REQUEST FOR PROPOSAL

FOR

CONCURRENT AUDIT

OF

DC / DR / NDR / IT OPERATONS / SECURITY OPERATION CENTER (SOC)

Ref No:HO.ID.Ex.ISA/005/ 2023-24

TAMILNAD MERCANTILE BANK LTD.,
Information Systems Audit Cell
Inspection Department
56 & 57, Beach Road
Thoothukudi – 628 001

email: isaudit@tmbank.in
website: www.tmb.in

1. Introduction

Tamilnad Mercantile Bank Ltd, has its Head Office at 57, V.E Road, Thoothukudi 628001. It's Department of Information Technology is located at 2nd and 3rd Floors, Pearl Tower, II Avenue, Anna Nagar West, Chennai & Subbiah Towers, 3rd Floor, No.458 V.E.Road, Thoothukudi.

Tamilnad Mercantile Bank Limited is hereinafter called "Bank", issues this 'Request for Proposal', hereinafter called "RFP". This RFP seeks to engage an Information Systems Audit Firm, which has the capability and experience, to conduct a comprehensive Concurrent IT Audit of Bank's critical IT infrastructure and to make appropriate recommendations, as covered under the Scope of Work. The aim of the RFP is to solicit proposals from qualified Applicants for Concurrent IT Audit assignment.

An applicant submitting the proposal in response to RFP for Concurrent IT Audit shall hereinafter be referred to as "Applicant / Systems Auditor" interchangeably.

The RFP document is neither an offer letter nor a legal contract, but an invitation for expression of interest. No contractual obligation on behalf of Bank whatsoever shall arise from the RFP process, unless and until a formal contract is signed and executed by duly authorized officers of Bank and the Applicant. The Bank may modify any / all of the terms of this RFP.

2. Bank Profile

Tamilnad Mercantile Bank Limited is a Private Sector Bank. Bank uses Information Technology in all spheres of its functioning by connecting all of its branches through its WAN and has migrated 100% of its branches to Core Banking Solution, Finacle.

Bank aims to leverage the centralized solution to support its growing business, improve operational efficiency across the counters and multi-delivery channels, to enhance focus on customers with a Customer Centric Approach.

Tamilnad Mercantile Bank Limited is having the record as the first private sector bank in India to introduce large scale computerization for branch level operations. The bank adopted modernization, as early in the year 1983. The bank is embarking total Branch Automation in technological partnership with M/s. Infosys Technologies Ltd., Bangalore and achieved 100% CBS implementation. Computerization has enabled the bank to render much better and satisfied service to its customers. The Bank has launched ATM Card from Nov 11, 2003. The bank has implemented new technologies like internet banking, mobile banking.

The modes of connectivity to the branches is achieved through a combination of leased lines, ISDN Lines, VSATs, GPRS and other emerging forms of connectivity.

TMB is proud to be among the select few banks in India having got certified for ISO / IEC 27001:2013 towards our secure information system management practices at IT & HR Dept (Thoothukudi) as well as Chennai IT Dept with effect from November 6, 2014.

Please refer Bank's website (http://www.tmb.in) for full profile.

3. Broad Scope of Concurrent IT Audit

The broad scope of Concurrent IT Audit are provided as follows:

A) Policies, Procedures, Standard Practices & other statutory and regulatory requirements:

i) Bank's Information Security Policy, Cyber Security Policy, IS Audit Policy, IT Policy, Delivery Channel policy, IT Outsourcing policy, other policies and SOPs of the Bank owned by IT / Information Security Department.

ii) Regulations/guidelines i.e.

a) Information Technology Act 2000 and subsequent amendments.

b) Gopalakrishna Committee Recommendations (DBS. CO. ITC. BC. No. 6 /31.02.008/2010-11 dated April 29, 2011).

c) Cyber Security Framework (DBS.CO/CSITE/BC.11/ 33.01.001 /2015-16 dated 2nd June,2016).

