THE KERALA STATE CO-OPERATIVE BANK LTD.
COBANK TOWERS, PALAYAM
THIRUVANANTHAPURAM-33
PH.No.0471-2547200/2317081
Website: www.keralacobank.com.

CORRIGENDUM NOTICE

Tender No.   KSCB/P&E/eprocurement/1663/3/2018-19 dated 3rd October 2018.

Tender Name : Information System Audit (2018-19)

Corrigendum Type : Date & Time

Sub: Extension of Bid submission and Tender opening dates.

The final bid submission & tender opening dates are revised as listed below:

Last date for submission of bids	2.11.2018 at 4.00 p.m.
Bid Opening	3.11.2018 at 11.00 A.M

Sd/-
Managing Director
Kerala State Co-operative Bank Ltd.

29.10.2018

RFP FOR INFORMATION SYSTEM AUDIT 2018-19

I.   <u>Introduction</u>

The Kerala State Cooperative Bank Ltd. is the apex bank of the Cooperative Banking structure in Kerala that is approved by the Registrar of Cooperative Societies, Government of Kerala. The 14 District Cooperative Banks in the State and the Government of Kerala are members and shareholders of the Bank. The Bank operates through a network of 20 branches. The Bank has three Regional Offices - one each at Thiruvananthapuram, Ernakulum and Kozhikode, for effective supervision and control of its own branches as well as the constituent District Co-operative Banks.

Since July 1966, KSCB is permitted to perform banking functions as per the Banking Regulation Act. The Bank is doing basic banking functions of accepting deposits, lending loans through its branches, ATM Operations with PoS, NEFT/RTGS. Facilities like mobile banking, internet banking etc are in the pipeline. The customer base of KSCB has grown considerably over the years and extending the conveniences of present day banking services to the customers of KSCB is hence seen as a necessity. The bank is already functioning with full-fledged international core banking software – Finacle 7.0.29.

II.   <u>Purpose of the RFP</u>

Information Systems Audit should cover entire Information Systems Infrastructure which includes Servers & other hardware items, Operating Systems, Databases, Application Systems, Technologies, Networks, Facilities, and Process & People. This RFP seeks to engage a Service Provider who has the capability and experience, to conduct the following:

Conducting Information Security Audit including technical, physical and administrative aspects and to make appropriate recommendations, as covered under the Scope of Work. Carrying out risk analysis of all IT assets of the Bank and preparation of Risk Matrix based on Guidelines issued by RBI and Govt. of India. Giving scope document, guidelines and devising framework for continuous audit of 100% Transactions. The aim of the RFP is to solicit proposals from qualified bidders for undertaking above detailed assignments.

III.   <u>Eligibility criteria</u>

Only those service providers who fulfill the following criteria are eligible to respond the RFP. Offers received from the service providers who do not fulfill all or any of the following eligibility criteria are liable to be rejected.

i. The service provider should be a current legal entity (Company /Firm /Organization/ independent subsidiary) in India.

ii. Should be in business of Information System auditing in India at least for last three years.

iii. Should be in net profit in at least two years out of last three financial   years.

iv. Should have conducted two Information System audits of data centers and other IT Infrastructure of banks in India

v. Should have conducted application audit of Core Banking Solution in at least two Banks with more than 20 branches.

vi.Should not have been blacklisted, as on the date of tender submission, by any nationalised Bank / RBI /IBA or any other Central/State Government department / agency.

vii. IS Auditors should be competent audit professionals with sufficient and relevant experience. Qualifications such as CISA (offered by ISACA0, DISA (offered by ICAI), or CISSP (offered by ISC2), along with 2 or more years of IS Audit experience are desirable.

viii. Should be eligible as per RBI Norms on eligibility, empanelment and selection of Statutory Central Auditors in Public Sector Banks from the year 2017-18 and onwards

IV.   Scope of work

The selected vendor has to go through the audit reports of previous years and has to check whether all the observations are complied. They have to comment on status of non-complied observations, while undertaking fresh audit under this RFP.

During the course of audit, if the service provider observes any major deficiencies, they should immediately bring such observations, deficiencies, areas of improvement and suggestions for improvement to the notice of the concerned persons. The service provider should also discuss with, guide/help the Bank staff in implementation of the critical and important suggestions. IS Audit should cover entire spectrum of computerized functioning including the areas with special reference to the following:

A. Policy, Procedures, Standard Practices & other regulatory requirements:
   i. Bank' s IT Security Policy & Procedures.
   ii. RBI guidelines on Information Security & other legal requirements.
   iii. Best practices of the industry

B. 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/ DRC, humidity control systems

5. Electrical supply, Redundancy of power level, Generator, UPS capacity.

6. Surveillance systems of DC / DRC

7. Physical & environmental controls.

8. Pest prevention (rodent prevention) systems

C. **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. Vulnerability assessment & hardening of Operating systems.

7. Users and Groups created, including all type of users management 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, its sufficiency, security, maintenance and backup.

