Replies to pre bid queries for GEM/2025/B/7033018 dated 22/12/2025 for Selection of Cert-In Empaneled Auditor for Conducting Comprehensive Vulnerability Assessment & Penetration Testing (VAPT) for the Half Year March 2026, Secure Configuration Audit & Secure Configuration Document Review and API Security Assessments for FY 2025-26 in Canara Bank

Sl. No.	Page No.	Section/ Annexure/ Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1	61	Annexure-2 Pre-Qualification Criteria	9. The Bidder should have provided at least one VAPT/SCA/ API Security Assessments in the last three years as on the bid submission date to any Central / State Govt Organization / PSU / Public Listed Company/BFSI sector in India.	The bidder has to provide relevant purchase order/ work order / engagement letter along with satisfactory project completion certificate/ Reference letter from the Concerned Organization/Email reference from the client. Kindly note that that Client's Email should be from their official Email IDs only, containing their name, designation & Contact number and duly marking a copy to 'dittenders@canarabank.com'	We request clarification on whether invoice copies issued to the customer, along with the relevant Purchase Order, can be considered as acceptable supporting documents, since the project is currently ongoing and the final completion sign-off is yet to be received.	RFP clause is self explanatory.Bidder to comply with the RFP terms and conditions.
2	12	SECTION B - INTRODUCTION	7.Pre-Qualification Criteria	7.2.The bidder who has successfully completed the VAPT, Secure Configuration Audit & Secure Configuration Document Review and API Assessments in at least one of the previous three procurements in Canara Bank, may be granted an exemption from other pre-qualification criteria subject to satisfactory performance duly considering their proven credentials at the sole discretion of the Bank.	Please confirm whether the exemption applies only to Pre-Qualification criteria or also to Technical Evaluation criteria.	Applicable to Pre-Qualification Criteria only.
3	71	Annexure-9	Scope of Work	1.The objective is to identify and address security gaps, enhance the security posture of the organization, and ensure compliance with regulatory guidelines, including those issued by the Reserve Bank of India (RBI), IT Act 2000/Amendment 2008, and other applicable regulations. The assessment must be conducted by professionals with a minimum of 5 years of relevant experience, and their credentials will be verified.	Will CV and self-declaration be sufficient, or will original certificates / background verification be required for resource validation?	CV, HR declaration to be provided along with copy of certificates, background verification of the resource.
4	11	SECTION B - INTRODUCTION	5.Requirement Details	5.1.Bank invites Proposal/offers in GeM Portal from Cert-in empaneled auditors for conducting Comprehensive Vulnerability Assessment & Penetration Testing (VAPT) for Half-Year March 2026, Secure Configuration Audit & Secure Configuration Document Review and API Assessments for FY 2025-26 as per the Terms & Conditions, Technical Requirements and Scope of Work described elsewhere in this document. This tender consists of requirement as given below:	Will the Bank provide a final and frozen asset list phase-wise prior to commencement of each assessment phase?	Please be guided by Bill of Material (Annexure-15) in RFP which are self explanatory.Bidder to comply with RFP terms and conditions.

