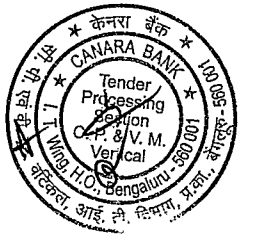
REPLIES TO THE PRE BID QUERIES OF THE GEM BID REF NO:GEM/2024/B/4680950 DATED 23/02/2024, ENGAGEMENT OF AUDITOR FOR CONDUCTING EXTERNAL VULNERABILITY ASSESSMENT & PENETRATION TESTING (VAPT) FOR THE HALF-YEAR ENDING MARCH 2024 IN CANARA BANK.

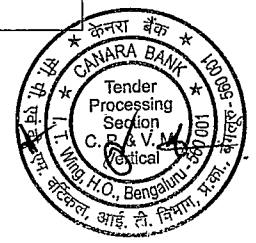
Sl. No.	Page. No	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Queries / Clarification	Bank Response
1	12	SECTION C - DELIVERABLE AND SERVICE LEVEL AGREEMENTS	1. Project Timelines	1.2 Risk categorization of the observation needs to be done as Critical, High, Medium and Low.	Is there any methodology defined by the Bank for the categorization of risks observation?	Based on Common Vulnerability Scoring System (CVSS), criticality of assets and ease of exploitness.
2	60	SECTION B - INTRODUCTION	Annexure - 9 Scope of Work	2.Assessment should be based on the guidelines issued by the relevant regulators time to time.	Is there any particular RBI circular which should be referred for the security assessment?	Vendor/Bidder must know all the RBI and regulartory circular and guidelines and Industry standerd cyber security guidelines and methodologies.
3	12	SECTION C - DELIVERABLE AND SERVICE LEVEL AGREEMENTS	1. Project Timelines	1.5. Phase 2 - Revalidation Scanning: Completion of verification scan and Clean reports	Our understanding is that only one round of revalidation will be performed for each asset/application during the revalidation phase. Please confirm if our understanding is correct.	Untill Clean report provided (Two Round of revalidation)
4	62	SECTION B - INTRODUCTION	Annexure - 9 Scope of Work	10.The techniques and the tools used should have been thoroughly tested and licensed.	Our understanding is that all the tools/licenses/laptops should be arranged by the bidder. Please confirm if our understanding is correct.	All license/tools/laptop should be arranged by bidders only.
5	11	SECTION B - INTRODUCTION	9. Scope of Work	9.4.The consultant should have pool of at least twenty (20 Nos) professionals, to deploy on site.	Can the external penetration testing activities be performed remotely?	External penetration testing activities should be performed in Bank premises only. However some tests can be performed remotely also. It is purely discretion of the Bank.
6	11	SECTION B - INTRODUCTION	9. Scope of Work	9.3. The consultant should have pool of at least twenty (20 Nos) professionals, to deploy on site. Internal	What is the location where the resources have to deployed onsite? Can the resources work from any of the Canara Bank locations across India?	Canara bank Head Office, Bengaluru, Karnataka only.
7	61	Annexure-9 Scope of Work	Annexure-9 Scope of Work	8. Malware attacks on the ATMS, PT for ATM on random basis based on regulatory guidelines (Bank will select the ATM on which VAPT need to be done).	Kindly confirm if the bidder needs to perform VAPT on the selected ATMs in addition to the count of servers/applications mentioned in Commerical Bid format.	Yes.The bidder needs to perform VAPT on the selected ATMs in addition to the count of servers/applications.
8	63	Annexure-9 Scope of Work	10. Scope of work for Penetration Testing/ External Attack Penetration Testing	On requirement, Auditors should carry out External attack penetration testing on lean business hours for the bank.	We assume that the External attack penetration testing shall be conducted during off business hours or weekends. Please confirm.	Auditors have to apprise Bank team before initiating the Testing. Critical Application testing will be tested during off Business hours/Weekends.
9	90	Appendix-G Draft Contract Agreement	11. INDEMNITY	11.2.2. The limits specified in above clause shall not apply to claims made by the Bank/third parties in case of infringement of Intellectual property rights or for claims relating to the loss or damage to real property and tangible personal property and for bodily injury or death and in these cases the liability will be unlimited.	Client is requested to delete exceptions to the limitation of liability. The exceptions render the limitation of liability ineffective and make the liability unlimited.	Bidder to comply with RFP terms and conditions



