

Replies to Pre bid Queries for GeM bid Ref. No: GEM/2025/B/6162604 dated 23/04/2025 for Selection of vendor for providing Subscription Services to Phishing Simulation Platform and Cyber Security Awareness Content Suite in Canara Bank for One Year

Sl. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidders Query	Bank's Reply
1	15	Section C - Deliverable and Service Level Agreements	2. Integration & Interfaces	2.1. The selected bidder has to work with different application vendors in order to integrate new solution to the existing workload or new workloads during contract period.	What is the estimated number of users/employees to be targeted in each type of exercise (phishing, vishing, smishing)? Are there specific user groups or roles (e.g., executives, finance team, IT admins) that will be prioritized for targeting?	Details will be shared with the selected bidder.
2	68	Annexure-8 Scope of Work	Bidder Scope of Work	Sl. No: 14 Phishing exercise: = The bidder shall be capable of performing Phishing exercises & send phishing simulated email from custom domains similar to the Bank Domain. = The tool should provide for automated simulation for select targeted groups. = The solution should support phishing campaigns including QR code, Deepfake phishing etc. = The emails to the recipients to be delivered on the same day and the entire activity to be completed in one day.	For deepfake phishing simulation—can the Bank clarify the scope and expectations (e.g., video calls, audio messages, fake voiceovers)	All variants of Deepfake phishing is required
3	68	Annexure-8 Scope of Work	Bidder Scope of Work	Sl. No: 18 The bidder shall include relevant phishing, vishing and smishing templates based on current threat landscape targeted to banking environment.	Will the Bank provide the call scripts and expected employee responses, or is the vendor expected to draft and get them approved?	Vendor is expected to draft and will be approved by bank
4	13	Section B - Introduction	6. Participation methodology:	6.4. In the event of the bidder being not able to perform the obligations as per the provisions of the contract, the OEM/OSD/principal should assume complete responsibility on behalf of the bidder for providing end-to-end solution i.e., technology, personnel, financial and any other infrastructure that would be required to meet intent of this RFP at no additional cost to the bank. To this effect bidder should provide a dealer/distributor certificate for the proposed solution as per Annexure-15.	Can the Bank clarify if it expects an on-premise deployment, cloud-hosted, or hybrid architecture?	RFP is for providing subscription services from vendor to Phishing Simulation Platform & Cyber Security Awareness Content Suite
5	67	Annexure-8 Scope of Work	Bidder Scope of Work	Sl. No: 7 Domains for the purpose of phishing simulation exercise must be procured by the bidder on need basis.	Will the Bank assist in whitelisting the custom phishing domains and email IPs to ensure delivery to internal mailboxes?	Yes, Bank will assist in whitelisting the custom phishing domains and email IPs
6	69	Annexure-8 Scope of Work	Bidder Scope of Work	Sl. No: 24 Bidder shall ensure that there is no restriction in number of phishing emails, number of calls, number of SMS to perform simulated phishing, vishing, smishing exercise.	What is the acceptable calling window (time of day) to conduct vishing calls to employees?	10.00 am to 06.00 pm on all bank Working days
7	68	Annexure-8 Scope of Work	Bidder Scope of Work	Sl. No: 16 Smishing exercise: = The bidder shall conduct Smishing exercises based on the frequency and number of target employees defined by the Bank. = The bidder shall provide, maintain and manage an independent SMS gateway to perform smishing activity as per bank's requirement. = The bidder shall maintain adequate security measures to protect Bank's data including any PII information submitted by users during the activity.	For the SMS gateway, are there approved telecom providers or compliance certifications required (e.g., DLT registration under TRAI)?	No, vendor is required to arrange their own SMS gateway applicable with TRAI guidelines



