rejection of the bid.

The Bidders are advised to strictly adhere to the proformas provided for that purpose in this document. Any deviation in this matter will lead to disqualification of the Bid.

4.1. SCHEDULE OF TENDER

4.1.1. The Tender Document will be available from <http://www.kccb.in> on 10.12.2022 at 10:00AM. The Bidder intends to compete may download it.

4.1.2. The prospective bidders may raise queries/clarifications through email on email Id isd@kccb.in on or before 16.12.2022 up to 5:00PM Any modification to the Tender Document, which may become necessary as a result of the queries/clarifications raised, shall be made by the Bank explicitly through the issue of an Addendum.

4.1.3. The sealed bids will be accepted till 01:00 pm on 27.12.2022. The Bank may at their discretion extend the bid submission date, if required. The modified target date & time will be notified on the web site of the Bank.

4.1.4. The Technical Bids will be opened at 3:00 pm on 27.12.2022. The Bidders or their authorized representatives may be present if they so desire.

4.1.5. The Commercial Bids of only technically qualified Bidders will be opened at a date Announced by the Bank at the time of opening of the Technical Bids. The Bidders who have been declared eligible after evaluation of the technical bids or their authorized representatives may be present if they so desire.

4.1.6. The address for all the above activities is:

The Kangra Central Cooperative Bank Limited,

Sehkar Jyoti Building, Civil Lines,

HO DHARAMSHALA. H.P., 176215.

PHONE 01892-222269 Ext.301

<http://www.kccb.in/> E-mail: isd@kccb.in

4.2. PROCEDURE FOR SUBMISSION OF BIDS

- i. It is proposed to have a two-bid system (Technical and Commercial) in five separate sealed covers for this tender.
 - a) Earnest Money Deposit & Tender Fee.
 - b) Technical Bid.
 - c) Commercial Bid.
 - d) Copy of Technical Bid.
 - e) Copy of Commercial Bid.

Please note that rates should not be indicated in the Technical Bid. Only Commercial Bid should indicate rates.

- ii. All the documents viz. Earnest Money Deposit, Tender Fee, Technical Bid and Commercial Bid prepared and sealed as hereinafter directed along with the Bid Covering Letter as per the proforma given in ANNEXURE-I post typed and signed on the Bidder's letterhead are to be kept in a single sealed cover super-scribed with your reference number, date of submission

and the words “**RFP for Vulnerability Assessment and Penetration Testing, due on 27.12.2022 upto 01:00pm NOT TO BE OPENED BEFORE TIME**”.

- iii. The cover thus prepared should also indicate clearly the name and address of the Bidder, to enable the Bid to be returned unopened in case it is received after the specified date and time.
- iv. The Bid shall be in the prescribed format and shall be signed by the Bidder or a person duly authorized to bind the Bidder to the contract. Relevant certificates / documents should be attached.
- v. All pages of the bid except un-amended printed literature shall be initialled by the person(s) signing the Bid. The bid shall contain no interlineations, erasures or over writing except as necessary to correct errors made by the Bidder, in which case such corrections shall be initialled by the person(s) signing the bid.
- vi. The Bids prepared by the Bidders shall thus comprise of following components:
 - a) Earnest Money Deposit, Tender Fee and Covering Letter neatly typed on the letterhead of the Bidder and duly signed by the authorized signatory in the proforma given in ANNEXURE-I and kept in a sealed cover super-scribed “EARNEST MONEY, TENDER FEE & COVERING LETTER” as detailed in Section 4.2.1 below.
 - b) Technical Bid, as directed below in Section 4.2.2 below and kept in a sealed cover super- scribed “TECHNICAL BID”.
 - c) Commercial Bid, as directed below in Section 4.2.3 below and kept in a sealed cover super-scribed “COMMERCIAL BID”.
 - d) Xerox copy of the technical bid without any cuttings, erasures or modifications, as directed below in Section 4.2.4 and kept in sealed cover super-scribed “COPY of TECHNICAL BID”.
 - e) Xerox copy of the commercial bid without any cuttings, erasures or modifications, as directed below in Section 4.2.5 and kept in sealed cover super-scribed “COPY of COMMERCIAL BID”.

4.2.1. TENDER FEE & EARNEST MONEY DEPOSIT:

- i. The Bidder shall deposit Rs. 5,000/- (Rupees Five Thousand Only) in the form of a Demand Draft favoring Managing Director, The Kangra Central Cooperative Bank Limited payable at Dharamshala being the **cost of the tender document/tender fee** along with the Bid. Payment made through any other mode will not be accepted and decision of the Bank in this regard shall be final, conclusive and binding on the Bidder.
- ii. The Bidder shall furnish, as part of its bid, **bid security** of an amount equal to Rs.50,000/- (Rupees Fifty Thousand Only). The bid security is required to protect the Bank against the risk of Bidder's conduct.
- iii. The bid security shall be denominated in the INDIAN RUPEES only and shall be in the form of a Demand Draft issued by an Indian Bank not earlier than the date of issue of this Tender, payable to The Managing Director, The Kangra Central Cooperative Bank Limited at Dharamshala, H.P. Any bid not secured in accordance with the above will be rejected as non-responsive.

- iv. Unsuccessful Bidder's bid security will be returned as promptly as possible but not later than 30 days after the expiration of the period of bid validity prescribed by the Bank.
- v. The successful Bidder's bid security will be discharged upon the Bidder signing the contract and furnishing the performance guarantee.
- vi. The bid security may be forfeited:
 - a. If a Bidder withdraws its bid during the period of bid validity, Or
 - b. If a Bidder makes any statement or encloses any form which turns out to be false, incorrect and or misleading at any time and / or conceals or suppresses material information, Or
 - c. In case of the successful Bidder, if the Bidder fails to sign the agreement or to furnish performance guarantee.

4.2.2. TECHNICAL BID:

- i. Technical bid proposal should be as given in ANNEXURE - II post, neatly typed on the letterhead of the Bidder, duly filled in, signed and complete in all respect. The Technical Bid should be submitted in a bound form and all pages continuously and serially numbered in one lot as one document. Supporting documents / Certificates etc. should be submitted in the bound document and not in a loose form. Bidders must ensure that all the documents are sealed and signed by the authorized signatory.
- ii. The Technical Bid submitted in response to this Tender Document along with the supporting material, will become the property of the Bank.

