केनरा बैंक Canara Bank

Expression of Interest

FOR

Empanelment of IT/ Cyber Security Auditors from CERT-In Empaneled Auditors under Group A category for period of three (03) years in Canara Bank

Issued by: Canara Bank,
Centralized Procurement & Vendor Management Wing,
1st Floor, Naveen Complex,
14, M G Road,
Bengaluru - 560 001
Email: dittenders@canarabank.com
Phone No: 080-25584040 Extension- 245/225/474

केनरा बैंक Canara Bank

Bid Details in Brief Description

Sl. No.	Description	Details
1.	EOI No. and Date	EOI 03/2024-25 dated 31/08/2024
2.	Name of the Wing	Centralized Procurement & Vendor Management Wing
3.	Brief Description of the EOI	Expression of Interest for Empanelment of IT/ Cyber Security Auditors from CERT-In Empaneled Auditors from under Group A category for a period of three (03) years in Canara Bank
4.	Bank's Address for Communication and Submission of Tender	Deputy General Manager Canara Bank, Centralized Procurement & Vendor Management Wing, 1st Floor, Naveen Complex, 14, MG Road, Bengaluru -560 001
		Senior Manager, Centralized Procurement and Vendor Management Wing, 1st Floor, Naveen Complex, 14, MG Road, Bengaluru -560 001 Tel - 080-25590070,25584873 Fax- 080-25596539 Email: dittenders@canarabank.com
5.	Date of Issue of EOI	31/08/2024, Saturday
6.	Tender Fee (Non-Refundable)	5,000/-
7.	Earnest Money Deposit (Refundable)	10,000/-
8.	Last Date and Time for Submission of Queries for Pre-Bid Meeting	06/09/2024, Friday, 5.00 PM
9.	Date of Pre-Bid Meeting	10/09/2024, Tuesday, 3.30 PM
10.	Last Date and Time for Submission of Bids	01/10/2024, Tuesday up to 3.00 PM
11.	Date of Opening of Bid	01/10/2024, Tuesday at 3.30 PM
12.	Location of Tender Box for submission of EOI	Canara Bank, Centralized Procurement & Vendor Management Wing, 1st Floor, Naveen Complex, 14, MG Road, Bengaluru -560 001
13.	Venue for Prebid Meeting and Bid Opening	Pre-bid meeting will be held on 10/09/2024, Tuesday, 3.30 PM Venue: Pre-Bid meeting will be held Online

Disclaimer

The information contained in this Expression of Interest ("EOI") document or information provided subsequently to bidders or applicants whether verbally or in documentary form by or on behalf of Canara Bank (or Bank), is provided to the bidder(s) on the terms and conditions set out in this EOI document and all other terms and conditions subject to which such information is provided. This EOI document is not an agreement and is not an offer or invitation by Canara Bank to any parties other than the applicants who are qualified to submit the bids (hereinafter individually and collectively referred to as "Bidder" or "Bidders" respectively). The purpose of this EOI is to provide the Bidders with information to assist the formulation of their proposals. This EOI does not claim to contain all the information each Bidder require. Each Bidder may conduct its own independent investigations and analysis and is free to check the accuracy, reliability and completeness of the information in this EOI. Canara Bank makes no representation or warranty and shall incur no liability under any law, statute, rules or regulations as to the accuracy, reliability or completeness of this EOI. The information contained in the EOI document is selective and is subject to updating, expansion, revision and amendment. It does not purport to contain all the information that a Bidder require. Canara Bank does not undertake to provide any Bidder with access to any additional information or to update the information in the EOI document or to correct any inaccuracies therein, which may become apparent.

Canara Bank reserves the right of discretion to change, modify, add to or alter any or all of the provisions of this EOI and/or the bidding process, without assigning any reasons whatsoever. Such change will be published on the Bank's Website https://www.canarabank.com/pages/expression-of-interest and it will become part and parcel of EOI.

Canara Bank in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this EOI. Canara Bank reserves the right to reject any or all the expression of interest / proposals received in response to this EOI document at any stage without assigning any reason whatsoever. The decision of Canara Bank shall be final, conclusive and binding on all the parties.