Sl. No.	Page No.	Section/ Annexure/ Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
5	11	SECTION B - INTRODUCTION	5.Requirement Details	5.1.Bank invites Proposal/offers in GeM Portal from Cert-in empaneled auditors for conducting Comprehensive Vulnerability Assessment & Penetration Testing (VAPT) for Half-Year March 2026, Secure Configuration Audit & Secure Configuration Document Review and API Assessments for FY 2025-26 as per the Terms & Conditions, Technical Requirements and Scope of Work described elsewhere in this document. This tender consists of requirement as given below:	In case of increase in assets, will payment be released strictly on per-asset unit rate as per the Bill of Material?	Yes, understanding is correct.
6	78	Annexure-9 Scope of Work	13.Scope of work for Penetration Testing/ External Attack Penetration Testing: -	•External attack Penetration Testing should include all the Public Facing Assets of the Bank.	Will the Bank provide an approved public-facing asset inventory to avoid accidental testing of third-party hosted assets?	Yes, details will be shared with successful bidder.
7	89	Annexure-9 Scope of Work	d.Port Scanning-	•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.	Will written approval, defined scope, and testing window be provided prior to conducting any DoS/DDoS testing activities?	Yes, details will be shared with successful bidder.
8	71	Annexure-9 Scope of Work	4.VAPT testing of any assets, applications etc. should contain but not limited to below details.	•Attempt to guess passwords using password-cracking tools.	Will test credentials be provided, or is the auditor expected to perform brute-force attempts on production systems?	Auditor is expected to perform brute-force attempts on Bank provided systems.
9	79	Annexure-9 Scope of Work	c.External Assessment -	•By-pass the Firewall, Web Application Firewall or any security controls	Does firewall/WAF bypass refer to logical rule review or active exploitation attempts during testing?	Bidder has to perform Active exploitation.
10	72	Annexure-9 Scope of Work	4.VAPT testing of any assets, applications etc. should contain but not limited to below details.	· Credentials based VAPT Scanning to identify missing latest patches (n-1).	Will privileged credentials be provided for servers, databases, and APIs to perform authenticated scans?	Yes, details will be shared with successful bidder.
11	79	Annexure-9 Scope of Work	c. External Assessment -	V.No remote access solutions will be provided by the bank under any circumstances	Please confirm the list of locations/cities and working hours during which on-premise testing can be conducted.	The location will be Bangalore and during Bank's working hours.
12	11	5.Requirement Details	5.1.Bank invites Proposal/offers in GeM Portal from Cert-in empaneled auditors for conducting Comprehensive Vulnerability Assessment & Penetration Testing (VAPT) for Half-Year March 2026, Secure Configuration Audit & Secure Configuration Document Review and API Assessments for FY 2025-26 as per the Terms & Conditions, Technical Requirements and Scope of Work described elsewhere in this document. This tender consists of requirement as given below:	4.Engagement of auditor for conducting API Security Assessments for FY 2025-26	Will the Bank provide a detailed API inventory including authentication type, environment, and sensitivity classification?	Yes, details will be shared with successful bidder.
13	85	Annexure-9 Scope of Work	V. Broken Access Control	•Metadata manipulation, such as replaying or tampering a JSON Web Token (JWT) or a cookie or hidden field manipulated to elevate privileges, or abusing JWT invalidation	Will the Bank provide test tokens, token expiry rules, and sample payloads for API security testing?	Yes, test tokens and sample payloads will be provided to the successful bidder.

Sl. No.	Page No.	Section/ Annexure/ Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
14	91	Annexure-9 Scope of Work	(C)SECURE CONFIG DOCUMENT REVIEW & SECURE CONFIG AUDIT FOR YEAR 2025-26	Secure Configuration Document Review:	Please confirm the approximate number of Secure Configuration Documents to be newly created versus reviewed.	Roughly 50 each for reviews and new creations. However no's may change during the period of assessment.
15	92	Annexure-9 Scope of Work	(C)SECURE CONFIG DOCUMENT REVIEW & SECURE CONFIG AUDIT FOR YEAR 2025-26	•Auditor should provide fixing script or files based on SCDs.	Is the execution of fixing scripts the responsibility of the Bank teams, with the auditor only providing recommendations/scripts?	Fixing scripts execution will be done by Bank team. However, bidder has to provide technical support for fixing scripts.
16	90	Annexure-9 Scope of Work	11.Reporting:	•Auditor has to use Bank's GRC (Governance, Risk & Compliance) solution to report, track and update the vulnerability status.	Will access, training, and SOPs for the Bank's GRC tool be provided before commencement of assessments?	Yes, details will be shared with successful bidder.
17	80	Annexure-9 Scope of Work	11.Reporting:	•Auditor should provide reports with sensitive data masked or any other format to any govt agencies such as RBI, NPCI, SEBI etc as when required by bank.	Please confirm the expected report format and turnaround time for submissions to RBI, NPCI, SEBI, or other regulators.	As and when sought by the authorities.
18	13	SECTION B - INTRODUCTION	8.Scope of Work	8.4.The auditor should have pool of at least twenty-five (25) 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.	Please clarify whether the pool of 25 professionals must be on direct payroll or if contractual resources are acceptable.	Yes, Professionals must be on direct payroll.
19	81	Annexure-9 Scope of Work	15.Acceptance of the Report:	17.The bidder should deploy at-least 8 professionals for VAPT for conducting the assessment with relevant qualifications and having a minimum of 5 years of experience in conducting the similar kind of assessment with no extra cost to the Bank. However, bidder should empanel additional resources in case of need to complete the tasks within the prescribed timelines.	Is concurrent deployment of 8 resources mandatory, or is this a peak requirement during the engagement?	Please be guided by Scope of work (Annexure-9) and Technical Evaluation Criteria (Annexure-10) in RFP which are self explanatory.Bidder to comply with RFP terms and conditions
20	91	Annexure-9	Scope of Work	14.The bidder should deploy at-least 4 professionals for conducting the API security assessment with relevant qualifications and having a minimum of 5 years of experience in conducting the similar kind of assessment with no extra cost to the Bank. However, bidder should empanel additional resources in case of need to complete the tasks within the prescribed timelines.	Can the same resources be shared across different assessment phases?	The same resource can be deployed for different phases. However, when the activities are happening parallelly, bidder has to provide different resource for each activity.
21	19	4.Penalties & Liquidated damages		Note: Average number of resources deployed for the assessment period will be considered for arriving at the LD.	Please clarify how the average number of deployed resources will be calculated for the purpose of LD computation.	This scenario is applicable when the bidder deploys additional resources over and above the mandatory resources required on daily basis.

