केनरा बैंक Canara Bank

**Request for Quotes [RFQ 071/2024-25]**

**For**

**Selection of empaneled CERT-IN Security Auditor for conducting Source Code Audits**

**Issued by: Canara Bank**
**Single Tender Enquiry Processing Section,**
**CP&VM Wing, HO (Annex)**
**1st Floor, Naveen Complex**
**14, M G Road**
**Bengaluru-560 001**
**Phone No:080- 25584033**
**Email:singletender@canarabank.com**

**This bid is restricted to the following vendors who are empaneled in Canara Bank through EOI-09/2023 dated 19/03/2024.**

1. M/s Digital Age strategies Pvt Ltd
2. M/s AAA Technologies Ltd
3. M/s KPMG Assurance and Consulting Services LLP
4. M/s Yoganandh & Ram LLP
5. M/s SecurEyes Techno Services Pvt Ltd
6. M/s AKS Information Technology Services Pvt Ltd
7. M/s PWC Pvt Ltd

## BID SCHEDULE

| Sl. No. | Description | Details |
|---|---|---|
| 1. | RFQ No. and Date | RFQ 071/2024-25 dated 23/12/2024 |
| 2. | Name of the Wing | CP&VM Wing |
| 3. | Brief Description of the RFQ | For selection of empaneled CERT-IN Security Auditor for conducting Source Code Audits |
| 4. | Location Address for submission of Bid/s [Address for Communication] | The Senior Manager<br>Canara Bank,<br>Single Tender Enquiry Processing Section,<br>CP & VM Wing<br>Head Office (Annex)<br>1st Floor, Naveen Complex<br>14, M G Road<br>Bengaluru -560 001<br>Karnataka |
| | | Tel - 080-25590070<br>Email: Singletender@canarabank.com |
| 5. | Date of Issue of RFQ | 23/12/2024, Monday |
| 6. | Last Date and Time for Submission of Bids | 03/01/2025, Friday up to 3:00 PM<br><br>Venue: Canara Bank, First Floor, Single Tender Enquiry Processing Section, CP&VM Wing, HO (Annex), Naveen Complex, 14 M G Road, Bengaluru 560001. |
| 7. | Date and Time of Opening Bid | 03/01/2025, Friday, at 03:30 PM |

केनरा बैंक Canara Bank

**Dear Vendor,**

**The Bank intends to Conduct Source Code Audits. Find the details below:**

| | | |
|---|---|---|
| 1. | Details of the Assessment | **Conducting Source Code Audits** |
| 2. | Technical Specification of the Item to be procured | **NA** |
| 3. | Scope of Work | **As per Annexure-II** |
| 4. | Time Lines for Delivery/ installation/ Implementation | **3 Months** |
| 5. | Warranty Period (If applicable) | **NA** |
| 6. | AMC /ATS/ Support Charges as Applicable | **NA** |
| 7. | Payment Terms | **As per Annexure-IV** |
| 8. | Bill of Material | **As per Annexure-III** |
| 9. | Mode of Submission of Bid/Quote | **Soft copy (Digitally Signed PDF file of the bid which is Password protected should be send to the below mentioned mail ID**<br>**Email ID: - singletender@canarabank.com**<br>**OR**<br>**Hard copy**<br>**(The bid should be submitted in sealed cover addressed to the Bank at the mentioned address within the date and time specified)** |
| 10. | Last Date and Time for Submission of Bids | **03/01/2025, Friday up to 3:00 PM**<br><br>**Venue: Canara Bank, First Floor, Single Tender Enquiry Processing Section, CP&VM Wing, HO (Annex), Naveen Complex, 14 M G Road, Bengaluru 560001.** |
| 11. | Other Terms and Conditions | • **Should be CERT-In Empaneled Auditor**<br>• **Technical requirements- CEH, CISA, CISSP, CISM etc. along with knowledge of respective standards, frameworks and technical skills.** |
| 12. | Any Other Information | **Nil** |

**Yours faithfully,**

**Authorized Signatory**
**Note: For further clarification, if any, please contact us.**

**Address:**
**The Senior Manager,**
**Canara Bank**
**Single Tender Enquiry Processing Section, CP&VM Wing**
**First Floor, Naveen Complex,**
**#14, MG Road,**
**Bangalore-560001**
**Phone No.: 080-25584033**

**ANNEXURE-I**

## 1. Objective

The Bank is looking at a highly professional relationship with the auditor who shall conduct Source Code Audits. The Auditor shall conduct/complete Assessment activities along with revalidations until clean report.

