Request for Proposal for selection of Service Provider For Conducting Red Team Exercise (Reference: RFP Reference: BCC:CISO:41:114/13 dated-7th April 2022- Prebid Reply/Clarification

S.No	Section	Page No	Description	Bidders-comment/suggestion/deviation/query	Bank Clarification
1	1.3.1	11	Identification of possible weak points in physical and logical security of DC and DR site	Physical breach simulation of the DC and DR sites to be covered? If yes, kindly share the location details of sites to be covered as a part of the scope	Location need to be identified by the successful bidder, who will be conducting red team exercise. No change as per RFP.
2	1.3.1	11	Vulnerability Assessment , verification and Recommended Solution to mitigate vulnerability in Local / remote networks (automated and manual)	Will this be an credentialed VA scan of the in-scope assets. Additionally, request you to provide a approximate count of the devices to be scanned as a part of the scope	Bank will not share any priviledge to the red team for conducting the exercise. No additional information will be shared. No change as per RFP.
3	1.3.1	11	Web application compromise and exploitation – physical and Cloud	It is assumed that physical is referred to on-premise hosted applications. Kindly confirm our understanding	Bank will not provide any information. Successful bidder need to identify the logical security weaknesses as part of the red team exercise. No change as per RFP.
4	1.3.1	11	Internal application Security Testing through Red team exercise	It is assumed that we will be conducting black box testing of application identified as a part of Internal Red Team assessment. However, for better understanding kindly share the count of applications to be covered as a part of the scope.	Bank will not provide any information. Successful bidder need to identify the logical security weaknesses as part of the red team exercise. No change as per RFP.
5	1.3.1	11	Conduct simulated cyber-attacks on the bank's infrastructure	Request you to elaborate your expectations on conducting simulated cyber attacks	Bank will not provide any information. Successful bidder need to identify the logical security weaknesses as part of the red team exercise. No change as per RFP.
6	1.3.1	11	Conduct simulated cyber-attacks on the bank's infrastructure	Is the bidder expected to conduct, simulated DDOS attack on the banks external network infrastructure	Bank will not provide any information. Successful bidder need to identify the logical security weaknesses as part of the red team exercise. No change as per RFP.
7	1.3.1	11	Blended, covert test that can encompass network testing, phishing, wireless, and physical attacks	Does this include wireless network pentesting. If yes, the details of location for which this needs to be covered	Bank will not provide any information. Successful bidder need to identify the logical security weaknesses as part of the red team exercise. No change as per RFP.
8	1.3.1	11	Blended, covert test that can encompass network testing, phishing, wireless, and physical attacks	Request you to kindly elaborate on the requirement of conducting physical attacks. Does this activity involve physically bypassing, the security controls in-order to gain access into the banks premises. If yes, kindly share the location details of sites to be covered as a part of the scope	Bank will not provide any information. Successful bidder need to identify the physical and logical security weaknesses as part of the red team exercise. No change as per RFP
9	1.3.1	11	Send email with malicious attachment to users	Will this be for users identified by BOB, or user accounts identified for compromise as a part of the Red Team activity	Bank will not provide any information. Successful bidder need to identify the physical and logical security weaknesses as part of the red team exercise. No change as per RFP
10	1.3.1	11	Scope of work	Does Bank will provide any workstation/laptop from where testing to be conducted ?	No Bank will not provide any workstation/laptop for this purpose. No change as per RFP.
11	1.5	13	The Breach scenario exercise & Carry out Red Team exercise	Is the assessment to be considered time based (10 weeks) or infrastructure based. Kindly elaborate	Red Team exercise need to be conducted during the given time period. No change as per RFP.
12	1.3.1	11	Scope of work	Does the the whole infrastructure to be considered for the external red team assessment? If yes, please share the count of domains.	Bank will not provide any information. Successful bidder need to identify the physical and logical security weaknesses as part of the red team exercise. No change as per RFP
13	1.3.1	11	Scope of work	Does Android Applications are to be considered for the scope of external testing.	Yes. No changes as per RFP.
