Pre Bid Replies GEM/2024/B/5637293 dated 22/11/2024 for Selection of Cert-In empaneled Auditor for conducting security assessments for the financial year 2024-25 in Canara Bank.						
Sl. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1	60	Annexure-2	Pre-Qualification Criteria	Clause 13. The bidder should not be a vendor/supplier for Software and Hardware components of the Bank. Documents to be Submitted: Self-declaration on Letterhead to be submitted for the same.	We request the bank to kindly allow System Integrators who are not direct suppliers/ OEMs to participate in this RFP.	Bidder to comply with RFP terms and conditions.
2	71	Annexure-9	Scope of Work	4.VAPT testing of any assets, applications etc. should contain but not limited to below details. •Information Gathering/ reconnaissance activity •Port Scanning •System Fingerprinting •Services Fingerprinting •Vulnerability Research and Verification Scanning •Application Security Assessment/Mobile Security Assessment •Attempt to guess passwords using password-cracking tools. •Buffer Overflow •Malicious Input Checks •Search for back door traps in the programs. •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. •Check if commonly known holes/trap doors in the operating system and Application Network Scanning system identification and trusted system scanning Vulnerability scanning •Malware scanning •Spoofing (Network, IP etc) •Password cracking, improper Authentication Error •Missing patches EOL and EOS Servers, Network Devices, Applications Software. •Improper validation and authorization •SQL injection, OS Command Injection •Cross Site (XSS) Scripting, Cross Frame Scripting (XFS) •Information leakage, Sensitive Information Passed as Clear Text in GET URL, Sensitive Information Cached, Information Exposure Through XML Entities •Frame injection, Missing Session Timeout •Hard-coded password or Key or sensitive information. •Credentials based VAPT Scanning to identify missing latest patches (n-1)	Do you want network assets, server and databases assessed only from the perspective of an attacker, or will you also provide configuration files for review of configuration? Please provide the number of devices for configuration review.	Auditor have to perform the secure configuration Adult based on SCDs. List of asset will be shared to selected bidder
3	71	Annexure-9	Scope of Work	4.VAPT testing of any assets, applications etc. should contain but not limited to below details. •Information Gathering/ reconnaissance activity •Port Scanning •System Fingerprinting •Services Fingerprinting •Vulnerability Research and Verification Scanning •Application Security Assessment/Mobile Security Assessment •Attempt to guess passwords using password-cracking tools. •Buffer Overflow •Malicious Input Checks •Search for back door traps in the programs. •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. •Check if commonly known holes/trap doors in the operating system and Application Network Scanning system identification and trusted system scanning Vulnerability scanning •Malware scanning •Spoofing (Network, IP etc) •Password cracking, improper Authentication Error •Missing patches EOL and EOS Servers, Network Devices, Applications Software. •Improper validation and authorization •SQL injection, OS Command Injection •Cross Site (XSS) Scripting, Cross Frame Scripting (XFS) •Information leakage, Sensitive Information Passed as Clear Text in GET URL, Sensitive Information Cached, Information Exposure Through XML Entities •Frame injection, Missing Session Timeout •Hard-coded password or Key or sensitive information. •Credentials based VAPT Scanning to identify missing latest patches (n-1)	Are the servers self-hosted or hosted elsewhere?	The Details will be shared to selected Bidder.

