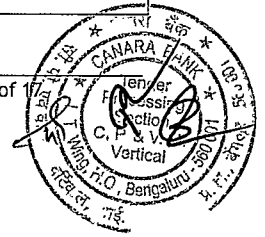


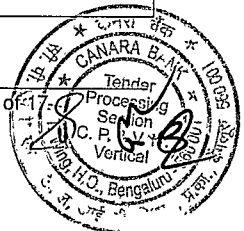
Replies to Pre Bid Queries to GeM Bid ref no. GEM/2023/B/3965630 dated 15/09/2023 for Engagement of Auditor for Conducting External Vulnerability Assessment & Penetration Testing (VAPT) for the half-year ending September 2023 in Canara Bank

Sl. No.	Page No.	Section/ Annexure/ Appendix	RFP Clause	Sub- Clause/Technical Specification	Bidders Query	Bank Reply
1	11	SECTION B - INTRODUCTION	9. Scope of Work	9.2. Bank reserves the right to modify the scope due to change in regulatory instructions, market scenario and internal requirement within the overall objective for conducting external VAPT.	Will there be any change in the commercials if the scope is modified during the contract duration?	As per PO Terms only.
2	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.	Can the external penetration testing activities be performed remotely?	Bank's premise only, Bengaluru (Negotiable)
3	12	SECTION C - DELIVERABLE AND SERVICE LEVEL AGREEMENTS	1. Project Timelines	1.1. Risk categorization of the observation needs to be done as Critical, High, Medium and Low.	Is there any methodology defined by the Bank for categorizing the risks of the observation?	CVSS Scoring and Criticality of the Asset
4	12	SECTION C - DELIVERABLE AND SERVICE LEVEL AGREEMENTS	1. Project Timelines	1.5. 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.	Revalidation will be 2 times. In case all observations are not closed it will be performed for each Asset/Application.



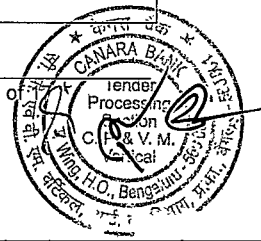
Replies to Pre Bid Queries to GeM Bid ref no. GEM/2023/B/3965630 dated 15/09/2023 for Engagement of Auditor for Conducting External Vulnerability Assessment & Penetration Testing (VAPT) for the half-year ending September 2023 in Canara Bank

Sl. No.	Page No.	Section/ Annexure/ Appendix	RFP Clause	Sub- Clause/Technical Specification	Bidders Query	Bank Reply
5	13	SECTION C - DELIVERABLE AND SERVICE LEVEL AGREEMENTS	3. Penalties & Liquidated damages	3.2. If the bidder does not meet the requirements of the GeM BID (RFP) during contract, the bidder shall rectify the same at bidders cost to comply with the requirements immediately to ensure completion of the activity, failing which the Bank reserves its right to invoke the Bank Guarantee.	What the requirements of the GeM Bid (RFP) to be followed during the contract?	Bidder has to deliver the services as per scope of work, specified in the RFP.
6	20	SECTION D: BID PROCESS	6. Earnest Money Deposit (EMD)/Bank Guarantee in lieu of EMD:	EMD Amount - Rs. 200000	AQM Technologies Pvt. Ltd. declare that we possess MSME certificate (Medium Enterprises), so we are requesting for the exemption for Earnest Deposit Money	The bidder seeking EMD exemption, must submit the valid supporting document for the relevant category as per GeM GTC with the bid. Under MSE category, only manufacturers for goods and Service Providers for Services are eligible for exemption from EMD.



Replies to Pre Bid Queries to GeM Bid ref no. GEM/2023/B/3965630 dated 15/09/2023 for Engagement of Auditor for Conducting External Vulnerability Assessment & Penetration Testing (VAPT) for the half-year ending September 2023 in Canara Bank

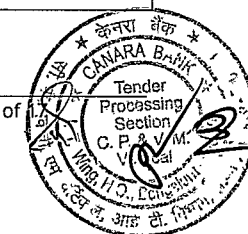
Sl. No.	Page No.	Section/ Annexure/ Appendix	RFP Clause	Sub- Clause/Technical Specification	Bidders Query	Bank Reply
7	52	Annexure 9: Scope of Work	Scope of Work	3. VAPT testing of any assets, Applications etc. should contains but not limited to below details.	Provide the total no of assets to be assessed as part of VAPT activity: a. Number of application servers (shared, non-shared) b. Number of Web servers (shared, non-shared) c. Number of DB Servers (Shared, non-shared) d. Number of Thin clients to assess e. Number of Thick clients to assess f. Number of Networking devices to assess along with type of devices g. Number of security devices to assess	Details are confidential and will be shared with the selected bidder after the end of bid process. Tentative Count has been shared as part of Bill of Material.
8	52	Annexure 9: Scope of Work	Scope of Work	3. Attempt to overload the system using DDoS (Distributed Denial of Service) and DOS (Denial of Service) attacks as and when instructed by the Bank to do so.	Do we need to perform DDOS & DOS Test?	Yes, when instructed by the Bank to do so.



Replies to Pre Bid Queries to GeM Bid ref no. GEM/2023/B/3965630 dated 15/09/2023 for Engagement of Auditor for Conducting External Vulnerability Assessment & Penetration Testing (VAPT) for the half-year ending September 2023 in Canara Bank

Sl. No.	Page No.	Section/ Annexure/ Appendix	RFP Clause	Sub-Clause/Technical Specification	Bidders Query	Bank Reply
9	52	Annexure 9: Scope of Work	Scope of Work	2. The security assessment should be designed to simulate a real-world attack keeping in view prevailing RBI guidelines, IT Act 2000/ (Amendment) 2008 and other applicable regulations in India.	Is there any particular RBI circular which should be referred for the security assessment guidelines?	Vendor should know all the RBI, IT Act and regulators guidelines.
10	52	Annexure 9: Scope of Work	Scope of Work	3. Attempt to overload the system using DDoS (Distributed Denial of Service) and DOS (Denial of Service) attacks as and when instructed by the Bank to do so.	Whether the services of Red teaming is required?	No Red teaming exercise is required.
11	53	Annexure 9: Scope of Work	Scope of Work	3. Hard-coded Password or Key or sensitive information.	Need Clarification	Sensitive information like source code/ Password/ keys/PI data which is visible on code of Assets like web Applications.

Replies to Pre Bid Queries to GeM Bid ref no. GEM/2023/B/3965630 dated 15/09/2023 for Engagement of Auditor for Conducting External Vulnerability Assessment & Penetration Testing (VAPT) for the half-year ending September 2023 in Canara Bank						
Sl. No.	Page No.	Section/ Annexure/ Appendix	RFP Clause	Sub-Clause/Technical Specification	Bidders Query	Bank Reply
12	53	Annexure 9: Scope of Work	Scope of Work	6. Presence of WAF available behind the Web Application.	1. Provide the no of application behind WAF. 2. Provide the no of External and Internal Application covered under DAST	1. Security Auditor has to verify and check if Application is behind WAF or not, is part of the assessment 2. We will share upon selected bidder after bidding
13	53	Annexure 9: Scope of Work	Scope of Work	7. OWASP Top 10 vulnerabilities (Mobile applications): - Penetration testing to be conducted for mobile applications	1. Provide the total no of mobile application(Android/IOS) in VAPT scope.	Please find below tentative count, It may vary: 18 - Android 10 - IOS 2 - Desktop
14	54	Annexure 9: Scope of Work	Scope of Work	8.b. Exercise should be carried out from the bank premises only, no travel charges will be paid by the bank	Provide the Location of DC and DR for VAPT assessment	Bank's premises only, Information Security Section, Bengaluru
15	54	Annexure 9: Scope of Work	Scope of Work	8.b. 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.	Yes, Tool/Licenses should be arranged by bidder. No outside/personal Devices or Laptop permitted to connect on Bank Intranet.



Replies to Pre Bid Queries to GeM Bid ref no. GEM/2023/B/3965630 dated 15/09/2023 for Engagement of Auditor for Conducting External Vulnerability Assessment & Penetration Testing (VAPT) for the half-year ending September 2023 in Canara Bank

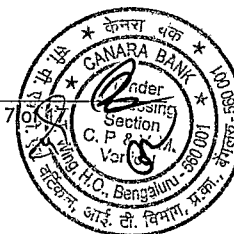
Sl. No.	Page No.	Section/ Annexure/ Appendix	RFP Clause	Sub- Clause/Technical Specification	Bidders Query	Bank Reply
16	54	Annexure 9: Scope of Work	Scope of Work	8.b. Vulnerability assessment shall be carried out for all servers, applications, network devices, security devices installed etc.	What are the different types of security devices that needs to be tested?	Details are confidential and will be shared with the selected bidder after the end of bid process. Tentative Count has been shared as part of Bill of Material.
17	54	Annexure 9: Scope of Work	Scope of Work	8.b. External attack Penetration Testing should include all the Public Facing Assets of the Bank.	What are the different types of assess that are public facing?	Tentative details are below: Web Application, Mobile Application. Detailed list will be shared to only selected bidder after bidding
18	55	Annexure 9: Scope of Work	Scope of Work	8.c. 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.	Plan of Action will shared with selected bidder after successful bidding



Canara Bank

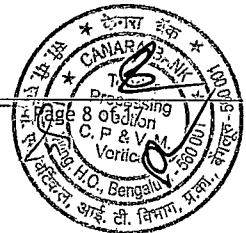
Replies to Pre Bid Queries to GeM Bid ref no. GEM/2023/B/3965630 dated 15/09/2023 for Engagement of Auditor for Conducting External Vulnerability Assessment & Penetration Testing (VAPT) for the half-year ending September 2023 in Canara Bank

Sl. No.	Page No.	Section/ Annexure/ Appendix	RFP Clause	Sub-Clause/Technical Specification	Bidders Query	Bank Reply
19	56	Annexure 9: Scope of Work	Scope of Work	Reporting: VAPT report should cover the remedial detail in case of vulnerabilities detected. After remedial solution implemented, the vendor should conduct VAPT again for verification of compliance of detected vulnerabilities and it should be completed within 3 months' post submission of VAPT report.	Is the revalidation time 2 months or 3 months post the submission of VAPT report?	Revalidation time is T+2 (months) post the submission of the VAPT Report. However, it can be extend on basis on technical dependencies.



Replies to Pre Bid Queries to GeM Bid ref no. GEM/2023/B/3965630 dated 15/09/2023 for Engagement of Auditor for Conducting External Vulnerability Assessment & Penetration Testing (VAPT) for the half-year ending September 2023 in Canara Bank

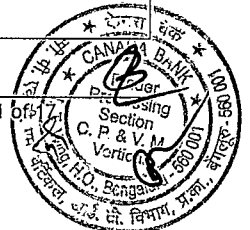
Sl. No.	Page No.	Section/ Annexure/ Appendix	RFP Clause	Sub- Clause/Technical Specification	Bidders Query	Bank Reply
20	58	Annexure 10: Technical Evaluation Criteria	Technical evaluation criteria	Sl No 2: The firm should have a pool of at least 20 professionals with active international accreditation like CISA (Certified Information Systems Auditor), CISSP (Certified Information Security Professional), CEH trained lead auditors employed with them. Minimum experience of the professionals' post qualification should be 5 years or more in similar kind of assessments.	We request to amend or modify the clause as "The firm should have a pool of at least 20 10 professionals with active international accreditation like CISA (Certified Information Systems Auditor), CISSP OSCP (Certified Information Security Professional), CEH trained lead auditors employed with them. Minimum experience of the professionals' post qualification should be 5 years or more in similar kind of assessments."	Bidder to comply with RFP Terms and Conditions



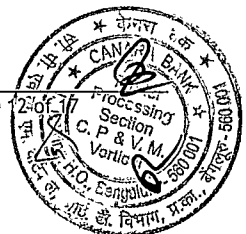
Replies to Pre Bid Queries to GeM Bid ref no. GEM/2023/B/3965630 dated 15/09/2023 for Engagement of Auditor for Conducting External Vulnerability Assessment & Penetration Testing (VAPT) for the half-year ending September 2023 in Canara Bank						
Sl. No.	Page No.	Section/ Annexure/ Appendix	RFP Clause	Sub- Clause/Technical Specification	Bidders Query	Bank Reply
21	58	Annexure 10: Technical Evaluation Criteria	Technical Evaluation Criteria	Sl No 2: The firm should have a pool of at least 20 professionals with active international accreditation like CISA (Certified Information Systems Auditor), CISSP (Certified Information Security Professional), CEH trained lead auditors employed with them. Minimum experience of the professionals' post qualification should be 5 years or more in similar kind of assessments.	Request you to include certifications oscp, cisa, cism, cssp, ISO 27001, etc and request you to reduce the minimum experience to 3 -4 Years	Active OSCP certification may be considered but minimum experience of the professionals' post qualification should be 5 years or more in similar kind of assessments.
22	62	Annexure 14: Bill of Material	Table A: Price details	3. VAPT as per scope of work (Mobile Applications, etc.)	We understand that there are 30 Mobile applications under scope. Please confirm the number of pages for each application and if both iOS and Android are under scope	Details will be shared with the selected bidder after the end of bid process.

Replies to Pre Bid Queries to GeM Bid ref no. GEM/2023/B/3965630 dated 15/09/2023 for Engagement of Auditor for Conducting External Vulnerability Assessment & Penetration Testing (VAPT) for the half-year ending September 2023 in Canara Bank						
Sl. No.	Page No.	Section/ Annexure/ Appendix	RFP Clause	Sub- Clause/Technical Specification	Bidders Query	Bank Reply
23	62	Annexure 14: Bill of Material	Table A: Price details	4. VAPT as per scope of work [No of Application (Application, Web Application Internal/ External)]	We understand that there are 420 Web applications under scope. Please confirm the number of pages for each application	Mostly Small size Web Application.

24	62	Annexure 14: Bill of Material	Table A: Price details	<p>1. VAPT as per scope of work No. of Network Assets (Switches, Routers, Security Devices, Load balancers etc.)</p> <p>2. VAPT as per scope of work Servers (App, DB, Web Servers, VM, Middleware, Storage etc.)</p> <p>3. VAPT as per scope of work (Mobile Applications, etc.</p> <p>4. VAPT as per scope of work [No of Application (Application, Web Application Internal/ External)]</p>	<p>Following are the details required for estimating the cost</p> <p>1. Total number of applications (External /internal):</p> <p>2. Size of each application required 0-150- Small, 151-500 - Medium ,500 n above - large</p> <p>2. Total number of mobile applications and its platform:</p> <p>4. Total number of screens in mobile application:</p> <p>5. Total number of API and its methods:</p> <p>6. Total number of server/network devices/security devices/database servers(External /internal):</p> <p>7. Can the auditors perform audit remotely - Please confirm</p>	<p>1. Total number of applications (External /internal): Details are shared upon selected bidder after bidding</p> <p>2. Size of each application required : Mostly small</p> <p>2. Total number of mobile applications and its platform: Tentative details - 18 - Andriod, 2 Desktop, 10 IOS</p> <p>4. Total number of screens in mobile application: Details are shared upon selected bidder after bidding</p> <p>5. Total number of API and its methods: Details are shared upon selected bidder after bidding</p> <p>6. Total number of server/network devices/security devices/database servers(External /internal): Details are shared upon selected bidder after bidding</p> <p>7. Can the auditors perform audit remotely - Please confirm- Bank's premise</p>
----	----	----------------------------------	---------------------------	---	---	---



Replies to Pre Bid Queries to GeM Bid ref no. GEM/2023/B/3965630 dated 15/09/2023 for Engagement of Auditor for Conducting External Vulnerability Assessment & Penetration Testing (VAPT) for the half-year ending September 2023 in Canara Bank						
Sl. No.	Page No.	Section/ Annexure/ Appendix	RFP Clause	Sub- Clause/Technical Specification	Bidders Query	Bank Reply
25	78	Appendix G: Draft Contract Agreement	Draft Contract Agreement	Contract Agreement	Do we need to execute this agreement in Stamp paper? If yes, then kindly confirm the Value of the Stamp Paper	Stamp Paper of Minimum Rs 200/- OR Stamp Act of State of Buyer (whichever is higher) to be followed.
26	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, in case if required for conducting the assessment, with relevant qualifications and having a minimum of 5 years of experience in conducting the similar kind of assessment.	1. We understand one resource is needed onsite throughout the project. Please confirm. 2. We understand that the audit location is Bangalore. Please confirm	1. Multiple resources are required on site to complete the project within the timelines. 2. Yes, Bengaluru only.

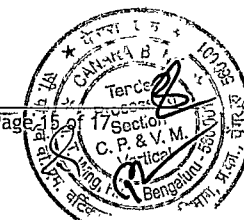


Replies to Pre Bid Queries to GeM Bid ref no. GEM/2023/B/3965630 dated 15/09/2023 for Engagement of Auditor for Conducting External Vulnerability Assessment & Penetration Testing (VAPT) for the half-year ending September 2023 in Canara Bank

Sl. No.	Page No.	Section/ Annexure/ Appendix	RFP Clause	Sub- Clause/Technical Specification	Bidders Query	Bank Reply
27	26	SECTION F - OWNERSHIP & AWARDDING OF CONTRACT	9. Security Deposit / Performance Bank Guarantee	9.2. Security Deposit should be submitted by way of DD drawn on Canara Bank payable at Bengaluru / Bank Guarantee may be obtained from any of the Scheduled Banks (other than Canara Bank).	The Percentage Value of the PGG has not been mentioned	An amount equivalent to 10% of the Contract Price plus GST
28	44	Annexure 2: Pre-Qualification Criteria	Pre-Qualification Criteria	7. The Bidder should have provided same Category of Assessment(s) in the last three Financial years before the bid opening date to any Central / State Govt Organization / PSU / Public Listed Company/BFSI sector.	Kindly confirm Number of work orders to be submitted	Bidder to submit minimum 2 Work Order for previous three Financial years

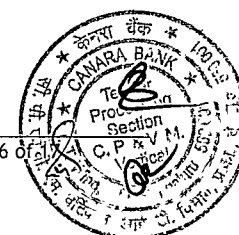
Replies to Pre Bid Queries to GeM Bid ref no. GEM/2023/B/3965630 dated 15/09/2023 for Engagement of Auditor for Conducting External Vulnerability Assessment & Penetration Testing (VAPT) for the half-year ending September 2023 in Canara Bank						
Sl. No.	Page No.	Section/ Annexure/ Appendix	RFP Clause	Sub- Clause/Technical Specification	Bidders Query	Bank Reply
29	68	Appendix E: Proforma of Bank Guarantee for Contract Performance	Proforma of Bank Guarantee for Contract Performance	To be submitted on Non-Judicial stamp paper of appropriate value Purchased in the name of the issuing Bank	Kindly confirm the Value of the Stamp Paper	Stamp Paper of Minimum Rs 200/- OR Stamp Act of State of Buyer (whichever is higher) to be followed.
30	71	Appendix F: Pre Contract Integrity Pact	Pre Contract Integrity Pact	This has to be submitted in the non-judicial Stamp Paper	Kindly confirm the Value of the Stamp Paper	Stamp Paper of Minimum Rs 200/- OR Stamp Act of State of Buyer (whichever is higher) to be followed.
31	58	Annexure 10: Technical Evaluation Criteria	Technical Evaluation Criteria	1. CERT-IN empanelled security Auditors with at-least 5 years (i.e. 2018-19, 2019-20, 2020-21, 2021-22 and 2022-23) continuous empanelment by CERT-IN without any de-empanelment.	Request that this be relaxed to 3 years of empanelment(2021-2022,2022-2023,2023-2024)	Bidder to comply with RFP Terms and Conditions

Replies to Pre Bid Queries to GeM Bid ref no. GEM/2023/B/3965630 dated 15/09/2023 for Engagement of Auditor for Conducting External Vulnerability Assessment & Penetration Testing (VAPT) for the half-year ending September 2023 in Canara Bank						
Sl. No.	Page No.	Section/ Annexure/ Appendix	RFP Clause	Sub- Clause/Technical Specification	Bidders Query	Bank Reply
32			General Query		The Quantity of Applications, devices has not provided for which VAPT has to be conducted. Need count of Applications, devices	Tentative Count Provided in Annex 14 - Bill of Material
33			General Query		No specific URL's or IPs provided that needs to be tested	Tentative Count Provided in Annex 14 - Bill of Material
34			General Query		Mobile application is also part of scope? (Android/IOS)	Yes, Both IOS and Andriod. Tentative Count Provided in Annex 14 - Bill of Material
35			General Query		As there is no remote access provided, please specify the physical location from where audit needs to be performed	Bank's premise only, Bengaluru
36			General Query		No. of Application/mobile/web external and Internal, No. of Assets, No. of Internal network, Sno. Of External networks, No of DB,	Tentative Count Provided in Annex 14 - Bill of Material




Replies to Pre Bid Queries to GeM Bid ref no. GEM/2023/B/3965630 dated 15/09/2023 for Engagement of Auditor for Conducting External Vulnerability Assessment & Penetration Testing (VAPT) for the half-year ending September 2023 in Canara Bank

Sl. No.	Page No.	Section/ Annexure/ Appendix	RFP Clause	Sub- Clause/Technical Specification	Bidders Query	Bank Reply
37			General Query		<p>Specify the assessment to be conducted (VA, BB-PT, GB-PT)</p> <ul style="list-style-type: none"> • Vulnerability Assessment (VA): <i>IP address scan, fingerprinting and identifying vulnerabilities - this is a basic test</i> • Black Box Penetration Test (BB-PT): <i>Vulnerability Assessment + Attempts to compromise the website, SQL injection, XSS, Input validation, privilege escalation, URL tampering etc</i> • Grey Box Penetration Test (GB-PT): <i>Vulnerability assessment + Black Box PT + Malicious activities by valid credential holders</i> 	Security Auditor has to perform the assessment as per Scope of Work.



Replies to Pre Bid Queries to GeM Bid ref no. GEM/2023/B/3965630 dated 15/09/2023 for Engagement of Auditor for Conducting External Vulnerability Assessment & Penetration Testing (VAPT) for the half-year ending September 2023 in Canara Bank						
Sl. No.	Page No.	Section/ Annexure/ Appendix	RFP Clause	Sub- Clause/Technical Specification	Bidders Query	Bank Reply
38			General Query		No. of network assets Switches, routers, security devices, load balancers and etc.	Tentative Count Provided in Annex 14 - Bill of Material. Detailed list will be shared with the selected bidder after bidding
39			General Query		Requesting you to please share the Number of Applications and External IPs part of the scope.	Tentative Count Provided in Annex 14 - Bill of Material. Detailed list will be shared with the selected bidder after bidding

Date: 04-10-2023
Place: Bengaluru


Deputy General Manager

