REPCO HOME FINANCE LIMITED

REQUEST FOR PROPOSAL
FOR CONDUCTING
VULNERABILITY ASSESSMENT AND
PENETRATION TESTING

EDP Department
Corporate Office
Repco Home Finance Ltd.,
Alexander Square Third Floor,
New No : 2,Old No : 34/35,
Sardar Patel Road, Guindy,
Chennai - 600032.
Phone : (044) - 42106650 / 42106652,
Mobile : 9884835519 Fax : (044) - 42106651,
E-mail : edp@repcohome.com

The consultants conducting VAPT should be Certified penetration testers and their registrationcertificate should be currently valid.(Attach proof)

I. ABOUT REPCO HOME FINANCE LTD (RHFL):

RHFL is a professionally managed housing finance company, head quartered in Chennai, Tamil Nadu. The company was incorporated in April 2000 to tap the growth potential in the housing finance market. We had been registered with National Housing Bank. As of now, RHFL is operating through 141 branches and **24** satellite centres in Tamil Nadu, Andhra Pradesh, Telengana, Jharkhand, Kerala, Karnataka, Maharashtra, Madhya Pradesh, Gujarat, Odisha, West Bengal and Puducherry.

II. OBJECTIVE

RHFL wishes to engage competent Service Provider (SP) for carrying out Vulnerability Assessment and Penetration Testing of internet facing applications and underlying infrastructure deployed at RHFL's Data Centre in Chennai, Disaster Recovery Centre in Bangalore, and 5 identified branches. Based on the contents of the RFP, the selected Bidder shall be required to independently arrive at approach and methodology, based on industry best practices and RBI guidelines, suitable for RHFL, after taking into consideration the effort estimate for completion of the same and the resource and the equipment requirements. The approach and methodology will be approved by RHFL. RHFL expressly stipulates that the Consultant's selection under this RFP is on the understanding that this RFP contains only the principal provisions for the entire assignment and that delivery of the deliverables and the services in connection therewith are only a part of the assignment. The selected Bidder shall be required to undertake to perform all such tasks, render requisite services and make available such resources as may be required for the successful completion of the entire assignment at no additional cost to RHFL.

III. REQUIREMENT SPECIFICATION:

SCOPE

Vulnerability Assessment and Penetration Testing should cover RHFL's Information System Infrastructure which includes Networking systems, Security devices, Servers, Databases, Applications, Systems accessible with public IP's, etc. Selected bidder should carry out an assessment of Threat & Vulnerabilities assessments and assess the risks in RHFL's Information Technology Infrastructure. This will include identifying existing threats, if any, and suggest remedial solutions and recommendations of the same to mitigate all identified risks, with the objective of enhancing the security of Information Systems. In addition to the remote Assessment, selected Bidder shall also perform the onsite assessment of the assets under the Scope of the RFP.

VAPT activities:

VAPT should be comprehensive but not limited only to the following activities:

•Network Scanning • Port Scanning • System Identification & Trusted System Scanning • Vulnerability Scanning • Malware Scanning • Spoofing • Scenario Analysis • Application Security Testing & Code Review • OS Fingerprinting • Service Fingerprinting • Access Control Mapping• Denial Of Service (DOS) Attacks • DDOS Attacks • Authorization Testing • Lockout Testing • Password

Cracking • Cookie Security • Functional validations • Containment Measure Testing • War Dialing• DMZ Network Architecture Review • Firewall Rule Base Review • Server Assessment (OS Security Configuration) • Security Device Assessment • Network Device Assessment • Database Assessment • Website Assessment (Process) • Vulnerability Research & Verification • IDS/IPS review & Fine tuning of Signatures • Man in the Middle attack • Man in the browser attack • Any other attacks.

Broad Details of the systems are given below:

Device Type	Quantity(DC)	Quantity(DR)
Servers	14	3
Database	3	0
Network Devices	3	2
Security Devices	1	1
Storage Devices	1	0
VAPT External IPs	1	1
VAPT Internal IPs	15	4

List of Applications:

- **Core Banking Solution**
- **Loan Originating System**

VAPT Phases: Vendor has to undertake VAPT/Security testing in phased manner as described below

Phase I: Conduct VAPT/Security testing as per the scope, Evaluation & Submission of Preliminary Reports of findings and discussions on the finding.