4.2.3. COMMERCIAL BID:

- i. Bid Rates for the fine-tuned VAPT neatly typed on the letter head of the Bidder, duly filled in, signed and complete as per the Prescribed Quotation Proforma as given in ANNEXURE -III.
- ii. The L1 Bidder shall be arrived at by considering the consolidated rate quoted in the Proforma Commercial Bid as given in ANNEXURE - III.

4.2.4. COPY OF TECHNICAL BID: Xerox copy of unmodified Technical Bid (exact replica) but duly signed and sealed.

4.2.5. COPY OF COMMERCIAL BID: Xerox copy of unmodified Commercial Bid (exact replica) but duly signed and sealed.

4.3. COSTS INCURRED WITH TENDERING

The Bidder shall bear all costs associated with the preparation and submission of its Bid, including cost of presentation for the purposes of clarification of the Bid, if so desired by the Bank and the Bank will in no case be responsible or liable for those costs, regardless of the conduct or outcome of the tendering process.

4.4. AMENDMENT IN TENDER DOCUMENT

- i. At any time upto the last date of receipt of Bids, the Bank may, for any reason, whether at its own initiative or in response to a clarification requested by a prospective Bidder,

modify the Tender Document by an amendment. All such amendments shall be binding on all the Bidder's.

- ii. In order to afford prospective Bidder's reasonable time to take the amendment into account in preparing their Bids, the Bank may, at its discretion, extend the last date for the receipt of Bids.

4.5. LANGUAGE OF BIDS

The Bids prepared by the Bidder and all correspondence and documents relating to the Bids exchanged by the Bidder and the Bank, shall be written in the English Language, provided that any printed literature furnished by the Bidder may be written in another language so long as it is accompanied by an English translation in which case, for purposes of interpretation of the Bid, the English translation shall govern.

4.6. BID CURRENCY

The prices in the bid document shall be expressed in Indian Rupees only.

4.7. VALIDITY

Bids shall remain valid for 90 days from the last date of submission. The Bidders may be required to give consent for the extension of the period of validity of the bid beyond initial 90 days, if so desired by the Bank in writing or by email. Refusal to grant such consent would result in rejection of bid without forfeiture of the EMD. However, any extension of validity of bids will not entitle the Bidder to revise / modify the bid. The decision of the Bank in this behalf will be final, conclusive and binding on the Bidder.

4.8. MODIFICATIONS & WITHDRAWAL

The bid submitted may be withdrawn or resubmitted before the expiry of the last date of submission by making a request in writing to the Managing Director of the Bank to this effect. No Bidder shall be allowed to withdraw the bid after the deadline for submission of bids.

4.9. BID EVALUATION PROCESS:

Bid evaluation process will be as follows: -

- i. After opening of the technical bids, all the documents and annexure (except commercial documents/offer) will be evaluated first by the Bank. The Bank will determine to its satisfaction whether the bidder selected as having submitted the best evaluated responsive bid is qualified to satisfactorily perform the contract. The decision of Bank will be final in this regard.
- ii. The determination will take into account bidder's financial, technical and support capabilities, based on an examination of documentary evidence submitted by bidders.

Technical Evaluation: The Bank will examine the bids to determine whether they are complete, whether required information have been provided as underlined in the bid document, whether the documents have been properly signed, and whether bid documents are generally in order. Compliance to Bidder's Qualification Criteria stipulated in Section 5 of the Tender. Review of written reply, if any, submitted in response to the clarification sought by the Bank only those bidders who satisfy the technical requirements, accept the terms and conditions of this tender document and submit the above certificate shall be short-listed for further evaluation.

Commercial Evaluation: The commercial bids for only those bidders will be opened who have qualified on the basis of technical evaluation and reviewed to determine whether the commercial bids are substantially responsive. Commercial bids that are not substantially

responsive or incomplete in any manner are liable to be disqualified. Evaluation will be done based on prices quoted as mentioned in commercial offer as per ANNEXURE – III.

The bidder offering lowest commercials will be considered as the successful bidder for award of contract.

The Bank is under no obligation to accept the lowest or any other offer received in response to this tender and reserves the right to reject any or all the offers including incomplete offers without assigning any reason whatsoever.

5. BIDDER'S QUALIFICATIONS

Systems Auditing Organisations (Bidder) has to fulfil the eligibility criteria as given below.

The bidder has to submit the supportive documents for the eligibility as per criteria as per ANNEXURE– II for Technical evaluation.

5.1. GENERAL CRITERIA

- i. The Bidder should be a Registered Company in India.
- ii. The Bidder should have ISO 9001/ 14001/ 18001 or any latest ISO certificate.
- iii. The Audit firm/company should have been in existence for at least five years as on 31.03.2022. The Firm will submit a suitable certificate in this regard duly signed by the authorized official with details. Bids without this certificate will not be considered for evaluation and will be rejected.
- iv. The Bidder must have a minimum average turnover of at least Rs.5.00 Crore from IS Audit/ IT Audit/ IT Security Service assignments in the past three years as on 31st March 2020, 31st March 2021, and 31st March 2022.
- v. The bidder firm must have been in profit for last 3 years in succession viz. financial years ending 31st March 2020, 2021 & 2022. The bidder should submit a copy of the full Balance Sheets duly certified as copy of the original by its Auditor for three years ending 31st March 2020, 2021 & 2022 along with qualifying remarks, disclosures, if any made therein.
- vi. The Bidder should not have been blacklisted / debarred by the Government of India or their undertakings/any State Governments or their undertakings or by Banks or any financial institution. In such cases the bid will be summarily rejected and no correspondence in this matter shall be replied by the Bank.
- vii. Bidders not complying with above terms and conditions or not providing complete information as described shall not be considered.
- viii. Organizations who are working in any of Bank's projects at present and/ or already engaged by the Bank as vendor for any software and/ or any hardware/ network/ security components and/ or involved directly or indirectly in implementing/ managing the Security/ Network infrastructure for the Bank are not eligible and proposal received from such Organizations will not be taken for consideration.

