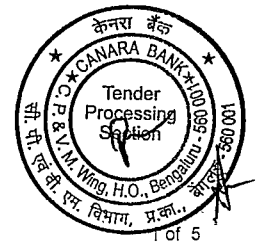
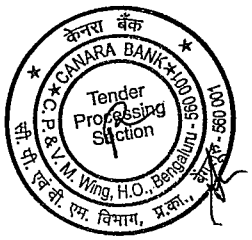
Replies to Pre bid Queries for GeM Bid ref. no: GEM/2024/B/5647828 dated 26/11/2024 for Engagement of Cert-In Empaneled Auditor for Conducting Pre-Go Live Assessments for period of One Year in Canara Bank						
Sl. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Reply
1	58	Annexure-2 Pre-Qualification Criteria	Sl. No: 13	Criteria: The bidder should not be a vendor/supplier for Software and Hardware components of the Bank Documents to be submitted for Compliance: Self-declaration on Letterhead to be submitted for the same.	Request to allow System Integrators (who are not direct suppliers/OEMs) to participate in this RFP.	Bidder to comply with RFP terms and conditions.
2	13	Section -C -Deliverables and Service Level Agreements	1. Project Timelines	1.4 The entire scope is classified in phases with timelines for each phase defined in the tables below: Timelines for Conducting Pre-Go-Live Assessments.	Request to consider the timeline for complex applications to be reduced to 5 days.	Bidder to comply with RFP terms and conditions.
3	66	Annexure 9 Scope of work	Annexure-I and Annexure- II Scope of Work- (Web Application & Mobile Application Testing)	III. VAPT testing of any assets, Applications etc. should contains but not limited to below details.	Do you want network assets, servers, and databases assessed only from the attacker's perspective, or will configuration files for review also be provided?	Bidder to refer Bill of Material for Assessments in Scope
4	66	Annexure 9 Scope of work	Annexure-I and Annexure- II Scope of Work- (Web Application & Mobile Application Testing)	III. VAPT testing of any assets, Applications etc. should contains but not limited to below details.	Please provide the number of devices for configuration review.	Secure configuration of server, network devices are not in scope.
5	66	Annexure 9 Scope of work	Annexure-I and Annexure- II Scope of Work- (Web Application & Mobile Application Testing)	III. VAPT testing of any assets, Applications etc. should contains but not limited to below details. Internal	Are the servers self-hosted or hosted elsewhere?	Details will be shared with the successful bidder while doing the assessments
6	66	Annexure 9 Scope of work	Annexure-I and Annexure- II Scope of Work- (Web Application & Mobile Application Testing)	III. VAPT testing of any assets, Applications etc. should contains but not limited to below details.	Are all in-scope systems (servers and databases) available from a single network segment?	Secure configuration Audit of server, network devices are not in scope.
7	66	Annexure 9 Scope of work	Annexure-I and Annexure- II Scope of Work- (Web Application & Mobile Application Testing)	III. VAPT testing of any assets, Applications etc. should contains but not limited to below details.	Please share the number of external and internal IP addresses in the scope of the network VAPT assessment.	Details of asset will be shared with the successful bidder.