No person of the Bank or the Contractors, vendors and third parties shall violate the Social Media Policy of the Bank. Non-adherence to the standards/guidelines in relation to Social Media Policy issued by the Bank from time to time and any omission or commission which exposes the Bank to actual or potential monetary loss or otherwise, reputation loss on account of non-adherence of social media related systems and procedures on the part of personnel of the Bank or Contractors, Vendors and third parties shall be construed as violation of Social Media Policy

Internal

		(through Microsoft Teams) and participants are requested to attend the meeting Online. Those who are interested in participating the pre bid meeting should share the scanned copy of authorization and Valid ID Card of the participant by email to dittenders@canarabank.com. (Physical copy should be submitted at later date) Upon perusal of the same the link / meeting id will be shared to the participant to participate in the meeting (Microsoft Teams). Pre-bid Queries should be sent to E-mail dittenders@canarabank.com and must reach us on or before **06/09/2024, Friday, 5.00 PM.** Subject of the email should be given as **"Pre Bid Queries for EOI 03/2024-25 dated 28/08/2024 - Expression of Interest for Empanelment of IT/ Cyber Security Auditors from CERT-In Empaneled Auditors under Group A category for a period of three (03) years in Canara Bank ". Queries reaching afterwards will not be entertained.**
This document can be downloaded from following websites https://www.canarabank.com/pages/expression-of-interest **Any amendments, modifications, Pre-bid replies and any communication etc., will be uploaded in the Bank's website only (i.e.,** https://www.canarabank.com/pages/expression-of-interest**).** **No individual communication will be sent to the bidders.**		

Internal

Abbreviations used in this Document

Sl. No.	Abbreviation	Description
1.	AMC	Annual Maintenance Contract
2.	ATS	Annual Technical Support
3.	CBS	Core Banking Solution
4.	CCNA	Cisco Certified Network Associate
5.	CCNP	Cisco Certified Network Professional
6.	CEH	Certified Ethical Hacker
7.	CHFI	Computer Hacking Forensic Investigator
8.	CISA	Certified Information Systems Auditor
9.	CISM	Certified Information Security Manager
10.	CISSP	Certified Information Systems Security Professional
11.	COBIT	Control Objectives for Information and Related Technologies
12.	CRISC	Certified in Risk and Information Systems Control
13.	CRISC	Certified In Risk and Information Systems Control
14.	CVC	Central Vigilance Commission
15.	DC	Data Centre
16.	DD	Demand Draft
17.	DISA	Diploma in Information System Audit
18.	DIT	Department of Information Technology
19.	DRC	Disaster Recovery Centre
20.	ECIH	EC-Council Certified Incident Handler
21.	ECSA	EC-Council Certified Security Analyst
22.	EOI	Expression of Interest
23.	GIAC	Global Information Assurance Certification
24.	IFSC	Indian Financial System Code
25.	ISO	International Organization for Standardization
26.	IT	Information Technology
27.	NEFT	National Electronic Fund Transfer
28.	NI ACT	Negotiable Instrument Act
29.	PAN	Permanent Account Number
30.	PCIDSS	Payment Card Industry Data Security Standard
31.	RFP	Request for Proposal

Sl. No.	Abbreviation	Description
32.	RFQ	Request for Quotation
33.	RTGS	Real Time Gross Settlement
34.	SOC	Security Operation Centre
35.	SSCP	Systems Security Certified Practitioner

केनरा बैंक Canara Bank

LIST OF CONTENTS

SUB: Expression of Interest for Empanelment of IT/ Cyber Security Auditors from CERT-In Empaneled Auditors from under Group A category for a period of three (03) years in Canara Bank

Ref: EOI 03/2024-25 dated 31/08/2024

1. About Canara Bank

1.1. CANARA BANK is one of the largest Public Sector Banks owned by Government of India. Canara Bank is a body Corporate and a premier Public Sector Bank established in the Year 1906 by Shri. Ammembal Subba Rao Pai and nationalized under the Banking Companies (Acquisition and Transfer of Undertakings) Act, 1970. Canara Bank Head office is located at 112, J C Road Bengaluru-560002 and Centralized Procurement and Vendor Management Wing located at Naveen Complex, No.14, M G Road, Bengaluru-560001.

