



**Department of Information Technology**

**Engagement of Service Provider for availing Red Team Exercise Services by using automated tools and techniques(Re-tendering)**

**RFP Ref. No.UCO/DIT/4401/2021-22 Date: 09.03.2022**

**Pre-Bid Responses/ Clarifications to Queries raised by the Bidder(s), Amendments, Addendums and Corrigendum's published on 25/03/2022**

Sl. No.	RFP Page No.	RFP Clause No.	Original RFP Clause	Subject/Description	Query Sought/Suggestions of the Bidder	Response
1.	33	Part – IV	SCOPE OF WORK	The Red Team Exercise should support attack replay & attack import from PCAP (i.e. PCAP files should be provided for all attacks for analyzing & displaying by tools like burp site).	Please brief us on the expectation.	Please refer corrigendum enclosed herewith.
2.	34	Part – IV- B	Fingerprinting/ Vulnerability Identification Phase	NA	Please provide the IT infrastructure details, Application details.	Details would be shared with selected bidder. For other general details you may visit our Bank's website <a href="http://www.ucobank.com">www.ucobank.com</a>
3.	NA	NA	NA	NA	Can we do this audit remotely?	Red Team activities to be carried out from bank premises ONLY.

4.	NA	NA	NA	NA	Please let us know how many locations that you are expecting that needs to be covered under the SOW	Details would be shared with selected bidder. For other general details you may visit our Bank's website <a href="http://www.ucobank.com">www.ucobank.com</a>
5.	Page 33	Part IV		Scope of Work-Red Teaming Exercise to uncover the vulnerabilities in the bank's perimeter/ internal network( DC/ DR/ All branches)	Please share Infra Details, Network Architecture and No. of branches	Details would be shared with selected bidder. For other general details you may visit our Bank's website <a href="http://www.ucobank.com">www.ucobank.com</a>
6.	Page 33	Part IV		Scope of work	Job is to be done onsite or offsite, If ONSITE do we have to sit in HO and do the audit activities remotely for other branches including DC & DR	Red Team activities to be carried out from Bank's HO premises ONLY. Detailed plan will be shared with the selected bidder.
7.	Page 88		Annexure XIV	Non-Disclosure Agreement	1. Do we need to provide the Non-Disclosure agreement in stamp paper filling the agreement form or a covering letter confirming the same will work, 2. If Agreement to be executed at all on non-judicial stamp paper of requisite value (What will be the value)?	During bid submission the signed annexure on A4 to be submitted. Later, on accepting the contract, NDA should be executed on Non-judicial stamp paper as per the WB State Stamp Duty Act.
8.	Page 33	Part IV		Scope of Work-Red Teaming Exercise to uncover the vulnerabilities in the bank's perimeter/ internal network( DC/ DR/ All branches)	Please share Infra Details, Network Architecture and No. of branches	Details would be shared with selected bidder. For other general details you may visit our Bank's website <a href="http://www.ucobank.com">www.ucobank.com</a>
9.	33 of 105	Part – IV	Part – IV	Scope of Work	No of IPs , Application URL and Device Details	Details would be shared with selected bidder. For other general details you may visit our Bank's website <a href="http://www.ucobank.com">www.ucobank.com</a>

10.	33 of 105	Part – IV	Part – IV	Scope of Work	Total no of employee for phishing activity.	Details would be shared with selected bidder. For other general details you may visit our Bank's website <a href="http://www.ucobank.com">www.ucobank.com</a>
11.		Generic Query	Eligibility Criteria		We seek clarification from UCO Bank on whether a 'Large' enterprise or non-MSME enterprise can bid and whether a consortium is allowed and if so, whether an LLP can be part of the consortium.	It is clarified that consortium is not allowed, the selected bidder may have back to back contract with third party however the single point of contact for the bank will be the selected bidder.
12.		Generic Query			Is consortium allowed between two parties in this bid?	It is clarified that consortium is not allowed, the selected bidder may have back to back contract with third party however the single point of contact for the bank will be the selected bidder.
13.	Page-12	Clause No-10	Eligibility Criteria	Bank's existing vendors who are security integrators, network integrators will not be allowed to participate in this RFP	Referring to points of "an existing vendor to UCO bank as either Network Integrator or Security Integrator" not allowed to participate. Bidder is only providing Dark Web services in UCO Bank and in such scenarios, are we eligible to participate?	Clause is self-explanatory. The service referred here does not bar the bidder from participation.
14.	Page 9 of 105	Bid Control Sheet	Last Date and Time for receipts of tender bids	06/04/2022 at 04:00 PM	May we request to extend the proposal submission date till 15 April 2022.	Please refer corrigendum enclosed herewith.
15.	Page 10 of 105	3. Eligibility Criteria	Criteria, Point 1	Bidder should be a limited company (Public/Private) registered in India under the Companies Act, 1956/2013 for the last 3 years as on RFP issuance date. Companies registered as MSME Entrepreneur & still categorized as MSME as on RFP submission date.	We are registered in Ministry of Corporate Affairs under the rules 32(1) of the LLP rules, 2009.  We request you to allow us to participate in the bidding process.	Please refer corrigendum enclosed herewith.