Sl. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Reply
8	45	Section G - General Conditions	21. Protection of Data:	21.2. Where the terms of the RFP/Gem Bid/PO/Agreement require any data to be maintained by the Bank, the Bank agrees to grant Vendor/Service provider such access and assistance to such data and other materials as may be required by Vendor/Service Provider, for the purposes of correcting loss or damage to Bank data. If any data to be shared between the Bank and Vendor/Service provider for the purpose of the contract, the same shall be shared through secured channels in an encrypted manner. The Vendor/ Service Provider shall process the relevant data at (furnish the location). If the Vendor/ Service Provider proposes any change in data processing location, the same shall be notified to the Bank before the change of location. Vendor/Service provider is required to adhere to RBI guidelines for storage of data in India as per regulatory requirements/instructions, also to provide complete details of data captured, processed and stored, maintain confidentiality of the bank's and its customer's data and report same to the bank. The data if any to be stored by the vendor shall be stored in an encrypted manner. Vendor/Service provider will be liable to bank for any event for security breach and leakage of data/information. No biometric data shall be stored/	Does the Bank expect voice recording and storage of vishing calls? If yes, what are the retention and security requirements?	Details will be shared with the selected bidder.
9	68	Annexure-8 Scope of Work	Bidder Scope of Work	Sl. No: 19 The bidder shall be capable to perform smishing, vishing activity in English, Hindi and major regional languages.	For manual vishing calls, which regional languages are the callers expected to be proficient in?	Details will be shared with the selected bidder.
10	68	Annexure-8 Scope of Work	Bidder Scope of Work	Sl. No: 19 The bidder shall be capable to perform smishing, vishing activity in English, Hindi and major regional languages.	Should the smishing messages be localized (in regional languages), or is English sufficient?	Details will be shared with the selected bidder.
11	69	Annexure-8 Scope of Work	Bidder Scope of Work	Sl. No: 24 Bidder shall ensure that there is no restriction in number of phishing emails, number of calls, number of SMS to perform simulated phishing, vishing, smishing exercise.	Will the Bank facilitate DNC (Do Not Call) list or employee opt-outs for vishing?	No
12	68	Annexure-8 Scope of Work	Bidder Scope of Work	Sl. No: 16 Smishing exercise: = The bidder shall conduct Smishing exercises based on the frequency and number of target employees defined by the Bank. = The bidder shall provide, maintain and manage an independent SMS gateway to perform smishing activity as per bank's requirement. = The bidder shall maintain adequate security measures to protect Bank's data including any PII information submitted by users during the activity.	Does the Bank have approval/consent to receive simulated smishing messages on employees' phones (especially via WhatsApp)?	Yes, Bank have approval to receive simulated Smishing messages on employees