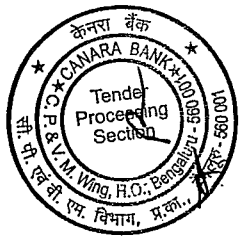
8	66	Annexure 9 Scope of work	Annexure-I and Annexure- II Scope of Work- (Web Application & Mobile Application Testing)	III. VAPT testing of any assets, Applications etc. should contains but not limited to below details.	Is credentialed vulnerability scanning of the servers required?	Yes
9	67	Annexure 9 Scope of work	Annexure-I and Annexure- II Scope of Work- (Web Application & Mobile Application Testing)	IV. Web Application Security Testing should cover the following or LATEST –OWASP Top 10 Web Application Security Risks which are illustrative but not exhaustive.	Are there applications hosted by a third party (e.g., AWS, Azure)? Is cloud testing in scope?	Details of asset will be shared with the successful bidder.
10	67	Annexure 9 Scope of work	Annexure-I and Annexure- II Scope of Work- (Web Application & Mobile Application Testing)	IV. Web Application Security Testing should cover the following or LATEST –OWASP Top 10 Web Application Security Risks which are illustrative but not exhaustive.	Approximately how many dynamic pages (or functionalities) exist per user role in the web applications?	Details of asset will be shared with the successful bidder.
11	67	Annexure 9 Scope of work	Annexure-I and Annexure- II Scope of Work- (Web Application & Mobile Application Testing)	IV. Web Application Security Testing should cover the following or LATEST –OWASP Top 10 Web Application Security Risks which are illustrative but not exhaustive.	Are the applications internet-facing or internal? Is a thick client in scope?	RFP clause is self explanatory. Bidder to refer RFP terms and conditions
12	67	Annexure 9 Scope of work	Annexure-I and Annexure- II Scope of Work- (Web Application & Mobile Application Testing)	VII. OWASP Top 10 vulnerabilities (Mobile applications): - Penetration testing to be conducted for mobile applications a. Mobile applications should be tested for vulnerabilities OWASP - Mobile Applications Verification Standards (MASVS).	Kindly share the approximate size of the in-scope applications: Small (0-50 pages), Medium (50-100 pages), Large (100-250 pages), Very Large (250+ pages).	Mostly Small and Medium Size Application. It may vary based on requirements
13	67	Annexure 9 Scope of work	Annexure-I and Annexure- II Scope of Work- (Web Application & Mobile Application Testing)	VII. OWASP Top 10 vulnerabilities (Mobile applications): - Penetration testing to be conducted for mobile applications a. Mobile applications should be tested for vulnerabilities OWASP - Mobile Applications Verification Standards (MASVS).	Which platforms are in scope: iOS or Android? Please share the count.	Yes, Both Platform are in scope. Details of asset will be shared with the successful bidder.
14	67	Annexure 9 Scope of work	Annexure-I and Annexure- II Scope of Work- (Web Application & Mobile Application Testing)	VII. OWASP Top 10 vulnerabilities (Mobile applications): - Penetration testing to be conducted for mobile applications	What specific components of ATM are in scope?	ATMs are not part of Scope

केनरा बैंक CANARA BANK Tender Processing Section C.P.&V.M. Wing, H.O., Bengaluru-560 005 सी.पी. एवं वी. एम. विभाग, प्र.का., बेंगलूरु-560 005

15	67	Annexure 9 Scope of work	Annexure-I and Annexure- II Scope of Work- (Web Application & Mobile Application Testing)	VII. OWASP Top 10 vulnerabilities (Mobile applications): - Penetration testing to be conducted for mobile applications	What is the approximate number of API endpoints? Will APIs be separate or integrated with the web application?	Details of asset will be shared with the successful bidder.
16	68	Annexure-9	Scope of Work	VII. OWASP Top 10 vulnerabilities (Mobile applications): - Penetration testing to be conducted for mobile applications b. Mobile applications should be tested for vulnerabilities as per the OWASP Mobile applications testing guide and OWASP Mobile Applications Reverse Engineering Prevention Project.	Will brute forcing the application be in scope?	Yes, Auditors have to inform Bank Team Before initiatation.
17	69	Annexure-9	Scope of Work	VIII. Scope of work for Penetration Testing/ External Attack Penetration Testing: c) External Assessment - Test at the minimum should cover but not limited to To expose security gaps and demonstrate the effectiveness or ineffectiveness of security measures. The security assessment should be done by skilled and experienced professionals only (Minimum 3 years of Experience, which will be verified). 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.	Will the bank provide laptops for auditors during the testing process? Auditor firm laptops are not allowed in banks.	No Laptop/ External Devices are allowed in Bank's Intranet.
18	69-70	Annexure 9 Scope of work	Annexure-I and Annexure- II Scope of Work- (Web Application & Mobile Application Testing)	Reporting	How many retest iterations will be included without additional cost?	Auditor have to conduct the verification scan until clean reports.
19	67	Annexure 9 Scope of work	Annexure-I and Annexure- II Scope of Work- (Web Application & Mobile Application Testing)	VIII. Scope of work for Penetration Testing/ External Attack Penetration Testing: b. Tests for Vulnerabilities that can be exploited:	Will commercial tool licenses be provided by the bank?	No, Bidder have to come with their own licenses