d) RBI advisory digest CO.DOS.CSITEG.SEC.No.12/31-01-015/2023-2024 on Consolidation of controls prescribed in the advisories issued dt 27.03.2024.

e) RBI Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices (DoS.CO.CSITEG/ SEC.7 /31.01.015/2023-24 dated November 7, 2023)

f) RBI Guidelines on Digital Lending (RBI/2022-23/111 DOR.CRE.REC.66/21.07.001/2022-23 dt 02.09.2022).

g) RBI Master Direction on Outsourcing of Information Technology Services (RBI/2023-24/ 102 DoS.CO.CSITEG/ SEC.1/31.01.015/2023-24 dated April 10, 2023).

h) SWIFT - Cyber Security Controls [DBS.CO/CSITE/BC.4/ 33.01.001/2016-17 dated 03-08-2016, DBS.CO/CSITE/ BC.4226/31.01.015/2016-17 dated 25th November 2016 and DBS (CO).CSITE/4493/31.01.015/2017-18 dated 20th February 2018] etc.

i) VISA, PCI-DSS, NPCI & other applicable guidelines.

j) CERT-In guidelines/advisories, CSITE guidelines.

k) Best practices of the ISO/IEC standards and any other legal and regulatory requirements as applicable.

l) National Cyber Security.

Verify the Compliances of various action points of RBI Cyber Security guidelines (CSITE advisories and alerts) and other advisories (including sustenance of compliance given to Reserve Bank of India RAR and RMP observations with respect to IT) during the course of audit of DC/DR/NDR/IT Operations/SOC. Check that action points are on continuous and sustainable and report if any non-compliances in reporting.

B) Timeline for the Audit and Report delivery:

S.No	Audit Area	Periodicity		Report Delivery within
1.	Data Centre	Monthly		7th of succeeding month
2.	IT Operations	Monthly		7th of succeeding month
3.	DR Site	Quarterly	Apr-Jun	15th Jul
			Jul-Sep	15th Oct
			Oct-Dec	15th Jan
			Jan-Mar	15th Apr
4.	Near DR	Quarterly	May-Jul	15th Aug
			Aug-Oct	15th Nov
			Nov-Jan	15th Feb
			Feb-Apr	15th May
5.	SOC	Quarterly	Jun-Aug	15th Sep
			Sep-Nov	15th Dec
			Dec-Feb	15th Mar
			Mar-May	15th Jun

C) Detailed Audit Coverage:

I. Scope of DC / DR / NDR:

1. Asset Management
2. Server Management
3. Capacity Management
4. Storage Management
5. Access controls measures, Surveillance systems, environmental monitoring
6. Backup and Restoration Management
7. Communication and Network Security
8. Change Management including Patch Updation
9. Incident Management
10. Adherence to SLA

II. Scope of IT Operations

1. Network Management
2. Database Management
3. Endpoint Management
4. Exception Management
5. Review of adherence to WFH/Remote access guidelines
6. Change Management

7. Review of VAPT process and Exception handling
8. IT Service Management
9. Review of compliance to the previous audit reports.

III. Scope of Security Operation Centre

1. Review of Configuration of SOC infrastructure/Security Tools.
2. Business justification/Risk assessment for devices not integrated with SIEM/SOC tools
3. Review of SOC processes, Review of SOC charter document, SOC KPI and Metrics.
4. Management and Monitoring of logs
5. Review of Human resource management, Training and Knowledge Management.
6. Review of Outsourcing services of SOC, SLA Management process for SOC
7. Review the configuration parameters of SOC
8. Custom rule review and custom application integration.
9. Incident reporting and Management.
10. Security monitoring services.
11. Security analysis and forensics and Threat intelligence.
12. Review of reporting responsibility and periodicity of report
13. Review of work authorization system between outsource service provider and bank's team
14. Access Control, Customer Data Privacy & Confidentiality.

IV. Method of Audit to be followed:-

Audit activities shall be conducted from Chennai for IT operations, Data Centre, NDR,SOC and from Bangalore for DR Site.