5.2. SPECIFIC CRITERIA

- i. The bidder must be a firm of sound repute empanelled with CERT-IN for IT/IS Audit/IS Security Audit/VAPT. Bidder shall produce certificate from CERT-IN in this regard. Bids without this certificate will not be considered for evaluation and will be rejected.

- ii. The bidder should have experience of VAPT, ethical hacking and risk assessment for at least 3 Banks or Financial Institutions (Both Public and Pvt and any cooperative bank) in India with a network of minimum of 250 branches each in the last 3 years in succession viz. financial year ending 31st March 2020, 2021 & 2022. (Statement of such tests conducted in relevant areas to be enclosed.)
- iii. The bidder should have (minimum 5) personnel having both domain and technical knowledge of Banking and IT areas. The technology area of expertise should include IS Audit of Enterprise Data Centre, VA&PT assignments, audit of hardware and software, Networking and Delivery channels, internet banking, Card Products, Treasury and Forex operations including testing and consulting services. Bio-data of personnel, authenticated by authorised official of bidder, to be enclosed.
- iv. The Bidder should have professionals with any of the international accreditation like CISA (Offered by ISACA, USA), CISSP (Certified Information System Security Professional), CCNA (CISCO Certified Network Associate), CEH, CISM, MCSE, CCIE and ISO27001 trained lead auditors employed with them since the last 3 years. The CVs of the professionals to be submitted along with the bid.
- v. The bidder should submit proof in support of all Technical Criteria while submitting the bid proposals. Failing which, the Bid proposal will not be considered for further evaluation and may be treated as technically non-responsive.
- vi. The Bank reserves the right not to consider the bids of vendors for further evaluation who do not meet Qualification Criteria.

6. TERMS & CONDITIONS OF THE TENDER

6.1. GENERAL CONDITIONS

- i. The Bank will neither provide nor shall pay any charges for boarding, lodging and transportation facilities for the Bidder or their Representative.
- ii. The Bidders are required not to impose their own terms and conditions to the bid.
- iii. It is implicit that the Bidder has guaranteed that all the equipment/techniques used to conduct the VAPT are of a very high standard as prevailing in the market.
- iv. The Bidder should cooperate with Bank or any other agency which has been entrusted with or involved in the work of providing and managing other components of the CBS project of the Bank.
- v. The Bidder shall ensure that the services being provided to conduct VAPT shall be in conformity with the requirements of applicable ISO standards, applicable provisions of Information Technology Act, 2000, Reserve Bank of India guidelines and other statutory and regulatory authorities.
- vi. The offer may not be evaluated and may be rejected by the Bank without any further reference in case of non-adherence to the format or partial submission of information as per the format given in the offer.
- vii. The Bidder shall not sublet / assign to anyone, in whole or in part, its obligations to perform under the contract.

- viii. Unless expressly overridden by the specific agreement to be entered into between the Bank and the bidder, the tender shall be the governing document for agreement between the Bank and the bidder.
- ix. The Bank reserves its right to cancel the order in the event of one or more of the following situations that are not occasioned due to reasons solely and directly attributable to the Bank alone.
- x. **Single Point of Contact:** The Bidder has to provide details of single point of contact viz. designation, address, telephone / mobile number.
- xi. The Bidder will have to hand over all the IT Infrastructure in 100% working condition on the termination or end of the contract. Any defect / breakdown call that has been reported before the termination of the service contract shall have to be corrected by the Bidder before handing over.
- xii. The Bank may continue the service contract with the existing Bidder for the subsequent years also at the same terms, conditions and SLA. However, Bank reserves the right to make amendments to the terms and conditions of the contract and renegotiate the rate at the time of renewal of the contract.
- xiii. It will not be obligatory for Bank to continue the service agreement if deficiency in service on part of the existing Bidder evaluates to a penal charge of more than 10% of the total value of contract. In such case, Performance guarantee will be forfeited.
- xiv. The Auditing team of Bidder shall invariably carry their ID cards with them, without which, the said representative(s) will not be allowed to access the systems.
- xv. The Auditing team of the Bidder shall have access to the computer systems / peripherals only after obtaining clearance of Bank's authorized officials. No data / log information will be taken out of Bank without clearance from Bank's authorized officials.
- xvi. The Bidder should not issue press release or public announcements etc. in this regard without prior permission of the Bank.
- xvii. Acceptance or rejection of bid: The Bank reserves the right to accept any bid, or to reject a particular bid at its sole discretion without assigning any reason whatsoever.
- xviii. The present RFP is for engaging the services of Information Security Auditor for a period of one year for undertaking various Audit/ Security jobs, as per the scope of work defined by the Bank. The selected IS Audit/ Security firm will be on the panel for a period of one year and the Bank may utilize its services for undertaking such IS Audit/ Security activities.
- xix. The Bank reserves the right to cancel the engagement without assigning the reason whatsoever.
- xx. The Bank reserves the right to audit the VAPT process by external empaneled Auditors appointed by the Bank/ inspecting official from the Reserve Bank of India or any regulatory authority, covering the risk parameters finalized by the Bank/ such auditors in the areas of products (IT hardware/software) and services etc. provided to the Bank.

- xxi. The Bank can make its expert assessment on the efficiency and effectiveness of the security, control, risk management, governance system and process created by bidder. The bidder shall, whenever required by the Bank/ Auditors, furnish all relevant information, records/data to auditors and/or inspecting officials of the Bank/ Reserve Bank of India and or any regulatory authority. Where any deficiency has been observed during audit based on the risk parameters finalized by the Bank or in the report submitted by the Auditors, the bidder shall correct/ resolve the same at the earliest and shall provide all necessary documents related to resolution thereof and the auditor shall further certify in respect of resolution of the deficiencies.
- xxii. The Bank reserves the right to retain any relevant material information/ reports including audit or review reports (e.g. financial, internal control and security reviews) and findings made.

6.2. **COMPLETION PERIOD:** The said project shall be completed within six weeks from the date of issue of award letter.

