

REQUEST FOR PROPOSAL
FOR
IS AUDIT OF RTGS AND NEFT RELATED SYSTEMS

Ref No:HO.ID.Ex.ISA/03/ 2024-25

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

Disclaimer

While the document has been prepared in good faith, no representation or warranty, express or implied, is or will be made, and no responsibility or liability will be accepted by Tamilnad Mercantile Bank Ltd., (TMB) or any of its employees, in relation to the accuracy or completeness of this document and any liability thereof expressly disclaimed. The RFP is not an agreement and is not an offer by TMB, but an invitation for bidder's responses. No contractual obligation on behalf of TMB, whatsoever, shall arise from the offer process unless and until a formal contract is signed and executed by duly authorized officials of TMB and the Bidder

1. Introduction

Tamilnad Mercantile Bank Ltd, has its Head Office at 57, V.E Road, Thoothukudi 628001.

Tamilnad Mercantile Bank Limited is hereinafter called “Bank”, issues this ‘Request for Proposal’, hereinafter called “RFP”. This RFP seeks to engage an Audit Firm, which has the capability to conduct independent review and to evaluate the effectiveness of the Bank’s Information Technology and Information Security Policies 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 Audit assignment.

An applicant submitting the proposal in response to RFP shall hereinafter be referred to as “Applicant / Audit Firm/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. Broad Scope of Work

The scope of work to conduct an Information Systems Audit of RTGS and NEFT related systems is including the following Baseline Cyber Security Guidelines of RTGS and NEFT issued by RBI:

- 1. Inventory Management*
- 2. Prevention of installation of unauthorized software*
- 3. Network Security*
- 4. Change and Patch Management*
- 5. Access Management*
- 6. Email Security*
- 7. Continuous surveillance*
- 8. Disaster recovery drills*
- 9. Backup*
- 10. Compliance to Master Direction on Digital Payment Security Controls related to Internet/ Mobile Banking (refer RBI Circular DoS.CO.CSITE.SEC. No.1852/ 31.01.015/ 2020-21 dated February 18, 2021), as updated from time to time.*
- 11. Application Security Life Cycle (ASLC)*
- 12. Log management*
- 13. Conduct Vulnerability Assessment (VA) and Penetration Testing (PT)*
- 14. Cryptographic controls – Adherence to latest IDRBT CA guidelines related to cryptographic devices and digital certificates.*
- 16. Transaction Monitoring*
- 17. Security Operations Centre (SOC)*
- 18. Adherence to rules & guidelines of INFINET, INFINET framework and SFMS, as updated from time to time.*
- 19. Compliance to the guidelines on storage of payment system data*

Detailed Baselines cyber security controls issued by RBI for RTGS and NEFT is enclosed as Annexure – I

3. Audit deliverables:

- The audit firm should follow applicable IS audit standards to provide reasonable assurance about the status of compliance to the guidelines mentioned in the Scope.
- The IS audit report shall be accompanied with the IS audit standards followed by the auditor along with detailed IS audit procedures employed.

- The report shall also be accompanied with artifacts and evidence collected in respect of each item to substantiate its observations.
- Audit firms shall submit a certificate confirming compliance by the Bank with baseline cyber security guidelines for RTGS and NEFT.

Audit firm has to submit draft findings/report of the Audit to IS Audit Cell on every Friday during the course of audit. In addition to the same, Executive summary is to be submitted in excel dash board.

Audit report to be submitted with criticality (Very High /High / Medium / Low) of the observation, Impact and Recommendation to mitigate the Risk as per the following format:

S.No	Audit area / Department	Observations	Risk Rating (Low/Medium/ High)	Risk / Implications	Recommendations

Auditor shall provide unbiased advice to the Bank in relation to the improvement in the process/IT System.