## 2. Requirement Details

Bank invites online/offline submission of bids from empaneled vendors for Conducting Source Code Audits as per the Terms & Conditions, Technical Requirements and Scope of Work described elsewhere in this document. This tender consists of requirement as given below:

| Sl. No. | Item Details | Tentative No. of Assets during the contract period |
|---|---|---|
| 1. | Source Code Audit | 70* |

***This is an indicative number. Bank on its discretion may increase or decrease the number of assessments.**

## 3. Project Timelines

**3.1.** Bidders are requested to keep the following timelines with regard to the completion of Assessment.

3.1.1. All Source Code Audits should be completed within 3 months from the date of acceptance of purchase order.

- Initial assessment report should be released to bank team within 3 days from the requested date along with initial report.
- Revalidation should be completed within 2 days from the requested date along with rescan report.

3.1.2 The activity shall be conducted by deploying at least 4 resources at bank's premises on all working days of bank.

## 4. Penalties & Liquidated damages on delay in completion of Assessment:

In case of delay in releasing the report as per timelines mentioned in para 3.1.1., penalty of 0.5% of unit cost per day will be imposed.

## 5. Subcontracting

The vendor shall not subcontract or permit anyone other than its personnel to perform any of the work, service or other performance required of the vendor under the contract without the prior written consent of the Bank.

## 6. Deliverables:

Main Report: Final report with approval of the bank after discussing draft report.

We comply with each point mentioned above without any deviations.

Date:

Signature with seal
Name :
Designation :

## Annexure- II

## SCOPE OF WORK

**SUB: RFQ 071/2024-25 dated 23/12/2024 for selection of empaneled CERT-IN Security Auditor for conducting Source Code Audits**

**Ref: Your RFQ 071/2024-25 dated 23/12/2024.**

1. The selected bidder should carry out an assessment for vulnerabilities, threats and risks in Web/Mobile application source code. Assessment will include identifying existing threats if any and suggests remedial solutions and recommendations for implementation of the same to mitigate all identified risks, with the objective of enhancing the security posture of the systems.
   - The Bank will call upon the selected bidder on the placement of the order to provide demonstration and walk-through of all specific aspects of the source code assessment activity at the Bank's desired location. All the expenses for the above will be borne by the concerned bidder.
   - The Assessment plan should be shared with the Bank, including the methodology, tools being used and prerequisites for conducting the test.
   - Only reputed software/ tools, preferably licensed, should be used for conducting the assessments on bank provided systems.
   - The schedule of the assessment is to be provided prior to the start of activity along with the team member's details. A dedicated Project Manager shall be nominated, who will be the single point of contact for the activity.
   - Bidder to ensure that only certified and experienced professionals should be deployed for carrying out the activity during the contract period.
2. The assessment is to be conducted as per the latest OWASP guidelines including but not limited to the following:

   **OWASP Top 10 for Secure Code Review: -**

   A1 Injection
   A2 Broken Authentication and Session Management
   A3 Cross-site Scripting
   A4 Insecure Direct Object Reference
   A5 Security misconfiguration
   A6 Sensitive Data Exposure
   A7 Missing function level Access Control
   A8 Cross-site Request Forgery (CSRF)
   A9 Using Components with Known vulnerabilities
   A10 Un-Validated Redirects and Forwards

   **The following activities need to be covered: -**

   1) General security vulnerabilities
   2) Privacy issues
   3) Business logic bugs
   4) Compliance issues (such as CWE, PCI DSS, IRDIA, CERT-IN, etc. whichever applicable)

5) Availability issues
6) Log & error handling issues
7) Cryptographic practices
8) Access control Verification
9) Code cleansing practices
10) Software composition Analysis

- Source Code Scanning using automated tools that run against a source code repository or module, Software composition analysis, OWASP dependency check, finding string patterns deemed to potentially cause security vulnerabilities.
- Secure Code Assessment by a security subject matter expert with minimum of 5 years of experience in the domain and should be certified (CEH/CISA/CISSP/CISM etc.) along with knowledge of respective standards, frameworks and technical skills.