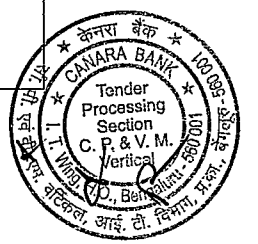
10		General Query		Limitation of Liability Indirect and consequential losses are not excluded from liability	Client is requested to include to clause to state that we will not be liable for any indirect and consequential losses or damages. This is as per GFR and MeitY guidelines and also the industry standard. Even the Contract Act, stipulates and remote and consequential damages are not payable. Client is requested to include the below clause: *"Purchase/Client agrees that Consultant will not be liable for (i) loss or corruption of data from your systems, (ii) loss of profit, goodwill, business opportunity, anticipated savings or benefits or (iii) indirect or consequential loss."*	Bidder to comply with RFP terms and conditions
11		General Query		Confidentiality Obligations Exceptions to confidential information are not provided	Client is requested to allow standard exceptions to confidential information, which is industry standard and reasonable. Not all information can be regarded as confidential. For eg., if the information is in public domain, we cannot be expected to keep it confidential at our end. Similarly, if any information is liable to be disclosed under the RTI, giving it a confidential status and obliging us to keep such information confidential is not correct. We request inclusion of following clause: *"Confidential information does not include any information which (i) is rightfully known to the recipient prior to its disclosure; (ii) is independently developed by the recipient without use of or reliance on confidential information; or (iii) is or later becomes publicly available without violation of this agreement or may be lawfully obtained from a third party; or (iv) which would be required to be disclosed under the (Indian) Right to Information Act."*	Bidder to comply with RFP terms and conditions
12		General Query		Confidentiality Obligations Parties to whom information can be disclosed is not documented	Client is requested to consider that we may have to disclose information for successful accomplishment of work and for regulatory and internal compliance purposes. However, to the extent legally permissible, we will ensure that even if the information is disclosed to any third party, such parties maintain confidentiality of such information. Client is therefore requested to kindly include the following clause: *"Consultant may disclose confidential information: (a) to its employees, directors, officers and subcontractors, on a need to know basis, as required for performance of services, provided such employees, directors, officers and subcontractors are bound by confidentiality obligations; (b) where required by applicable law or regulation or for regulatory and compliance (both internal and external) purposes."*	Bidder to comply with RFP terms and conditions
13	33,89	Indemnity	Cl. 9 , Cl. 10	Indemnities for IPR infringement claims without exceptions	We request client 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 non-infringing equivalent; iii. Modify it to make it non-infringing.* *3. The foregoing remedies constitute Indemnified Party's sole and exclusive remedies and Indemnifying Party's entire liability with respect to infringement."*	Bidder to comply with RFP terms and conditions

केनरा बैंक CANARA BANK Tender Processing Section C. P. V. M. Vertical Bengaluru-560 001

14	90	Appendix-G Draft Contract Agreement	11. INDEMNITY	Indemnity for breach of contract obligations	There are several remedies available under law and contract to you for such breach of obligations. For eg., there are penalties and LDs that may be imposed for some of these breaches. Seeking indemnities for such breaches frustrates the entire purpose of such remedies available to you. We understand that remedies other than indemnity will be sufficient for such breaches. We request you to kindly delete this section. If you still insist on retaining this section, then we request you to at least make them subject to overall cumulative liability cap of total contract value and subject to final determination of court/arbitrator.	Bidder to comply with RFP terms and conditions
15	90	Appendix-G Draft Contract Agreement	General	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 MeitY in its guidelines.	Bidder to comply with RFP terms and conditions
16	90	Appendix-G Draft Contract Agreement	General	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 favour 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	Bidder to comply with RFP terms and conditions
17		General Query		Termination Termination without notice and rectification period	To uphold the principles of natural justice, we request client to notify us and give us a rectification period of at least 30 days, prior to invoking this clause.	Bidder to comply with RFP terms and conditions
18		General Query		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 client to give us the right to terminate the contract in case client breaches any of its material obligations under the contract, provided a notice for such breach is given to client along with a rectification period of 30 days.	Bidder to comply with RFP terms and conditions
19		General Query		Cancellation Cancellation / Recission of Contract	Cancellation / Rescission means voiding the contract and making the contract ineffective from its inception, thereby restoring the parties to the positions they would have occupied if no contract had ever been formed. In this scenario, bidder may be deprived of any payment and refund of all payments made already may be sought. Request deletion of this clause	Bidder to comply with RFP terms and conditions
20		General Query		Risk purchase	Request client to limit our liability under this clause to 10% of the value of corresponding goods/services not delivered by us. Please also confirm that client will use government procurement norms (including price discovery) for procurement of such services from third parties.	Bidder to comply with RFP terms and conditions