Sl. No.	Page No.	Section/ Annexure/ Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
22	22	SECTION C - DELIVERABLE AND SERVICE LEVEL AGREEMENTS	11.Right to Audit	11.1.The VENDOR has to get itself annually audited by internal/ external empaneled Auditors appointed by the PURCHASER/inspecting official from the Reserve Bank of India or any regulatory authority, covering the risk parameters finalized by the PURCHASER/such auditors in the areas of products (IT hardware/software) and services etc., provided to the PURCHASER and the VENDOR is required to submit such certification by such Auditors to the PURCHASER. The VENDOR and or his/their outsourced agents/subcontractors (if allowed by the PURCHASER) shall facilitate the same. The PURCHASER can make its expert assessment on the efficiency and effectiveness of the security, control, risk management, governance system and process created by the VENDOR. The VENDOR shall, whenever required by the Auditors, furnish all relevant information, records/data to them. All costs for such audit shall be borne by the PURCHASER.	Please clarify the frequency and scope of audits to be conducted on the selected bidder during the contract period	Bidder to comply with RFP terms and conditions
23			General Query	Scope Related	Kindly confirm whether the VAPT scope includes both internal and external infrastructure testing, or only internet-facing assets.	It covers internal, public facing and cloud assets
24			General Query	Scope Related	Please clarify whether cloud-hosted assets (AWS/Azure/GCP) are included in the scope. If yes, specify whether configuration review of cloud services is also required.	Yes, cloud-hosted assets (AWS/Azure/GCP etc.,) are included in the scope. Also, configuration review of cloud services is also included.
25			General Query	Scope Related	For web applications, kindly confirm: Number of applications Technology stack Whether source code review is in scope Environment type (Production / UAT)	Please be guided by Bill of Material (Annexure-15) in RFP which are self explanatory. Source code review is not in scope.
26			General Query	Scope Related	For mobile application security testing, please clarify: Number of Android and iOS applications Whether testing is to be performed on production or test builds Whether source code review is in scope	Detailed breakup will be shared with successful bidder. Testing to be performed on production/test builds as shared by the Bank. Source code review is not in scope.

Sl. No.	Page No.	Section/ Annexure/ Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
27			General Query	Scope Related	For API Kindly confirm whether API security testing is mandatory for all applications or only for identified APIs. What is the API count? REST or SOAP API?	Detailed breakup will be shared with successful bidder. API details also will be shared with the bidder.
28			General Query	Scope Related	Please clarify whether ATM VAPT is applicable to: Physical ATMs ATM switch / middleware Both	ATM VAPT is applicable to Physical ATMs only.
29			General Query	Scope Related	Is external attack surface testing limited to Bank-owned assets only, or does it include third-party hosted services?	External attack surface testing is limited to Bank-owned assets only
30			General Query	Scope Related	Kindly confirm whether secure configuration review is required for: OS Databases Network devices Security devices Cloud configurations	Please be guided by Bill of Material (Annexure-15) in RFP which are self explanatory. Bidder to comply with RFP terms and conditions.
31			General Query	Scope Related	Please clarify whether social engineering / phishing simulations are part of the VAPT scope.	Social engineering / phishing simulations are not part of the VAPT scope.
32			General Query	Access-Related	Kindly confirm whether the Bank will provide written authorization / approval letter prior to commencement of VAPT activities.	Mail request will be sent
33			General Query	Access-Related	Will the Bank provide test credentials (white-box testing) for applications, APIs, and servers?	Bank will insist on credential based testing (white-box testing) only. In cases where it is not feasible Blackbox to be conducted which will be intimated by the Bank team during the audit.
			General Query		If not, should the assessment be treated as black-box only?	
34			General Query	Access-Related	Kindly confirm whether IP whitelisting will be required for assessment tools.	Details will be provided to successful bidder. All tools must be deployed in bank premises only to conduct VAPT on internal asset. For external facing there is no IP whitelisting is required.
35			General Query	Access-Related	For on-site activities, kindly confirm: Location Duration Access requirements	The on-site activity location will be Bangalore.