## 3. Reporting & support

### 3.1. Submission of Reports

a. On completion of the assessment, the auditor should share the detailed assessment report highlighting the description, remediation and POC for the reported vulnerability along with the severity (Critical, High, Medium, Low).
b. A detailed report of the vulnerabilities along with evidence and mitigation/ recommendations should be furnished as per the Bank's prescribed format (PDF and Excel).
c. The vulnerabilities should be scored following the latest Common Vulnerability Scoring System (CVSS).
d. The report should include but not limited to Executive Summary, Project Scope, Methodology, Environment testing, findings, severity, impact of vulnerabilities and tools used for test etc.,
e. Each individual finding should include Reference Number, Severity/Risk Factor, Title, CVSS vector and score, CWE ID, Proof of Concept for the vulnerability, Recommendations with literature references, link to references etc.
f. Auditor should support over call for any queries from the Bank during the closure of vulnerabilities / for any clarifications sought by the Bank.
g. All the reports submitted should be signed by technically qualified persons and he/she should take ownership of document and he/she is responsible and accountable for the document/report submitted to the Bank.
h. A standard report template will provide enough information to enable the code reviewer to classify and prioritize the software vulnerabilities based on the applications threat model. This report does not need to be pages in length, it can be document based or incorporated into many automated code review tools. A report should provide the following information:
   - Date of review.
   - Application name, code modules reviewed.
   - Developers and code reviewer names.
   - Task or feature name, (TFS, GIT, Subversion, trouble ticket, etc.)
i. A brief sentence(s) to classify and prioritize software vulnerability if any and what if any remedial tasks need to be accomplished or follow up is needed.
j. Link to documents related to task/feature, including requirements, design, testing and threat modeling documents.
k. Code Review checklist if used, or link to organization Code Review Checklist. (see Appendix A)

l. Testing the developer has carried out on the code. Preferably the unit or automated tests themselves can be part of the review submission
m. If any tools such as FxCop, BinScope Binary Analyzer, etc. were used prior to code review.

**Appendix A**

## CODE REVIEW CHECKLIST

| CATEGORY | DESCRIPTION | PASS | FAIL |
|---|---|---|---|
| General | Are there backdoor/unexposed business logic classes? | | |
| Business Logic and Design | Are there unused configurations related to business logic? | | |
| Business Logic and Design | If request parameters are used to identify business logic methods, is there a proper mapping of user privileges and methods/actions allowed to them? | | |
| Business Logic and Design | Check if unexposed instance variables are present in form objects that get bound to user inputs. If present, check if they have default values. | | |
| Business Logic and Design | Check if unexposed instance variables present in form objects that get bound to user inputs. If present, check if they get initialized before form binding. | | |
| Authorization | Is the placement of authentication and authorization check correct? | | |
| Authorization | Is there execution stopped/terminated after for invalid request? i.e. when authentication/authorization check fails? | | |
| Authorization | Are the checks correct implemented? Is there any backdoor parameter? | | |
| Authorization | Is the check applied on all the required files and folder within web root directory? | | |
| Authorization | Are security checks placed before processing inputs? | | |
| Business Logic and Design | Check if unexposed instance variables are present in form objects that get bound to user inputs. If present, check if they have default values. | | |
| Business Logic and Design | Check if unexposed instance variables present in form objects that get bound to user inputs. If present, check if they get initialized before form binding. | | |
| Authorization | Is there execution stopped/terminated after for invalid request? i.e. when authentication/authorization check fails? | | |
| Business Logic and Design | Are the checks correct implemented? Is there any backdoor parameter? | | |
| Business Logic and Design | Is the check applied on all the required files and folder within web root directory? | | |
| Business Logic and Design | Is there any default configuration like Access- ALL? | | |
| Business Logic and Design | Does the configuration get applied to all files and users? | | |
| Authorization | Incase of container-managed authentication - Is the authentication based on web methods only? | | |
| Authorization | Incase of container-managed authentication - Does the authentication get applied on all resources? | | |