14	1.3.1	11	Scope of work	Does the red team assessment focused only on the targeted objectives ?	Yes. No changes as per RFP.
15	1.3.1	11	Scope of work	How many devices/URL/IP address are involved in the red team assessment.	Bank will not provide any information. Successful bidder need to identify the physical and logical security weaknesses as part of the red team exercise. No change as per RFP
16	1.3.1	11	Scope of work	Does Bank Core network considered for the scope of internal/external testing.	Bank will not provide any information. Successful bidder need to identify the physical and logical security weaknesses as part of the red team exercise. No change as per RFP
17	1.3.1	11	Scope of work	Does Bank will allow serivce provider's laptops inside bank premises?	Bank will not provide any priviledged access to the Red team. No change as per RFP.
18	1.3.1	11	Scope of work	Does Bank will provide sitting space during the on premise visit?	Bank will not provide any priviledged access to the Red team. No change as per RFP.
19	1.3.1	11	Scope of work	Does red team will require to take prior vulnerability exploitation approval from the bank during the entire assessment?	Yes. No changes as per RFP.
20		11	Scope of work	Does Bank will provide on premise sitting arrangement ?	Bank will not provide any priviledged access to the Red team. No change as per RFP.
21	1.3.1	11	Scope of work	Does the penetration testing exercise limits to only identification of the vulnerability or post exploitation actives to be performed.	Yes. No changes as per RFP.

22	1.3.1	11	Scope of work	Does the red team assessment involves physical security testing using social engineering ?	Yes. No changes as per RFP.
23	1.3.1	11	Scope of work	Does the red team assessment involves cloud security testing?	Yes. No changes as per RFP.
24	1.3.1	11	Scope of work	Does Bank will provide bailout letter for red team assessment?	Yes, if the Human resource is involved the details of the person to be shared with Bank. No change as per RFP.
25	1.3.1	11	Scope of work	Does Bank will provide dummy user account for internal red teaming?	Bank will not provide any information. Successful bidder need to identify the physical and logical security weaknesses as part of the red team exercise. No change as per RFP
26	1.3.1	11	Scope of work	Does Bank allows only business hours time bound activity for red teaming?	No. No change as per RFP.
27	1.3.1	11	Scope of work	Does Bank will provide list of subnets to be excluded from the internal red teaming assessment?	No. No change as per RFP.
28	4.21	42	Limitation of Liability- There are following exceptions to the limitation of liability - Willful Misconduct Gross Negligence of Bidder, its employees and Subcontractors Infringement of patents, trademarks, copyrights or such other Intellectual Property Rights Breach of confidentiality obligation	BoB is requested to delete exceptions to the limitation of liability. The exceptions render the limitation of liability ineffective and make the liability unlimited.	No. No Change as per RFP
29	4.15 & 4.16	38 & 39	Indemnity - Indirect and consequential losses are not excluded from liability	BoB is requested to include to clause to state that we will not be liable for any indirect and consequential losses or damages. This is as per GFR and Meity guidelines and also the industry standard. Even the law, Contract Act, stipulates and remote and consequential damages are not payable. BoB is requested to include the below clause: Purchase/BoB agrees that Consultant will not be liable for (i) loss or corruption of data	No Change as per RFP
30	4.8	34	Confidentiality Obligations: Obligations to survive for post expiry or termination of contract	We request BoB to reduce the survival period of confidentiality obligations to one year post expiry or termination.	No Change as per RFP
31	4.8	34	Confidentiality Obligations: Obligation to return all confidential information / destroy all confidential and no right to retain a copy	We request BoB to allow us to retain our working papers and a copy of confidential information for our records and any future reference or audit requirements, subject to confidentiality obligations under this Agreement.	No Change as per RFP