1.2. The Bank is having pan India presence of more than 9616 branches, 26 Circle offices and 177 Regional Offices situated across the States. The Bank also has offices abroad in London, Dubai, and New York.

1.3. The Bank is a forerunner in implementation of IT related products, services, and continuously making efforts to provide the state of art technological products to its customers.

2. Definitions:

2.1. Bank' means, unless excluded by and repugnant to context or the meaning thereof, shall mean 'Canara Bank', described in more detail in Paragraph 1 above and which has invited bids under this Expression of Interest and shall be deemed to include it successors and permitted assigns.

2.2. 'EOI' means Expression of Interest for "Empanelment of IT/ Cyber Security Auditors from under Group A category from CERT-In Empaneled Auditors for period of three (03) years in Canara Bank".

2.3. The firms, institutions & companies submitting the proposal in response to this EOI shall hereinafter be referred to as 'Bidder'.

2.4. 'Contract' means the agreement signed/ Terms & conditions accepted by empaneled bidder(s) and the Bank at the conclusion of empanelment process, wherever required.

2.5. 'Proposal' means that Technical/ Eligibility proposal including all documents submitted by the bidder as per the formats prescribed in the EOI.

3. About EOI

3.1. Bank intends to empanel IT/ Cyber Security Auditors from CERT-In Empaneled Auditors who can provide suitable and appropriate audit services to the Bank.

3.2. The EOI document is not a recommendation or invitation to enter the contract, agreement or any other arrangement in respect of the services. The provision of the services is subject to compliance to selection process and appropriate documentation being agreed between the bank and selected vendors as identified by the bank after completion of the selection process.

4. Objective:

4.1. Canara Bank invites application from reputed Bidders to submit their "Expression of Interest" who fulfills the eligibility criteria as given in **Annexure-3** for empanelment of IT/Cyber Security auditors from Cert-In empaneled auditors under Group A category for a period of three years.

4.2. The bidders satisfying the Eligibility Criteria as per the EOI and having experience in IT / Cyber Security Audit services may respond.

5. Eligibility Criteria

5.1. Interested bidders, who are capable of providing auditing services, mentioned in the present EOI document and meet the Eligibility Criteria as per Annexure-3, may respond.

5.2. Non-compliance to any of the eligibility criteria would result in outright rejection of the bidder's proposal. The bidder is expected to provide proof for each of the points for eligibility criteria evaluation. The proof provided must be in line with the details mentioned in "Documents to be submitted in compliance with Qualification Criteria". Any credential detail mentioned in "Qualification Criteria" not accompanied by relevant proof documents will not be considered for evaluation.

5.3. Canara Bank, reserves the right to verify/evaluate the claims made by the bidder independently. Any deliberate misrepresentation will entail rejection of the offer.

6. Scope of Empanelment:

6.1. Broadly the audits are conducted in view of applicable Regulatory requirements/ Industry best practices/ Bank's internal policies as relevant to existing environment/ ISO 27001/ PCI DSS/ OWASP standards and other national/ international standards that are applicable to the Audit that is being conducted. Methodologies/ Tools used should be industry approved, preferably those meeting the requirements of specific relevant standards. Since every security audit has the purpose of assurance on the level of Information/Cyber Security preparedness, every audit should invariably consider the existing risk profile for each of the assets that are being audited, the controls available and deficiencies, the same should be documented along with recommendations for corrections as well as suggestions for improvement.

6.2. Empanelment would be for Security Auditors for the below mentioned I.T. Audit services but not limited to:

a. Vulnerability Assessment
b. Penetration Testing
c. Source Code Audit
d. Application /web/ mobile security Audit
e. Ethical Hacking
f. Forensic Audit
g. Incident Response
h. Cloud Security Assessment
i. Secure Configuration Review & Audit

j. API Functionality and Information Security Review

k. Gateway Audit (API Gateway, Payment Gateway etc.)

l. BCP / DR (Preparedness / Readiness) Audit

m. Network Audit including Virtualization, wireless, IoT & Mobile Technologies

n. Secure Architecture review

o. Software Composition Analysis

p. Network Security Audit

q. Database Audits

r. Migration Audit

s. ATM Infra Audit- Switch/ATM Terminals/ ATM Network

t. Vendor Security Risk Assessment

u. Open-Source Software /Tools Security Assessments

v. Comprehensive cyber-Security Audit

w. Any other activity including regulatory audit / assessment such as Advanced /New IT Technology, Cloud Technology, AI & ML Technology, Developing /Reviewing of Policies/ Procedure, Audit of Critical Infrastructure etc. as decided by the Bank during the empanelment period.