| CATEGORY | DESCRIPTION | PASS | FAIL |
|---|---|---|---|
| Cryptography | Are database credentials stored in an encrypted format | | |
| Business Logic and Design | Does the design support weak data stores like flat files | | |
| Business Logic and Design | Does the centralized validation get applied to all requests and all the inputs? | | |
| Business Logic and Design | Does the centralized validation check block all the special characters? | | |
| Business Logic and Design | Does are there any special kind of request skipped from validation? | | |
| Business Logic and Design | Does the design maintain any exclusion list for parameters or features from being validated? | | |
| Imput Validation | Are all the untrusted inputs validated?<br>Input data is constrained and validated for type, length, format, and range. | | |
| Cryptography | Is the data sent on encrypted channel? Does the application use HTTPClient for making external connections? | | |
| Session Management | Does the design handle sessions securely? | | |
| Authorization | Incase of container-managed authentication - Is the authentication based on web methods only? | | |
| Authorization | Is Password Complexity Check enforced on the password? | | |
| Cryptography | Is password stored in an encrypted format? | | |
| Authorization | Is password disclosed to user/written to a file/logs/console? | | |
| Logging and Auditing | Do audit logs log connection attempts (both successful and failures)? | | |
| Logging and Auditing | Is there a process(s) in place to read audit logs for unintended/malicious behaviors? | | |
| Cryptography | Is all PI and sensitive information being sent over the network encrypted form. | | |
| Authorization | Does application design call for server authentication (anti-spoofing measure)? | | |
| Authorization | Does application support password expiration? | | |
| Cryptography | Does application use custom schemes for hashing and or cryptographic? | | |

| | | | |
|---|---|---|---|
| Session Management | Does the design involve session sharing between components/modules? Is session validated correctly on both ends? | | |
| Business Logic and Design | Does the design use any elevated OS/system privileges for external connections/commands? | | |
| Business Logic and Design | Is there any known flaw(s) in API's/Technology used? For eg: DWR | | |
| Business Logic and Design | Does the design framework provide any inbuilt security control? Like <%: %> in ASP.NET MVC? Is the application taking advantage of these controls? | | |
| Business Logic and Design | Are privileges reduce whenever possible? | | |
| Business Logic and Design | Is the program designed to fail gracefully? | | |
| Logging and Auditing | Are logs logging personal information, passwords or other sensitive information? | | |

We hereby comply with each point of the above Scope of Work without any deviations.

**Date:**

**Signature with seal**
**Name:**
**Designation :**

**Annexure-III**

**Bill of Material**

**Sub: RFQ 071/2024-25 dated 23/12/2024 for selection of empaneled CERT-IN Security Auditor for conducting Source Code Audits.**

**[Amount in Rupees]**

| Sl. No | Description | Unit Cost Per Assessment | | | Tentative No. of Assets during the contract period | Total cost | |
|---|---|---|---|---|---|---|---|
| | | (Excl. of Tax) | Tax for Column A | | | (Excl. of Tax) | (Incl. of Tax) |
| | | A | B % of tax | C Tax Amt | D | E=D*A | F=D*(A+C) |
| 1 | Fee for conducting Source Code Audit | | | | 70* | | |
| Total Project Cost | | | | | | | |

***This is an indicative number. Bank on its discretion may increase or decrease the number of assessments.**

- **Payment will be released for the actual number of assessments completed during the contract period**
- **Total Cost of the Project shall be sum total of Col. E (Excl. of Tax) and L1 bidder shall be decided on the basis of lowest value quoted under Col. E (Excl. of Tax) by the Bidder.**

Date :

Signature with seal
Name:
Designation:

## Annexure-IV

## Payment Term and Conditions

**Sub: RFQ 071/2024-25 dated 23/12/2024 for selection of empaneled CERT-IN Security Auditor for conducting Source Code Audits.**

1. 100% payment will be released for the actual number of assessments completed during the contract period.
2. Bank will not pay any amount in advance.
3. Initial assessment report should be released to bank team within 3 days from the requested date along with initial report.
4. Revalidation should be completed within 2 days from the requested date along with rescan report.
5. In case of delay in releasing the report as per above timelines, penalty of 0.5% of unit cost per day will be imposed.
6. The payments will be released through NEFT/RTGS and the selected bidder has to provide necessary bank details like account number, bank's name with branch name, Correct IFSC code etc.

**Locations details are as mentioned below:** Location for conducting audit is from onsite only at the following location of the Bank.

| Sl. No | Section / Wing | Location |
|---|---|---|
| 1. | VAPT Section, Cyber Security Wing, HO | Bengaluru |

We comply to all the points mentioned in RFQ, Scope of work, without any deviation.

| | |
|---|---|
| Date: | Signature with seal:<br>Name :<br>Designation : |