Selected Audit Firm required to provide the audit checklist with risk parameter prior to conduct of audit. Resumes of the auditors assigned for the project to be provided to the Bank beforehand and they should be deputed to the assignment only after Bank's Consent. Required background verification shall be done by the selected audit firm and provided to the bank before deputing Auditor to the field to commence the audit as per the scope of Audit.

Document the security gaps i.e. vulnerability, security flaws, loopholes, etc. observed during the course of the review. Document recommendations for addressing these security gaps and categorize the identified security gaps based on their criticality, resource/effort requirement to address them.

The auditor shall keep all the working papers / evidence/ audit documents collected during the course of audit and may be submitted to the Bank when called for.

V Submission of Report of the Audit Findings:-

Audit Firm has to submit report of the Audit findings to IS Audit Cell after completing audit of each month / quarter as applicable.

The report should define Process Owner, Risk Owner, Risk of the Observation, Impact and Recommendation to mitigate the Risk. In addition to the same

- Executive summary in excel dash board
- Detailed findings/Checklists/In Depth Analysis of findings/ Corrective Measures & Suggestions along with Risk Analysis.
- Pending compliance of previous months Concurrent IT Audits.

The detailed findings shall be brought in the report covering the details of all aspects viz. identification of flaws / gaps /vulnerabilities in the systems (specific to equipment/resources –indicating name and IP address of the equipment with Office and Department name), identifications of threat sources, identification of Risk , Identification of inherent weaknesses, Servers/Resources affected with IP Addresses etc. Report should classify the observations into Critical /Non Critical category and asses the category of Risk Implication as VERY HIGH/HIGH/MEDIUM/LOW RISK based on the impact. The various checklist formats , designed and used while conducting the IS Audit as per the scope, should also be annexed in the report separately for Servers (different for different OS), RDBMS, Network equipment's , security equipment's etc , so that they provide minimum domain wise baseline security standard /practices to achieve a reasonably secure IT environment for technologies deployed by Bank. The Reports should be substantiated with the help of snap shots/evidences /documents etc. from where the observations were made. Excel format will be shared by the bank. Necessary dashboard containing high risk, medium risk and low risk observations with open/closed status on monthly basis required to be maintained by the audit service provider on monthly basis.

Audit Reports shall be shared through email with digitally signed in A-4 size. (Soft copies of all the documents properly encrypted in MS Word /MS Excel /PDF format).

VI. Terms & Conditions:

Quarterly basis payment will be made after completion and submission of audit reports after deducting applicable taxes and penalties.

a. Penalty:

Delayed start of audit, delayed completion of audit and delayed submission of report as per agreed terms defined in scope of audit will attract penalty of 0.25 % per day of default/delay of total amount payable for that quarter – (maximum up to 10% of the fees of that quarter). If the report is not submitted within agreed days after completion of audit, the Bank may cancel the order.

b. Disclaimer

Subject to any law to the contrary, and to the maximum extent permitted by law, Bank and its officers, employees, contractors, agents, and advisers disclaim all liability from any loss or damage (whether foreseeable or not) suffered by any person acting on or refraining from acting because of any information, including forecasts, statements, estimates, or projections contained in this RFP document or conduct ancillary to it whether or not the loss or damage arises in connection with any negligence, omission, default, lack of care or misrepresentation on the part of Bank or any of its officers, employees, contractors, agents, or advisers.

c. If selected, the Audit Firm has to execute Non-Disclosure Agreement on the terms and conditions mentioned by the Bank to maintain confidentiality of Banks Information.

d. Bank reserves the right to cancel / modify the entire process at its discretion without assigning any reason at any time.

VII Tenure

This assignment of Concurrent IT Audit shall be valid for a period of three years (subject to renewal every year) on a contractual basis, subject to termination clause stated in this letter. This assignment is based on your overall performance which includes proper conduct of audit, timely submission of report, maintenance of quality report, report on compliance / rectification of features, suggestions for improvement of IT operations, etc.