6.3. RESPONSIBILITIES OF THE BIDDER

- i. The bidder is responsible for managing the activities of its personnel and will hold itself responsible for any misdemeanors.
- ii. The bidder will treat as confidential all data and information about the Bank, obtained in the execution of his responsibilities, in strict confidence and will not reveal such information to any other party without the prior written approval of the Bank.
- iii. All the bills raised for the supplies/ services made under this RFP shall be from the same Office/Branch from where the bids are submitted against this RFP. If billing being done from any other branch of the bidder, same is to be clearly mentioned in the Bid and should not change till validity of the contract expires.
- iv. Selected Bidder shall hold the Bank, its successors, Assignees and administrators fully indemnified and harmless against loss or liability, claims actions or proceedings, if any, that may arise from whatsoever nature caused to the Bank through the action of its employees, agents, contractors, subcontractors, etc. However, the Selected Bidder would be given an opportunity to be heard by the Bank prior to taking a decision in respect of such loss or damage.

6.4. RESPONSIBILITIES OF THE BANK

- i. The Bank shall provide appropriate space to the engineers performing the VAPT. On day-to-day basis the officials of the Bank shall help the engineers deputed by the Bidder for the job in their capacity.
- ii. The Bank shall provide appropriate environmental conditions, necessary power facilities for the system, and necessary access of its network/systems to the deputed engineers of the bidder.

6.5. DELIVER AND PAYMENT TERMS

- i. Payments will be released from our office within 30 days of claim after satisfactory completion of the audit, upon – Submission of Claim/ Invoice by the vendor.
- ii. Arranging for a presentation/ discussion on the final findings of VAPT with the officials of Bank's Department of Information Technology (DIT) at Head Office Dharamshala by deputing a senior official.

- iii. Submission of Final Audit Report (hard copy and soft copy) including reports mentioned under 'Scope of Work' by the vendor to Bank's Inspection Department and Department of Information Technology (DIT) at Head Office Dharamshala.
- iv. Vendor has to submit complete set of documents/ invoices/ audit reports for each audit.

6.6. EARNEST MONEY: Earnest Money @ Rs. 50,000/- (Rupees fifty thousand Only) should be submitted along with the Tender in the form of Demand Draft payable in favour of the Managing Director, The Kangra Central Cooperative Bank Limited at Dharamshala. Tenders without Earnest Money shall be out rightly rejected.

6.7. PENALTY: In case of delay in completing the VAPT beyond 45 days from the date of Orders issued by the bank, the Bank reserves the right to impose penalties at the rate of 0.5% of the cost of the assignment per week or part thereof subject to a maximum of 10% of the Total Basic Cost of the Contract value. After that order will be cancelled and PBG will be forfeited. The decision of the Bank in this regard shall be final, conclusive and binding.

6.8. PERFORMANCE GUARANTEE

- i. The successful Bidder(s) within thirty days from purchase order shall furnish a security in the form of bank guarantee @ 10% of the total value of the order to the Bidder, valid for 1 years + 90 days from the date of order, which shall be discharged thereafter.
- ii. Failure of the successful Bidder to comply with the requirement of accepting the purchase order/ executing Contract and/ or submitting Performance Security (BG) shall constitute sufficient grounds for the annulment of the award and forfeiture of the bid security, in which event the Purchaser may make the award to any other next lowest evaluated bidder at the price quoted by bidder or any other price which cannot be more than L2 bidders price. In such an eventuality bank retains the right to call fresh bids under this RFP barring the defaulting bidder.

6.9. TERMINATION:

The Bank reserves its right to cancel the entire/ unexecuted part of the contract, at any time by giving 30 days written notice, without assigning reasons and without prejudice to any other remedy for breach of contract, in the event of one or more of the following conditions:

- i. If the vendor fails to deliver any or all of the Services within the period(s) specified in the Contract or within any extension thereof granted by the Purchaser (Bank).
- ii. If the vendor fails to perform any other obligation(s) under the Contract.
- iii. Delay in conducting the audit/ s beyond the specified periods.
- iv. Non satisfactory performance of the Project during implementation.
- v. Failure to integrate/ implement the project as per the requirements of the Bank.
- vi. Serious discrepancies noted in the implementation of the project.
- vii. Breaches in the terms and conditions of the Purchase Order.
- viii. Non satisfactory performance of the Project in terms of affecting the Core Systems of the Bank or the Core Business of the Bank and the functioning of the Branches/ Offices of the Bank.

6.10. INDEMNITY

The Bidder shall indemnify, protect and save the Bank against all claims, losses, costs, damages, expenses, action suits and other proceedings, resulting from infringement of any law pertaining to patent, trademarks, copyrights, etc.

6.11. CONFIDENTIALITY

As the successful bidder(s) will have access to the data/ information of the bank while auditing the security, Bank will require the bidder(s) to sign a confidentiality/ non-disclosure agreement ANNEXURE -V and VAPT Agreements (ANNEXURE - VI) within 30 days of accepting the Purchase Order, undertaking not to disclose or part with any information relating to the bank and its data to any person or persons, as may come into possession of the successful bidder(s) during the course of Vulnerability Assessment and Penetration Testing.

6.12. COMPLIANCE TO LAWS IN INDIA

- i. The Information Systems/ Security Auditor will undertake to comply with all the prevailing laws and regulations in India relevant for Information Systems Audit.
- ii. The Information Systems/ Security Auditor will also undertake to comply with all the requirements of the guidelines of Reserve Bank of India or other appropriate agencies as regards Information Systems Security Standards issued from time to time.

Note: - Bank reserves the right to inform IBA/ GOI/ RBI in case any major vulnerability is noticed after Security Audit within 6 months from the date of security audit.

6.13. LIMITATION OF LIABILITY : Notwithstanding anything to the contrary contained in the contract, the Bidder's aggregate liability arising out of or in connection with the contract, whether based on contract, tort, statutory warranty or otherwise, be limited to a maximum of 100% of the contract value. The Bidder shall not be liable for any special, indirect, incidental or consequential damages of any kind including but not limited to loss of use, data, profit, income, business, anticipated savings, reputation, and more generally, any loss of an economic or financial nature, whether these may be deemed as consequential or arising directly and naturally from the incident giving rise to the claim.