6.3. Geographical scope of project: Canara Bank DC/DR/Near site (Bengaluru/ Mumbai).

6.4. Empanelment would be for three (3) years and is subjected to annual review. However, the Bank reserves the right to cancel or extend the validity period of empanelment. Bank's decision will be final in this regard.

6.5. Bank will float limited tenders amongst the qualified empaneled vendors and seek responses for various requirements. Individual tender/s will contain detailed terms and conditions, instructions, location details and detailed scope of work. Such limited tenders shall be floated by Bank.

6.6. Bank at its own discretion may not call a vendor for a particular audit in case of conflict of interest. For ex. Vendor who has conducted VAPT, source code audit and Application audit may not be called for Forensic Audit.

6.7. Bank at its own discretion may not call a vendor for a particular audit in case if the same audit is previously carried out by the same vendor. For ex. Bank may not call a vendor who has previously conducted VAPT services in the Bank.

7. Empanelment Procedure:

The IT/ Cyber Security Auditors will be empaneled as per the following process:

7.1. IT/ Cyber Security Auditors satisfying the eligibility criteria will be short listed after due scrutiny of documents submitted by the bidder.

7.2. All the shortlisted intending bidders have to make a presentation before a panel of Bank Officials at the discretion of the Bank. The date of presentation shall be intimated to the short-listed bidders in advance.

7.3. Based on the documents submitted, and the presentations made and the expertise subject to Eligibility qualification, the panel shall select the IT/ Cyber Security Auditors for empanelment.

8. Duration of Empanelment

Post the evaluation process, the shortlisted bidders will be empaneled for a period of 3 years subject to annual review.

9. De-empanelment of bidders:

9.1. During empanelment period, the Bank reserves the right to de-empanel any vendor. The Bank's decision will be final in this regard.

9.2. The bidder is required to ensure active empanelment throughout the 3 years' empanelment period. In the event of being de-empaneled by the CERT-In, the bank will also de-empanel the bidder.

9.3. Bank should retain with themselves the authority to blacklist or bar a bidder for a specified period of the time from participating in its procurement process where the Bank has authentic information the bidder has been debarred from participating in the procurement process by a foreign country, international organization or by a local organization on ground of fraud or corruption or for some other reason which, in the opinion of the Bank is not compatible with its procurement policy and ethical standard.

9.4. If the service provided by the vendor is found to be unsatisfactory or if at any time it is found that the information provided for empanelment or for any tender is false or if irregularities shown by the vendor when applying for the tenders, the Bank reserves the right to remove such Bidders from the empaneled list without giving any notice to the vendor in advance.

9.5. Empaneled Vendors not submitting their response continuously for Three (3) limited tenders may be de-listed from our empanelment list at the discretion of the Bank. However, those services which are not provided by the bidder at the time of empanelment will not be counted.

10. Clarification to the EOI and Pre-Bid Queries

10.1. The bidder should carefully examine and understand the scope, terms and conditions of EOI and may seek clarifications, if required. The bidders in all such cases seek clarification in writing in the same serial order of that of the EOI by mentioning the relevant page number and clause number of the EOI as per the format mentioned below:

Sl. No.	Bidder's Name	Page No.	Section	EOI Clause	Clause/Technical Specification	Bidder's Query
1						
2						
3						
4						
5						
...						

10.2. All communications regarding points requiring clarifications and any doubts shall be given in writing to The Deputy General Manager, Canara Bank, Centralized Procurement and Vendor Management Wing, HO(Annex), #14, Naveen Complex, MG Road, Bengaluru-560001 in email to dittenders@canarabank.com by the intending bidders as per the bid schedule.

10.3. No queries will be entertained from the bidders after the due date and time mentioned in the EOI document.

10.4. No oral or individual consultation shall be entertained.

11. Pre-Bid meeting

11.1. A pre-bid meeting of the intending bidders will be held online as scheduled in Bid schedule to clarify any point/doubt raised by them in respect of this EOI. No separate communication will be sent for this meeting.