Sl. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Reply
13	68	Annexure-8 Scope of Work	Bidder Scope of Work	<p>Sl. No: 16</p> <ul style="list-style-type: none"> Smishing exercise: The bidder shall conduct Smishing exercises based on the frequency and number of target employees defined by the Bank. The bidder shall provide, maintain and manage an independent SMS gateway to perform smishing activity as per bank's requirement. The bidder shall maintain adequate security measures to protect Bank's data including any PII information submitted by users during the activity. Smishing attacks shall be conducted through Whatsapp and Message application. <p>Sl. No: 16</p> <ul style="list-style-type: none"> Smishing exercise: The bidder shall conduct Smishing exercises based on the frequency and number of target employees defined by the Bank. The bidder shall provide, maintain and manage an independent SMS gateway to perform smishing activity as per bank's requirement. The bidder shall maintain adequate security measures to protect Bank's data including any PII information submitted by users during the activity. 	<p>For WhatsApp-based smishing, will the Bank provide or require official WhatsApp Business API access, or can vendor use a third-party service?</p>	No, bidder has to use their own service
14	68	Annexure-8 Scope of Work	Bidder Scope of Work	<p>Sl. No: 16</p> <ul style="list-style-type: none"> Smishing exercise: The bidder shall conduct Smishing exercises based on the frequency and number of target employees defined by the Bank. The bidder shall provide, maintain and manage an independent SMS gateway to perform smishing activity as per bank's requirement. The bidder shall maintain adequate security measures to protect Bank's data including any PII information submitted by users during the activity. <p>Sl. No: 17</p> <ul style="list-style-type: none"> The bidder shall provide an Annual Action Plan for observing Cyber Jagrookta Diwas (sharing creatives, webinars and quizzes etc.) on first Wednesday of every month (All of which has to be copyright free content and open file of the creatives need to be shared) 	<p>Are there any specific content restrictions (e.g., no links, no financial references) in smishing messages due to regulatory concerns?</p>	<p>Details will be shared with the selected bidder.</p>
15	67	Annexure-8 Scope of Work	Bidder Scope of Work	<p>Sl. No: 17</p> <ul style="list-style-type: none"> The bidder should provide an Annual Action Plan for observing Cyber Jagrookta Diwas (sharing creatives, webinars and quizzes etc.) on first Wednesday of every month (All of which has to be copyright free content and open file of the creatives need to be shared) 	<p>Do we need to share the open file for all the infographics</p>	<p>Yes, open file need to be shared for all the infographics</p>
16	68	Annexure-8 Scope of Work	Bidder Scope of Work	<p>Sl. No: 14</p> <ul style="list-style-type: none"> Phishing exercise: The solution should support phishing campaigns including QR code, Deepfake phishing etc. 	<p>Does Deepfake here stands for Audio and Video, kindly specify the same, in case if it refer to email based kindly help us with the example</p>	<p>All variants of Deepfake phishing is required</p>
17	68	Annexure-8 Scope of Work	Bidder Scope of Work	<p>Sl. No: 15</p> <ul style="list-style-type: none"> Vishing exercise: The bidder shall be capable of performing vishing exercises in both automated and manual methods. 	<p>Does Bank is referring for Human Made call in Manual Method, If yes what will be the Quantity and expected scenario's</p>	<p>Human based call in manual method. Details will be shared with the selected bidder</p>
18	68	Annexure-8 Scope of Work	Bidder Scope of Work	<p>Sl. No: 19</p> <ul style="list-style-type: none"> The bidder shall be capable to perform smishing, vishing activity in English, Hindi and major regional languages. 	<p>Kindly specify all the language required by Bank</p>	<p>Details will be shared with the selected bidder.</p>
19	68	Annexure-8 Scope of Work	Bidder Scope of Work	<p>Sl. No: 16</p> <ul style="list-style-type: none"> Smishing exercise: The bidder shall provide, maintain and manage an independent SMS gateway to perform smishing activity as per bank's requirement. 	<p>In case of Our SMS Gateway we need to encapsulate Vendor name in the template, also is there any possibility of using bank SMS gateway ? And also does independent means dedicated to Bank ?</p>	<p>No, bidder need to use their own SMS Gateway</p>
20	68	Annexure-8 Scope of Work	Bidder Scope of Work	<p>Sl. No: 22</p> <ul style="list-style-type: none"> Trouble shooting: In case, the issue is not resolved for more than 8 hours, support personnel should visit Bank's CISO Office at Bangalore to resolve the issue. 	<p>The issue mentioned here are related to P0 and P1 level issue? P0 - Issues causing a complete outage or severe impact on Products P1 - Significant functionality issues impacting critical features of products, but not causing a complete outage.</p>	<p>Any issues unresolved for more than 8 hours</p>



