

Amendments and Clarifications - Ref: CO:ITD:774/R1:2018-19 Date: 21/03/2019 - Identification of a Service Provider for conducting Red Team Exercise in order to assess Bank's defensive, detection and response capabilities in the event of a cyber security incident and to identify the vulnerabilities and subsequent business risk due to cyber incidents

Date: 09/04/2019

S. No.	Page# / Clause No.	Point	RFP Clause	Clarifications / Amendments Sought	Bank's Response
1.	Pg. No. 28 / Clause No. 3	Qualification Criteria	Bidder should have an average turnover of minimum of Rs.3.50 crores for the immediate past 3 financial years.	With Regard to evaluation criteria mentioned in pages 43, turnover of minimum Rs.3.50 Crores, we request you to kindly consider Rs.2 Crores Annual turnover for last 3 Financial Years that is 2015-16, 2016-17 and 2017-18	Amended Clause: Bidder should have an average turnover of minimum of Rs 2.00 crores for the immediate past 3 financial years.
2.	Pg. No. 19 / Point No. 24	Information system service and support	The successful bidder is obliged to provide maintenance and support services on 24 X 7 basis, as per the terms of this contract, during the contract period of two years.	Maintenance and support services do not apply to red teaming activity. Kindly reconsider.	Amended Clause: The Clause stands deleted
3.	Pg. No. 22 / Point No. 27	Conducting the cyber security readiness assessment	Conducting the cyber security readiness assessment for the bank to identify the existing vulnerabilities associated with the existing information security set up of the bank	As this activity is extensive for a bank like Indian Bank, kindly clarify if this assessment scope would be restricted to vulnerabilities identified as part of the red team exercise alone	Yes, it is restricted to the vulnerabilities identified as part of Red Team exercise.
4.	Pg. No. 26 / Point No. J	Deliverables	After review successful bidder has to provide confirmation that functioning of network system is in compliance with Bank's IT security policy Bank's cyber security policy RBI information security guidelines...	A blanket compliance statement cannot be provided as we are not performing an assessment across all requirements of frameworks like the RBI's Cyber Security Framework. The red team exercise report will serve as confirmation whether the bank's security defenses are adequate or not for the tested attack scenarios only. Kindly clarify.	Yes, confirmation has to be provided that Bank's security defenses are adequate or not for the tested scenarios as per the scope of work.

Amendments and Clarifications - Ref: CO:ITD:774/R1:2018-19 Date: 21/03/2019 - Identification of a Service Provider for conducting Red Team Exercise in order to assess Bank's defensive, detection and response capabilities in the event of a cyber security incident and to identify the vulnerabilities and subsequent business risk due to cyber incidents

Date: 09/04/2019

S. No.	Page#/ Clause No.	Point	RFP Clause	Clarifications / Amendments Sought	Bank's Response
5.	Pg. No. 27/ Point No. M	Remediation and re-testing	Remediation re-testing to be provided at no additional cost.	Re-testing of scenarios cannot be possible given that 10 scenarios have to be tested in 24 months, and re-testing would involve the same effort as the original test. However revalidation of specific system vulnerabilities identified as part of the red team exercise alone can be performed. Kindly clarify.	Revalidation of critical / high vulnerabilities must be carried out.
6.	Pg. No. 27/ Point No. N	Other general requirements	Successful bidder should benchmark policies, procedures, standards, against standards recommended by RBI.....should report areas observed which are non compliant with RBI guidelines	This is an exercise which will require substantial effort and will not fall under the scope of the red team exercise activities. Kindly clarify what is expected as the scope of this requirement is very broad.	The scope provided as part of Red Team exercise must be mapped with RBI policies and confirmation must be provided.
7.	Pg. No. 28/ Clause No. 5	Qualification Criteria	The bidder should have provided red team assessment test services to a minimum of 2 Banks/PSU/Govt. Organisations during the last five years (2013 to 2018)	The Bidder/ OEM should have provided red team assessment test service to a minimum of 2 Banks/ PSU/ Govt. Organizations during the last five years (2013 to 2018)	Please adhere to terms and conditions of the RFP
8.	Pg No. 43/ Point 10	Checklist	Rs 2000/- in the form of Demand Draft.	Please confirm if the cost of bid document is INR 5000/- or INR 2000/- INR 5000/- is mentioned in Page 3 Point 4 and Page 4 Point 5(b) and as INR 2000/- in Page 43 Point 10 under Checklist.	Amended Clause: Please read the clause as: Rs 5000/- in the form of Demand Draft.
9.	Pg No. 21/ Clause I	SCOPE OF WORK	User awareness against social engineering <input type="checkbox"/> Phishing <input type="checkbox"/> Vishing	Scope of Work: User Awareness - Does the Social Engineering activity of Phishing / Vishing	Full scope of work given in the RFP needs to be carried out in all the 4 phases.