Phase II: Submission of Final Report

Phase I

a. Conduct VAPT as per the scope defined in RFP without disturbing operations

RHFL will call upon the selected Bidder, on placement of the order, to carry out demonstration and/or walkthrough, and/or presentation and demonstration of all or specific aspects of the VAPT activity.

VAPT schedule to be provided 7 working days prior to the start of activity along with the team member details. A dedicated Project Manager shall be nominated, who will be the single point of contact for VAPT Activity in Chennai and other locations.

Execute Vulnerability Assessment and Penetration testing of RHFL's IT Infrastructure and Applications as per the scope on the written permission of RHFL and in the presence of RHFL's Officials.

b. Detailing the Security Gaps

Detailing the System setup used and the tests conducted in assessment.

Analysis of the findings and Document the security gaps i.e. vulnerability, security flaws, loopholes, threats, etc. observed during the course of the VAPT activity as per the scope of work.

Document recommendations and solutions for addressing these security gaps and categorize the identified security gaps based on their criticality.

Chart a roadmap for RHFL to ensure compliance and address these security gaps.

c. Addressing the Security Gaps

Recommend Actionable fixes for systems vulnerabilities in design or otherwise for application systems and network infrastructure. If recommendations for Risk Mitigation /Removal could not be implemented as suggested, alternate solutions to be provided.

Suggest changes/modifications in the Security Policies implemented along with Security Architecture including Network and Applications of RHFL to address the same.

The Draft report of the VAPT findings should be submitted to RHFL for Management comment.

Phase II

a. **Submission of Final Reports**
   The Service Provider should submit the final report of VAPT findings as per the report format mentioned in Deliverables. All the VAPT reports submitted should be signed by technically qualified persons and he/she should take ownership of document and he/she is responsible and accountable for the document/report submitted to RHFL. The final report has to be submitted within 15days of submission of the initial draft report. Service provider will also submit the Executive Summary Report of RHFL's Internet facing environment.

b. **Acceptance of the Report**
   The Report shall be accepted on complying with the formats of VAPT Report as mentioned in the RFP and acceptance of the audit findings.

Deliverables:

The deliverables for VAPT activity are as follows:

a. Execution of Vulnerability Assessment and Penetration Testing for the identified network devices, security devices, servers, applications, websites, interfaces(part of application) etc. as per the Scope mentioned in this RFP and Analysis of the findings and guidance for resolution of the same
b. VAPT Report

The VAPT Report should contain the following:

- Identification of Auditee (Address & contact information)
- Dates and Locations of VAPT

- Terms of reference
- Standards followed
- Summary of audit findings including identification tests, tools used and results of tests performed (like vulnerability assessment, penetration testing, application security assessment, website assessment, etc.)
    - Tools used and methodology employed
    - Positive security aspects identified
    - List of vulnerabilities identified
    - Description of vulnerability
    - Risk rating or severity of vulnerability
    - Category of Risk: Very High / High / Medium / Low
    - Test cases used for assessing the vulnerabilities
    - Illustration of the test cases
    - Applicable screenshots.
    - Analysis of vulnerabilities and issues of concern
    - Recommendations for corrective action
    - Personnel involved in the audit

The Service Provider may further provide any other required information as per the approach adopted by them and which they feel is relevant to the audit process. All the gaps, deficiencies, vulnerabilities observed shall be thoroughly discussed with respective RHFL officials before finalization of the report.

The VAPT Report should comprise the following sub reports:

VAPT Report – Executive Summary:

The vendor should submit a report to summarize the Scope, Approach, Findings and recommendations, in a manner suitable for senior management. Selected Bidder will also detail the positive findings (No Gap found) for various tests conducted.

VAPT Report – Core Findings along with Risk Analysis:

The vendor should submit a report bringing out the core findings of the VAPT conducted for network devices, security devices, servers and websites.

VAPT Report – Detailed Findings/Checklists:

The detailed findings of the VAPT would be brought out in this report which will cover in details all aspects viz. identification of vulnerabilities/threats 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 for conducting the VAPT activity as per the scope, should also be included in the report separately for Servers (different for different

OS), application, Network equipment, security equipment etc , so that they provide minimum domain wise baseline security standard /practices to achieve a reasonably secure IT environment for technologies deployed by RHFL. The Reports should be substantiated with the help of snap shots/evidences /documents etc. from where the observations were made.