VIII Termination Clause

Your overall performance will be reviewed from time to time and, in case, if the Bank thinks, your performance is not found satisfactory, even during the term of

assignment, your service is liable to be terminated at the sole discretion of the Bank. Failure on your part to notice and report any major irregularities / fraud perpetrated during your audit period renders you liable for negligence and the Bank has the right to initiate action as deemed fit including legal action as applicable apart from termination of the assignment as well as informing RBI and other authorities for suitable action.

4. Eligibility Criteria

Employees of the Audit Firm who is going to engage in the audit should possess skills that are commensurate with the technology used by the bank. Auditors shall possess Qualifications such as CISA (offered by ISACA) or CISSP (offered by ISC2), along with two or more years of relevant Audit experience. They should be competent audit professionals with sufficient and relevant experience as required and also shall confirm that they fully comply with the eligibility criteria in the Pro-forma (Annexure I).

Disqualification / Conflict of Interest: The Applicant shall refuse to take up the assignment and inform the Bank, in case they are disqualified under any of the following provisions:

1. The proprietor / partner of the audit agency is also a director in the Bank;
2. The audit agency is already entrusted with statutory audit in the Bank;
3. Associate firms / sister concerns of the audit agency has been entrusted with statutory audit in the Bank;
4. The auditor is indebted to the Bank for an amount exceeding Rs.1,000/- or any guarantee has been given for any security in connection with the indebtedness of any third person to the bank for any amount exceeding Rs.1,000/-;
5. In case the auditor is a sole proprietary concern, and the proprietor is not a full-time practicing IS Auditor, or is employed elsewhere;
6. The Auditor/Agency was involved in the development of the software / application for the Bank which is the subject matter of the audit;
7. The Auditor/Agency is currently associated with the Bank by way of consultancy, supplying of systems, system development, maintenance, system integration, etc. related to IT or Networking services, or has rendered such services during the preceding 24 months.
8. There shall be no legal actions / restrictions on the auditing firm / auditors by any regulatory authority that would affect the ability to deliver audit deliverables.

5. Application Processes

General Terms of Bid Submission

- The offer should be made strictly as per the formats enclosed.
- Each applicant should not submit more than one RFP. RFPs arriving beyond the stipulated time will not be accepted.
- The RFP should be signed by the applicant or any person duly authorized to bind the RFP. The signatory should give a declaration that the person is empowered to sign the RFP document.
- Bank may accept or reject, in full or in part, any or all the offers, without assigning any reason whatsoever.
- Bank may at its discretion abandon the process of the selection of IS Auditor anytime before notification of award.
- All responses should be in English language. All responses to this Request for proposal shall be binding on such applicants for a period of 180 days from the date of bid closure.
- The original and all copies of applications shall be typed or printed in a clear typeface. Copies may be good quality photocopies of the original.
- Bank will not be responsible for any delay due to postal service or any other means

Amendments to RFP

- Amendments to the RFP 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 Applicant, prior to the deadline for the submission of applications.
- The amendments will be binding on all the applicants. 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 applicants reasonable time to take the amendment into account in preparing their bid, the Bank may at its discretion extend the deadline for submission of applications.

Confidentiality

- Applicants agrees that all information gathered from the Bank including oral enquires, letters, documents, emails, presentations, interactions, technical

documentation, discussions with Bank / it's service providers and documents gathered from Bank / it's service providers etc,. related to the Bank's business and other information are to be treated as confidential information of Bank.

- The Bank would insist on signing a 'Non-Disclosure Agreement' with the Applicants who further qualify for the audit assignment.
- Unauthorized disclosure of any such confidential information will amount to breach of contractual terms and in such cases Bank may pre-maturely terminate the contract and initiate any legal action as deemed fit.
- This RFP document is the property of the Bank and this cannot be copied or used in any other manner except for the purpose of responding to this expression of interest notice or without written permission from the Bank.
- All the documents submitted along with applications shall also become the property of the Bank and retained by the Bank unless otherwise specifically mentioned.
- The applicant should mention whether the applicant is having any contractual obligation presently with the Bank, its status and any conflict of interest has arisen in such contractual obligation.