6.14. FORCE MAJEURE DURING THE PENDENCY : During the pendency of the contract if the performance in whole or part thereof by either party is prevented / delayed by causes arising due to any war, hostilities, civil commotion, act of public enemy, sabotage, fire, floods, explosion, epidemics, non-availability of raw material, and other consumables, or any other causes including breakdown of equipment beyond their reasonable control neither of the two parties shall be made liable for loss or damage due to delay or failure to perform the contract during the pendency of forced conditions provided that the happenings are notified in writing within 7 days from the date of occurrence. The work shall be resumed under the contract as soon as possible after resumption of normalcy.

6.15. ARBITRATION

All disputes, differences, claims and demands arising under or pursuant to or touching the contract shall be referred to the sole arbitrator to be appointed by the Managing Director, Kangra Central Cooperative Bank Limited, Dharamshala, H.P. The award of the sole arbitrator shall be final and binding on both the parties under the provisions of the Arbitration and Conciliation Act, 1966 or by statutory modification/re-enactment thereof for the time being in force. Such arbitration shall be held at Dharamshala.

6.16. APPLICABLE LAWS & JURISDICTION OF COURTS

In all matters and disputes arising here under, shall be governed in accordance with the Laws of India for the time being enforced and will be subject to the exclusive jurisdiction of courts having jurisdiction in Himachal Pradesh.

ANNEXURE - I

(Bid Covering Letter Proforma)

To:
The Managing Director,
The Kangra Central Cooperative Bank Limited,
Dharamshala. H.P.
176 215.

Dear Sir,

Conducting Vulnerability Assessment and Penetration Testing .

1 Terms & Conditions

- 1.1 I / We, the undersigned Bidder(s), having read and examined in detail the specifications and all bidding documents in respect of this Request for Proposal do hereby propose to provide services as specified in the bidding document.
- 1.2 I / We, the undersigned Bidder(s) having submitted the qualifying data as required in your Request for Proposal, do hereby bind ourselves to the conditions of your Request for Proposal. In case any further information/documentary proof in this regard before evaluation of our bid is required, I / We agree to furnish the same on demand to your satisfaction.

2 Rates & Validity

- 2.1 All the rates mentioned in our proposal are in accordance with the terms as specified in bidding documents. All the rates and other terms and conditions of this proposal are valid for a period of 90 days from the date of opening of the bid.
- 2.2 I / We have studied the Clauses relating to Indian Income Tax Act and hereby declare that if any Income Tax, surcharge on Income Tax and any other Corporate Tax is altered under the law, I / we shall pay the same.

3 Deviations

I / We declare that all the services shall be performed strictly in accordance with the Technical specification, Time Schedule and other terms of the Request for Proposal Document. Further, I/We agree that additional conditions, if any, found in the proposal documents, shall not be given effect to.

4 Bid Pricing

I / We further declare that the rates stated in our proposal are in accordance with your terms and conditions in the bidding document.

5 Earnest Money

I / We have enclosed the earnest money as required vide Request for Proposal Document. In case of default, it is liable to be forfeited in accordance with the provisions enumerated therein.

6 Details of cost of RFP Document:

Value	
Demand Draft / Cash Deposit Receipt Number with Date	
Name and Branch of the Bank	

7 Performance Guarantee

I / We shall submit a Bank Guarantee as required in Request for Proposal Document.

8

Declaration

I / We hereby declare that my / our proposal is made in good faith, without collusion or fraud and the information contained in the proposal is true and correct to the best of my / our knowledge and belief and nothing has been concealed there from.

Thanking you,

Yours faithfully,

(Signatures)

Date:

Place:

Name:

Designation:

ANNEXURE - II

(PROFORMA TECHNICAL BID)

Sr. No.	Eligibility Criteria	Support documents to be submitted	Annexure Number to be assigned
1	Bidder's Proposal Reference No. & Date		
2	Bidder's Name & Address		
3	Contact Person Designation Telephone Number Fax Number e-mail Address		
4	Name and Designation of the Person Authorized to make Commitments to the Bank		
5	GST registration copy		Annexure T-0
6	Bidder should be a registered company.	Certificate of incorporation.	Annexure T -1
7	Bidder should have ISO 9001/ 14001/ 18001 or any latest ISO certificate.	Xerox copy of latest Certificate issued	Annexure T-2
8	The Audit firm/company should have been in existence for at least five years as on 31.03.2022	A suitable certificate in this regard duly signed by the authorised official	Annexure T - 3
9	The Bidder must have a minimum average turnover of at least Rs.5.00 Crore from IS Audit/ IT Audit/ IT Security Service assignments in the past three years as on 31 st March 2020, 31 st March 2021, and 31st March 2022	Audited Financial Statements, B/ S	Annexure T - 4
10	The bidder firm must have been in profit for last 3 years in succession viz. financial years ending 31st March 2020, 2021 & 2022.	Audited Financial Statements, B/ S or P&L	Annexure T - 5
11	The Bidder should not have been blacklisted / debarred by the Government of India or their undertakings/any State Governments or their undertakings or by Banks or any financial institution.	Undertaking from the bidder should be enclosed	Annexure T - 6
12	Bidders should be from CERTIN empanelled Information Systems Audit Organizations	Certificate from CERT-IN	Annexure T -7
13	The bidder should have experience of VAPT, ethical hacking and risk assessment for at least 3 Banks or Financial Institutions (Both Public and Pvt and any cooperative bank) in India with a network of minimum of 250 branches each in the last 3 years in succession viz. financial year ending 31st March, 2020, 2021 & 2022.	Xerox copy of Purchase Order or Letter from Banks/ Financial institutions for having conducted VAPT along with Statement of such tests conducted in relevant areas.	Annexure T -8

- | | | | |
|----|---|---|---------------|
| 14 | The bidder should have (minimum 5) personnel having both domain and technical knowledge of Banking and IT areas. The technology area of expertise should include IS Audit of Enterprise Data Centre, VA&PT assignments, audit of hardware and software, Networking and Delivery channels, internet banking, Card Products, Treasury and Forex operations including testing and consulting services. | Bio-data of personnel, authenticated by authorized official of bidder, | Annexure T-9 |
| 15 | The Bidder should have at least 3 professionals with any of the international accreditation like CISA (Offered by ISACA, USA), CISSP (Certified Information System Security Professional), CCNA (CISCO Certified Network Associate), CEH, CISM, MCSE, CCIE and ISO27001 trained lead auditors employed with them since the last 3 years | The CVs of the professionals along with Xerox copies of certificate/ s showing their qualification/s. | Annexure T-10 |

(Signatures)

Date:

Place:

Name:

Designation:

ANNEXURE - III

(Performa Commercial Bid)

Sl.No.	Description / Name of the Project/ Assignment	Cost of ONE VAPT (in Rs.)
1	Vulnerability Assessment & Penetration Testing of CBS Network, Mobile Banking Internet Banking, IMPS, NPCI Products/Services, Equipment's installed in Bank, Web Applications and RTGS/NEFT infrastructure etc., for the Bank (as per Scope of work)	

Notes: The successful bidder has to undertake to conduct the audit strictly as per scope of work.