11.2. If the meeting date is declared as a holiday under NI Act by the Government subsequent to issuance of EOI, the next working day will be deemed to be the pre-bid meeting day. Authorized representatives of interested bidders shall be present during the scheduled time. In this connection, Bank will allow a maximum of Two (2) representatives from each Bidder to participate in the pre-bid meeting.

11.3. Bank has the discretion to consider any other queries raised by the bidder's representative during the pre-bid meeting.

11.4. Bank will have liberty to invite its technical consultant or any outside agency, wherever necessary, to be present in the pre-bid meeting to reply to the technical queries of the bidders in the meeting.

11.5. The Bank will consolidate all the written queries and any further queries during the pre-bid meeting and the replies for the queries shall be made available in the Bank's website and no individual correspondence shall be made. The clarification of the Bank in response to the queries raised by the bidder/s, and any other clarification/amendments/corrigendum furnished thereof will become part and parcel of the EOI and it will be binding on the bidders.

11.6. Non receipt of reply to the queries raised by any of the Bidders shall not be accepted as a valid reason for non-submission of Bid. In addition, non-reply to any query may not be deemed the version of the Bidder as reflected in the query has been accepted by the Bank.

12. Amendment to EOI

12.1. At any time prior to deadline for submission of Bids, the Bank, for any reason, whether, at its own initiative or in response to a clarification requested by prospective bidder, may modify the bidding document, by way of an amendment.

12.2. Notification of amendments will be put up on the Bank's website (www.canarabank.com) and will be binding on all bidders and no separate communication will be issued in this regard.

12.3. In order to allow prospective bidders reasonable time in which to take the amendment into account in preparing their bids, the Bank, at its discretion, may extend the deadline for a reasonable period as decided by the Bank for the submission of Bids.

13. Bid System Offer

This EOI has following two parts:

13.1. Technical cum Eligibility Proposal:

Indicating the response to the Eligibility Criteria Declaration, Scope of Work, Technical Evaluation Criteria and other terms & conditions. The format for submission is as per Annexure-1.

13.2. Technical Evaluation of Bidders

a. Bidders will be evaluated technically on the basis of marks obtained in Technical evaluation criteria as mentioned in **Annexure-4.**

b. Bidder should secure minimum 75% marks under Technical cum Eligibility evaluation to become qualified for empanelment.

14. Preparation of Bids:

14.1. Before submitting the bid, the bidders should ensure that they conform to the Eligibility Criteria Declaration as stated in Annexure-3 of this EOI document. Only after satisfying themselves of the Eligibility Criteria, the Offer should be submitted.

14.2. All bids and supporting documents shall be submitted in English and on A4 size paper, spirally bound securely and in serial order. The response should be submitted in a structured format as per the checklist (Annexure-1) appended.

14.3. All pages of EOI should be stamped and signed by Authorized Signatory of the Bidder. All pages of the bid document should be serially numbered and shall be signed by the authorized person/s only. The person/s signing the bid shall sign all pages of the bid and rubber stamp should be affixed on each page. The bidder should submit a copy of Board Resolution or power of attorney document showing that the signatory has been duly authorized to sign the bid document.

14.4. The Conformity to Eligibility Criteria should be complete in all respects and contain all information sought for, as per **Annexure 1.**

14.5. It is mandatory to provide the compliance to Scope of Work in the exact format of Annexure-10 of this EOI document.

15. Tender Fee & Earnest Money Deposit

15.1. Bidders can also submit the Tender Fee and EMD with Account Payee Demand Draft in favour of Procurement Group payable at Bangalore.

15.2. Bidder has to submit scanned copy / proof of the DD along with bid and has to ensure delivery of hardcopy to the Buyer within 5 days of Bid End date / Bid Opening date.

15.3. Bidders can also submit the Tender Fee and EMD with Payment online through RTGS / internet banking to the following:

Beneficiary name: DIT Procurement

Account No.:0792201002351

IFSC Code: CNRB0000792

Internal

Bank Name: Canara Bank

Branch address: Trinity Circle Bangalore.