Pre Bid Replies GEM/2024/B/5637293 dated 22/11/2024 for Selection of Cert-In empaneled Auditor for conducting security assessments for the financial year 2024-25 in Canara Bank.						
Sl No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
4	71	Annexure-9	Scope of Work	4.VAPT testing of any assets, applications etc. should contain but not limited to below details. •Information Gathering/ reconnaissance activity •Port Scanning •System Fingerprinting •Services Fingerprinting •Vulnerability Research and Verification Scanning •Application Security Assessment/Mobile Security Assessment •Attempt to guess passwords using password-cracking tools. •Buffer Overflow •Malicious Input Checks •Search for back door traps in the programs. •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. •Check if commonly known holes/trap doors in the operating system and Application Network Scanning system identification and trusted system scanning Vulnerability scanning •Malware scanning •Spoofing (Network, IP etc) •Password cracking, improper Authentication Error •Missing patches EOL and EOS Servers, Network Devices, Applications Software. •improper validation and authorization •SQL injection, OS Command injection •Cross Site (XSS) Scripting, Cross Frame Scripting (XFS) •Information leakage, Sensitive Information Passed as Clear Text in GET URL, Sensitive Information Cached, Information Exposure Through XML Entities •Frame injection, Missing Session Timeout •Hard-coded password or Key or sensitive information. •Credentials based VAPT Scanning to identify missing latest patches (n-1)	Are all of the in-scope systems(Servers and Databases) available from a single network segment?	Details of asset will be shared to selected bidder
5	71	Annexure-9	Scope of Work	4.VAPT testing of any assets, applications etc. should contain but not limited to below details. •Information Gathering/ reconnaissance activity •Port Scanning •System Fingerprinting •Services Fingerprinting •Vulnerability Research and Verification Scanning •Application Security Assessment/Mobile Security Assessment •Attempt to guess passwords using password-cracking tools. •Buffer Overflow •Malicious Input Checks •Search for back door traps in the programs. •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. •Check if commonly known holes/trap doors in the operating system and Application Network Scanning system identification and trusted system scanning Vulnerability scanning •Malware scanning •Spoofing (Network, IP etc) •Password cracking, improper Authentication Error •Missing patches EOL and EOS Servers, Network Devices, Applications Software. •improper validation and authorization •SQL injection, OS Command injection •Cross Site (XSS) Scripting, Cross Frame Scripting (XFS) •Information leakage, Sensitive Information Passed as Clear Text in GET URL, Sensitive Information Cached, Information Exposure Through XML Entities •Frame injection, Missing Session Timeout •Hard-coded password or Key or sensitive information. •Credentials based VAPT Scanning to identify missing latest patches (n-1)	Please share the number of external IP and Internal IP addresses in scope of network VAPT assessment.	The Details will be shared to selected Bidder.

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

Pre Bid Replies GEM/2024/B/5637293 dated 22/11/2024 for Selection of Cert-In empaneled Auditor for conducting security assessments for the financial year 2024-25 in Canara Bank.						
Sl No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
6	71	Annexure-9	Scope of Work	4.VAPT testing of any assets, applications etc. should contain but not limited to below details. •Information Gathering/ reconnaissance activity •Port Scanning •System Fingerprinting •Services Fingerprinting •Vulnerability Research and Verification Scanning •Application Security Assessment/Mobile Security Assessment •Attempt to guess passwords using password-cracking tools. •Buffer Overflow •Malicious Input Checks •Search for back door traps in the programs. •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. •Check if commonly known holes/trap doors in the operating system and Application Network Scanning system identification and trusted system scanning Vulnerability scanning •Malware scanning •Spoofing (Network, IP etc) •Password cracking, improper Authentication Error •Missing patches EOL and EOS Servers, Network Devices, Applications Software. •improper validation and authorization •SQL Injection, OS Command Injection •Cross Site (XSS) Scripting, Cross Frame Scripting (XFS) •Information leakage, Sensitive Information Passed as Clear Text in GET URL, Sensitive Information Cached, Information Exposure Through XML Entities •Frame injection, Missing Session Timeout •Hard-coded password or Key or sensitive information. •Credentials based VAPT Scanning to identify missing latest patches (n-1)	Is credentialed vulnerability scanning of the servers to be carried out?	Yes.
7	72	Annexure-9	Scope of Work	5.The web application security testing should cover the OWASP Top 10 vulnerabilities: •A01-Broken Access control •A02-Cryptographic Failures •A03-Injection •A04-Insecure Design •A05-Security Misconfiguration •A06-Vulnerable and Outdated Components •A07-Identification and Authentication Failures •A08-Software and Data Integrity Failures •A09-Security logging and Monitoring Failures •A10-Server-Side Request Forgery	Are there any applications to be tested that are hosted or managed by a third party, such as AWS, Azure, etc.? Is cloud testing in scope?	Yes, The Details will be shared to selected Bidder.
8	72	Annexure-9	Scope of Work	5.The web application security testing should cover the OWASP Top 10 vulnerabilities: •A01-Broken Access control •A02-Cryptographic Failures •A03-Injection •A04-Insecure Design •A05-Security Misconfiguration •A06-Vulnerable and Outdated Components •A07-Identification and Authentication Failures •A08-Software and Data Integrity Failures •A09-Security logging and Monitoring Failures •A10-Server-Side Request Forgery	Approximately, How many Dynamic Pages (Or functionalities) are there in each user role for web applications?	Details of asset will be shared to selected bidder
9	72	Annexure-9	Scope of Work	5.The web application security testing should cover the OWASP Top 10 vulnerabilities: •A01-Broken Access control •A02-Cryptographic Failures •A03-Injection •A04-Insecure Design •A05-Security Misconfiguration •A06-Vulnerable and Outdated Components •A07-Identification and Authentication Failures •A08-Software and Data Integrity Failures •A09-Security logging and Monitoring Failures •A10-Server-Side Request Forgery	Are the applications internet-facing or internal? Is thick client in scope?	Internet Facing, Thick Client and Internal application are in the scope, Details of asset will be shared to selected bidder