21	38,40	SECTION G - GENERAL CONDITIONS	21.Conflict of interest 24. Responsibilities of the Bidder	21.2. BIDDER/VENDOR/ SERVICE PROVIDER represents and warrants that if any such actual or potential conflict of interest arises under this Agreement, Vendor/Service Provider shall immediately inform the Bank in writing of such conflict. 24.4. BIDDER/VENDOR/ SERVICE PROVIDER represents and warrants that if any such actual or potential conflict of interest arises under this Agreement, Vendor/Service Provider shall immediately inform the Bank in writing of such conflict.	We wish to highlight that we are a large organization providing various services to various state and central government departments, PSUs, international organizations and private clients. We wish you to note that while we have a mechanism in place to identify patent and direct conflict of interests, it may not always be possible to identify any or all indirect or remote conflict of interests. Kindly appreciate that our no conflict confirmations will be subject to the foregoing.	Bidder to comply with RFP terms and conditions
22	88	Appendix-G Draft Contract Agreement	8. ORDER CANCELLATION/TERMINATION OF CONTRACT:	8.2.7.If deductions on account of liquidated Damages exceeds more than 10% of the total contract price.	We request client to cap the liquidated damages/penalties cumulatively to 5% of the total contract value.	Bidder to comply with RFP terms and conditions
23		General Query		Liquidated damages Not sole and exclusive remedy	We understand that as per Contract Act, where LDs are stipulated, generally any other damages cannot be claimed. Therefore we request you to kindly make imposition of liquidated damages as sole and exclusive remedy for corresponding breaches.	Bidder to comply with RFP terms and conditions
24		General Query		Liquidated damages Not limited to solely our fault	We understand that we would be liable to pay liquidated damages to the extent corresponding breach is solely attributable to us. Kindly confirm.	Bidder to comply with RFP terms and conditions
25		General Query		INTELLECTUAL PROPERTY RIGHTS No protection to our pre-existing IPRs	There are innumerable IPRs that exist with us which we would like to use to your benefit while delivering our services to you. These are our pre-existing IPRs and we use it for all clients. We will not be able to give ownership in such IPRs to you just because we are using them for providing services to you, like we use these for other clients. We request that we are allowed to retain ownership of our pre-existing IPRs, else we might be not be able to use these in providing services to you in order to protect our ownership in them. We request you to kindly include the below clause. This is also the standard mentioned by MeitY in its guidelines. *"Notwithstanding anything to the contrary in this agreement, Consultant will retain the ownership of its pre-existing intellectual property rights (including any enhancement or modification thereto) even if such IPRs are used for creating deliverables, are incorporated in the deliverables, etc. To the extent such pre-existing IPRs are included/incorporated in the deliverables, upon receipt of all due and payable payment in full, the Consultant shall grant a non-exclusive, perpetual and fully paid up license to the Purchaser/Client to use such pre-existing IPRs for use of deliverables for the purpose for which such deliverables are meant for client's internal business operations."*	Bidder to comply with RFP terms and conditions
26	16	SECTION C - DELIVERABLE AND SERVICE LEVEL AGREEMENTS	8. Right to Audit	8. Right to Audit	We wish to clarify that we will retain our records as per our records retention policies. Upon reasonable notice, we will allow Client 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.	Bidder to comply with RFP terms and conditions
27		General Query		No third party disclaimer 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.	Bidder to comply with RFP terms and conditions