Sl. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Reply
21	69	Annexure-8 Scope of Work	Bidder Scope of Work	Sl. No: 25 The bidder shall ensure that the Bank shall have complete freedom to choose any topic of Cyber Security awareness and should be able to assign the same to any target group desired by Bank.	Is it limited to Bank OU unit or course/content can be published to outside world ? If yes what will be target audience domain and count	Details will be shared with the selected bidder.
22	69	Annexure-8 Scope of Work	Bidder Scope of Work	Sl. No: 24 Bidder shall ensure that there is no restriction in number of phishing emails, number of calls, number of SMS to perform simulated phishing, vishing, smishing exercise.	Will required Basic target count and also in case of outside bank the user consent will be required (Should be under Bank's responsibility)	Details will be shared with the selected bidder.
23	70	Annexure-8 Scope of Work	Solution Capability	Sl. No: 25 The Solution shall support unlimited number (if tomorrow we extend for customers also) of email IDs for a campaign.	Will required Basic target count and also in case of outside bank the user consent will be required (Should be under Bank's responsibility)	Details will be shared with the selected bidder.
24	70	Annexure-8 Scope of Work	Solution Capability	Sl. No: 29 The Solution should support integration with bank's security stack such as SIEM, SOAR, UEBA etc., as per bank's requirement.	SIEM integration is supported, kindly help us with the use case of SOAR integration	Details will be shared with the selected bidder.
25	71	Annexure-8 Scope of Work	Solution Capability	Sl. No: 33 The solution should be able to map complete lifecycle of cyber awareness process of each user and represent the same information through a real-time dashboard.	We will required clarification with reference "map complete lifecycle"	Complete life cycle means, from initiation to completion of the activity of each user
26	71	Annexure-8 Scope of Work	Solution Capability	Sl. No: 41 The solution should have MIS/ Dashboard flexibility to accommodate Bank's requirement.	Does Bank is looking for separate dashboard related to information, as the admin portal already contains all the required information related to Tool ?	The dashboard should be customizable as per the requirement of the bank
27	72	Annexure-8 Scope of Work	Solution Capability	Sl. No: 51 Feedback may be provided to employees to educate them on the risks and how to avoid them.	Need clarification on this ? Is it related to instant awareness page or something else	No, a separate feedback page should be provided for the campaign users
28	72	Annexure-8 Scope of Work	Dashboard	Sl. No: 2 The dashboard should be flexible and be customizable as per Bank's requirement.	Kindly define to what extent changes will be required	Details will be shared with the selected bidder.
29	73	Annexure-8 Scope of Work	Reports	Sl. No: 8 The reports shall normally be provided in CSV, Excel, PDF formats in general and in PPT format if required.	Tool does support Report in CSV, PDF format, we need clarification on what details required in ppt.	All the campaign related reports should be provided in CSV, Excel, PPT and PDF format as per the requirement of bank
30	60	Annexure-2 Pre-Qualification Criteria	Sl. No: 11	Pre-Qualification Criteria: The bidder should have support office in Bengaluru for 24x7 supports. Documents to be submitted In compliance with Pre-Qualification Criteria: The Bidder should submit the details viz., address, phone no., email id and contact person Name & Mobile no. etc.	Can support be provided online,. The support offices are in India (not Bangalore)	Bidder to refer Corrigendum-1.
31	67	Annexure-8 Scope of Work	Bidder Scope of Work	Sl. No: 8 The bidder shall be responsible for arranging requisite Hardware, middleware / software required for the Platform. The bidder should arrange necessary Infrastructure like SIM Cards, SMS facility for smishing and vishing.	Who will manage cabling while deploying the hardware within canara bank DC & DR	RFP is for providing subscription services from vendor to Phishing Simulation Platform & Cyber Security Awareness Content Suite. In case the subscription requires hardware to be installed the same may be borne by vendor. The Vendor.



Sl. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Reply
32	15	Section C - Deliverable and Service Level Agreements	1. Project Timelines	1.3. Bidder should adhere to the following timelines for completion of the scope of work: Activity: Subscription and Implementation of Phishing Simulation Platform and Cyber Security Awareness Content Suite as per Scope of Work and Technical requirements. Timeline: 14 days from the Date of acceptance of Purchase order	Please considering the relaxation for the Project Timelines as 25 days from the Date of acceptance of Purchase order	Bidder to comply with RFP terms and conditions.
33	74	Annexure-9 Technical Evaluation Criteria	Sl. No: 1 Criteria: The Bidder should have provided phishing simulation and creation of awareness contents of Cyber Security in India in any PSUs/ PSBs as on 31/03/2025.	Evaluation Parameters: No. of PSUs/ PSBs: More than 2 clients - 15 Marks 1-2 client - 10 Marks	The Bidder/OEM should have provided phishing simulation and creation of awareness contents of Cyber Security in India in any PSUs/ PSBs/PVT BANK as on 31/03/2025.	Bidder to refer Corrigendum-1.
34	74	Annexure-9 Technical Evaluation Criteria	Sl. No: 2 Criteria: The bidder should have provided phishing simulation and creation of awareness contents of Cyber Security in India in any Commercial Bank (SCB)/ BFSI Sector during the last 5 years.	Evaluation Parameters: No. of Clients in Schedule Commercial Bank (SCB)/ BFSI Sector: More than 5 clients - 15 Marks 3-5 clients - 12 Marks 1-2 clients - 8 Marks	The bidder /OEM should have provided phishing simulation and creation of awareness contents of Cyber Security in India in any Schedule Commercial Bank (SCB)/ BFSI/PSU/PVT BANK Sector during the last 5 years	Bidder to refer Corrigendum-1.
35	74	Annexure-9 Technical Evaluation Criteria	Sl. No: 1 Criteria: The Bidder should have provided phishing simulation and creation of awareness contents of Cyber Security in India in any PSUs/ PSBs as on 31/03/2025.	Evaluation Parameters: No. of PSUs/ PSBs: More than 2 clients - 15 Marks 1-2 client - 10 Marks	The Bidder/OEM should have provided phishing simulation and creation of awareness contents of Cyber Security in India in any PSUs/ PSBs as on 31/03/2025.	Bidder to refer Corrigendum-1.



