

REQUEST FOR PROPOSAL
FOR
INFORMATION SYSTEMS AUDIT of TMB

Ref No:HO.ID.Ex.ISA/01/ 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

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 Information Systems 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 IS Audit assignment.

An applicant submitting the proposal in response to RFP for IS Audit 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 for IS Audit

A Risk based IS audit report shall indicate ratings for High, Medium and low risk areas and recommendations. The Broad Scope of work for Audit follows:

S.No	Audit Areas																																																										
1.	Availability and adequacy of the documented policies/Plan/SOPs etc., Audit on 55 Nos of Applications / Security Solutions.																																																										
2.	<table border="1"> <thead> <tr> <th>S.No</th> <th>Name of application/Solution</th> </tr> </thead> <tbody> <tr><td>1</td><td>QRADAR - SIEM</td></tr> <tr><td>2</td><td>Forescout - Network Access Control (NAC)</td></tr> <tr><td>3</td><td>Forcepoint Data Leakage Prevention (DLP)</td></tr> <tr><td>4</td><td>F 5 WAF and IBM Guardium DAM</td></tr> <tr><td>5</td><td>Trend Micro XDR</td></tr> <tr><td>6</td><td>ATM Terminal Security Solution (TSS) - NCR (EPO)</td></tr> <tr><td>7</td><td>ATM Terminal Security Solution (TSS) - NCR - (Securedoc)</td></tr> <tr><td>8</td><td>ATM Terminal Security Solution (TSS) - Hitachi - (HIPA)</td></tr> <tr><td>9</td><td>ATM Terminal Security Solution (TSS) - Hitachi - (Scanplus)</td></tr> <tr><td>10</td><td>ATM Terminal Security Solution (TSS) - Hyosung - (Checker)</td></tr> <tr><td>11</td><td>ATM Terminal Security Solution (TSS) - OKI - (Checker)</td></tr> <tr><td>12</td><td>Manage Engine</td></tr> <tr><td>13</td><td>Deep Security Solution</td></tr> <tr><td>14</td><td>Zabbix Monitoring Tool</td></tr> <tr><td>15</td><td>Dynatrace - CBS Application Monitoring Tool</td></tr> <tr><td>16</td><td>Attivo Networks - Deception Services (Honeypots)</td></tr> <tr><td>17</td><td>Microsoft System Center Configuration Manager (SCCM)</td></tr> <tr><td>18</td><td>Big Fix Solution</td></tr> <tr><td>19</td><td>Bio-metric Application</td></tr> <tr><td>20</td><td>Online Dispute Resolution System</td></tr> <tr><td>21</td><td>PFMS Solution</td></tr> <tr><td>22</td><td>MSME - Leading Origination System (LOS)</td></tr> <tr><td>23</td><td>Altum Application - Call Center</td></tr> <tr><td>24</td><td>Privileged Access Management (PAM)</td></tr> <tr><td>25</td><td>Integrated API Management solution</td></tr> <tr><td>26</td><td>Online Deposit Opening</td></tr> <tr><td>27</td><td>ATM - OTC – Securam</td></tr> <tr><td>28</td><td>ATM - OTC - S N G</td></tr> </tbody> </table>	S.No	Name of application/Solution	1	QRADAR - SIEM	2	Forescout - Network Access Control (NAC)	3	Forcepoint Data Leakage Prevention (DLP)	4	F 5 WAF and IBM Guardium DAM	5	Trend Micro XDR	6	ATM Terminal Security Solution (TSS) - NCR (EPO)	7	ATM Terminal Security Solution (TSS) - NCR - (Securedoc)	8	ATM Terminal Security Solution (TSS) - Hitachi - (HIPA)	9	ATM Terminal Security Solution (TSS) - Hitachi - (Scanplus)	10	ATM Terminal Security Solution (TSS) - Hyosung - (Checker)	11	ATM Terminal Security Solution (TSS) - OKI - (Checker)	12	Manage Engine	13	Deep Security Solution	14	Zabbix Monitoring Tool	15	Dynatrace - CBS Application Monitoring Tool	16	Attivo Networks - Deception Services (Honeypots)	17	Microsoft System Center Configuration Manager (SCCM)	18	Big Fix Solution	19	Bio-metric Application	20	Online Dispute Resolution System	21	PFMS Solution	22	MSME - Leading Origination System (LOS)	23	Altum Application - Call Center	24	Privileged Access Management (PAM)	25	Integrated API Management solution	26	Online Deposit Opening	27	ATM - OTC – Securam	28	ATM - OTC - S N G
	S.No	Name of application/Solution																																																									
	1	QRADAR - SIEM																																																									
	2	Forescout - Network Access Control (NAC)																																																									
	3	Forcepoint Data Leakage Prevention (DLP)																																																									
	4	F 5 WAF and IBM Guardium DAM																																																									
	5	Trend Micro XDR																																																									
	6	ATM Terminal Security Solution (TSS) - NCR (EPO)																																																									
	7	ATM Terminal Security Solution (TSS) - NCR - (Securedoc)																																																									
	8	ATM Terminal Security Solution (TSS) - Hitachi - (HIPA)																																																									
	9	ATM Terminal Security Solution (TSS) - Hitachi - (Scanplus)																																																									
	10	ATM Terminal Security Solution (TSS) - Hyosung - (Checker)																																																									
	11	ATM Terminal Security Solution (TSS) - OKI - (Checker)																																																									
	12	Manage Engine																																																									
	13	Deep Security Solution																																																									
	14	Zabbix Monitoring Tool																																																									
	15	Dynatrace - CBS Application Monitoring Tool																																																									
	16	Attivo Networks - Deception Services (Honeypots)																																																									
	17	Microsoft System Center Configuration Manager (SCCM)																																																									
	18	Big Fix Solution																																																									
	19	Bio-metric Application																																																									
	20	Online Dispute Resolution System																																																									
	21	PFMS Solution																																																									
	22	MSME - Leading Origination System (LOS)																																																									
	23	Altum Application - Call Center																																																									
	24	Privileged Access Management (PAM)																																																									
	25	Integrated API Management solution																																																									
	26	Online Deposit Opening																																																									
27	ATM - OTC – Securam																																																										
28	ATM - OTC - S N G																																																										