Executive Summary, including positive observations and areas where further improvements are needed is to be provided. Audit Reports shall be shared through e-mail with digitally signed in A-4 size. (Soft copies of all the documents properly encrypted/password protected in MS Word /MS Excel /PDF format). In additions, Audit observations and Executive summary are to be shared in excel.

4. Resources requirement:

Audit activities shall be conducted from IT Department, Chennai and Thoothukudi. The list of Audit team members, project manager to be assigned to this project and their profile, copy of certifications, relevant experience and background check should be submitted to the Bank along with RFP.

The resource to be engaged with the Bank must have IS Audit Experience of 2 or more years and should be on permanent roll of the organization. Franchise / Sub-Contracting of IS Auditor work will not be permitted under any circumstances. Resources to be provided onsite along with Team leader, who should possess CISA / CISSP certification.

5. Eligibility Criteria

1. Audit Firm shall be a Cert-In empaneled organization.
2. Audit Firm should have more than two years of experience in doing Bank / FIs IS Audit. [Evidence shall be shared].
3. Auditors shall possess requisite qualifications such as CISA (offered by ISACA) or CISSP (offered by ISC2), along with two or more years of IS Audit experience in auditing Bank/Financial Institutions. They should be competent audit professionals with sufficient and relevant experience.
4. Auditors should possess skills to carry out the audit on the above mentioned scope of work
5. Audit firm should earn profit for at least last two years.

Audit Experience, Resource competency, Man-days requirement and commercials quoted are the major consideration factors for selection of the audit firm.

Disqualification / Conflict of Interest: The Applicant is not eligible to take up the assignment, in case they fall 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 have 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.

6. Application Processes

General Terms of Bid Submission

- Each applicant should not submit more than one RFP. RFPs arriving beyond the stipulated time will not be accepted. Bank will not be responsible for any delay due to postal service or any other means.
- The RFP should be signed by the applicant or any person duly authorized to bind the firm. 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 any time before notification of award without assigning any reason.
- All responses should be in English language. All responses to this RFP shall be binding on such applicants for a period of 180 days from the date of bid closure.

Amendments to RFP

- Amendments to the RFP 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.

- Applicant who further qualifies for the audit assignment shall execute a 'Non-Disclosure Agreement' with the Bank as per Bank's format.
- 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.

7. Other Terms and Conditions

- 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 RFP 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.
- The firm should not have abandoned any project, i.e mid-way previously.
- No adverse remarks or disciplinary proceedings should be pending or initiated against the firms or proprietor or any of its partners with respect to the professional matters of conduct.
- The auditors / audit firms should not sub-contract the audit assigned to them.
- The RFP shall be governed by and construed in accordance with the laws of India, and any disputes arising out of or in connection with this RFP shall be subject to the jurisdiction of the courts in Thoothukudi.
- By submitting a proposal, the Bidder acknowledges that they have read, understood and accepted the terms and conditions specified in the RFP.
- Terms of Payment: Professional fee sanctioned will be paid after completion of the audit and submission of reports. All out of pocket expenses, travelling, boarding and lodging expenses for the entire team of assignment shall be included in the quoted commercial and the firms is not entitled to charge any additional costs on account of any items or services or by any of any out-of-pocket expenses, including travel, boarding and lodging etc., No escalation in

the costs / Fees / charges of services rendered by IS Auditor is permitted for any reason whatsoever. Bank will not pay any out-of-pocket expenses.

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 technical and commercial bid is as below and to be duly signed and made in firm's letter head. ***The same should be submitted in a separate sealed cover with the application:-***

Format for quoting for technical and commercial bid

Name of the audit assignment	Composition of the team	Man-days requirement	Audit Professional fee (₹)	Taxes, if any (₹)	Total cost (₹)
IS Audit of RTGS and NEFT related systems					

Sealing and Marking of Applications

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

CONFIDENTIAL
BID FOR IS AUDIT OF RTGS AND NEFT RELATED SYSTEMS OF THE BANK

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

Last date for application

Last date for application along with commercial bid to reach the above address: **18.03.2025**