Sl. No.	Page No.	Section/ Annexure/ Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
36			General Query	Execution	Kindly clarify the testing window (business hours / non-business hours).	The testing window will be mostly Banking working hours
37			General Query	Execution	Please confirm whether non-intrusive testing only is expected, or if controlled exploitation is permitted.	Both non-intrusive testing and controlled exploitation testing is expected.
38			General Query	Execution	Is Denial-of-Service (DoS) testing explicitly excluded from scope?	Denial-of-Service (DoS) testing is part of the scope. Please refer (Annexure-9)Scope of work page no 71, 78, 79 etc of the RFP
39			General Query	Execution	Please clarify whether re-testing / re-validation post remediation is included in the scope and number of cycles expected.	Please be guided by project timelines in RFP which are self explanatory.
40			General Query	Reporting & Compliance	Will reports need to be uploaded to a GRC / portal? If yes, kindly share the platform details.	Yes, Details will be shared with the successful bidder
41			General Query	Reporting & Compliance	Please clarify whether digitally signed compliance letters are mandatory.	Yes, digitally signed compliance letters are mandatory.
42			General Query	Reporting & Compliance	Is there a requirement to submit masked or redacted reports for regulatory purposes?	Yes, based on requirement
43			General Query	Tool	Are there any mandatory tool restrictions or approvals to be followed during execution?	For infrastructure scanning, Bank will provide Tenable SC+ and bidder to use the same for testing. For all other requirements, bidder to arrange appropriate licensed tools to be installed in bank premise. Refer to "Sec G --> 2.Roles & Responsibility during Project Implementation"
44			General Query	Timeline	Kindly confirm the expected timeline for completion of VAPT post issuance of work order.	Please be guided by project timelines in RFP which are self explanatory. Bidder to comply with RFP terms and conditions
45			General Query	Timeline	Please clarify whether the scope is one-time or recurring (quarterly / annual) during the contract period.	It is a one time activity.

Sl. No.	Page No.	Section/ Annexure/ Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
46	16	SECTION C - DELIVERABLE AND SERVICE LEVEL AGREEMENTS	3.Payment Terms	Phase-1 - Initial Scanning: Completion of VAPT for assets of the bank along with submission of reports - 70% of the eligible amount per asset based on actual no of assets assessed in Phase 1. Phase-2 - Revalidation Scanning: Completion of verification scan and Clean reports for all the Assets - 30% of the eligible amount per asset based on actual no. of assets revalidated in Phase 2.	Please considering the relaxation for the Payment terms as "85% of the eligible amount per asset based on actual no of assets assessed in Phase 1" "15% of the eligible amount per asset based on actual no. of assets revalidated in Phase 2"	Bidder to comply with RFP terms and conditions.
47	60	Annexure-2 Pre-Qualification Criteria	S. no. 6	The Bidder should be CERT-IN empaneled security Auditor as on date of RFP bid submission with at-least 3 years (i.e., 2022-23, 2023-24 and 2024-25) continuous empanelment by CERT-IN without any de-empanelment.	We are CERT-IN empaneled, and have been active service provider for businesses related to security for more than two decades. However, our empanelment has been completed recently. We hence request the bank to modify the clause as below: The Bidder should be CERT-IN empaneled security Auditor as on date of RFP bid submission with at-least 3 years (i.e., 2022-23, 2023-24 and 2024-25) of business experience in security domain.	Bidder to comply with RFP terms and conditions.
48	62	Annexure-2 Pre-Qualification Criteria	S. no. 13	The bidder should not be a vendor/supplier for Software and Hardware components of the Bank	We are existing vendors to Canara Bank for multiple hardware and software solutions. However, we have a separate team that takes care of VAPT audits and there will not be any conflict of interest. Hence, we request bank to remove this clause.	Bidder to comply with RFP terms and conditions.
49	94	Annexure-10 Technical Evaluation Criteria	S. no. 3	The bidder should not be involved in implementing Security solutions and network infrastructure of the Canara Bank at Data Center, Treasury and DRC level.	We are existing vendors to Canara Bank for multiple hardware and software solutions. However, we have a separate team that takes care of VAPT audits and there will not be any conflict of interest. Hence, we request bank to remove this clause.	Bidder to comply with RFP terms and conditions.