				Bidder/Partner/Investor must adhere cross border sharing/FDI/FEMA and other regulatory guidelines of Govt of India. The bidder should not be a subsidiary of a foreign company.		
16.	Page 11 of 105	3. Eligibility Criteria	Criteria, Point 4	Bidder should have experience in Red Team Exercise assignment completed/ under implementation in at least 01 Scheduled Commercial Bank having Business Mix (Deposits + Advances of Scheduled Commercial Bank) of Rs. 2 Lakhs Crores and above in last 3 years in India as on bid submission date.	May we request to change the clause as follows for ease of participation: Bidder should have experience in Red Team Exercise assignment completed/ under implementation in at least 01 BFSI company/organization in last 3 years in India as on bid submission date.	Clause stands as per RFP
17.	Page 12 of 105	3. Eligibility Criteria	Criteria, Point 9	The Bidder should have at least 05 Offensive Security Certified Professional (OSCP) from offensive-security/ Certified Ethical Hacker (CEH) from EC-Council/ Licensed Penetration Tester (LPT) from EC-Council / GPEN: GIAC Penetration Tester from SANS/ GWAPT: GIAC Web Application Penetration Tester from SANS/ any other Red Team or Penetration Testing related certification as full time employee.	Part – IV Scope of Work, Page 37 states that: The Bidder should have at least 02 Offensive Security Certified Professional (OSCP) from offensive-security/ Certified Ethical Hacker (CEH) from EC-Council/ Licensed Penetration Tester (LPT) from EC-Council / GPEN: GIAC Penetration Tester from SANS/ GWAPT: GIAC Web Application Penetration Tester from SANS/ any other Red Team or Penetration Testing related certification as full time employee associated with the project team delivering the Red Team Exercise services in the role of Project Manager/ Co-ordinator for providing the proposed services to the UCO Bank.	Clause stands as per RFP,

					May we request to change the eligibility criteria aligning with Scope of Work requirement limiting to 2 OSCP certified professionals.	
18.	Page 15 of 105	PART – II INVITATION FOR BIDS AND INSTRUCTIONS TO BIDDERS	4. Earnest Money Deposit	RFP for engagement of service provider for availing Red Team Exercise services by using automated tools and techniques (Re-tendering)	Based on the quantity of work, may we request to change the EMD amount to Rs. 50,000/- (Rupees Fifty Thousand Only)	Clause stands as per RFP.
19.	Page 37 of 105	Part – IV SCOPE OF WORK	Clause D.	The Red Team Exercise should support executing external attacks from internet towards internal controls	May we request to clarify us if the assessment to be carried out from: 1) Internet, or; 2) Intranet, or; 3) Both internet and intranet	Clause stands as per RFP. Details would be shared with selected bidder. For other general details you may visit our Bank's website <a href="http://www.ucobank.com">www.ucobank.com</a>
20.	Page 10 of 105	PART I	2 Overview or Objective	Bank intends to engage a service provider for availing Red Team Exercise services by using automated tools and techniques (Re-tendering). Its objective is to simulate real scenario external attacks using automated tools under controlled environment that should facilitate the bank to identify the physical, hardware, software and human vulnerabilities that affect systems security across the organization.	If intranet will be included in the scope, please provide us the IT landscape that includes number of applications, server, OS, DB, number of internal & external IP address, etc.	