- The vendor has to quote the above prices excluding taxes.
- GST/Service Tax / VAT, at actual, is payable extra.
- TDS will be deducted as applicable.
- The prices quoted should be valid for one year from the date of acceptance of purchase order.

(Signatures)

Date:

Place:

Name:

Designation:

ANNEXURE - IV

DETAILS OF SERVERS, NETWORKING EQUIPMENTS ETC.

Details of Hardware and Network (Specific details will be provided individually)

Sr.No.	Description of Hardware	OS	Quantity	
			At DC	At DRC
1	Servers, Systems, web servers like IIS, Apache etc. (Specific details will be provided individually to selected firm)	RHEL, Windows, Centos, IIS, Apache etc	'40+	'5+
2	SAN switch		2	2
3	SAN Storage		2	1
4	Network & Security Devices (Routers, Switches, Modems, Firewalls, Load balancers, IPS, HSM, KVM, IDS)		'15+	'5+
5	Seperate routers/switches & modems in all branches : '230+			
6	Databases 60+			
7	No of web pages 1500+			

Annexure - V

(NON DISCLOSURE AGREEMENT)

This Agreement is made as of the day of 2022, between....., a company registered under the Companies Act, 1956 and having its Head Office and The Kangra Central Cooperative Bank Ltd , a banking entity incorporated and functioning under the provisions of HP State Cooperative Societies Act 1968 and having its Head Office at Dharamsala – 176215, Himachal Pradesh (hereinafter collectively referred to as “the Parties”).

In order to pursue the mutual business purpose contemplated under this Mutual Non-Disclosure Agreement (hereinafter referred to as the “**Agreement**”, and such mutual business purpose hereinafter referred to as the “**Business Purpose**”), the Parties recognize that there is a need to disclose to one another certain confidential information of each party to be used only for the Business Purpose and to protect such confidential information from unauthorized use and disclosure.

In consideration of the other party’s disclosure of such information, the Parties agree as follows:

1. This Agreement will apply to all plans, information (whether written or oral), documentation and support material contained within all analyses, compilations, studies, reports records and other documents which are shown or provided by one party to the other, whether or not any portion thereof is or may be validly copyrighted, trademarked or patented (hereinafter referred to as “**Confidential Information**”). The terms confidential Information shall also include all information provided to M/ s, for undertaking VAPT.
 - Vulnerability Assessment and Penetration Testing (VAPT) of Bank’s CBS (Core Banking Solutions) Internal as well as External Systems/ Networks.
 - Application security testing of web/ mobile applications throughout their lifecycle (pre-implementation, post-implementation, after changes) in environment closely resembling or replica of production environment, etc., as per ‘*Scope of Work*’.
 - Any other job on need basis of the Bank etc., as per the Scope of Work and terms & conditions mentioned in the Request For proposal ref no.dated.....
2. Each party agrees (i) to hold the other party’s Confidential Information in strict confidence , (ii) not to disclose such Confidential Information to any third parties, and (iii) not to use any confidential Information for any purpose except for the business purpose. Without limiting the generality of the aforesaid restrictions, neither party shall use any Confidential Information in connection with any activities or ventures competitive with the business of the other. Each party may disclose the other party’s Confidential Information to its directors, officers, employees attorneys and other advisors (collectively, “Representatives”) on a bona fide need to know basis, but only to the extent necessary to carry out the Business Purpose. Each party agrees to instruct all such Representatives not to disclose such Confidential Information to third parties including consultants, without the prior written permission of the disclosing party.
3. Confidential Information will not include information which;
 - i. is now, or hereafter becomes through no act or failure to act on the part of the receiving party, become generally known or available to the public;
 - ii. was acquired by the receiving party before receiving such information from the disclosing party and without restriction as to use or disclosure;
 - iii. is hereafter rightfully furnished to the receiving party by a third party, without restriction as to use or disclosure;
 - iv. is information which the receiving party can document, was independently developed by the receiving party;
 - v. is required to be disclosed pursuant to law, provided the receiving party provides the other party, to the extent legally permissible, with prompt written notice of such requirement so that the other party may seek an appropriate protective order with respect thereto; or
 - vi. is disclosed with the prior written consent of the disclosing party.
4. The Parties agree to exercise extreme care in protecting the confidentiality of any Confidential information, which is removed from the disclosing party’s premises. The Parties agree to comply with

any and all terms and conditions, the disclosing party may impose upon any such removal, such as conditions that the removed confidential Information and all copies must be returned by a certain date, and that no copies are to be made off of the premises.