Amendments and Clarifications - Ref: CO:ITD:774/R1:2018-19 Date: 21/03/2019 - Identification of a Service Provider for conducting Red Team Exercise in order to assess Bank's defensive, detection and response capabilities in the event of a cyber security incident and to identify the vulnerabilities and subsequent business risk due to cyber incidents

Date: 09/04/2019

S. No.	Page# / Clause No.	Point	RFP Clause	Clarifications / Amendments Sought	Bank's Response
			<input type="checkbox"/> SMSGing <input type="checkbox"/> USB Drop exercise <input type="checkbox"/> Through Social Media	etc need to be carried out across all the 4 instances over 2 years.	
10.	Pg No. 22 / Clause I	SCOPE OF WORK	Physical Facilities - Offices, Data Centres	Physical Facilities - Data centres Assessment – Will service provider be granted access to Data center.	Entry to Data Center for the service provider will be arranged.
11.	--	--	--	Please confirm the number of employees in the bank.	Approximately 20,000.
12.	--	--	--	Will the activity be limited to bank employees only or also to employees across branch locations.	Applicable to all Bank employees across all locations.
13.	Pg No. 24 / Point A.3	Technical Specifications For Red Team Assessment	One member should be certified in network technologies like Cisco or juniper certified.	For Red Teaming nothing to do with Cisco Certification, better you can remove this.	Please adhere to terms and conditions of the RFP
14.	Pg No. 24 / Point B	Technical Specifications For Red Team Assessment	Network & Security Testing: Network surveying Port scanning System identification/OS finger printing Services identification Phishing Web and mobile applications testing Router testing Firewall testing Intrusion detection system testing	This is VAPT testing request.. removed from RED team tender.	Please adhere to terms and conditions of the RFP

Amendments and Clarifications - Ref: CO:ITD:774/R1:2018-19 Date: 21/03/2019 - Identification of a Service Provider for conducting Red Team Exercise in order to assess Bank's defensive, detection and response capabilities in the event of a cyber security incident and to identify the vulnerabilities and subsequent business risk due to cyber incidents

Date: 09/04/2019

S. No.	Page# / Clause No.	Point	RFP Clause	Clarifications / Amendments Sought	Bank's Response
			Trusted systems testing Password cracking Malware defense capability testing Denial of service (DOS) testing Exploiting vulnerabilities remotely Authentication testing Identity management testing Authentication testing Input validation testing Custom exploit/script writing Document grinding (electronic dumpster diving) Any other testing method		
15.	Pg No. 25 / Point F	Technical Specifications For Red Team Assessment	Physical Security: Access controls testing Perimeter review Alarm response testing Location review Environment review Physical Intrusion Any other	Not required - need to be removed.	Please adhere to terms and conditions of the RFP
16.	--	--	Additional Clauses	To be Added as request in Testing : Proactively identify & mitigate complex security vulnerabilities. Help Improve their detection , response capabilities.	Please adhere to terms and conditions of the RFP

Amendments and Clarifications - Ref: CO:ITD:774/R1:2018-19 Date: 21/03/2019 - Identification of a Service Provider for conducting Red Team Exercise in order to assess Bank's defensive, detection and response capabilities in the event of a cyber security incident and to identify the vulnerabilities and subsequent business risk due to cyber incidents

Date: 09/04/2019

S. No.	Page# / Clause No.	Point	RFP Clause	Clarifications / Amendments Sought	Bank's Response
				<p>Deep knowledge of APT & attacker behavior on real world attacker scenario.</p> <p>Give an input on whether our critical data is at risk and how easily it may be obtained by a malicious actor.</p> <p>To Enhance our team's ability to prevent, detect and respond to incidents in a controlled and realistic environment.</p> <p>To Test our security tools and procedures in a controlled attack scenario</p> <p>To Identify and mitigate complex security vulnerabilities before an attacker exploits them</p> <p>To Attain fact-based risk analysis findings and recommendations for improvement</p> <p>To Assess the security of our environment against a realistic "no-holds-barred" attacker.</p> <p>An incident responder works with our security team</p> <p>To help detect the red team assessment is in progress and to advise on appropriate response tactics if activity is detected.</p> <p>Once the assessment is completed, members of the red team and embedded incident responder work with our internal security team to build a plan to enhance</p>	

Amendments and Clarifications - Ref: CO:ITD:774/R1:2018-19 Date: 21/03/2019 - Identification of a Service Provider for conducting Red Team Exercise in order to assess Bank's defensive, detection and response capabilities in the event of a cyber security incident and to identify the vulnerabilities and subsequent business risk due to cyber incidents

Date: 09/04/2019

S. No.	Page# / Clause No.	Point	RFP Clause	Clarifications / Amendments Sought	Bank's Response
				prevention, detection and response to prevent future such attacks.	
17.	--	--	Additional Clauses	To be Added in Reporting : Technical details with step-by step information that allows you to recreate the findings Fact-based risk analysis so you know a critical finding is relevant to our environment Tactical recommendations for immediate improvement Strategic recommendations for long-term improvement Invaluable experience responding to a real-world incident without the pressure of a potential headline causing breach	Please adhere to terms and conditions of the RFP