Date: 05.03.2025

Place: Thoothukudi

Applicant Profile (To be annexed to the Application)

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:
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 :
Applicant's organization has been in existence since (date)	
Applicant is registered with Cert-IN	
Applicant firms is earning profit for at least last two years?	
Applicant is engaged in Information Systems Audits since (month & year)	

Description	Details																				
Whether Information Systems Audit is the core function of the applicant?																					
Details of prior IS audit projects withdrawn / cancelled before completion.																					
Details of assignments where the Applicant has performed Audit of RTGS and NEFT Related Systems.	<p><u>List of Public Sector Banks/Private Sector Banks/Financial Institutions:</u></p> <p>(Please enclose relevant evidence)</p>																				
Names of the Banks where IT/IS Audit was undertaken by the applicant from 01.01.2020 till 31.01.2025.	<table border="1" data-bbox="678 828 1460 1075"> <thead> <tr> <th>Name of the Bank</th> <th>Name of the Audit</th> <th>Audit Start Date</th> <th>Audit end-date</th> </tr> </thead> <tbody> <tr><td> </td><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td><td> </td></tr> </tbody> </table> <p>(Please enclose relevant evidence)</p>	Name of the Bank	Name of the Audit	Audit Start Date	Audit end-date																
Name of the Bank	Name of the Audit	Audit Start Date	Audit end-date																		
Legal actions / restrictions by any regulatory authority that would affect the ability to deliver audit deliverables.	(Please submit in letter head)																				
Compliance to the “Eligibility Criteria” as mentioned in the RFP Page No.5.	(Please submit in letter head)																				
Total No of IS Auditors in the Firm																					
Number of professional resource available for IS audits	<p style="text-align: right;">Number</p> <p>1. CISA : 2. CISSP : 3. CCNA/CCNE : 4. Others :</p>																				
Name of the project Manager to be engaged in the proposed project (Please enclose the profile of project Manager)	<table border="1" data-bbox="678 1769 1460 1870"> <thead> <tr> <th>S.No</th> <th>Name of the project manager</th> <th>Qualification</th> <th>IS Audit Experience</th> </tr> </thead> <tbody> <tr> <td>1.</td> <td> </td> <td> </td> <td> </td> </tr> </tbody> </table> <p>(Note: If any change in the above list, while taking up the audit or during the audit, prior approval from Bank should be obtained)</p>	S.No	Name of the project manager	Qualification	IS Audit Experience	1.															
S.No	Name of the project manager	Qualification	IS Audit Experience																		
1.																					

Description	Details																								
<p>Total number of field level auditors (Team lead and other auditors) to be engaged in the proposed project: (Please enclose the profile of each of the field level auditors)</p>	<p>List of the Auditors to be engaged in field level auditing:</p> <table border="1" data-bbox="678 425 1460 627"> <thead> <tr> <th>S.No</th> <th>Name of the Field level Auditor</th> <th>Qualification</th> <th>IS Audit Experience</th> </tr> </thead> <tbody> <tr> <td>1.</td> <td></td> <td></td> <td></td> </tr> <tr> <td>2.</td> <td></td> <td></td> <td></td> </tr> <tr> <td>3.</td> <td></td> <td></td> <td></td> </tr> <tr> <td>4.</td> <td></td> <td></td> <td></td> </tr> <tr> <td>5.</td> <td></td> <td></td> <td></td> </tr> </tbody> </table> <p>(Note: If any change in the Field level auditors, while taking up the audit or during the audit, prior approval from Bank should be obtained)</p>	S.No	Name of the Field level Auditor	Qualification	IS Audit Experience	1.				2.				3.				4.				5.			
S.No	Name of the Field level Auditor	Qualification	IS Audit Experience																						
1.																									
2.																									
3.																									
4.																									
5.																									
<p>Man-days estimate</p> <p>(Estimate for presentation to Top Management shall also be included)</p>																									

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 :