15.4. Bidder to indicate bid number and name of bidding entity in the transaction details field at the time of online transfer. Bidder has to send scanned copy / proof of the Online Payment Transfer along with bid.

15.5. As per the extant guidelines by Government, Micro and Small Enterprises (MSE) and Startup companies are exempted from submitting Earnest Money Deposit (EMD).

16. Submission of Bids

16.1. The sealed envelope containing the response to EOI along with the required documents shall be superscribed on the top of the envelope **"Expression of Interest for Empanelment of IT/ Cyber Security Auditors from CERT-In Empaneled Auditors from under Group A category for period of three (03) years in Canara Bank"**. The Name and address of the bidder should also be specifically mentioned on the top of the sealed envelope. The EOI response should be deposited in the Tender Box at the Place, Venue, Date and Time mentioned in the Bid details in brief description.

16.2. If the last day for submission of bids is declared as a holiday under NI Act by the Government subsequent to issuance of EOI, the next working day will be deemed to be the last day for submission of the EOI. The Bid/s which is/are deposited after the said date and time shall not be considered.

16.3. Bids sent through post/courier will not be accepted/evaluated. No offer will be accepted directly.

16.4. If envelope containing bid documents is not sealed and marked in the prescribed manner, the Bank will assume no responsibility for the bid's misplacement or premature opening.

16.5. The following officials will facilitate in bid related queries and make arrangements for deposit of bid documents.

First Official	Alternate Official
Senior Manager Canara Bank CP & VM Wing, First Floor, Naveen Complex, 14 M G Road, Bengaluru - 560 001. Tel - 080 25584873	Divisional Manager Canara Bank CP & VM Wing, First Floor, Naveen Complex, 14 M G Road, Bengaluru - 560 001.

16.6. In case bid documents are too bulky to be placed inside the tender box, arrangements will be made by the above-mentioned officials to receive the tender. However, bidder should reach the venue before the date and time stipulated in the Bid details in Bid schedule.

16.7. The bidder should make all the necessary arrangements to ensure that the sealed and marked tender documents are dropped in the Tender Box only at the Place, Venue, Date and Time mentioned in Bid schedule.

16.8. The bidder shall bear all costs associated with the preparation of and submission of the bid including cost of preparation/presentation etc. The Bank will not be responsible or liable for these costs, regardless of the conduct or outcome of the bidding process.

17. Bid Opening

17.1. EOI will be opened in the presence of the Bidder's representative/s who may choose to attend the bid opening as per schedule specified in the Bid details in brief description.

17.2. Bidder's representative may be present in the place and venue well in time along with an authorization letter in hand for each bid opening under this EOI, as per the format (Annexure-6) enclosed and sign in Register of Attendance during opening of EOI.

Note: Authorization letter should be carried in person and shall not be placed inside in any of the bid covers.

17.3. If any of the bidders or all bidders who submitted the tender are not present during the specified date, time and venue of opening, it will be deemed that such bidder is not interested to participate in the opening of the Bid/s and the bank at its discretion will proceed further with opening of the EOI in their absence.

17.4. The Bidders may note that no further notice will be given in this regard. Further, in case the bank does not function on the aforesaid date due to unforeseen circumstances or holiday, then the bid will be accepted up to 3.00 PM on the next working day and bids will be opened at 3:30 PM at the same venue on the same day.

18. Evaluation of EOI

18.1. The Bank will evaluate the bid/s submitted by the bidder/s under this EOI by the officers of the bank. The Bank may engage an external agency for evaluation of the bid. It is Bank's discretion to decide at the point of time.

18.2. The Bank will scrutinize the Bid/s received to determine whether they are complete in all respects as per the requirement of EOI, whether the documents have been properly signed and whether items are offered as per EOI requirements, whether technical documentation as required to evaluate the offer has been submitted. The Bank may, at its discretion, waive any minor non-conformity or any minor irregularity in the bid which does not constitute a material deviation. Bank's decision with regard to 'minor non-conformity' is final and the waiver shall be binding on all the bidders and the Bank reserves the right for such waivers.