21.	Page 33 of 109	Part – IV SCOPE OF WORK		The Red Team Exercise should support attack replay & attack import from PCAP (i.e. PCAP files should be provided for all attacks for analyzing & displaying by tools like burp suite).	May we request the Bank to include both Burp state file and PCAP based on the tools requirement for this assessment.	Please refer corrigendum enclosed herewith.
22.	Page 33 of 105	Part – IV SCOPE OF WORK		Non-Destructive simulation Initiator would only be allowed to generate lightweight traffic. Tests in the production network should not be destructive (i.e. are only transport, not execution) - destructive behaviour tests are only done in the secure containers, a sandbox separated from the production network. Most network tests should be measured in hundreds of Kilobytes, which is very small.	RFP states to perform non-destructive simulation however, RFP also states to Carryout DDos attack exercise (Refer page 35 clause - I) and extract credentials and password hashes from operating systems memory (refer page 34 Clause C.iii)  May we request the Bank to clarify the approach for the Red Teaming exercise as DDoS is a destructive exercise.	Clause stands as per RFP.  It is clarified that the DDos attack should not be destructive in nature and may be configured accordingly.
23.	Page 33 of 109	Part – IV SCOPE OF WORK		The objective of this RFP is to conduct the Red Team Exercise for a finite period of 15 days in the first month of every 4 month block of the contract period to uncover the vulnerabilities in the bank's perimeter/ internal network( DC/ DR/ All branches) and attempt to exploit the identified vulnerabilities to gain access to the bank's critical infrastructure.		Clause stands as per RFP.

24.	Page 42 of 109	Part – V	3. Payment Terms	Balance 25% will be payable after completion of the compliance-review and submission of reports.	<p>Since there is a dependency on the Bank, we request to change the clause as below: Bank shall be responsible to mitigate the identified risk/vulnerability within 30 days of report submission.</p> <p>If there is any delay from Bank, balance 25% will be paid within 30 days of complete Red Team Exercise report submission.</p>	Clause stands as per RFP,
25.	Page 42 of 109	Part – V	4. Penalty		<p>Since there is a dependency on the Bank, we request to include below statement: Delays shall not be attributed to the bidders in case of any delay from the Bank and payment shall be made to the Bidders on submission of AS-IS report if the delay can't be attributed to the bidder.</p>	Clause stands as per RFP,



**UCO BANK**

**Department of Information Technology**

**Engagement of Service Provider for availing Red Team Exercise Services by using automated tools and techniques**

**RFP Ref. No.UCO/DIT/4401/2021-22 Date: 09.03.2022**

**Amendments, Addendums and Corrigendum's published on 25.03.2022**

Sl.No.	RFP Clause No.	Existing Clause	Modified Clause
1.	Eligibility criteria point no.1 Page 10 of 105	<p>Bidder should be a limited company (Public/Private) registered in India under the Companies Act, 1956/2013 for the last 3 years as on RFP issuance date.</p> <p>Companies registered as MSME Entrepreneur &amp; still categorized as MSME as on RFP submission date.</p> <p>Bidder/Partner/Investor must adhere cross border sharing/FDI/FEMA and other regulatory guidelines of Govt of India.</p> <p>The bidder should not be a subsidiary of a foreign company.</p>	<p>Bidder should be a limited company (Public/Private) registered in India under the Companies Act, 1956/2013 for the last 3 years as on RFP issuance date. LLP may be permitted to participate in the bidding process provided they have proper registration under LLP act.</p> <p>Companies registered as MSME Entrepreneur &amp; still categorized as MSME as on RFP submission date.</p> <p>Bidder/Partner/Investor must adhere cross border sharing/FDI/FEMA and other regulatory guidelines of Govt of India.</p> <p>The bidder should not be a subsidiary of a foreign company.</p> <p>Proof of documents required:</p> <ol style="list-style-type: none"> <li>1. Certificate of Incorporation issued by Registrar of Companies along with</li> <li>2. Copies of Memorandum of Association</li> <li>3. Copies of Articles of Association</li> <li>4. Shareholding pattern</li> <li>5. PAN, TAN, GSTIN Certificate and any other tax related document if applicable is required to be submitted along with the eligibility bid.</li> </ol> <p>Registration from DIC, KVIB, NSIC,</p>



			KVIC, DIHH, UAA or any other body specified by Ministry of MSME. 6. LLP registration certificate.
<b>2.</b>	Part – IV SCOPE OF WORK  Page 33 of 105	The Red Team Exercise should support attack replay & attack import from PCAP (i.e. PCAP files should be provided for all attacks for analyzing & displaying by tools like burp suite).	The Red Team Exercise should support attack replay & attack import from PCAP (i.e. PCAP files should be provided for all attacks for analyzing & displaying by tools like burp suite, In addition burp state files may also be provided).
<b>3.</b>	Part – V  3.Payment Terms point no. iv Page 42 of 105	Balance 25% will be payable after completion of the compliance-review and submission of reports	Balance 25% will be payable after completion of the compliance-review and submission of reports or maximum within 60 days of complete Red Team Exercise report submission.

**Note:** All other terms and conditions of the above RFP & subsequent pre-bid responses/addendum/corrigendum will remain unchanged and will be part & parcel of this tender.