EVEREST BANK LIMITED

Head Office, EBL House, Lazimpat

REQUEST FOR PROPOSAL

TO

INFORMATION SYSTEM AUDIT

AT

EVEREST BANK LIMITED

Reference: EBL-ISA-2019

Table of Contents

Request For Proposal:
INFORMATION SYSTEM AUDIT

First Published Date: 19-09-2019

Everest Bank Limited invites proposals from certified/qualified firms/companies to conduct Information System Audit of the Bank.

Interested firms/companies are, therefore, requested to submit their detail Technical/ Commercial proposal for the same at the following address within 10 days from the date of publication of this notice.

Everest Bank Limited
IT Dept.
Head Office
Lazimpat, Kathmandu

RFP document for IS Audit can be downloaded from the Bank's website https://www.everestbankltd.com/everest-bank-form-downloads/

EVEREST BANK LIMITED
(A Joint-Venture with Punjab National Bank, India)

BID DETAILS

1	BID Reference	EBL-ISA-2019
2	Date of advertisement	19-09-2019
3	Last date and time for receipt of Bidding Document as per first Tender Notice	29-09-2019
4	Validity of the Bid	30 days from last date of bid submission
5	Date and Time of opening of Technical/Commercial Bid	30-09-2019
6	Place of opening of Bids & Address for Communication	Everest Bank Ltd., Head Office, Lazimpat, Kathmandu
7	Cost of RFP document	NPR 2,500/- (Non-refundable)
8	Bank Account Number	0000-7610-524-01
9	Contact to Bidders	IT Department Head Office, Lazimpat, Kathmandu, Nepal Phone :+977-1-4443377

Note: Bids will be opened in presence of Bank's designated committee. Bidders' shall be intimated accordingly upon selection of the bidder for the service after due analysis of the bids. Bank reserves the right to change the date, timing mentioned above or elsewhere mentioned in the RFP.

Letter of Undertaking on Company Letter Head to be Submitted by Bidders

To,

Everest Bank Limited
Head Office
Lazimpat, Kathmandu

Dear Sir,

Reg.: Bid for Conducting Information System (IS) Audit

We submit our Bid Document herewith

We understand that

- The Bank may accept the lowest or any bid received by the Bank which you may consider, and the Bank may reject all or any bid.
- If our Bid for the above job is accepted, we undertake to enter into and execute at our cost, when called upon by the Bank to do so, a contract in the prescribed form. Unless and until a formal contract is prepared and executed, this bid together with your written acceptance thereof shall constitute a binding contract between us.
- If our bid is accepted, we are to be jointly and severally responsible for the due performance of the contract.
- We have examined the above referred RFP document. As per the terms and conditions specified in the RFP document, and in accordance with the schedule of prices indicated in the commercial bid and made part of this offer.
- We have gone through the terms contained in the above referred RFP document. We declare that all the provisions of this RFP are acceptable to us. We further certify that below signed persons are the authorized signatory of this company and, therefore, competent to make this declaration.
- If our offer is accepted, we undertake, to start the assignment under the scope immediately after receipt of order from the Bank.
- We also certify that the information/data/particulars furnished in our bid are factually correct and also accept that in the event of any information / data / particulars are found to be incorrect, Bank will have the right to disqualify us.

- We undertake to comply with the terms and conditions of the bid document. We understand that Bank may reject any or all of the offers without assigning any reason whatsoever.
- All declaration required are duly signed by authorized signatory of the bidder and enclosed.

Dated at _____

Name of the Authorized person of the Company:

Designation:

Yours faithfully

_____

Company Seal & Bidder's Signature

INSTRUCTIONS FOR BIDDER

1. Introduction

Catering to more than 10 lacs customers, Everest Bank Limited (EBL) is a name you can depend on for professionalized & efficient banking services. Founded in 1994, the Bank has been one of the leading banks of the country and has been catering its services to various segments of the society. With clients from all walks of life, the Bank has helped develop the nation corporately, agriculturally & industrially.

EBL was established in 1994 October. At present, the Bank has its presence across the country with a branch network of 94 Branches, 120 ATM Counters, 3 extension counters & 28 Revenue Collection Counters.