32	4.16	38 & 39	Indemnity: Indemnities for IPR infringement claims without exceptions	We request BoB to include the following exceptions and procedure as these are industry standards and reasonable. They are also mentioned in the MeitY guidelines. 1. Notwithstanding anything contained in this agreement, if the Indemnified Party promptly notifies Indemnifying Party in writing of a third party claim against Indemnified Party that any Service provided by the Indemnifying Party infringes a copyright, trade secret or patents incorporated in India of any third party, Indemnifying Party will defend such claim at its expense and will pay any costs or damages, that may be finally awarded against Indemnified Party. 2. Indemnifying Party will not indemnify the Indemnified Party, however, if the claim of infringement is caused by: a) Indemnified Party's misuse or modification of the Service; b) Indemnified Party's failure to use corrections or enhancements made available by the Indemnifying Party; c) Indemnified Party's use of the Service in combination with any product or information not owned or developed by Indemnifying Party; However, if any service, information, direction, specification or materials provided by Indemnified Party or any third party contracted to it, is or likely to be held to be infringing, Indemnifying Party shall at its expense and option either: i. Procure the right for Indemnified Party to continue using it; ii. Replace it with a no infringing equivalent; iii. Modify it to make it no infringing. 3. The foregoing remedies constitute Indemnified Party's sole and exclusive remedies and Indemnifying Party's entire liability with respect to infringement.	No Change as per RFP
33			Indemnities not subject to final determination by court/arbitrator	We agree to indemnify to the extent the damages/losses are finally determined by a competent court or arbitration. Please make indemnities subject to final determination by court/arbitrator. This is also the industry standard and prescribed by Meaty in its guidelines.	No Change as per RFP

34			No process for indemnity	The indemnities set out in this agreement shall be subject to the following conditions: (i) the Indemnified Party as promptly as practicable informs the Indemnifying Party in writing of the claim or proceedings and provides all relevant evidence, documentary or otherwise; (ii) the Indemnified Party shall, at the cost of the Indemnifying Party, give the Indemnifying Party all reasonable assistance in the Defense of such claim including reasonable access to all relevant information, documentation and personnel provided that the Indemnified Party may, at its sole cost and expense, reasonably participate, through its attorneys or otherwise, in such Defense; (iii) if the Indemnifying Party does not assume full control over the Defense of a claim as provided in this clause, the Indemnified Party may participate in such defense at its sole cost and expense, and the Indemnified Party will have the right to defend the claim in such manner as it may deem appropriate, and the cost and expense of the Indemnified Party will be included in losses; (iv) the Indemnified Party shall not prejudice, pay or accept any proceedings or claim, or compromise any proceedings or claim, without the written consent of the Indemnifying Party; (v) all settlements of claims subject to indemnification under this Clause will: a) be entered into only with the consent of the Indemnified Party, which consent will not be unreasonably withheld and include an unconditional release to the Indemnified Party from the claimant or plaintiff for all liability in respect of such claim; and b) include any appropriate confidentiality agreement prohibiting disclosure of the terms of such settlement; (vi) the Indemnified Party shall account to the Indemnifying Party for all awards, settlements, damages and costs (if any) finally awarded in favor of the Indemnified Party which are to be paid to it in connection with any such claim or proceedings; (vii) the Indemnified Party shall take steps that the Indemnifying Party may reasonably require to mitigate or reduce its loss as a result of such a claim or proceedings; (viii) in the event that the Indemnifying Party is obligated to indemnify an Indemnified Party pursuant to this clause, the Indemnifying Party will, upon payment of such indemnity in full, be subrogated to all rights and defenses of the Indemnified Party with respect to the claims to which such indemnification relates; and (ix) if a Party makes a claim under the indemnity set out under Clause above in respect of any particular loss or losses, then that Party shall not be entitled to make any further claim in respect of that loss or losses (including any claim for damages).	No Change as per RFP
35			Termination: We do not have any right to terminate	To uphold the principles of natural justice and to bring parity in the contract, we request BoB to give us the right to terminate the contract in case BoB breaches any of its material obligations under the contract, provided a notice for such breach is given to BoB along with a rectification period of 30 days.	No Change as per RFP
36	4.13	37	Widely worded audit rights	We wish to clarify that we will retain our records as per our records retention policies. Upon reasonable notice, we will allow BoB to inspect our invoicing records under this engagement; such inspection shall be done in a pre-agreed manner and during normal business hours. For avoidance of doubt, such inspection should not cause us to be in breach of our organizational confidentiality requirements. Please acknowledge that our audit related obligations will be subject to foregoing statement.	No Change as per RFP
37			There is no restriction on the usage of deliverable. No third party disclaimers.	We will be providing services and deliverables to you under the contract. We accept no liability to anyone, other than you, in connection with our services, unless otherwise agreed by us in writing. You agree to reimburse us for any liability (including legal costs) that we incur in connection with any claim by anyone else in relation to the services. Please confirm our understanding is correct.	No Change as per RFP
38			No acceptance criteria	If the project is to be completed on time, it would require binding both parties with timelines to fulfill their respective part of obligations. We request you that you incorporate a deliverable acceptance procedure, perhaps the one provided by Meity in their guidelines, or the one suggested below, to ensure that acceptance of deliverables is not denied or delayed and comments, if any, are received by us well in time. You may consider including the below simple clause: Within 10 days (or any other agreed period) from BoB's receipt of a draft deliverable, BoB will notify Consultant if it is accepted. If it is not accepted, BoB will let Consultant know the reasonable grounds for such non acceptance, and Consultant will take reasonable remedial measures so that the draft deliverable materially meets the agreed specifications. If BoB does not notify Consultant within the agreed time period or if BoB uses the draft deliverable, it will be deemed to be accepted.	No Change as per RFP
39	3.6.7	27	The Bidder further represents that the documentation to be provided to the Bank shall contain a complete and accurate description of the deliverables and services (as applicable), and shall be prepared and maintained in accordance with the highest industry standards.	We request BoB to kindly confirm that we will prepare the deliverables using the generally accepted standards.	No Change as per RFP
40	4.8	34	confidentiality: Oral Disclosure	In the case of Confidential Information that is disclosed only orally, the Disclosing Party shall, within seven days after such disclosure, deliver to the Receiving Party a brief written description of such Confidential Information; identifying the place and date of such oral disclosure and the names of the representatives of the Receiving Party to whom such disclosure was made. It is expected that such information will bear a legend or label of “Confidential” or other similar designation manifesting intent that the information is confidential.	No Change as per RFP

41			Deployment of Resources: Covid 19 Crisis	If there are any circumstances that reasonably restricts travel or physical presence of our personnel at your office / location, then without prejudice to your payment obligations, you shall allow such personnel to work from home or other remote location till the time such reasonable restrictions exist. Any delay / default in performing our obligations arising from such restrictions, shall not be attributable to us and shall not be considered a breach of contract on our part and no consequent damages / penalties etc. arising therefrom would be imposed on us under the Contract.	Bidder will not penalized for reason beyond their control such as earthquake, flood, cyclone, pandemic, covid. No change as per RFP
42			Scope	Provide total no. of locations as a part of scope for Red Teaming Exercise.	Location need to be identified by the successful bidder, who will be conducting red team exercise. No change as per RFP.
43			Scope	Please provide locations details of DC & DR?	Location need to be identified by the successful bidder, who will be conducting red team exercise. No change as per RFP.
44			Scope	Please confirm whether this is an Onsite or Offsite activity? If on-site, how many locations to be covered?	Red team scope covers - Physical and logical security weakness identification and exploitation test. Location need to be identified by the successful bidder, who will be conducting red team exercise. No change as per RFP.
45			Scope	Provide Infrastructure details such as Network, people, applications, etc.	Bank will not provide any information. Successful bidder need to identify the logical security weaknesses as part of the red team exercise. No change as per RFP.
46			Scope	Mention tentative applications in scope (Internal and External).	Bank will not provide any information. Successful bidder need to identify the logical security weaknesses as part of the red team exercise. No change as per RFP.
47			Scope	Do we need to perform any grey box security assessment of the application?	Bank will not provide any information. Successful bidder need to identify the logical security weaknesses as part of the red team exercise. No change as per RFP.