20	75	Annexure-10 Technical Evaluation Criteria	Sl. No: 1	Criteria: The bidder should deploy at-least 5 professionals on site, if required for conducting the assessment on Bank's request with relevant qualifications and having a minimum of 5 years of experience (Post qualification) in conducting the similar kind of assessment. Documents to be submitted for Compliance: Letter from HR of the company for acceptance of this clause.	Should all five resources be stationed at the Bangalore branch, or will they need to travel to a specific location?	Bangalore. If requirement asrise, Auditor have to conduct the assessment from any other locations as well.
21	66	Annexure 9 Scope of work	Annexure-I and Annexure- II Scope of Work- (Web Application & Mobile Application Testing)	III. VAPT testing of any assets, Applications etc. should contains but not limited to below details.	Are there specific timelines or milestones for script delivery, assessments, and final report submissions?	RFP clause is self explanatory. Bidder to refer RFP terms and conditions
22	66	Annexure 9 Scope of work	Annexure-I and Annexure- II Scope of Work- (Web Application & Mobile Application Testing)	II. 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.	Are additional compliance standards/frameworks (besides RBI guidelines and IT Act 2000/Amendment 2008) applicable?	Bidder should follow guidelines published by regulator/industry standards from time to time.
23	67	Annexure 9 Scope of work	Annexure-I and Annexure- II Scope of Work- (Web Application & Mobile Application Testing)	VIII. Scope of work for Penetration Testing/ External Attack Penetration Testing: b. Tests for Vulnerabilities that can be exploited:	How do you prioritize audit report findings (e.g., critical, high, medium, low)?	Critical, High, Medium, Low



24	68-69	Annexure 9 Scope of work	Annexure-I and Annexure- II Scope of Work- (Web Application & Mobile Application Testing)	VIII. Scope of work for Penetration Testing/ External Attack Penetration Testing: c) External Assessment - Test at the minimum should cover but not limited to To expose security gaps and demonstrate the effectiveness or ineffectiveness of security measures. The security assessment should be done by skilled and experienced professionals only (Minimum 3 years of Experience, which will be verified). 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.	Will the audit cause downtime or business disruption, or can it be conducted with minimal impact?	Bank will provide specific instruction for conducting the Assessments to selected Bidder
25	69-70	Annexure 9 Scope of work	Annexure-I and Annexure- II Scope of Work- (Web Application & Mobile Application Testing)	Reporting	Should reports on the vendor's letterhead include certification details beyond CERT-IN empanelment information?	No, if requirement arises, Bank will intimate to Auditor.
26	69-70	Annexure 9 Scope of work	Annexure-I and Annexure- II Scope of Work- (Web Application & Mobile Application Testing)	Reporting	Should the auditor document tools/processes used to identify and remove false positives?	Yes
27	69-70	Annexure 9 Scope of work	Annexure-I and Annexure- II Scope of Work- (Web Application & Mobile Application Testing)	Reporting	What is the process/timeline for resubmitting reports if inconsistencies/issues are identified by the bank?	Penalties will be applicable as per RFP Terms.

Date: 11/12/2024
Place: Bengaluru

Deputy General Manager

केनरा बैंक CANARA BANK C.P.&V.M. Wing, H.O., Bengaluru - 560 001 Tender Processing Section सी. पी. एवं वी. एम. विभाग, प्र.का., बेंगलूरु - 560 001