Sl. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Reply
36	74	Annexure-9 Technical Evaluation Criteria	Sl. No: 2 Criteria: The bidder should have provided phishing simulation and creation of awareness contents of Cyber Security in India in any Schedule Commercial Bank (SCB)/ BFSI Sector during the last 5 years.	Evaluation Parameters: No. of Client/s in Schedule Commercial Bank (SCB)/ BFSI Sector: More than 5 clients - 15 Marks 3-5 clients - 12 Marks 1-2 clients - 8 Marks	The bidder /OEM should have provided phishing simulation and creation of awareness contents of Cyber Security in India in any Schedule Commercial Bank (SCB)/ BFSI Sector during the last 5 years	Bidder to refer Corrigendum-1.
37	Generic	Annexure-8 Scope of Work	Generic	Email Compatibility:	Please confirm if there are any specific technical restrictions or configurations required to integrate the solution with Microsoft365 where the data related to phishing/vishing/smishing simulations can be hosted? Is on-premises deployment mandatory or is cloud-hosted within India acceptable?	The selected bidder has to share the details with Bank for any integration requirement with Bank's email application.
38	Generic	Annexure-8 Scope of Work	Generic	Data Residency	What is the approved location(s) within India where the data related to phishing/vishing/smishing simulations can be hosted? Is on-premises deployment mandatory or is cloud-hosted within India acceptable?	Pan India
39	Generic	Annexure-8 Scope of Work	Generic	SMS and Call Infrastructure:	Can the bank provide clarity on the number of SIM cards/channels expected for smishing/vishing? Is there any preferred telecom provider or regulatory compliance needed for the SMS gateway?	Bidder has to use their own SIM cards and channels for Smishing and Vishing Campaigns
40	Generic	Annexure-8 Scope of Work	Generic	Frequency and Scale:	Can the bank provide an estimated number of employees to be covered under simulations and awareness campaigns? For "unlimited" phishing exercises, is there an expected minimum monthly volume or frequency?	No. of users to be covered under the simulation campaign is 65000 with ± Increase of 10%. The frequency of the activity will be shared with the selected bidder
41	Generic	Annexure-8 Scope of Work	Generic	Languages Support:	Please provide a list of regional languages required for smishing, vishing, and training content delivery. Are the bidders expected to provide translation and voiceover services?	Details will be shared with the selected bidder.
42	Generic	Annexure-8 Scope of Work	Generic	Integration Expectations:	What specific SIEM/SOAR/UEBA platforms are currently used by the Bank for security integration?	Details will be shared with the selected bidder.
43	Generic	Annexure-8 Scope of Work	Generic	Deepfake and QR Code Phishing:	Can the Bank elaborate on the expectations for "Deepfake phishing"? Are video/audio-based simulations required?	All variants of Deepfake phishing required