2. Criteria for evaluation of IS Audit Company

Following shall be the basic eligibility criteria to select the IS audit company:

- Must be registered in the Office of Company Registrar / Dept. of Commerce / Office of Commerce etc. in bidder's country.
- IS audit company should be in existence for at least 3 years.
- Must have experience of conducting IS audit of at least three 'A' class commercial Banks of a business of equivalent of NPR 10000 crores and above.
- Experience in conducting IS audit of international companies.
- The company should have a team of engineers with minimum 5 years of experience along with CISA/DISA/CISM/CISSP qualified personnel.
- The company should have ISO 27001 certified personnel (preferable).
- The company should have CEH/Certified penetration tester personnel.

The tender shall be awarded as per the financial by-laws of the Bank.

3. Scope of work

Information Systems Audit should cover entire Information Systems Infrastructure which includes Servers & other hardware items, Operating Systems, Databases, Application Systems,

Technologies, Networks, ATM switching system, SWIFT and Process & People of the undernoted locations:

1. Data Center
2. DR Site
3. 2 valley branches and 2 outside valley branches
4. 3rd party product & interfaces

Detailed scope of audit:-

IS Audit should cover entire range of computerized functioning as listed above including Internet/Mobile Banking & functional areas with special reference to the following:

1	Policy, Operating Procedures, Standard Practices & other regulatory requirements	1. Bank's IT related policy and operating procedures. 2. NRB IT guideline & other legal requirements. 3. Best practices of the industry.
2	Physical and Environmental Security	1. Access control systems 2. Fire / flooding / water leakage / gas leakage etc. 3. Assets safeguarding, Handling of movement of Man /Material/ Media/ Backup / Software/ Hardware / information. 4. Air-conditioning of DC/ DR, humidity control systems 5. Electrical supply, Redundancy of power level, Generator, UPS capacity. 6. Surveillance systems of DC / DR, branch, ATMs 7. Physical & environmental controls. 8. Pest prevention (rodent prevention) systems
3	Operating Systems Audit of Servers, Systems and Networking Equipments	1. Setup & maintenance of Operating Systems Parameters 2. Updating of OS Patches 3. OS Change Management Procedures 4. Use of root and other sensitive Passwords 5. Use of sensitive systems software utilities 6. Internal/external Vulnerability assessment, penetration testing & hardening of Operating systems. 7. Users and groups created, including all type of usersmanagement ensuring password complexity, periodic changes etc. 8. File systems security of the OS 9. Review of Access rights and privileges. 10. Services and ports accessibility 11. Review of Log Monitoring, itssufficiency, security, maintenance and backup.
4	Application level Security Audit	1. Only authorized users should be able to edit, input or update data in the applications or carry out activities as per

		their role and/or functional requirements 2. User maintenance, password policies are being followed are as per bank's IT policy 3. Segregation of duties and accesses of production staff and development staff with access control over development, test and production regions. 4. Review of all types of Parameter maintenance and controls implemented. 5. Authorization controls such as Maker Checker, Exceptions, Overriding exception & Error condition. 6. Change management procedures including testing & documentation of change. 7. Application interfaces with other applications and security in their data communication. 8. Internal/external Vulnerability assessment and penetration testing 9. Identify gaps in the application security parameter setup in line with the banks security policies and leading best practices 10. Audit of management controls including systems configuration/ parameterization & systems development. 11. Audit of controls over operations including communication network, data preparation and entry, production, file library, documentation and program library, Help Desk and technical support, capacity planning and performance, monitoring of outsourced operations. 12. To review all types of Application Level Access Controls including proper controls for access logs and audit trails for ensuring Sufficiency & Security of Creation, Maintenance and Backup of the same.
5	Audit of DBMS and Data Security	1. Authorization, authentication and access control are in place. 2. Audit of data integrity controls including master table updates. 3. Confidentiality requirements are met. 4. Logical access controls which ensure the access to data is restricted to authorized users. 5. Database integrity is ensured to avoid concurrency problems. 6. Separation of duties. 7. Database backup management. 8. Security of oracle systems files viz. control files, redo log files, archive log files, initialization file, configuration file, Table space security etc. 9. Password checkup of Systems and Sys Users 10. Checking of database privileges assigned to DBAs