5. Upon the disclosing party's request, the receiving party will promptly return to the disclosing party all tangible items containing or consisting of the disclosing party's Confidential Information and all copies thereof.
6. The Parties recognize and agree that nothing contained in this Agreement will be construed as granting any rights to the receiving party, by license or otherwise, to any of the disclosing party's Confidential Information, except as specified in this Agreement.
7. The parties acknowledge that all of the disclosing party's Confidential Information is owned solely by the disclosing party (or its licensors) and that the unauthorized disclosure or use of such Confidential Information would cause irreparable harm and significant injury, the degree of which may be difficult to ascertain. Accordingly, the Parties agree that the disclosing party will have the right to obtain, without the necessity of proving actual damages or posting any bond or other security, temporary and permanent injunctive relief including, but not limited to, specific performance of the terms of this Agreement, as well as the right to pursue any and all other rights and remedies available at law or in equity for such a breach.
8. All references herein to the Parties shall also refer to all entities owned or controlled by the parties, all entities that own or control, or are under common control with, the Parties and their respective offices, directors, employees, shareholders, agents attorneys and other advisors.
9. This Agreement will be construed, interpreted, and applied in accordance with the laws of India. This Agreement is the complete and exclusive statement regarding the subject matter hereof and supersedes all prior agreements, understandings and communications, whether oral or written, express or implied, between the Parties regarding the subject matter of this Agreement.
10. This Agreement will remain in effect for one years from the date of the last disclosure of Confidential Information, at which time it will terminate.
11. All Confidential Information and Confidential Materials are and shall remain the property of Disclosing Party(ies). By disclosing information to the other Party(ies), Disclosing Party(ies) or Receiving Party does not grant any express or implied right to the other party's patents, copyrights, trademarks, or trade secret information.
12. This Agreement constitutes the entire agreement between the parties with respect to the subject matter hereof. It shall not be modified except by a written agreement dated subsequent to the date of this Agreement and signed by both parties. None of the provisions of this Agreement shall be deemed to have been waived by any act or acquiescence on the part of Disclosing Party(ies), its agents, or employees, but only by an instrument in writing signed by an authorised officer of Disclosing Party(ies). No waiver of any provision of this Agreement shall constitute a waiver of any other provision(s) or of the same provision on another occasion.
13. This Agreement shall be governed by and construed interpreted and enforced in accordance with the internal substantive laws of India.
14. If any provision of this Agreement shall be held by a court of competent jurisdiction to be illegal, invalid or unenforceable, the remaining provisions shall remain in full force and effect.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement by their duly authorized officers or representatives

For The KCC Bank

For.....

Signature

Signature

Name

Name

Title

**ANNEXURE – VI
(VAPT AGREEMENT)**

This AGREEMENT is made at Dharamsala on this day of, 2022 between **The Kangra Central Cooperative Bank Ltd**, a banking entity incorporated and functioning under the provisions of HP State Cooperative Societies act 1968 having its Head Office at Dharamsala – 176215, Himachal Pradesh (Hereinafter referred to as the ‘BANK’, which term shall mean and include its successors and assigns) of the ONE PART

AND

M/ S. a company incorporated and functioning under the provisions of the Companies Act, 1956, having its Head Office at represented by its Authorised Signatory (Hereinafter referred to as the ‘IS Auditor’, which term shall mean and include its successors and assigns) of the OTHER PART.

WHEREAS:

- (a) The Bank has implemented Core Banking Solution and Internet Banking with Data Centre at Dharamsala.
- (b) The Bank is desirous of engaging the services of Information Security Auditor for a period of one year only for undertaking Penetration Testing & Vulnerability Assessment of CBS Network and Internet Banking.
- (c) For this purpose, the Bank had called for bids as per Request For Proposal no..... dated.....from potential audit services providers, pursuant to which the IS Auditor has been selected. The I S Auditor will be on the Bank’s panel for a period of one year only from the date of the agreement and the Bank may utilize the services for undertaking such testing. Generally the Testing will be conducted at half yearly.
- (d) Both the parties have arrived at and agreed upon the terms and conditions on the basis of which the IS Auditor will provide its services to the Bank, as set out here in below.

NOW THIS AGREEMENT WITNESSETH:

1. TENURE OF THE AGREEMENT:

1.1 This agreement is valid for one year from the date of the agreement.

2. SCOPE OF WORK:

2.1 The Scope of Work of the IS Auditor shall be as set out in the Schedule annexed and marked as ‘Annexure A’ hereto. While the Bank do not anticipate any change in scope of work for the current half year, should there be any change for next half year, the Bank has right to change the same, by way of additions or deletions. If the Scope of Work is modified for future assignments, the remuneration etc will be decided as detailed in the RFP.

2.2 The implementation of the services of the IS Auditor will be as per a mutually agreed Implementation and Security Integration Schedule to be finalised between the parties.

2.3 The IS Auditor acknowledges and confirms that it shall endeavour to comply with and abide by the agreed Schedule to the best of its abilities.

3. PRICE:

3.1 For each assignment the Bank shall pay a total sum of Rs. (Rupees only) (inclusive of tools license cost) exclusive of taxes for the services rendered by the IS Auditor. The contract amount will remain the same for subsequent such audits/ assignments that may be entrusted by the Bank during the tenure of the contract/ agreement.

3.2 The above amount of Rs. is towards payment of the professional fees of the IS Auditor and applicable taxes will be paid in addition to the above-mentioned amount. (TDS as per applicable laws).

3.3 The IS Auditor confirms that there shall be no further amounts payable by the Bank to the IS Auditor on any account whatsoever, other than that provided under 3.2. In the event of any additional amount of money being required to be paid in respect of the services being rendered by the IS Auditor to the Bank, such monies, if any, shall be paid by the IS Auditor only.

3.4 The amount of Rs. and applicable taxes shall be paid by the Bank to the IS Auditor in the following manner:

100% after the successful completion of the audit assignment, payable through NEFT/RTGS favouring M/ s

4. QUALITY AND COMPLIANCES:

4.1 The IS Auditor shall engage / employ the services of qualified CISA / CISSP professionals only. Such professionals shall have requisite prior expertise / experience in Information Systems and Security Audits. Also, the IS Auditor shall abide by the responsibilities as detailed in RFP.

4.2 It shall be the responsibility of the IS Auditor to ensure full and complete compliance with all the requirements and guidelines of the Reserve Bank of India and / or any other appropriate authorities regarding the standards set out for the Information Systems Security Audits, Penetration Testing & Vulnerability Assessment. Bank reserves the right to inform IBA/ GOI/ RBI in case any major vulnerability, which is not brought out by the I S Auditor during the security audit, is noticed within 6 months from the date of such security audit.

4.3 It shall be the responsibility of the IS Auditor to ensure full and complete compliance with all the requirements and applicable laws, rules and / or regulations, as applicable in India, regarding the standards for Information Systems Security Audits, Penetration Testing & Vulnerability Assessment.

4.4 The I S Auditors will have to audit the Security Architecture / carry out Penetration Testing & Vulnerability Assessment at the designated locations within the mutually agreed time period specified for this purpose by the Bank.