Sl. No.	Page No.	Section/ Annexure/ Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
50	19	4. Penalties & Liquidated damages	If the VAPT Assessments are not completed within the Phase wise timelines as per clause no.1.4 of section C, Bank will impose penalty @0.50% (In case number of professionals/resources are deployed as per the scope of work) or @0.70% (In case number of professionals /resources are not deployed as per the scope of work) per week delay and part thereof on the total cost mentioned in Table A of Annexure 15 (Bill of Material) of the Assessment for each phase. However, the total Penalty/LD to be recovered shall be restricted to 10% of total cost mentioned in Table A of Annexure 15(Bill of Material). Note: Average number of resources deployed for the assessment period will be considered for arriving at the LD.	4.1.	We assume that Bank will provide all 6340 nos.of asset for VAPT in the beginning only within 3 days of start of work. Because if we deploy 8 resources and all assets are not provided then our resources will remain idle and it will be a huge financial loss to our organization. We kindly request you to impose only one penalty on LD on executed value of work, not based on the manpower counts.	Bidder to comply with RFP terms and conditions.
51	19	4. Penalties & Liquidated damages	4.2. If Secure Configuration Review and Audit is not completed within the timelines mentioned as per clause no.1.5 of section C, then for each asset assessment Bank will impose penalty @ 0.50% (In case number of professionals/resources are deployed as per the scope of work) or @0.70% (In case number of professionals/resources are not deployed as per the scope of work)per week delay and part thereof on the total cost of per asset assessment as per Table B of Annexure 15 (Bill of Material) of the Assessment. However, the total Penalty/LD to be recovered shall be restricted to 10% of total cost of the Table B of Annexure 15 (Bill of Material) Note: Average number of resources deployed for the assessment period will be considered for arriving at the LD.	4.2	We assume that Bank will provide all 100 nos.of documents for Secure Configuration Review and 7765 nos. of assets for conducting Secure Configuration Audit in the beginning only within 3 days of start of work. Because if we deploy 6 resources and all assets are not provided then our resources will remain idle and it will be a huge financial loss to our organization. We kindly request you to impose only one penalty on LD on executed value of work, not based on the manpower counts.	Bidder to comply with RFP terms and conditions.

Sl. No.	Page No.	Section/ Annexure/ Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
52	19	4. Penalties & Liquidated damages	4.3. If API Security Assessment is not completed within the timelines mentioned as per clause no.1.6 of section C, then for each asset assessment Bank will impose penalty @ 0.50% (In case number of professionals/resources are deployed as per the scope of work) or @0.70% (In case number of professionals/resources are not deployed as per the scope of work)per week delay and part thereof on the total cost of per asset assessment as per Table C of Annexure 15 (Bill of Material) of the Assessment. However, the total Penalty/LD to be recovered shall be restricted to 10% of total cost of the Table C of Annexure 15 (Bill of Material). Note: Average number of resources deployed for the assessment period will be considered for arriving at the LD.	4.3	We assume that Bank will provide all 2000 nos. of APIs for security assessments in the beginning only within 3 days of start of work. Because if we deploy 4 resources and all API's are not provided then our resources will remain idle and it will be a huge financial loss to our organization. We kindly request you to impose only one penalty on LD on executed value of work, not based on the manpower counts.	Bidder to comply with RFP terms and conditions.
53	94	Annexure 10	Technical Evaluation Criteria S.No.1	The bidder should deploy at-least 8 professionals for VAPT, 6 professionals for SCD review and Audit, 4 professionals for conducting API security assessment with relevant qualifications and having a minimum of 5 years of experience in conducting the similar kind of assessment. However, bidder should empanel additional resources in case of need to complete the tasks within the prescribed timelines.	The bidder should deploy at-least 8 professionals for VAPT, 6 professionals for SCD review and Audit, 4 professionals for conducting API security assessment with relevant qualifications and having a minimum of 3 years of experience in conducting the similar kind of assessment. However, bidder should empanel additional resources in case of need to complete the tasks within the prescribed timelines.	Bidder to comply with RFP terms and conditions.
54	61	Annexure 2	Pre-Qualification Criteria S.No.6	The Bidder should be CERT-In empanelled Security Auditor as on date of RFP bid submission with at least 3 years (i.e., 2022-23, 2023-24 and 2024-25) continuous empanelment by CERT-In without any deempanelment	We are empanelled with CERT-In since October 2023 and continue to be empanelled as on date. Kindly clarify whether bidders empanelled during FY 2023-24, without any deempanelment, are eligible to qualify for this criterion.	Bidder to comply with RFP terms and conditions.