	29	GBM Solution
	30	Asset Liability Management & Funds Transfer Pricing OFSAA
	31	Board Pac Meeting application
	32	Credit Card Online Registration
	33	Online Demat Account opening
	34	Delight Card Online
	35	Online Scholarship
	36	Risk Control and Self Assessment (RCSA) training portal
	37	Auto EXE – Robotic Process Automation (RPA)
	38	Trade Connect
	39	VAPT compliance
	40	UPI QR view portal
	41	Asset Inventory Management (One touch portal)
	42	Knowledge Management Tool
	43	e-Circular
	44	Pensioner Life Certificate Portal
	45	Career Portal
	46	Veeam Backup Solution
	47	Commvault Backup Solution
	48	Document Management System
	49	E-Learning – TMB Smart
	50	eThics – Stock Audit Application
	51	Online card Tokenization portal
	52	CORMS
	53	KTM kiosk tool Monitoring
	54	RBI DEAF
	55	Ticketing Tool (OTRS)
3.	API Security Audit.	
4.	Audit of ATM Application, ATM Switch Functionality, Interface Audit, Audit Trails, Transmission Security, Review of fallback/ fail over procedures, DR capabilities, Operational Control, Reconciliation/ Functional Managerial activities, Card / PIN Management cum Security Review, Malware analysis in select 5 Nos of ATMs.	
5.	Network security architecture review, Network administration, User administration and access management on DC / DR and critical network components, Privileged access to DC / DR network components, Network / device redundancy, Network monitoring, security event identification, Firewall and security component configuration, Security in Digital payment	

	products gateways, Remote access management, Patch management, Auditing and logging, Network utilization, Access to Network resources and control
6.	Swift Operation and functionality, Assessment on Swift Customer Security Controls Framework
7.	Bank's website, Mail system and Social media audit
8.	Information Systems audit of minimum 3 CBS branches (along with onsite and offsite ATMs, CVMs, CDK, BNA, E-Lobby, etc.. attached to the identified Branches)
9.	Asset Management, Access Control, HSM Security, BCP and DR preparedness, Change Management, Incident Management, Database & Server Management, Log Management, Capacity Management, Backup Management, Patch Management, Record Management and media handling.
10.	Compliance validation of CSITE advisories and Regulatory directions.

3. Submission of report of the Audit Findings: -

Audit activities shall be conducted from IT Department, Chennai and Thoothukudi. Required background verification of the project manager and field level auditors shall be done by the selected audit firm and provided to the bank before commencement of audit as per scope. Selected Audit firm required to provide the audit checklist with risk parameter prior to conduct of audit.

Document the security gaps i.e. vulnerability, security flaws, loopholes, etc. observed during the course of the review. Document the risk and offer recommendations for addressing these security gaps and categorize the identified security gaps based on their criticality.

The auditor shall surrender all the working papers / evidence / audit documents collected during the course of audit to the Bank at the end of assignment.

Audit firm has to submit draft findings/report of the Audit to IS Audit Cell on every Friday during the course of audit. Separate report for each of the line items of Point No.1-10 (Page No.3-5: Scope of Work for IS Audit) to be submitted with criticality (Very High /High / Medium / Low) of the observation, Impact and Recommendation to mitigate the Risk. In addition to the same, Executive summary is to be submitted in excel dash board.

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 (for each 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.

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

4. Eligibility Criteria

Applicant should possess skills that are commensurate with the technology used by the bank. 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 as required and also shall confirm that they fully comply with the eligibility criteria in the Pro-forma (Annexure).

Audit firm enrolled in the empanelment of the Cert-IN as an IT security Auditing Organizations are also eligible for conducting IS audit.

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. The cooling period of an Audit firm, after the service of two years will be one year, provided they have not in any way conducted any form of auditing in the bank during that cooling period.
9. 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.
10. Audit Firm should earn profit for at least last two years.

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 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 of IS Auditor anytime before notification of award without assigning any reason.
- 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 of good quality.
- 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.
- 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.

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 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.
- The firm should not have abandoned any project, i.e mid-way previously.

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 for TMB					

Sealing and Marking of Applications

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

<p><u>CONFIDENTIAL</u></p> <p>BID FOR TMB IS AUDIT SERVICES</p>

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: **18.01.2025**

Date: 26.12.2024

Place: Thoothukudi