Sl. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Reply
44	Generic	Annexure-8 Scope of Work	Generic	Training Delivery:	Will the in-person training session be conducted at a single location or across multiple zones? What Learning Management System (LMS), if any, does the bank currently use or expect the solution to integrate with?	The training should be provided to the 3-5 bank officials
45	Generic	Annexure-8 Scope of Work	Generic	Customization Scope:	Is there a limit to the number of custom templates/scenarios/landing pages required? What is the expected turnaround time for customization during the contract?	Details will be shared with the selected bidder.
46	Generic	Annexure-8 Scope of Work	Generic	Reporting Requirements:	Is there a preferred format/layout for dashboards and reports for alignment with internal MIS structures? Will the Bank provide user metadata like department/location/designation for report mapping?	Details will be shared with the selected bidder.
47	Generic	Annexure-8 Scope of Work	Generic	Security Standards:	Is there a specific frequency for conducting VAPT (Vulnerability Assessment & Penetration Testing)? Are there existing security audit vendors or should the bidder propose third-party VAPT services?	The VA & PT report shall be shared to the bank as and when bank demands
48	Generic	Annexure-8 Scope of Work	Generic	Data Privacy:	Are there any specific RBI/CERT-IN directives or internal bank guidelines bidders must comply with (apart from OWASP)?	Any directions issued by regulator from time-to-time
49	Generic	Annexure-8 Scope of Work	Generic	Incident Management:	What is the expected SLA for resolving critical issues? Is the Bank expecting a 24x7 support setup or support limited to working hours?	The support time will be shared to the selected bidder
50	79	Annexure-13 Escalation Matrix	Full Clause	Full Clause	Will the Bank share its own escalation matrix for smoother coordination, or does it expect only bidder's matrix?	Details will be shared with the selected bidder.
51	Generic	Annexure-8 Scope of Work	Generic	Renewal and Extension	Is there any provision or clause regarding extension after one year, or should pricing be fixed only for 12 months?	Bidder to comply with RFP terms and conditions.
52	Generic	Annexure-8 Scope of Work	Generic	Ownership of Content:	Does the Bank require perpetual rights over the created awareness content (videos, creatives, posters)?	Yes.
53	Generic	Annexure-8 Scope of Work	Generic	Evaluation Criteria:	Can the bank share details of technical and commercial evaluation methodology (weightages, marks, etc.)?	RFP Clause is self explanatory. Bidder to comply with RFP terms and conditions.
54	Generic	Annexure-8 Scope of Work	Generic	Point of Contact:	Who will be the SPOC from the bank's side during the implementation and support phase?	Details will be shared with the selected bidder.

Date: 07-05-2025



Sl. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Reply
---------	----------	-------------------------------	------------	-------------------------------------	----------------	--------------

Place: Bengaluru

Deputy General Manager



Corrigendum-1 to GeM bid Ref. No: GEM/2025/B/6162604 dated 23/04/2025 for Selection of vendor for providing Subscription Services to Phishing Simulation Platform and Cyber Security Awareness Content Suite in Canara Bank for One Year.

It is decided to amend the following in respect of the above RFP:

Sl. No	Section/Annexure/Appendix of GeM Bid	Clause No.	Existing Clause	Amended Clause
1.	Annexure-2 Pre- Qualification Criteria	Sl.No. 11	<p>Pre-Qualification Criteria:</p> <p>The bidder should have support office in Bengaluru for 24x7 supports. Documents to be submitted In compliance with Pre-Qualification Criteria:</p> <p>The Bidder should submit the details viz., address, phone no., email id and contact person Name & Mobile no. etc.</p>	<p>Pre-Qualification Criteria:</p> <p>The bidder should have support office in India for 24x7 supports. Documents to be submitted In compliance with Pre-Qualification Criteria:</p> <p>The Bidder should submit the details viz., address, phone no., email id and contact person Name & Mobile no. etc.</p>
2.	Annexure- 9 Technical Evaluation Criteria	Entire Annexure	Existing Annexure-9 Technical Evaluation Criteria	Amended Annexure-9 Technical Evaluation Criteria

All the other instructions and terms & conditions of the above RFP shall remain unchanged.

Please take note of the above amendments while submitting your response to the subject RFP

Date: 07/05/2025
Place: Bengaluru


Deputy General Manager



Amended Annexure-9
Technical Evaluation Criteria

(Should be submitted on Company's letter head with company seal and signature of the authorized person)

SUB: Selection of vendor for providing Subscription Services to Phishing Simulation Platform and Cyber Security Awareness Content Suite in Canara Bank for One Year

Ref: GEM/2025/B/6162604 dated 23/04/2025.