Sl. No.	Page No.	Section/ Annexure/ Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
55	96	Annexure 10	Technical Evaluation Criteria S.No.2	The firm should have a pool of at least 25 professionals with active international accreditations (CISA/CISM/CISSP/OSCP/ECSA/EJPT/CPENT/LPT/CEH) and minimum 5 years postqualification experience	We are an MSME/start-up organization with a pool of 20 certified professionals, some of whom have less than 5 years of post-qualification experience. Kindly clarify whether relaxation is applicable for MSME/start-up bidders for this criterion.	Bidder to comply with RFP terms and conditions.
56	101	Annexure 15	Bill of Material	Tentative number of Web Applications - 600	Kindly clarify whether there is any size or complexity definition (e.g., small/medium/large applications, lines of code, modules, user base) for the stated 600 web applications.	Details will be shared with successful bidder.
57	102	Annexure 15	Bill of Material Table C - API Security Assessment	Tentative number of assets - 2000	Kindly clarify whether the mentioned 2000 assets refer to distinct APIs or individual API endpoints under the APIs.	Mentioned 2000 assets refer to distinct APIs .
58	94	Annexure 10	Technical Evaluation Criteria S.No.2	The firm should have a pool of at least 25 professionals with active international accreditation like CISA (Certified Information Systems Auditor)/CISM/ CISSP (Certified Information Security Professional)/ OSCP/ ECSA/ EJPT/ CPENT/ LPT/ 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 modify this clause as follows: The firm should have a pool of at least 15 professionals with active international accreditation like CISA (Certified Information Systems Auditor)/CISM/ CISSP (Certified Information Security Professional)/ OSCP/ ECSA/ EJPT/ CPENT/ LPT/ CEH/ ISO 27001 LA trained lead auditors employed with them.	Bidder to comply with RFP terms and conditions.
59	14	SECTION C - DELIVERABLE AND SERVICE LEVEL AGREEMENTS	1. Project Timeline	1.4 Timelines for Conducting Comprehensive Vulnerability Assessment & Penetration Testing (VAPT)	Kindly confirm whether parallel execution of activities across applications/modules is permitted in order to meet the overall project timelines.	Yes, parallel execution of activities across applications is permitted.
60	91	Annexure 9 - Scope of Work	(C) SECURE CONFIG DOCUMENT REVIEW & SECURE CONFIG AUDIT FOR YEAR 2025-26	Secure Configuration Audit should be conducted as per Bank Approved Secure Configuration Documents by using relevant nessus scripts	Kindly confirm whether vulnerability scanners other than Nessus are acceptable, provided they are industry-standard and produce equivalent or superior results.	For infrastructure scanning, Bank will provide Tenable SC+ and bidder to use the same for testing. For all other requirements, bidder to arrange appropriate licensed tools to be installed in bank premise. Refer to "Sec G --> 2.Roles & Responsibility during Project Implementation"