5. OTHER OBLIGATIONS OF THE IS AUDITOR:

5.1 The IS Auditor shall not, without the Bank's written consent, disclose the contents of this Agreement and / or any specifications, information and / or documents furnished to the IS Auditor by and / or on behalf of the Bank and / or which may come to the knowledge or in possession of the IS Auditor in the course of the implementation of its services either relating to the Bank and/ or its customers etc., to any third party other than such person(s) as would be employed / engaged by the IS Auditor for the fulfilment and performance of its obligations and responsibilities under this Agreement.

5.2 Any disclosure of any information, by and / or on behalf of the IS Auditor to such person(s) as mentioned above, shall be subject to further non-disclosure to any other person(s) and it shall be the responsibility of the IS Auditor to ensure that such person(s) to whom the IS Auditor may disclose any information shall comply, in all respects, with the requirement / obligation of non-disclosure to any other person(s).

5.3 All information and / or documents, which may be furnished to the IS Auditor by and / or on behalf of the Bank and / or which may come to the knowledge or in possession of the IS Auditor in the course of the implementation of its services, shall, at all times, remain the property of the Bank and the IS Auditor shall have no rights, of whatsoever nature, in respect thereof.

5.4 All information and / or documents, which may be furnished to the IS Auditor by and / or on behalf of the Bank and / or which may come to the knowledge or in possession of the IS Auditor in the course of the implementation of its services, shall be utilised / relied upon by the IS Auditor, solely, for the purposes of the implementation of its services only and for no other purposes of whatsoever nature.

5.5 The IS Auditor is aware, admits and acknowledges that any breach, of whatsoever nature, in respect of the any of the terms above, shall be viewed seriously by the Bank and the IS Auditor shall be liable for the consequences of such breach as set out elsewhere in this Agreement.

6. INDEMNITY:

6.1 The IS Auditor is aware that, for the purposes of the implementation of its services, it is required to deal with extremely sensitive and confidential data, information, documents, systems, etc. Hence, the IS Auditor does hereby indemnify and shall keep the Bank indemnified at all times from any loss, claim, damages, etc., caused to and / or suffered by the Bank due to any loss or damage to any data, information, documents, systems, etc. and any violation of any of the terms of this agreement including the secrecy, that may be caused due to or may arise out of any negligence or fault or acts of commission or omission on the part of the IS Auditor and/ or the persons engaged by IS Auditors.

7. BREACH AND CONSEQUENCES THEREOF:

7.1 Any default on the part of the IS Auditor in complying with and / or in fulfilling any of its obligations set out in this Agreement, including timely completion of the audit, confidentiality and non-disclosure, etc., shall constitute a breach of this Agreement.

7.2 In the event of such a breach on the part of the IS Auditor and the same remaining un-remedied / un-rectified for a period of 30 days from the receipt of Notice thereof from the Bank, the Bank shall be entitled to either, forthwith, without any Notice, terminate this Agreement and / or claim Damages from the IS Auditor.

8. GOVERNING LAWS & DISPUTE RESOLUTION:

8.1 This Agreement and all issues between the parties shall be subject to the laws of India.

8.2 All disputes, differences, claims and demands arising under or pursuant to or touching the contract shall be referred to the sole arbitrator to be appointed by the Managing Director, Kangra Central Cooperative Bank Limited, Dharamshala, H.P. The award of the sole arbitrator shall be final and binding on both the parties under the provisions of the Arbitration and Conciliation Act, 1966 or by statutory modification/re-enactment thereof for the time being in force. Such arbitration shall be held at Dharamshala.

8.3 Only the Courts in Dharamshala shall have exclusive jurisdiction over all matters arising out of or connected with this Agreement.

9. MISCELLANEOUS PROVISIONS:

9.1 : The Services of IS Auditor will be govern as under in case of dispute:

9.1.1 In spite of any disputes / differences having arisen between the parties, the IS Auditor shall be obliged to continue to provide its services under this Agreement unless terminated by the Bank and / or called upon by the Bank to cease to provide its services and / or the nature of the disputes / differences is such that the IS Auditor cannot possibly continue to provide its services till any interim order / final decision is obtained from the Arbitrator / court.

9.1.2 Irrespective of the above the Bank can terminate this Agreement by giving 15 day's notice without assigning any reasons.

9.2 All Notices issued by one party to the other under this Agreement shall be sent in writing, by registered post or hand delivery or cable or facsimile (in case of the last two, to be confirmed later in writing), and shall be effective on the day of receipt thereof by the party to whom it is addressed or on the expiry of the 5th day from the date when issued by the party addressing the Notice, whichever is earlier.

9.3 Any amendment to this Agreement shall be effective only if it is in writing and is executed by both the parties.

9.4 Either party shall not be liable for any delays or non-performance of any contractual obligation caused due to war, blockage, revolution, civil unrest, riot, strikes, acts of God, plague or other epidemics, fire, flood, acts of Government, or any other like event, beyond the control of the concerned party, which directly or materially or adversely affects the ability of the concerned party to fulfil its obligations and / or responsibilities.

9.5 In the event of a Force Majeure situation, as stated above, the concerned party shall, promptly, inform the other party, in writing, of the existence of the event and shall, simultaneously, attempt to find out alternative means to fulfil its obligations and / or responsibilities.

9.6 If the event of Force Majeure continues for a period of more than 30 days then the Bank shall be entitled to terminate this Agreement and the IS Auditor shall be entitled only to pro-rata payment for the services rendered by it till the date of commencement of the Force Majeure event.

9.7 All other issues, not specifically provided for in this Agreement shall be governed as per the prevailing laws of India.

9.8 It is clearly understood by the parties that the RFP is a part of the agreement and shall be referred in the case of any doubt and/ or dispute. The provisions of this agreement shall prevail in-case of any inconsistency.

9.9 The IS Auditor will abide by the security policy of the Bank as applicable to them.

9.10 The IS Auditor would use all the tools for which they have valid license and/ or free tools which do not require any licenses.

IN WITNESS WHEREOF, the Parties hereto have affixed their respective stamps and signatures on the date first hereinabove mentioned.

**For The Kangra Central cooperative Bank Ltd
(Authorised Signatory)**

**For M/ S.
(Authorised Signatory)**

Witness :

- 1)
- 2)

Witness :

- 1)
- 2)