Pre Bid Replies GEM/2024/B/5637293 dated 22/11/2024 for Selection of Cert-In empaneled Auditor for conducting security assessments for the financial year 2024-25 in Canara Bank.						
Sl No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
10	72	Annexure-9	Scope of Work	9. Mobile applications should be tested for vulnerabilities OWASP - Mobile Applications Security Verification Standards (MASVS). OWASP Mobile Applications Reverse Engineering Prevention Project.	kindly share the approx. size of the in-scope applications as per below reference Small : 0-50 pages Medium : 50-100 pages Large : 100-250 Very Large : 250+	Small and Medium mostly, Details of asset will be shared to selected bidder.
11	72	Annexure-9	Scope of Work	9. Mobile applications should be tested for vulnerabilities OWASP - Mobile Applications Security Verification Standards (MASVS). OWASP Mobile Applications Reverse Engineering Prevention Project.	Which platforms are in scope: iOS or Android? Please share the count	Both platforms are in scope, Details of asset will be shared to selected bidder.
12	72	Annexure-9	Scope of Work	10. 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).	Will we be provided with the necessary credentials and access to perform the ATM Penetration testing?	Access to ATM machie will be provided to selected Bidder.
13	72	Annexure-9	Scope of Work	10. 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).	Are there specific regulatory guidelines we need to adhere to during ATM Penetration testing?	Bidder should follow guidelines published by regulator time to time.
14	72	Annexure-9	Scope of Work	10. 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).	What specific components of ATM are in scope?	VAPT & Malware Scan will be in scope.
15	72	Annexure-9	Scope of Work	11.OWASP Top 10 API Security Risks & Penetration testing to be conducted for API applications •API1: Broken Object Level Authorization •API2: Broken Authentication •API3: Broken Object Property Level Authorization •API4: Unrestricted Resource Consumption •API5: Broken Function Level Authorization •API6: Unrestricted Access to Sensitive Business Flows •API7: Server-Side Request Forgery •API8: Security Misconfiguration •API9: Improper Inventory Management •API10: Unsafe Consumption of APIs	What is the approximate total number of API endpoints? Will the APIs be separate, or will they be integrated with the web application?	The Details will be shared to selected Bidder.
16	68	Annexure-9	Scope of Work	12.b.White Box Approach VA/API /Application Assessment (Using Credentials) i.Vulnerability scanning ii.Access controls iii.Login authorization controls iv.Parameter / Data tampering v.Session related controls vi.Privilege escalations vii.OWASP Top 10 & SANS 25 vulnerabilities viii.Manual VAPT to execute business logic flaws and validate false-positives. ix.Website Assessment (Security Configuration, Security Certificates, Services etc.) x.Backdoor traps xi.Attempts to check vulnerabilities such as directory traversal, SQL and XSS related vulnerabilities, weak encryption, authentication mechanisms, information disclosure, remote code execution, Weak SSL certificates and Ciphers, Missing patches and vulnerabilities.	Will brute forcing the application be in scope	Yes, Auditors have to inform Bank Team Before initiatation.
17	73	Annexure-9	Scope of Work	13-V.Auditor's laptops or computers will not be allowed in our Bank LAN.	Will the bank provide the laptops for auditors to use during the testing process? as it mention Auditor firm laptop not allowed in banks	No Laptop/ External Devices are allowed in Bank's Intranet.
18	81	Annexure-9	Scope of Work	15.Acceptance of the Report: •On receipt of the report from the vendor, the Bank will scrutinize and after satisfying the completeness of the report, the Bank will accept the report. If there are any inconsistencies in the report the vendor should conduct proper test and resubmit the report to the Bank without any additional cost to the Bank	How many retest iteration will be there without any additional cost?	Auditor have to conduct the verification scan until clean reports.