18.3. EOI submitted by the bidder will be evaluated based on the documents mentioned in Annexure-1. Bidders who will qualify from Eligibility Criteria Evaluation will be empaneled. The short-listed applicants will be notified in due course. Only shortlisted applicants will be invited to participate in the tender/RFP. No interim enquiries will be entertained. The decision taken by the Bank shall be final and no representation or correspondence shall be entertained.

19. Erasures or Alterations

The Offers containing erasures or alterations or overwriting will not be considered. There should be no hand-written material, corrections or alterations in the offer. Technical details must be completely filled in. Correct technical information of the product being offered must be filled in. Filling up of the information using terms such as "OK", "accepted", "noted", "as given in brochure/manual" is not acceptable. The

Bank may treat such Offers as not adhering to the tender guidelines and as unacceptable.

20. Clarifications of Offers

20.1. During the process of scrutiny, evaluation and comparison of offers, the Bank may, at its discretion, seek clarifications from all the bidders/any of the bidders on the offer made by them. The request for such clarifications and the Bidders response will necessarily be in writing and it should be submitted within the time stipulated by the Bank.

20.2. The Bank may go through a process of evaluation and normalization of the bids to the extent possible and feasible, to ensure that shortlisted bidders are more or less on the same footing by seeking incremental bid submission in part of the requested clarification by the Bank OR Revised submissions of the entire bid in the whole.

20.3. The Bank can repeat this normalization process at every stage of bid submission till Bank is satisfied. The shortlisted bidders agree that, they have no reservation or objection to the normalization process and all the technically shortlisted bidders will, by responding to this EOI, agree to participate in the normalization process and extend their co-operation to the Bank during this process.

20.4. The shortlisted bidders, by submitting the response to this EOI, agree to the process and conditions of the normalization process.

21. Modification/Cancellation of EOI

21.1. The EOI is not an offer by Canara Bank but an invitation to get the response from the interested bidders for short listing the bidders for Bank's requirements. No contractual obligations whatsoever shall arise from the Expression of Interest process.

21.2. The Bank reserves the right to cancel EOI process at any time, without thereby incurring any liabilities to the affected bidder[s]. Reasons for cancellation, as determined by the Bank in sole discretion include but are not limited to, the following:

a. Services contemplated are no longer required

b. Change in the scope of work or due to unforeseen circumstances and/or factors and or/or new developments

c. The project is not in the best interest of the Bank

d. Any other reason

21.3. The Bank also reserves the right to modify/cancel/re-tender without assigning any reasons whatsoever. The bank shall not incur any liability to the affected bidder(s) on account of such rejection. Bank shall not be obliged to inform the affected bidder(s) of the grounds for the Bank's rejection.

22. Conflict of Interest

22.1. The bidders shall not receive any remuneration in connection with the assignment except as provided in the contract. The bidders and its affiliates shall not engage in auditing or other activities that conflict with the interest of the employer under the contract.

केनरा बैंक CANARA BANK Tender Processing Section C.P.&V.M. Wing, H.O., Bengaluru

22.2. Participation by IT/ Cyber Security Auditors with a conflict-of-interest situation will result in the disqualification.

22.3. The scope of work is defined on the understanding the requirement for engaging Auditor.

23. Responsibility for completeness:

23.1. The Bidder shall be responsible for any discrepancies, errors and omissions in the bid, or other information submitted by him irrespective of whether these have been approved, reviewed or otherwise accepted by the Bank or not. The Bidder shall take all corrective measures arising out of discrepancies, error and omissions in the bid and other information as mention above within the time schedule.

23.2. Willful misrepresentation of any fact within the Bid will lead to the disqualification of the Bidder without prejudice to other actions that Bank may take. All the submission, including any accompanying documents, will become property of Canara Bank.

23.3. The Bank reserves the right to verify the validity of bid information and to reject any bid where the contents appear to be incorrect, inaccurate or inappropriate at any time during the process of EOI or even after the award of contract.

24. Intimation to the successful Bidders:

The Bank will prepare the list of Bidders on the basis of evaluation. The short-listed applicants will be notified on the Bank's website (www.canarabank.com) /Notice Board. No separate intimation will be sent to individual Bidders.

25. Issuance of limited RFP/RFQ

25.1. Only shortlisted applicants will be invited to participate in the limited RFP/RFQ Process.

25.2. No interim enquiries will be entertained. The decision taken by the Bank shall be final and no representation or correspondence shall be entertained.