		13. Internal/external Vulnerability assessment and penetration testing
6	Network Security	1. Understanding the traffic flow in the network at LAN & WAN level. 2. Audit of Redundancy for Links and Devices in DC 3. Analyze the Network Security controls, which include study of logical locations of security components like firewall, IDS/IPS, antivirus server, email systems, etc. 4. Study of incoming and outgoing traffic flow among web servers, application servers and database servers, from security point of view. 5. Routing protocols and security controls therein. 6. Study and audit of network architecture from disaster recovery point of view. 7. Privileges available to Systems Integrator and outsourced vendors if any. 8. Review of all types of network level access controls, logs, for ensuring sufficiency & security of creation, maintenance and backup of the same. 9. Secure Network Connections for CBS, ATM and Mobile/Internet Banking including client/ browser based security. 10. Evaluate centralized controls over Routers installed in Branches & their Password Management. 11. Checking of VLAN Architecture 12. TCP ports 13. Checking of Firewall Access control List 14. Routers and Switches are using AAA model for all User authentication 15. Enable passwords on the Routers are encrypted form and password comply with minimum characters in length. 16. Local and remote access to network devices is limited and restricted. 17. Internal/external vulnerability assessment and penetration testing
7	Audit of ATM Switch, ATM Card Management, ATM PIN management	1. Audit of ATM Switch covering Application, Network Security, Switch Functionality, Interface, Audit Trails, transmission security, authorization, Fallback / fail over procedures, Status Update, compliance to VISA & other standards. 2. PIN Management (Generation & Re-generation etc.) of ATMs. 3. Adequacy of security defenses. 4. Connectivity to other networks 5. Card management (Delivery of cards / PIN, hot listing of cards and reconciliation with settlement agency.)

		6. ATM Switch operational controls, & Reconciliation 7. ATM machine security adequacy
8	Backup & Recovery Testing	1. Audit of backup & recovery testing procedures. 2. Sufficiency checks of backup process. 3. Audit of access controls, movement and storage of backup media. 4. Audit of media maintenance procedures. 5. Security of removable media. 6. Controls for prevention of data leakage through removable media or other means. 7. Media disposal mechanisms and Database archival & purging procedures. 8. Synchronization between DC & DRC databases. 9. DR Services to be up for branches, as per RTO & RPO of BCP.
9	SWIFT	1. Network security 2. Access control 3. Environmental security
10	Others	1. Inventory movement controls & maintenance, equipment maintenance and disposal measures, change & configuration management processes, 2. Audit of Logging and monitoring processes 3. Audit of delivery channels, 3rd Party Products and various other interfaces which are integrated with the Core Systems. 4. Follow up audit to mark off the observations responses of the Bank, quarterly.

4. Amendments to bid Documents

i. Amendments to the bid document may be issued by the bank for any reason, whether at its own initiative or in response to a clarification requested by a prospective bidder, prior to the deadline for the submission of bids.

ii. The amendments so placed will be binding on all the bidders. From the date of issue, amendments to terms and conditions shall be deemed to form an integral part of the RFP.

Further, in order to provide, prospective bidders, reasonable time to take the amendment into account in preparing their bid, the Bank may, at its discretion extend the deadline for submission of bids.

5. Bidding Procedure

i. Bidders shall submit single bid only.

ii. Technical & Financial proposal must be submitted at the same time giving full particulars in separate sealed envelopes duly marked as "IS Audit Technical Proposal" and "IS Audit Financial Proposal". These envelopes containing technical and financial proposals shall then be enclosed in one single envelope. The envelope shall bear registered name and complete address of the bidder.

iii. The bidder will take care of submitting the proposal properly filed so that the papers are not loose. The Proposals, which are not sealed as indicated above, are also liable for rejection.

iv. The bid not submitted in the prescribed format or incomplete in details is liable for rejection. The Bank is not responsible for non-receipt of bid within the specified date and time due to any reason including postal delays or Holidays.

v. The Bidder must deposit non-refundable amount included in bid to submit the bid. The original deposit voucher of the same must be enclosed along with submission of the Bids.

vi. The Bidder must submit the below documents
    a. Tax/Clearance Certificate
    b. PAN/VAT
    c. Registered Certificate with renewal

vii. The Bids may be rejected, if found incomplete and received after the deadline.