Sl. No.	Page No.	Section/ Annexure/ Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
61	81	SECTION C - DELIVERABLE AND SERVICE LEVEL AGREEMENTS	(B) Scope of Work for API Functionality And Information security review 2025-26	4. API Security Assessment/VAPT testing of any API should contain but not limited to below details.	Kindly confirm the definition of Bank dependency that qualifies for timeline extension, including examples of dependencies that would be considered valid.	The delay referred to specific cases like delay in remediation by Bank, delay in providing assets, infrastructure etc., due to any unforeseen circumstances.
62	16	SECTION C - DELIVERABLE AND SERVICE LEVEL AGREEMENTS	3. Payment Terms	% Of Payment to be released	Kindly confirm whether payments are linked to the submission of assessment deliverables or only upon formal acceptance/sign-off by the Bank.	Payments are linked to submission of Final report acceptance to the Bank.
63	17	SECTION C - DELIVERABLE AND SERVICE LEVEL AGREEMENTS	3. Payment Terms	Payment schedule for Conducting Secure Configuration Document Review & Audit on successful Assessment of Domains in each Phase:	Kindly confirm whether payments are processed per completed SCD/application/module or only after completion of the entire scope of work.	Please be guided by Payment Terms in RFP which are self explanatory. Bidder to comply with RFP terms and conditions.
64	14	SECTION C - DELIVERABLE AND SERVICE LEVEL AGREEMENTS	1. Project Timeline	1.4 Timelines for Conducting Comprehensive Vulnerability Assessment & Penetration Testing (VAPT)	Kindly confirm whether access for revalidation activities will be guaranteed by the Bank within a three-month window from initial submission of findings.	Please be guided by project timelines in RFP which are self explanatory. Bidder to comply with RFP terms and conditions
65	15	SECTION C - DELIVERABLE AND SERVICE LEVEL AGREEMENTS	1. Project Timeline	1.4 Timelines for Conducting Comprehensive Vulnerability Assessment & Penetration Testing (VAPT)	Kindly confirm whether access for revalidation activities will alternatively be guaranteed within a two-month window, if applicable, and which timeline will be contractually binding.	Please be guided by project timelines in RFP which are self explanatory. Bidder to comply with RFP terms and conditions.
66	16	SECTION C - DELIVERABLE AND SERVICE LEVEL AGREEMENTS	1. Project Timeline	1.4 Timelines for Conducting Comprehensive Vulnerability Assessment & Penetration Testing (VAPT)	Kindly confirm the defined execution window for security testing activities, including any traffic thresholds, rate-limiting, or caps that must be adhered to during testing.	Details will be shared with successful bidder.
67	71	Annexure 9 - Scope of Work	(A) Scope of Work for Comprehensive Vulnerability Assessment and Penetration Testing for half-year March 2025-26	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.	Kindly confirm the defined execution window for security testing activities, including any traffic thresholds, rate-limiting, or caps that must be adhered to during testing.	Details will be shared with successful bidder.

Sl. No.	Page No.	Section/ Annexure/ Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
68	72	Annexure 9 - Scope of Work	(A) Scope of Work for Comprehensive Vulnerability Assessment and Penetration Testing for half-year March 2025-26	Mobile Application security testing should cover the latest OWASP Top 10 vulnerabilities	Kindly confirm the mobile platforms in scope (Android and/or iOS) and the application distribution method (public app store, enterprise distribution, APK/IPA sharing, etc.).	Mobile platforms both Android and iOS are in scope of assessment. Further Details will be shared with successful bidder.
69	99	Annexure-15 - Bill of Materials	Table A - Cost for VAPT Assessment for the half year March 2026	Cloud Assets	Kindly confirm the scope definition for cloud assets and containerized environments, including whether it covers cloud infrastructure, managed services, Kubernetes, container images, and runtime configurations.	Details will be shared with the successful bidder
70	72	Annexure 9 - Scope of Work	(A) Scope of Work for Comprehensive Vulnerability Assessment and Penetration Testing for half-year March 2025-26	Malware attacks on the ATMS, PT for ATM on random basis based on regulatory guidelines (Bank will select the 10 ATMs on which VAPT need to be done).	Kindly confirm whether the 10 ATMs identified for VAPT are Windows-based or Linux-based, whether access to a dedicated test or cloned ATM environment will be provided, and the ATM types along with the corresponding access requirements.	Identified ATMs are Windows-based ATMs. Access modalities will be shared with the successful bidder
71	122	Appendix-G - Draft Contract Agreement	23. Service levels	23.2 In relation to any undertaking and under any circumstances, the service provider shall exercise the degree of skill, diligence, prudence, and foresight that would reasonably be expected from a highly skilled and experienced professional engaged in the same type of undertaking under similar circumstances. Further the vendor/service provider shall identify and designate skilled personnel necessary for the operation of critical functions under this agreement. Such personnel shall be considered essential and must be available to work on-site during exigencies including but not limited to emergencies and pandemics. The service provider shall provide the bank with a list of these essential personnel and any associated backup arrangements and ensure their availability as required.	Please confirm whether all the applications will be provided in single location or multiple locations	The base location for the project execution will be Bangalore.