VAPT Report – In Depth Analysis of findings /Corrective Measures & Recommendations along with Risk Analysis: -

The findings of the entire VAPT Process should be critically analysed and controls should be suggested as corrective /preventive measures for strengthening / safeguarding the IT assets of RHFL against existing and future threats in the short /long term. Report should contain suggestions/recommendations for improvement in the systems wherever required.If recommendations for Risk Mitigation /Removal could not be implemented as suggested, alternate solutions to be provided. Also, if the formal procedures are not in place for any activity, evaluate the process and the associated risks and give recommendations for improvement as per the best practices.

Documentation Format:

- All documents will be handed over in three copies, signed, legible, neatly and robustly bound on A-4 size, good-quality paper.
- Soft copies of all the documents properly encrypted in MS Word /MS Excel /PDF format also to be submitted in CDs/DVDs along with the hard copies.
- All documents shall be in plain English.

Adherence to Standards:

The vendor should use the latest ISO27001 and PCI-DSS standards, RBI and Cert-In Guidelines in carrying out task as per Scope of Work. The vendor should adhere to all the applicable laws of land and rules, regulations and guidelines prescribed by various regulatory, statutory and Government authorities.

Estimated work plan and time schedules for providing services for this assignment.

- Effort estimate and elapsed time are to be furnished.
- Details of inputs, infrastructure requirements required by the Vendor to execute this assignment.

Details of the Vendor's proposed methodology/approach with reference to the scope of work.

IV. PRE-QUALIFICATION CRITERIA

1. Partnership Firm/ Public or Private Limited Company / Government Institutions / Public Sector / Private Companies / Any other entity, those have completed 5 years of business after the date of incorporation of business.
2. Minimum turnover of Rs.2 crores in any two years of last three financial years.
3. Applicant must be an RBI / Cert-in registered person with good credentials.

4. They must have performed VAPT in any Govt Institutions / Public sector Banks / private sector Banks / large corporate across the country. A satisfactory work completion letter from the customer has to be provided.
5. The applicants must have their Corporate Office / branch office in Chennai.
6. The participating vendors should submit a declaration that they have not been blacklisted by any organization elsewhere.

V. Method of Submission:

Details required, if any, can be collected from Mr. Pandiarajan K, AGM, EDP Dept at 044 42106650 or by person on any working day between 10 AM and 5 PM or email to edp@repcohome.com.

A large size cover containing the following Technical and Commercial details should be submitted to Chief Operating Officer in Corporate Office.

1. Technical details clearly describing the company profile, past work history with client list, proof of eligibility criterion should be submitted in a sealed envelope super scribing the envelope with **"Technical Proposal for conducting Vulnerability Assessment and Penetration Testing".**
2. The Commercial Proposal should be submitted in another sealed envelope super scribing the envelope with **"Commercial Proposal for conducting Vulnerability Assessment and Penetration Testing".**

Both the sealed envelopes should be submitted to the following address in a large size sealed envelope super scribing with **"Proposal For conducting Vulnerability Assessment and Penetration Testing",** on or before **06-11-2018, 05:00 pm by Speed Post/Courier.**

The Chief Operating Officer,
Repco Home Finance Ltd.,
III Floor, Alexander Square,
#2, Sardar Patel Road,
Guindy, Chennai - 600 032.

Proposals can also be dropped in the box available at the Corporate Office within the working hours on or before 06-11-2018, 5.00PM

After the closing date, the envelope containing the Technical proposal will be unsealed first by RHFL's Technical / Purchase Committee. The envelope containing the Commercial proposal will be unsealed only if the Technical proposal submitted by the vendor consists of the specification details as mentioned in "Requirement Details" and also the submission of necessary documentary proof for the details mentioned in "Pre-Qualification Criteria".

If the cover does not contain Technical and commercial proposals in separate sealed envelopes, then the same will not be considered by our Purchase Committee and the cover will be returned back to the vendor.

VI. Disclaimer:

RHFL reserves the right not to consider the proposals submitted by any vendor without assigning any reason whatsoever. Bringing any outside influence will lead to disqualification.

VII. GRIEVANCE MECHANISM:

Any Vendor participating in this process but aggrieved by the decision of the Company may submit his/her representation in writing (within 10 days of completion of the process) to:

The Chief Operating Officer,
REPCO HOME FINANCE LTD,
Third Floor, Alexander Square,
New No: 2, Sardar Patel Road, Guindy,
Chennai - 600 032.