6. Cost of Bidding

The Bidder shall bear all costs associated with the preparation and submission of its bid and the Bank will in no case be responsible or liable for these costs, regardless of the conduct or outcome of the bidding process.

7. Language of Bid

The bid prepared by the Bidder, all correspondence and documents relating to the bid exchanged by the Bidder & the Bank shall be written in English.

8. Deadline for Submission of Bid

Bids must be received by the Bank at the address specified not later than the time and date specified in the Bid document. In the event of the specified date for the submission of bids being declared a holiday for the Bank, the bids will be received on the next working day. Any bid received by the Bank after the deadline for submission of bids prescribed by the Bank, in invitation for bid, will be rejected and returned unopened to the bidder.

9. Bid Opening

The Bank will open only the technical proposals as per the schedule mentioned. The financial proposal for technically qualified bidders only will be opened on a later date subsequent to the technical evaluation.

10. Clarifications of Bid

To assist in the scrutiny, evaluation and comparison of offers the Bank may, at its discretion, ask some or all bidders for clarification of their offer. The request for clarification and the response shall be in writing and no change in the price or substance of the bid shall be sought, offered or permitted. Each Recipient should notify Bank of any error, omission, or discrepancy found in this RFP document.

11. Preliminary Examination

- The Bank will examine the bids to determine whether they are complete, whether any computational errors have been made, whether the documents have been properly signed and whether the bids are generally in order.
- Arithmetical errors if any will be rectified on the following basis
  i. If there is discrepancy between the unit price and the total price that is obtained by multiplying the unit price and quantity, the unit price shall prevail and the total price shall be corrected.
  ii. If there is a discrepancy between words and figures, the amount in words will prevail.

12. Evaluation of Proposals

The Technical Proposal opened will be evaluated by the Bank on the basis of following criteria:

i. Completeness of the technical proposal in all respects and availability of all information asked for
ii. Responsibilities including scope and deliverables as per the bidding documents
iii. Experiences of the bidder
iv. Work plan and methodologies
v. Qualifications and experiences of the auditors

Financial proposal of technically qualified bidders will be evaluated on the basis of the proposed cost, project duration etc.

14. Bank's Right

a) The Bank reserves the sole discretionary right to accept or reject any proposal, and to annul the bidding process and reject all bids at any time prior to award of contract, without thereby incurring any liability to the affected Bidder or Bidders or any obligation to inform the affected Bidder or Bidders of the grounds for the Bank's action.
b) Bank reserves the sole discretionary right to modify any terms, conditions and scope of work of the bidding document.
c) Bank reserves the sole discretionary right to obtain revised financial proposal from the bidder with regards to changes in RFP clauses or if the Bank is not satisfied with the price offered.
d) Bank reserves the sole discretionary right to accept or reject any Bid in part or whole without assigning any reason.

15. No Commitment to Accept Lowest or Any Bid

The Bank shall be under no obligation to accept the lowest or any other offer received in response to this bid documents and shall be entitled to reject any or all offers including those received late or incomplete offers without assigning any reason whatsoever.

i. The Bank reserves the right to make any changes in the terms and condition of the purchase.

ii. The Bank will not be obliged to meet and have discussions with any bidder and/or to listen to any representations.

16. Miscellaneous

i. Bidder should observe the highest standard of ethics during the process of bidding and execution of the contract.

ii. The bank reserves the sole discretionary right to reject a proposal for award if it determines that the bidder recommended for award has found engaged in corrupt or fraudulent practice during the process of bidding, bid evaluation and bid award.

iii. Dispute or differences, if any, arise between bank and the bidder from misconstruing the meaning and operation of RFP will be resolved amicably.

-x-x-x-