Sl. No.	Page No.	Section/ Annexure/ Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
72	14	SECTION C - DELIVERABLE AND SERVICE LEVEL AGREEMENTS	1. Project Timeline	1.4 Timelines for Conducting Comprehensive Vulnerability Assessment & Penetration Testing (VAPT)	Incase in second phase the vulnerabilities are found found so do we need to perform another round of audit. please confirm us the frequency of audit	Please be guided by project timelines in RFP which are self explanatory. Bidder to comply with RFP terms and conditions.
73	78	Annexure 9 - Scope of Work	(A) Scope of Work for Comprehensive Vulnerability Assessment and Penetration Testing for half-year March 2025-26	Appropriate updated commercial tools (e.g., Appscan, Nessus, Accunetix, Burp suite, Qualys etc. and other duly tested tools/ techniques) should be used for each phase of the test to increase the efficiency effectiveness of audit. The auditor is to ensure that only licensed/proprietary audit tools are used for carrying out all the audit activities. The use of freeware/shareware shall be avoided and auditor shall inform the details of audit tools in advance.	Kindly confirm whether licenses for tools such as AppScan, Nessus, BurpSuite, etc. will be provided by the Bank or are to be arranged by the vendor. Also, please clarify whether the Bank mandates the use of specific tools or if equivalent commercial tools with similar capabilities are acceptable.	For infrastructure scanning, Bank will provide Tenable SC+ and bidder to use the same for testing. For all other requirements, bidder to arrange appropriate licensed tools to be installed in bank premise. Refer to "Sec G --> 2.Roles & Responsibility during Project Implementation"
74	81	Annexure 9 - Scope of Work	(A) Scope of Work for Comprehensive Vulnerability Assessment and Penetration Testing for half-year March 2025-27	17. The bidder should deploy at-least 8 professionals for VAPT for conducting the assessment with relevant qualifications and having a minimum of 5 years of experience in conducting the similar kind of assessment with no extra cost to the Bank. However, bidder should empanel additional resources in case of need to complete the tasks within the prescribed timelines.	Kindly confirm the deployment duration per assessment, given that a minimum of 8 professionals is requested, and also clarify whether the deployment is required to be full-time onsite or partially remote, specifying the same module-wise	Please be guided by project timelines in RFP which are self explanatory . The requirement is full time, On-site deployment.
75			General Query	Infrastructure VAPT	Total number of servers in scope Server classification: Windows servers - count Linux/Unix servers - count Number of Public facing servers Number of Internal Servers Number of Network and Security Devices in Scope; - Firewall - Routers - Switches - Load Balancers - WAF - IDS/IPS	Please be guided by Bill of Material (Annexure-15) in RFP which are self explanatory. Additional Details will be shared with successful bidder.

Sl. No.	Page No.	Section/ Annexure/ Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
76			General Query	Web Application Penetration Testing	Total number of in-scope web applications for VAPT Please provide a list of web applications along with: - Number of Dynamic pages and user roles per application Are source code reviews expected, if yes then the number of applications in source code review and number of lines of code with each application	Please be guided by Bill of Material (Annexure-15) in RFP which are self explanatory. Additional Details will be shared with successful bidder.
77			General Query	Mobile Application Penetration Testing	Total number of mobile applications in scope. Number of Android Applications in scope and number of screens per application and user roles with each application Number of iOS Applications in scope and number of screens per application and user roles with each application	Please be guided by Bill of Material (Annexure-15) in RFP which are self explanatory. Additional Details will be shared with successful bidder.
78			General Query	API Security Assessment	Total number of APIs in scope for security testing.	Please be guided by Bill of Material (Annexure-15) in RFP which are self explanatory. Additional Details will be shared with successful bidder.
79			General Query	ATM Penetration Testing	10 ATMs will be selected by the Bank (as per scope)?	Yes, understanding is correct.
80			General Query	Secure Configuration Document Review	What asset categories are in scope for Secure Configuration Document (SCD) review (OS, database, middleware, network, security, cloud)? number of distinct platforms and versions under each in-scope asset category How many Secure Configuration Documents are already available for review? And how many new documents to be created?	Please be guided by Bill of Material (Annexure-15 in RFP which are self explanatory. Additional details will be shared with the successful bidder
81			General Query	Secure Configuration Audit	total number of assets in scope for Secure Configuration Audit?	Please be guided by Bill of Material (Annexure-15) in RFP which are self explanatory.Bidder to comply with RFP terms and conditions.
82			General Query	Additional	Is all the activity to be conducted onsite or offsite? If onsite, what will be the location what is the number of retest needed	The base location for the project execution will be Bangalore.

Date: 06/01/2026
Place: Bengaluru

Deputy General Manager