28		General Query		Acceptance No acceptance criteria	If the project is to be completed on time, it would require binding both parties with timelines to fulfil 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 Client's receipt of a draft deliverable, Client will notify Consultant if it is accepted. If it is not accepted, Client 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 Client does not notify Consultant within the agreed time period or if Client uses the draft deliverable, it will be deemed to be accepted."*	Bidder to comply with RFP terms and conditions
29	65	Annexure 10 Technical Evaluation Criteria	Sl No:1	CERT-IN empaneled security Auditors with at-least 6 years (i.e. 2018-19, 2019-20, 2020-21, 2021-22 and 2022-23, 2023-24) continuous empanelment by CERT-IN without any de-empanelment.	"We have been recognized as a CERT-IN empaneled vendor since 2021, providing services to various banks such as Central Bank of India, UCO Bank, Indian Bank, IDFC First Bank, Kotak Bank, Yes Bank, and Punjab National Bank. Kindly consider extending the relaxation to include CERT-IN empanelment for the years 2021-22, 2022-23, and 2023-24, enabling our continued participation."	Bidder to comply with RFP terms and conditions
30	60	Annexure 9 Scope of work		General Query	Should Infrastructure VAPT & Appsec conducted in a greybox or blackbox manner?	Yes, grey box and black box will be there. Bank will infrom the auditor based on the criticality of assets.
31	62	Annexure 9 Scope of work	Annexure 9 Scope of work	10.Scope of work for Penetration Testing/ External Attack Penetration Testing: -	Can we conduct External penetration testing remotely or do we have to conduct it from bank premises ?	External penetration testing activities should be performed in Bank premises only. However some tests can be performed remotely also. It is purely discretion of the Bank.
32	12	SECTION C - DELIVERABLE AND SERVICE LEVEL AGREEMENTS Section C	1. Project Timelines	1.6The selected Bidder should meet the deadlines for completion of the Scope of Work as per RFP terms and conditions.	Since the penalty clause is mentioned in Section C 3.1pertaining to the delay, we would request to include another clause under Section C 1.6 stating below: - Bank shall endeavour to close the findings as reported in Phase 1 within seven (07) days of reporting in order to meet the deadlines. In case of any delay on and above seven days, this timeline is excluded from overall Phase 1 and Phase 2 timeline.	Bidder to comply with RFP terms and conditions
33	13	SECTION C - DELIVERABLE AND SERVICE LEVEL AGREEMENTS Section C	3. Penalties & Liquidated damages	3.1.If the VAPT Assessment is not completed within the Phase wise timelines as per clause no.1.5, Bank will impose penalty @ 0.50% per week delay and part thereof on the total cost of the VAPT Assessment for each phase. However, the total Penalty/LD to be recovered shall be restricted to 10% of total cost of the VAPT Assessment.	May we request to include below statement in addition to clause 'Section C 3.1: If there is any delay in addressing the initial findings that extends beyond 7 days, bidders cannot be held responsible for these delays.	Bider to refer clause 3.10 in Section C. Bidder to comply with RFP terms and conditions
34	13	SECTION C - DELIVERABLE AND SERVICE LEVEL AGREEMENTS Section C	3. Penalties & Liquidated damages	3.2.Penalties/Liquidated Damages for non-performance: If the selected bidder does not meet the specifications/terms of the RFP during various tests/stages, the selected bidder shall rectify the same at bidders cost to comply with the specifications/terms of the RFP immediately to ensure the committed uptime/terms, failing which the Bank reserves its right to withhold the payment, impose penalty and invoke the Bank Guarantee/ nullify the contract.	May we request to include below statement in addition to clause 'Section C 3.2: In the event of any delays not caused by bidders, the Bank will proceed with payment for the completed milestone without any further obligation. Bidders will be notified at least 07 days in advance to resume work once the delays have been resolved at Bank's end.	Bidder to comply with RFP terms and conditions

केनरा बैंक CANARA BANK Tender Processing Section I. T. Wing, H.O., Bengaluru - 560 001