Commercial Quote

The Commercial quote should contain the total project cost, on a fixed cost basis. Bank will not provide any reimbursement for traveling, lodging/ boarding, local conveyance or any other related expenses. Format for quoting for commercial bid is as below and be made in firm's letter head and annexed to the application:-

Format for quoting for commercial bid

Name of the audit assignment	Audit Professional fee (Rs.)	Taxes, if any (Rs.)	Total cost (Rs.)
Concurrent IT Audit			

Sealing and Marking of Applications

The offer should be submitted in sealed covers, super scribed as below:

CONFIDENTIAL **BID FOR TMB CONCURRENT IT AUDIT**

Contact Details

The contact details for submitting the proposal is as follows:

The Head of Internal Audit
Tamilnad Mercantile Bank Ltd.,
IS Audit Cell, Inspection Department,
56 & 57, Beach Road (Upstairs)
Thoothukudi – 628 001
(Tel: 0461-2332113)

Last date for application

Last date for application along with commercial bid to reach the above address: **08.04.2024**

Encl: As above.

Date: 28.03.2024
Place: Thoothukudi

ANNEXURE – I

(Annexed to the application for the Concurrent IT Audit assignment)

Applicant Profile

Description	Details
The registered name of the Applicant	
Constitution	
Names of Proprietor / Partners	
Applicant's registered address	
Contact addresses if different from above	
Applicant address for correspondence	Address: STD- phone: e-mail Id: FAX No:
Contact name of the official who can commit on the contractual terms and the name of an alternate official who may be contacted in the absence of the former	Primary contact: Name: Designation: STD- phone no: Mobile phone : e-mail ID : Alternate contact: Name : Designation: STD- phone no: Mobile phone : e-mail ID :
Core business of applicant	
Applicant's organization has been in existence since (date)	
Applicant is registered with Cert-IN	

<table>
<tr><th>Description</th><th>Details</th></tr>
<tr><td>Applicant is engaged in Concurrent IT Audits since (month & year)</td><td></td></tr>
<tr><td>Whether Concurrent IT Audit is a core function of the applicant?</td><td></td></tr>
<tr><td>Details of assignments where the Applicant has performed Concurrent IT Audits in Banks.</td><td></td></tr>
<tr><td>Names of the Banks where Concurrent IT Audit was undertaken by the applicant till 31.03.2024</td><td>
<table>
<tr><td>Name of the Bank</td><td>Audit begin-date</td><td>Audit end-date</td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
</table>
Explain audit experience in Concurrent IT Audits:

Indicate if any of the audit scope that was outsourced:
</td></tr>
<tr><td>Concurrent IT Audits carried out till 31.03.2024 at other organizations</td><td></td></tr>
<tr><td>Concurrent IT Audit Methodology used</td><td></td></tr>
<tr><td>Applicant’s experience in Concurrent IT Audits</td><td></td></tr>
<tr><td>Applicant confirms that there are no legal actions / restrictions by any regulatory authority that would affect the ability to deliver audit deliverables</td><td></td></tr>
<tr><td>The applicant confirms that they fully comply with the “Eligibility Criteria (4)” as mentioned in the RFP.</td><td></td></tr>
</table>

Description	Details
Qualifications of project leads that have led prior Concurrent IT Audit assignments in a Bank	CISA : CISSP : Individual Curriculum Vitae of project leads and other key personnel enclosed.
Number of professional manpower available for Concurrent IT Audits	Number 1. CISA/CISM : 2. CISSP : 3. BS7799/ ISO 27001 LA: 4. CCNA/CCNE : 5. DISA/ISA : 6. Others :
Total number of employees (Please attach profile of each employee)	
Man days estimate	

Certified that the above particulars are true and correct to the best of our knowledge and belief.

Authorized signatory with seal
(To be signed by the legally authorized signatory)

Date :

Place: