Selection Of Information Security Service Provider **For a period of THREE years for availing:** **Spear Phishing Simulation and Security Awareness/Training Solution** **(ON SITE/PREMISES DEPLOYMENT)** **RFP No: IB:CO/ISSD/273/2021-2022 DATED:25.11.2021**	

REPLY TO QUERIES RAISED BY BIDDERS IN THE PRE BID MEETING HELD THROUGH WEBEX ON 03.12.2021 at 15:30 hrs

Sr. No.	Referred Point/Clause No.	Point	Queries raised by Bidders	Bank's Replies to queries
1	13.1.2	The proposed Spear Phishing Simulation and Security Awareness Training shall include minimum three (3) years license for Spear Phishing simulation and Learning/Training Management System that runs on the same platform.	1. How many hours of Computer Based Training is IB looking for? (Which needs to be hosted on the Learning Management System) 2. The trainings to be developed in which all languages?(English, Hindi, Any Regional Language) 3. How many users/employees will be accessing the training platform? 4. Is IB ok with Open Source LMS implementation? 5. If no, can we onboard subcontractors towards fulfilling the LMS requirement.	1. Spear Phishing Simulation and Security awareness/ training Solution, as per the Scope defined in the RFP, for 25000 Bank employees /users for a period of 3 (THREE) years (Refer the page 32 of the RFP). There is no restriction on the hours/video in a particular session 2. Training to be developed in English and preferably in Hindi. 3. Refer point no. 1

				4. The Bidder shall have the responsibility for managing the LMS 5. The application should be owned by the bidder and the Bank will have contract only with the selected Bidder
2	13.1.3	The solution should handle any reported suspicious emails notified by users through the solution's Phishing Alert mechanism (optional).	This RFP point is mentioned as optional. Will this capability be counted in technical evaluation of vendor?	As per RFP. However, non-compliance to "optional" points will not be taken as a criteria for disqualification
3	13.1.5	The solution should have a phishing simulation solution that runs on the same purpose-built on Site/Premise platform, improves employee response to phishing attacks, and empowers employees to provide real-time threat intelligence by immersing them in a real-world spear phishing experience.	How many phishing simulation is expected by the vendor in a year? Is vendor allowed setup Phishing environment over the cloud (SaaS based) instead of on premise ?	25000 users to be covered in each quarter without any restriction on the number of campaigns or number of employees to be covered in a campaign. As per RFP it is "on premise" only.
4	13.1.6	The solution shall have customizable scenarios that focus on emulating the most relevant threats and providing in-the-moment feedback and education to recipients who fall victim to these exercises. Solution should be able	How many spear-phishing scenarios to be conducted by the vendor in the period of three years. (1/ Per Month). Additionally, how many Indian Bank	Refer to page no 13 (clause no. 13.1.13) & refer to page no. 32.

		to run an unlimited number of scenarios to recipient groups during the period of the license.	employee should be considered to be part of these scenarios ?	
5	13.1.7	The solution shall provide a light-weight email client plug-in button to Office 365 that should give our employees a safe way to report email threats. When our employee reports a simulated phishing test, the user's correct action should be reported in the console. When the user reports a non-simulated phishing email, the email should be forwarded directly to our Incident Response team (optional).	This RFP point is mentioned as optional. Will this capability be counted in technical evaluation of vendor?	As per RFP. However, non-compliance to "optional" points will not be taken as a criteria for disqualification
6	13.1.12	The solution console shall be capable of providing real-time statistics on how many users have opened the email, responded to the email, click on the link/attachments and enter contents such as IDs or credentials.	Does the bank team want to download it themselves or require the bidder to provide these as reports ?	The solution should have the facility of generating and downloading reports, the bidder should train the Bank staff as per RFP.

7	13.1.13	The solution console shall come with minimum 100-200 pre-built phishing scenario templates, and have the ability to build our own, unique mock phishing emails based on real attacks targeting our organization.	Generally, these solutions don't have 100-200 templates. This is what will be out of the box, does the bank need the bidder to create additional templates ?	As per RFP
8	13.1.15	All server/application logs must be fully exportable and may be integrated into SIEM	Which logs are these referring to the phishing simulation logs ?	All the applicable Server level logs need to be captured into SIEM
9	13.1.18	The solution may be able to conduct specialized searches to help the Bank understand what kind of information is publicly-available about their users. The information gathered is obtained from social media sites, past data breaches, documents and files posted on the web, and more (optional).	How many users will be part of scope of this RFP point. Vendor would need the email address and basic details of employees to crawl the internet. Will bank be able to share such details with vendor. This RFP point is mentioned as optional. Will this capability be counted in technical evaluation of vendor?	As per RFP. However, non-compliance to "optional" points will not be taken as a criteria for disqualification
10	13.1.19	The solution console may include an industry benchmarking data to help the Bank identify how our phishing and training results	Is this a mandatory requirement as this data may not be available out of the box ?	As per RFP

		compare with other similar industry customers. The feature must be able to monitor how our Security Awareness plan develops and performs, from the point of our initial baseline phishing test, to after 90 days of phishing and training, to after a year of phishing and training.		
11	13.1.21	The solution must be able to provide at least 50 unique training and video modules	Vendor would provide 50 Videos as part of this RFP point related to security awareness based on current threats. Is our understanding correct.	As per RFP
12	13.1.24	The solution must be able to create targeted spear-phishing emails that have no click or attachments but will simulate an actual spear-phish and allow admins to see which users respond and/or attach compromising information.	How many spear-phishing scenarios to be conducted by the vendor in the period of three years. (1/ Per Month). Additionally, how many Indian Bank employee should be considered to be part of these scenarios.	25000 users to be covered in each quarter without any restriction on the number of campaigns or number of employees to be covered in a campaign. For number of scenarios refer point no. 13.1.13 page no. 16
13	13.1.25	The solution must be able to generate a security awareness program with task and scheduling by answering answer specific questions as to the breadth and nature of the organization, goals for	The program could be a Multiple Choice Question and Answer Quiz that assess the security awareness of Indian bank employees and it is one time activity during the period	It shall be an ongoing activity over a period of three years. The Solution should provide an MIS from where bank will be able to assess the strength

		security awareness program and timeline.	of three years. Is our understanding correct.	and weakness of the employees
14	13.1.26	The solution must be able to assign a security awareness proficiency assessment from the console to Bank users to assess our users' understanding of security awareness. The results will provide a breakdown of Bank's strengths and weaknesses to be used to create more targeted campaigns to better suit the needs of our users.	The assessment could be a Multiple Choice Question and Answer Quiz that assess the security awareness of Indian bank employees and it is one time activity during the period of three years. Is our understanding correct.	It shall be an ongoing activity over a period of three years. The Solution should provide an MIS from where bank will be able to assess the strength and weakness of the employees
15	13.1.27	The solution console must be able to provide Vishing (voice-phishing) that allows Bank to test its Employees on if they are prone to entering sensitive information through the phone when prompted (optional).	How many Vishing scenario is expected to be conducted by the Vendor in the period of three years (1/ Per Month). Additionally, how many Indian Bank employee should be considered to be part of these scenarios.

This RFP point is mentioned as optional. Will this capability be counted in technical evaluation of vendor? | As per RFP. However, non-compliance to "optional' points will not be taken as a criteria for disqualification |

16	13.1.36	The Bidder should have the provision for One Dedicated Account Manager for the bank for overall supervision of the Solution throughout the contract period.	IB is also looking for AMC support towards the administration and maintenance activities of the LMS for 3 years or the platform will be managed by the trained staff post implementation and handover?	As per RFP
17			Number of employees that would be targeted for phishing simulation	Spear Phishing Simulation and Security awareness /training Solution, as per the Scope defined in the RFP, for 25000 Bank employees /users for a period of 3 (THREE) years (Refer the page 32 of the RFP).
18			Frequency of phishing simulation monthly/quarterly etc)	25000 users to be covered in each quarter without any restriction on the number of campaigns or number of employees to be covered in a campaign. For number of scenarios refer point no. 13.1.13 page no. 16
19			Number of customised templates per campaign apart from the default templates present in the library (Email and phishing would be customised	Refer RFP point no. 13.1 13

			with customers logos and colour theme)	
20			Number of employees that needs to be targeted for Vishing exercise	As per RFP
21			Frequency of Vishing drills	As per RFP
22			Number of employees that needs to be targeted for SmiShing exercise	As per RFP
23			Frequency of SmiShing drills	As per RFP
24			Number of employees who would have access to the LMS portal	Spear Phishing Simulation and Security awareness /training Solution, as per the Scope defined in the RFP, for 25000 Bank employees /users for a period of 3 (THREE) years (Refer the page 32 of the RFP).

25			Number of customised videos required annually part from the default templates resent in the library(Videos should be customised with customers logos and colour theme)	As per RFP point no.13.1.21
26			Number of customised infographics, wallpapers, bit-size posters required annually apart from the default templates present in the library (Content would be customised with customers logos and colour theme)	As per RFP point no. 13.1.13
27			Is the turnover non-negotiable for MSME	Turnover criteria is not negotiable for MSE.
28.			Is Indian saas service provider on Indian cloud accepted?	As per RFP
29			We came across a Tender requirement (Ref: CO/ISSD/273/2021-22: Spear Phishing Simulation and Security	As per RFP

			Awareness/Training Solution in your website. Would like to know if we can quote for a Cloud version because KnowBe4 does not have an on-prem version of the same.	