<table>
<tr><td>35</td><td>14</td><td>SECTION C - DELIVERABLE AND SERVICE LEVEL AGREEMENTS Section C</td><td>3. Penalties & Liquidated damages</td><td>3.7Bank may impose penalty to the extent of damage to its any equipment, if the damage was due to the actions attributable to the staff of the selected bidder.</td><td>May we request to include below statement in addition to clause 'Section C 3.7:
In the event of any delays not caused by bidders, the Bank will proceed with payment for the completed milestone without any further obligation. Bidders will be notified at least 07 days in advance to resume work once the delays have been resolved at Bank's end.</td><td>Bidder to comply with RFP terms and conditions</td></tr>
<tr><td>36</td><td>14</td><td>SECTION C - DELIVERABLE AND SERVICE LEVEL AGREEMENTS</td><td>4. Payment Terms</td><td>Payment schedule on successful Assessment of Domains in each Phase:</td><td>Based on the volume of the scope of work and required effort, may we request to change the payment terms as follows:
<table><tr><th>Scope of Work</th><th>Payment Stage</th><th>% of Payment to be released</th></tr><tr><td>Milestone 1</td><td>On completion of initial VAPT as per scope of work No. of Network Assets (Switches, Routers, Security Devices, Load balancers etc.)</td><td>10%</td></tr><tr><td>Milestone 2</td><td>On completion of initial VAPT as per scope of work Servers (App, DB, Web Servers, VM, Middleware, Storage etc.)</td><td>10%</td></tr><tr><td>Milestone 3</td><td>On completion of initial VAPT as per scope of work for Mobile Applications, etc.</td><td>20%</td></tr><tr><td>Milestone 4</td><td>On completion of initial VAPT as per scope of work web application (Internal/External)</td><td>30%</td></tr><tr><td>Milestone 5</td><td>On completion of Completion of verification scan and clean reports</td><td>30%</td></tr></table></td><td>Bidder to comply with RFP terms and conditions</td></tr>
<tr><td>37</td><td>28</td><td>SECTION F - OWNERSHIP & AWARDING OF CONTRACT</td><td>9. Performance Security</td><td>9.1. The successful bidder should submit a Security Deposit / Performance Bank Guarantee equivalent to 5% of the Total Cost of Ownership (TCO) value as specified in Bid Schedule within 15 days from the date of acceptance of the Purchase Order with the validity period of 6 months from the date of acceptance of order and shall be retained till the completion of Contract period.
9.2. If the Security Deposit /Performance Guarantee is not submitted within the time stipulated above, penalty at 0.50% for each completed calendar week of delay or part thereof on the total value of the order will be deducted from the delivery payment or from any other payments for the delay in submission of Bank Guarantee. The total penalty under this clause shall be restricted to 2.5% of the total order value.</td><td>May we request to include below statement in addition to clause 'Section C 9.2:
In the event of any delays not caused by bidders, the Bank will proceed with payment for the completed milestone without any further obligation. Bidders will be notified at least 07 days in advance to resume work once the delays have been resolved at Bank's end.</td><td>Bidder to comply with RFP terms and conditions</td></tr>
<tr><td>38</td><td>28</td><td>SECTION G - GENERAL CONDITIONS</td><td>1. Human Resource Requirement</td><td>Background Police Verification report - Duly attested photocopy by candidate and bidder HR</td><td>May we request to remove this clause as the bidder is solely responsible to hire the resource under the bidders payroll.</td><td>Bidder to comply with RFP terms and conditions</td></tr>
<tr><td>39</td><td>58</td><td>Annexure 7</td><td>List of Major Customers of the Bidder in Last 3 Years and References</td><td>Satisfactory Letter from customer to be Enclosed or Purchase Orders to be enclosed</td><td>Since satisfactory letter from customer is not available post completion of each project, please allow us to furnish compensative document such as final payment release communication or other relevant information to comply this clause.</td><td>Bidder to comply with RFP terms and conditions</td></tr>
</table>

Date:07/03/2024
Place: Bengaluru

Deputy General Manager

केनरा बैंक CANARA BANK Tender Processing Section C. P. & V. M. Vertical H.O., Bengaluru - 560 001