Pre Bid Replies GEM/2024/B/5637293 dated 22/11/2024 for Selection of Cert-In empaneled Auditor for conducting security assessments for the financial year 2024-25 in Canara Bank.						
Sl No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
19	79	Annexure-9	Scope of Work	13-b. b. Tests for Vulnerabilities that can be exploited: •Insecure services such as SNMP •Missing patches and versions, default passwords. •Vulnerabilities based on version of the device/server •SQL, XSS and other web application-related vulnerabilities, weak encryption, port Scan, SSL Certificate and Ciphers, SMTP Related vulnerabilities such as open mail relay robust authentication scheme, DOS vulnerabilities, sample and default applications/pages, DNS-related Vulnerabilities such as DNS cache poisoning, information disclosure such as internal IP disclosure, potential backdoors, older vulnerable version etc. •The Penetration Tests should cover but not be limited to CWE/SANS TOP 25 Most Dangerous Software Errors. •Exploiting Open Ports which is not used for Business purposes. •Testing should not disrupt the Bank's services. Test cases should not be selected that are destructive. The techniques and the tools used should have been thoroughly tested and licensed. •Exercise should be carried out from the bank premises only. •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. •Vulnerability assessment shall be carried out for all servers, applications, network devices, security devices installed etc. •External attack Penetration Testing should include all the Public Facing Assets of the Bank.	Commercial tool's licenses will be provided by the Bank?	No, Bidder have to come with their own licenses.
20	83	Annexure-10	Technical and Functional Specifications	1.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 Complaince: Letter from HR of the company for acceptance of this clause.	will all 5 resources should be in Bangalore branch or any specific location bank need to travel?	Bangalore. If requirement arise, Auditor have to conduct the assessment from any other location as well.
21	68	Annexure-9	Scope of Work	Scope of Work - Secure Configuration Audit	Is there an expected timeline or milestones for delivering scripts, conducting assessments, and submitting final reports?	As per RFP Terms (SECTION C - DELIVERABLE AND SERVICE LEVEL AGREEMENTS)
22	68	Annexure-9	Scope of Work	Scope of Work - Secure Configuration Audit	Are there any other compliance standards or frameworks, besides RBI guidelines and the IT Act 2000/Amendment 2008, that the assessment needs to follow?	Bidder should follow guidelines published by regulator/industry standards from time to time.
23	68	Annexure-9	14.Report	14.Report	How do you prioritize findings in the audit report(Eg: critical, high, medium, low?)	Critical, High, Medium, Low.
24	68	Annexure-9	Timeline	NA	Will the audit require any downtime or disruption to biz operations or can it be conducted with minimal impact?	Bank will provide the details with the selected Bidder during the assessment.
25	69	Annexure-9	Report	NA	Should the reports on the vendor's letterhead include any additional certification details apart from the CERT-IN empanelment information?	No, If requirement arises, Bank will intimate to Auditor.
26	69	Annexure-9	Report	NA	Should the auditor document the process or tools used to identify and remove false positives	Yes.
27	70	Annexure-9	Report	NA	What is the process and timeline for resubmitting reports if the bank identifies inconsistencies or issues?	Penalties will be applicable as per RFP Terms.
28		Section-13	Third Party Risk	NA	Are third party vendors (eg., payment processors, cloud service providers) assessed for security risks?	Query is not clear,Bidder to comply with RFP terms and conditions.
29	68	Annexure-9	Scope of Work	Scope of Work for VAPT & API Functionality and Information Security Review	Please provide digital inventory (hardware, software, applications, APIs, Lisences) count for VAPT and SCD.	Details will be shared to the selected Bidder.

Pre Bid Replies GEM/2024/B/5637293 dated 22/11/2024 for Selection of Cert-In empaneled Auditor for conducting security assessments for the financial year 2024-25 in Canara Bank.						
Sl No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
30	23	Clause 6	Earnest Money Deposit (EMD)/Bank Guarantee in lieu of EMD	The bidder shall furnish Non interest earning Earnest Money Deposit (EMD) amount as mentioned in the Bid Schedule by way of Insurance Surety Bonds, account payee demand draft drawn on any Scheduled Commercial Bank in India in favour of Canara Bank, payable at Bengaluru, fixed deposit receipt, or banker's cheque or Bank Guarantee from any of the Commercial Banks or payment online in an acceptable form, safeguarding the Bank's interest in all respects. The bid security should remain valid for a period of 45 (forty-five) days beyond the final bid validity period.	We are MSME registered (Medium enterprise), and MSME registered companies are exempted from paying the amount of Tender document Fee & EMD for any Tender issued in India. Considering the same, kindly exempt us from the submission of Tender document Fee & EMD.	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. Traders are excluded from the purview of this Policy Further ,please refer the SECTION H-PURCHASE PREFERENCE for MSE Guidelines.

Date: 10.12.2024
Place Bangalore

Deputy General Manager

केनरा बैंक CANARA BANK Tender Processing Section C.P.&.V.M. Wing, H.O., Bangalore - 560 002