The technical evaluation of the bidder will be carried as per the details furnished below:

Sl. No.	Criteria	Evaluation Parameters	Documents to be submitted	Max. Marks
1	The Bidder/OEM should have provided phishing simulation and creation of awareness contents of Cyber Security in India in any PSUs/ PSBs as on 31/03/2025.	No. of PSUs/ PSBs: More than 2 clients - 15 Marks 1-2 client - 10 Marks	Purchase Order/ Work order along with invoice/ work completion letter/ Satisfactory letter to be submitted from the clients with the details of implementation.	15
2	The Bidder/OEM should have provided phishing simulation and creation of awareness contents of Cyber Security in India in any Schedule Commercial Bank (SCB)/ BFSI Sector during the last 5 years.	No. of Client/s in Schedule Commercial Bank (SCB)/ BFSI Sector: More than 5 clients - 15 Marks 3-5 clients - 12 Marks 1-2 clients - 8 Marks	Purchase Order/ Work order along with invoice/ work completion letter/ Satisfactory letter to be submitted from the clients with the details of implementation.	15
3	The Bidder/OEM should be capable of creating Awareness & Training contents in Hindi, English & in any 5 regional languages.	Contents with less than 5 languages will not be considered.: Posters - 4 Marks, Videos/ Reels - 4 Marks, Quizzes/ Games- 4 Marks, Content for Hack shows- 4 Marks Social Media Campaigns- 4 marks	Sample posters, videos, quizzes & templates for hack show & social media campaigns submitted to past clients/ customers with supporting documents as proof of submission along with Purchase order/ work order.	20
4	Technical Presentation on Proposed Solution by the Bidder	Technical presentation will be evaluated on the following parameters: <ul style="list-style-type: none"> Quality and completeness of Proposed solution - 7 Marks Approach, methodology & quality of sample reports- 7 marks User base handled for conducting the simulation activity- 5 Marks Credentials (in India and globally)- 3 Marks Value addition to the organization- 3 Marks 		25



5	Proof of Concept (POC) of the proposed solution to be demonstrated to bank Staff in accordance with the RFP's Scope of Work to evaluate its capabilities. The brief Scope of Work for the POC is as under:			25	
	#	POC Component	Description		Marks
	1	Phishing Simulation	Simulate phishing emails with user click tracking, redirect users to a custom video training and quiz page.		9
	2	Smishing	Execute SMS phishing campaign with click tracking.		2
	3	Vishing	Demonstrate vishing attack using scripted live or automated voice calls.		2
	4	Scenario Customization & BFSI Relevance	Showcase ability to tailor phishing/smishing/vishing scenarios for the BFSI sector.		3
	5	Behavior Analytics	Provide dashboards showcasing the user actions, training completions, and risk profiling.		2
	6	Cybersecurity Awareness Materials - Posters & Videos	Present samples of awareness videos and posters designed for employee sensitization.		3
7	Interactive Content - Quizzes & Live Hack Show Demos	Showcase gamified quizzes and creative content for live hack demos or awareness sessions.	4		
Total Maximum Marks				100*	

Note: *The bidder should score minimum 70% marks (i.e., 70 Marks out of 100 marks) total marks for qualifying under Technical Evaluation. The bidders qualified under Technical Proposal Evaluation will be eligible for commercial opening.

Bidder to note that all features must be available for demonstration during Presentation/ Product Demonstration. During evaluation, if any of the criteria mentioned as compliant is not found in the solution, marking will be modified in the respective category as evaluated by the Bank & Bank's decision shall be binding on the bidders. It is mandatory for Bidders to have all functionalities listed. Any non-compliance may lead to bidder's disqualification.

Terms & Conditions:

1. Bank reserves the right to conduct interviews of the proposed team members.
2. In case of absence of the allotted resource, the standby should perform the job of the absentee.
3. Bank may reject such manpower if bank is not satisfied with his/her performance.

Declaration: We hereby confirm that the information submitted above is true to the best of our knowledge. We understand that in case any discrepancy is found in the information submitted by us, our response to this RFP is liable for rejection.

Date:
Place:

Signature with seal
Name:
Designation:

