बैंक ऑफ़ बड़ौदा
Bank of Baroda

Bank's Clarification to Pre Bid Queries (GEM/2024/B/5371843 dated 11.09.2024) RFP for Selection of Service Provider for Vulnerability Assessment and Penetration Testing of Bank's Internet facing applications, Intranet applications and its Infrastructure

Bank's Clarification to the Pre-Bid Queries

Sr.no.	Page #	Point/Section #	Clarification point as stated in the tender document	Comment/ Suggestion	Bank's Clarification to Pre-bid queries
1	33	Annexure 2 : B. Technical Bid Evaluation	NOTE 2: For manpower consideration, the Employee should be on the payroll of the Bidding Company as on date of submission of this bid response. For this proof in the form of employment letter duly accepted by the employee or suitable declaration jointly signed by the Employer and Employee stating date of joining on the Bidding Company's letterhead should be submitted.	Is this declaration required from all employees who are certified as per Criteria mentioned in point 4 of Section B: Technical Bid Evaluation.	Yes joint declaration of (employee and employer) required for employees who will be deployed onsite for VAPT as per annexure 28. And for annexure 25 bidder has to obtain declaration from their employee and annexure to be submitted by bidder.
2	33	Annexure 2 : B. Technical Bid Evaluation	VAPT activity Management tool/solution as per # Note 3	1. Please specify if Bank will provide infrastructure such as server, database for provisioning of this VAPT Management tool at no additional cost to bidder.	Yes. However installation, maintenance, upgrade will be done by selected bidder only. Bidder to provide prerequisite and infra details for VAPT tool installation
3	57	Annexure 11 – Project Details & Scope of Work	1. Project Scope Vulnerability Assessment and Penetration Testing should cover the internet facing application, intranet applications and its components including web server, app server, DB Server, Thick client, Thin clients, Mobile applications, Networking systems, Security devices, load balancers, integration with other applications and APIs etc.	1. Please specify count of unique servers including web,app,DB, networking systems, security devices, Load balancers 2. Please specify count of web applications, thick client apps, thin client apps, android apps,ios apps, APIs.	As per RFP tentative application count is 340 for half yearly VAPT assessment. As such application count will be 680 applications per year.

4	57	Annexure 11 – Project Details & Scope of Work	1. Project Scope Vulnerability Assessment and Penetration Testing should cover the internet facing application, intranet applications and its components including web server, app server, DB Server, Thick client, Thin clients, Mobile applications, Networking systems, Security devices, load balancers, integration with other applications and APIs etc.	2. Please specify is configuration review, database review, firewall rule-based review is part of scope.	No
5	57	List of activities under VAPT	VAPT should be comprehensive but not limited to following activities for the application and related infrastructure under audit	As per our understanding scope of work is limited to conducting application security assessment only and it does not include ATM review, device review, infrastructure VAPT, architecture review, etc. Kindly confirm.	Yes. Application security assessment and its associated infrastructure should be in scope excluding ATM review, device review, architecture review.
6	57	List of activities under VAPT	VAPT should be comprehensive but not limited to following activities for the application and related infrastructure under audit	Kindly specify if there is any vulnerability assessment tool deployed by bank that should be leveraged by bidder for conducting internal Vulnerability assessment.	No tool will be provided by bank. Successful bidder to deploy licensed tool at his own cost as per scope of VAPT RFP.
7	57	Project Scope	The frequency for conducting VAPT should be at half yearly. However, the Bank at its own discretion can change the frequency.	1. Please confirm if 340 applications would be tested twice a year which makes the count as 680 applications per year or a set of 170 applications would be tested per half year.	340 applications have to be tested half yearly. As such application count will be 680 applications per year.

बैंक ऑफ़ बड़ौदा
Bank of Baroda

Bank's Clarification to Pre Bid Queries (GEM/2024/B/5371843 dated 11.09.2024) RFP for Selection of Service Provider for Vulnerability Assessment and Penetration Testing of Bank's Internet facing applications, Intranet applications and its Infrastructure

8	59	Indicative Number of Applications	Indicative Number of Applications	1. Please confirm if total of 680 applications would be tested over a period of 2 years or is 340 overall count of applications for 2 years.	340 applications must be tested half yearly. As such application count will be 680 applications per year.
9	60	Annexure 11 – Project Details & Scope of Work 4. VAPT Phases:	In case of compliance verification, verifying the observations for closure of findings	1. As per our understanding maximum 3 retests are required to verify the closure of issues. However, please confirm	Yes
10	60	Annexure 11 – Project Details & Scope of Work	Addressing the Security Gaps highlighted in VAPT reports.	1. Please specify if remediation is part of scope or will be performed by Bank and bidder's roles is limited to suggesting recommendations.	Remediation recommendation should be provided by successful bidder
11	60	Annexure 11 – Project Details & Scope of Work	Suggest changes/modifications in the Security Policies implemented along with Security Architecture including Network and Applications of the Bank to address the same.	1. Please specify if process review or architecture review is part of scope. 2. Kindly specify what is the expected as part of this activity from the bidder.	NO As per RFP
12	60	4. VAPT Phases:	Chart a roadmap for the Bank to ensure compliance and address these security gaps.	1. Our assumption is that recommendations should be provided in the final report for addressing the security issues. However, please specify if separate roadmap plan needs to be prepared for bank on an annual basis?	Remediation recommendation should be provided by successful bidder in draft report first and should be made part of final report as well.

बैंक ऑफ़ बड़ौदा
Bank of Baroda

Bank's Clarification to Pre Bid Queries (GEM/2024/B/5371843 dated 11.09.2024) RFP for Selection of Service Provider for Vulnerability Assessment and Penetration Testing of Bank's Internet facing applications, Intranet applications and its Infrastructure

13	62	VAPT Report – Detailed Findings/Checklists	The various checklist formats, designed and used for conducting the VAPT activity as per the scope, should also be included in the report separately for Servers (different for different OS), application, Network equipment's, security equipment's etc., so that they provide minimum domain wise baseline security standard /practices to achieve a reasonably secure IT environment for technologies deployed by the Bank.	1. Kindly confirm if minimum baseline security standards are to be created as part of scope. If yes, please specify approx. number of devices	As per RFP tentative application count is 340 for half yearly VAPT assessment.
14	63	Deliverables	Perform compliance verification of closure of findings.	1. Kindly specify what is the expected as part of this activity from the bidder. 2. Please mention the frequency of compliance verification.	Compliance verification of observations as fixed by bank team. Maximum 3 retests are required to verify the closure of issues.
15	62	VAPT Report – In Depth Analysis of findings /Corrective Measures & Recommendations along with Risk Analysis	Separate reports should be provided for international territories. Separate reports should be provided for common infrastructure assets and Applications.	1. Kindly mention what is the format for international territories and with whom these reports would be shared. Please specify if this is bank's overseas regulatory requirement or it is for fulfilling client requirements	Same report format will do and reports should be submitted to bank VAPT team. Yes it is as per RBI and overseas regulatory requirement.
16	65	Details of Infrastructure at Bank's DC/DR	Bank has state of the art Data Centre/DR sites at Mumbai and Hyderabad as per tier 3 standard. DC/DR sites is connected to all the Branches in India, overseas territories,	We understand that resources would be required at Mumbai location. However, if applications are hosted at other sites/DC/DR sites please confirm if travel would be required or remote connectivity would be provided from Mumbai location.	As per RFP

बैंक ऑफ़ बड़ौदा
Bank of Baroda

Bank's Clarification to Pre Bid Queries (GEM/2024/B/5371843 dated 11.09.2024) RFP for Selection of Service Provider for Vulnerability Assessment and Penetration Testing of Bank's Internet facing applications, Intranet applications and its Infrastructure

17	104	Annexure-27: VAPT Tools and certification/Training :	Details of VAPT tools and team members trained/certified on tools	Kindly specify what details are required here and is for which evaluation criteria. Please specify the reference page number of RFP for same. Please specify what documents are required for this as proof	Details of certifications done by VAPT team members, including experience of using various VAPT tools and technologies proposed to be deployed. Refer annexure 27
18	106	Annexure-29: commercial bid format	For applications sharing common platforms, VAPT cost of one application shall be paid @ 100 % of highest applicable effort estimation and subsequent applications shall be paid at 50% of the cost of VAPT, based on efforts estimation (High/Medium/Low) as common infrastructure components will need not be tested again Bank reserves the right to avail any one or more services from the above line items	Please specify what number of applications are sharing common platforms.	Tentative count is 80 applications.
19	76	14. Confidentiality:	14.4 The Service Provider shall return all the Confidential Information that is in its custody, upon termination/expiry of this Agreement.	We please suggest the inclusion of the below language to the client: "Notwithstanding anything to the contrary herein, the Service Provider shall be entitled to retain sufficient copies of the Confidential Information to evidence the work performed by it, as per its internal document archiving policy or as per law." Kindly confirm.	Since the documents are sensitive in nature same may be return to. We may not allow such request

20	82	20. Audit	All Service Provider records with respect to any matters covered by this Agreement shall be made available to auditors and or inspecting officials of the Bank and/or Reserve Bank of India and/or any regulatory authority, at any time during normal business hours, as often as the Bank deems necessary, to audit, examine, and make excerpts or transcripts of all relevant data. Said records are subject to examination. Bank's auditors would execute confidentiality agreement with the Service Provider provided that the auditors would be permitted to submit their findings to the Bank, which would be used by the Bank. The cost of the audit will be borne by the Bank. The scope of such audit would be limited to Service Levels being covered under the contract, and financial information would be excluded from such inspection, which will be subject to the requirements of statutory and regulatory authorities. The Bank and its authorized representatives, including Reserve Bank of India (RBI) or any other regulator shall have the right to visit any of the Service Provider's premises without prior notice to ensure that data provided by the Bank is not misused. The Service Provider shall cooperate with the authorized representative/s of the Bank and shall provide all information/ documents required by the Bank.	We suggest that any audit or inspection performed must be preceded by prior written notice only and that any result of such audit or inspection must be discussed with the Service Provider prior to finalization of the audit report. Kindly confirm.	As audit is sensitive and we clarify in our RFP as suggested that without prior notice is meant to ensure that data should not be compromised or misused at any point of time with respect of services availed by the Bank.
21	57	Annexure 11.1	The bidder should provide minimum 04 onsite resources for the purpose of VAPT at Bank's premises in Mumbai location and 1 dedicated project manager during the contract period.	Apart from Mumbai, will the resources need to travel to any other locations?	Primary location will be Mumbai only and secondary will be as per the requirement of bank.

22	57	Annexure 11.1	Vulnerability Assessment and Penetration Testing should cover the internet facing application, intranet applications and its components including web server, app server, DB Server, Thick client, Thin clients, Mobile applications, Networking systems, Security devices, load balancers, integration with other applications and APIs etc.	Need more clarification on below - 1. Is source code review in scope of activity? If yes, then Number of applications and average lines of code to be reviewed per application 2. Need detailed information on scope for configuration review such as types of assets and counts of assets 3. Need detailed information on scope of Network VAPT such as total count of External/Internal IPs 4. Need scope bifurcation of Application such total count of web, Mobile and API 5. Frequency of Network architecture review activity	As per scope of RFP
23	11	7	Auditor shall have to certify that their Laptops, tools being used are free from malware.	Need more clarification on from client on what is expected here	Auditor shall have to certify that their Laptops, tools being used are free from malware and hardening should be done as per best security practices.
24	11	9. Payment Terms	The SP's fees will be paid in the following manner for VAPT activity which is described in the Commercial Proposal.	Request you to please clarify the Payment terms whether it's quarterly/application based.	As per RFP
25	32				No change. As per RFP

		B. Technical Bid Evaluation(Point 2)	No of schedule commercial banks experience in conducting VA & PT of bank's applications and related infrastructure (Servers, Network devices, Security Devices, Databases) in last 3 years e.g. 2021-22, 2022-23 and 2023-24 For each schedule commercial bank, experience of VAPT assignment (3 Marks per schedule commercial bank) 5 or more banks= 15 marks	Request you to kindly consider different PO's from the same bank.	
26	32	B. Technical Bid Evaluation(Point 4)	Certified and skilled resources available for bank's onsite location i.e. Mumbai on payroll with experience of at least 2 years having Certified on any one or more certifications such as CCE/CEH/GCFE/ CCFE/ OSCP/ ECSA/ CPTE/ CHFI/ LPT/ CPT/ CEPT/ GPEN and CMWAPT Number of Resources ≥30-15 marks ≥20& <30 – 12 marks ≥10 & <20 – 08 marks ≥5 & <10 – 05 marks	Request you to kindly amend: Number of Resources ≥25 -15 marks ≥10 & <25 – 10 marks ≥5 & <10 – 05 marks	No Change. As per RFP
27	33	B. Technical Bid Evaluation(Point 5)	Experience in VA & PT of the Bank's applications - 1mark per application per year for below applications: Mobile Application, Web Application, API Testing, Core Banking solutions (CBS), Swift/XMM, ATM Switch, Global Treasury Application, NEFT-RTGS, Network PT in last 3 years e.g. 2021-22, 2022-23, 2023-24 in Schedule commercial Banks As per Annexure 26 with Documentary Proof of order / contract copy / customer citation	We have signed NDA with the customer hence disclosing the application details is not possible. Request you to kindly consider the PO mentioning VAPT, Web Application , Mobile Application etc without the count of application as banks will be	No change-As per RFP

				having average of 200+ applications.	
28	63	4. VAPT Phases	EFFORT ESTIMATION CRITERIA ON HIGH MEDIUM LOW PARAMETERS	Kindly clarify efforts estimation score is based on man-days or any other criteria.	Effort estimation criteria is based on criticality of application as High, Medium and Low
29	2	Schedule of RFP, A.4	Last Date & Time of Submission of bids: 03:00 PM on 01st October 2024	On GeM Portal, the bid due date of submission is mentioned as 3rd Oct 2024 by 3:00 p.m. so please clarify regarding the bid due date of submission	Refer addendum in Bank website
30	57	Annexure 11, 11.1 (Project Scope)	Selected Bidder required to perform onsite assessment of the assets under the Scope of the RFP and the period of VAPT contract shall be 2 years subject to satisfactory conduct of assignment during 1st year. Bank reserves the right to continue the contract after 1st Year.	In the GeM Tender & RFP , the contract period has been mentioned as 2 years so please clarify whether the selected bidder shall enter into an agreement for a period of 01 year/ 02 years with the bank within one month from the issuance of the Engagement Letter	As per RFP- The period of VAPT contract shall be 2 years subject to satisfactory conduct of assignment during 1st year. Bank reserves the right to continue the contract after 1st Year.
31	57	Annexure 11 – Project Details & Scope of Work	List of activities under VAPT	We request you to please provide the details of Infra like number of Switches, Routers, Laptop/Desktop, etc	340 applications have to be tested half yearly .As such application count will be 680 applications per year.
32	57	Annexure 11 – Project Details & Scope of Work	Number of Application (344)	Please clarify Whether we need to carry out VAPT of 344 Application in a year or 344 Application in two years	340 applications have to be tested half yearly .As such application count will be 680 applications per year.

33	31	B. Technical Bid Evaluation	No of Years' experience in conducting VA & PT of bank's applications and related infrastructure (Servers, Network devices, Security Devices, Databases) in last 3 years e.g. 2021-22, 2022-23 and 2023-24 in Schedule commercial Banks in India	Could you please clarify whether the experience in conducting VAPT should be highlighted specifically for the last three years, or if we should provide the total number of years of experience.	Experience should be highlighted specifically for the last three years. As per RFP
34	57	Annexure 11 – Project Details & Scope of Work	VAPT should be comprehensive but not limited to following activities for the application and related infrastructure under audit: 11. Denial Of Service (DOS) Attacks 12. DDOS Attacks	Please confirm whether a DDoS attack simulation is included in the scope of work.	Yes. DDoS attack simulation is included in the scope of work. As per RFP
35	57	Annexure 11 – Project Details & Scope of Work	VAPT should be comprehensive but not limited to following activities for the application and related infrastructure under audit: 22. Security Device Assessment 23. Network Device Assessment	Please confirm if the scope includes only VAPT for security and network devices, or if configuration and solution reviews are also part of it. If Yes, could you provide the approximate number of security and network devices	Yes. Application security assessment and its associated infrastructure should be in VAPT scope excluding ATM review, device review, architecture review.
36	57	Annexure 11 – Project Details & Scope of Work	VAPT should be comprehensive but not limited to following activities for the application and related infrastructure under audit: 24. Database Assessment	Kindly confirm if database configuration review to be conducted. If yes please provide approx. count of database servers	Yes As per the scope of RFP.

बैंक ऑफ़ बड़ौदा
Bank of Baroda

Bank's Clarification to Pre Bid Queries (GEM/2024/B/5371843 dated 11.09.2024) RFP for Selection of Service Provider for Vulnerability Assessment and Penetration Testing of Bank's Internet facing applications, Intranet applications and its Infrastructure

37	57	Annexure 11 – Project Details & Scope of Work	VAPT should be comprehensive but not limited to following activities for the application and related infrastructure under audit: 21. Server Assessment (OS Security Configuration)	Please confirm if only an OS configuration review will be conducted. If yes, could you provide the approximate number of servers to be included in the scope	Yes As per the scope of RFP.
38	NA	NA	NA	The bank will provide the tools required for conducting the testing or the bidder is expected to bring their own tools.	No tool will be provided by bank. Successful bidder to deploy licensed tool at his own cost as per scope of VAPT RFP.
39	63	Annexure 11 – Project Details & Scope of Work Deliverables	Perform compliance verification of closure of findings.	Could you please confirm the expected number of rounds for revalidation	Compliance verification of observations as fixed by bank team. Maximum 3 retests are required to verify the closure of issues.
40	31	B. Technical Bid Evaluation	No of schedule commercial banks experience in conducting VA & PT of bank's applications and related infrastructure (Servers, Network devices, Security Devices, Databases) in last 3 years e.g. 2021-22, 2022-23 and 2023-24	Request you to modify the clause as: No of schedule commercial banks/BFSI experience in conducting VA & PT of applications and related infrastructure (Servers, Network devices, Security Devices, Databases) in last 3 years e.g. 2021-22, 2022-23 and 2023-24	No change - As per RFP

41	31	B. Technical Bid Evaluation	No of Years' experience in conducting VA & PT of bank's applications and related infrastructure (Servers, Network devices, Security Devices, Databases) in last 3 years e.g. 2021-22, 2022-23 and 2023-24 in Schedule commercial Banks in India	Request you to modify the clause as: No of Years' experience in conducting VA & PT of applications and related infrastructure (Servers, Network devices, Security Devices, Databases) in last 3 years e.g. 2021-22, 2022-23 and 2023-24 in Schedule commercial Banks/BFSI in India	No change - As per RFP
42	NA	NA	NA	Request you to kindly provide an extension of 1 week i.e 8th Oct'24 for submitting RPF Response.	No change - As per RFP
43	Page - 57			As per expected sow statement, are we expected to carry Network Penetration Testing for its components including web server, app server, DB Server and Networks components, Security devices, load balancers as well ? If yes then give us the count	340 applications have to be tested half yearly .As such application count will be 680 applications per year.

44	Page - 57			The frequency for conducting VAPT should be at half yearly. However, the Bank at its own discretion can change the frequency. We need a fixed testing frequency	No change - As per RFP
45	Page - 59			Indicative Number of Applications out of total 340 App kindly provide No.of Web, Mobile, Thick Client and API Applications	340 applications have to be tested half yearly .As such application count will be 680 applications per year.
46	Page - 63			Deliverables a) The Bidder must support for migration of data to proposed tool or as decided by bank before expiry of the contract and provide the declaration that no data of the bank is moved out of the bank. b) The Bidder should provide tool which is compiled with information security standards and other industry practices. Could you explain in detail what as your requirement for this pointer	Please refer RFP as query is not specific to the point
47	Page - 106			Commercial Bid Format. Could you explain in detail what as your requirement for this pointer	Please refer RFP as query is not specific to the point