D. **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 security 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. Search for back door trap in the program.

9. Check for commonly known loopholes in the software.

10. Identify gaps in the application security parameter setup in line with the banks security policies and leading best practices

11. Audit of management controls including systems configuration/ parameterization & systems development.

12. 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.

13. 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.

E. Network Security

Security architecture of the entire network including: 1. Understanding the traffic flow in the network at LAN & WAN level.

2. Audit of Redundancy for Links and Devices in CBS Setup.

3. Analyze the Network Security controls, which include study of logical locations of security components like firewall, IDS/IPS, proxy server, 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.

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 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 in encrypted form and check password compliance with minimum strength.

16. Local and remote access to network devices is limited and restricted.

F. 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 NGRTGS, NEFT, NACH, CTS and E-mail Systems which are integrated with the Core Systems.

V.   Terms and Conditions

1. All the queries and clarifications must be sought in writing to the email id: cobankit@gmail.com

   Single point of contact:- Deputy General Manager, IT Department, Kerala State Co-Operative Bank Ltd., Cobank Towers, Vikasbhavan P.O, Palayam, Thiruvananthapuram-695033

2. One hard copy of the Technical Bid and One Copy of the Commercial Bid must be submitted at the same time, giving full particulars in separate sealed envelopes at the Bank's address given below on or before the schedule given in section VI.

   Address: The Kerala State Co-operative Bank Ltd.
                    Co-bank Towers, Vikas Bhavan PO
                    Palayam. PIN-695033

3. All the envelopes must be super scribed with the following information –
   Proposal for Conducting IS Audit- 2017-18 (Technical bid)
   Proposal for Conducting IS Audit- 2017-18 (Commercial Bid)

4. The offer should remain valid for a period of 180 days from date of submission of the proposal. At the option of the Bank, the vendor should extend the validity of offers for such required period (s), as the Bank may require during the evaluation process.

5. The technical proposal must contain the following: -
   - Bidders profile
   - Details of professional personnel
   - Details of lead audit certification from leading certification Bodies
   - Details of the similar assignments executed by the bidder in other Banks
   - Proposed Methodology and work plan
   - Estimated time to complete the audit

6. The commercial proposal must contain the following:-
   - The Commercial Proposal should provide all relevant price information in Indian Rupees only
   - It should not contradict the unpriced technical proposal in any manner.
   - The responses should be strictly as per the terms and conditions of this RFP. Service Providers are advised not to attach or specify any terms and

conditions. The Bank reserves its right to reject the proposals received with any additional terms and conditions specified by the Service provider.

- The Commercial Bid should include all taxes, duties, fees, and other charges as may be levied under the applicable law as on the date of submission of the proposal. However, the tax component of the prices should be shown separately
- The total must be quoted in WORDS AND FIGURES. In case of discrepancy between the words and figures, lower of the two would be considered as the price quoted and the same will be binding on the vendor.
- The price quoted should be inclusive of following: Professional Charges Travel and Halting expenses, including local conveyance Out of pocket expenses All applicable taxes, duties and levies
- Work Contract tax, if any, applicable should be borne by the Service provider.

7. The Contract with the selected bidder 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 at Thiruvananthapuram (with the exclusion of all other Courts).

8. The Managing Director, KSCB reserves the right to reject any proposal/tender/RFP with or without assigning any reason at any time and to restrict the list of firms to any number deemed suitable.

VI. <u>Schedule</u>

Description	Due Date***
Issue tender notification	11/10/2018
RFP submission	29/10/2018; 1:00p.m.
Bid opening	29/10/2018; 1:15p.m.
Evaluation of technical proposal	Will be informed later
Commercial evaluation	Will be informed later
Discussions and negotiations	Will be informed later
Award of contract	Will be informed later

***All dates mentioned above are tentative dates and the bidder acknowledges that it cannot hold the Bank responsible for breach of any of the dates

THE KERALA STATE CO-OPERATIVE BANK LTD.

Cobank Towers, Palayam, Trivandrum-33
Ph No : 0471-2547200/2317081

No: KSCB/P&E/e procurement/ 1663/3/2018-19

NOTICE INVITING TENDER

On behalf of Kerala State Co-operative Bank Ltd.,its Managing Director invites sealed tenders from reputed firms for **conducting Information System Audit (ISA)** should cover entire information systems infrastructure which includes hardware and peripherals, operating systems, databases, application systems, technology, networks, facilities, process and people.

The last date of submission of tenders will be at 1.00 PM on 29th October 2018. The tender will be opened at 1.15 PM on the same day. for details please visit our website www.keralacobank.com

Thiruvananthapuram

10th October 2018

Sd/-
Managing Director