25.3. Canara Bank reserves the right to accept / reject any or all expression of interest received in response to this advertisement without assigning any reasons, whatsoever.

25.4. The Bank may issue limited RFP/RFQ to the shortlisted bidders as part of EOI. The Bank reserves the right to issue limited RFP/RFQ based on the responses and the requirement of the Bank.

25.5. The Bank reserves the right to avail services independently on its own without reference to shortlisted bidders of EOI.

26. Subcontracting

26.1. Principal bidder only can participate and bidder should not sub-contract to any other company/firm/trust. After Selection process of the bidder and order placement, resources deployed should be employed with the selected bidder and they should be on the payroll of the selected bidder.

26.2. The selected bidder shall not subcontract or permit anyone other than its personnel to perform any of the work, service or other performance required of

the selected bidder under the contract without the prior written consent of the Bank.

26.3. In case subcontracting is warranted in interest of the project, the selected bidder should take consent of the Bank before undertaking any such agreement. The selected bidder should further ensure subcontracting agreement is vetted by the Bank.

26.4. Even if the selected bidder gets into subcontracting, accountability and responsibility of the resource provided shall lie with selected bidder only. Bank shall hold correspondence only with the selected bidder.

26.5. The selected bidder should not sub-contract works to any contractor from a country which shares a land border with India unless such contractor is registered with the Competent Authority (refer: No.F.7/10/2021-PPD (1) dated 23/02/2023 of Public Procurement Division, Department of Expenditure, Ministry of Finance). Any false declaration and non-compliance of the above would be a ground for immediate termination of the contract and further legal action in accordance with the laws.

27. Social Media Policy

27.1. No person of the bank or the contractors and third parties shall violate the social media policy of the bank.

27.2. The following acts on the part of personnel of the bank or the contractors and third parties shall be construed as violation of social media policy:

27.2.1. Non-adherence to the standards/guidelines in relation to social media policy issued by the Bank from time to time.

27.2.2. Any omission or commission which exposes the Bank to actual or potential monetary loss or otherwise, reputation loss on account of non-adherence of social media related systems and procedures.

27.2.3. Any unauthorized use or disclosure of Bank's confidential information or data.

27.2.4. Any usage of information or data for purposes other than for Bank's normal business purposes and / or for any other illegal activities which may amount to violation of any law, regulation or reporting requirements of any law enforcement agency or government body.

28. Independent External Monitors:

28.1. The Name and Contact details of the Independent External Monitor (IEM) nominated by the Bank are as under:

Smt. Dolly Chakrabarty Email: dollychakrabarty@gmail.com	Sri. Hem Kumar Pande Email : hempande@hotmail.com

29. Exemptions for Micro & Small Enterprises [MSEs] & Start-Up:

As mentioned in Section-II of O.M. No.F.20/2/2014-PPD(Pt.) dated 20.09.2016 of Procurement Policy Division, Department of Expenditure, Ministry of Finance on Prior turnover and prior experience, relaxations may be applicable for all Micro & Small

Enterprises and start-ups [whether Micro & Small Enterprises (MSEs) or otherwise] subject to meeting of the quality and technical specifications specified in EOI document. The Micro & Small Enterprises (MSEs) and Startups are also exempted from submission of EMDs and tender fee subject to submission of documentary proof like Udyam Registration certificate, Certificate of recognition by department for promotion of industry and internal trade, Ministry of Commerce, GOI.

DEPUTY GENERAL MANAGER

Internal

Annexure-1

Checklist

The bidder shall confirm whether following are submitted in their bid. The bidder shall indicate the page no. where the details are furnished; otherwise, bid is liable for rejection.

Sl. No	Details	Reference/ Clause Nos	Complied & Submitted (Yes/No)	Page No. at which details are enclosed
1.	Covering Letter.	Annexure- 2		
2.	The documents in support of Eligibility criteria declaration, wherever required as mentioned in this EOI.	Annexure- 3		
3.	Technical Eligibility Criteria	Annexure- 4		
4.	Applicant's Profile	Annexure- 5		
5.	Authorization letter format for Bid Opening (to be carried by the person who is authorized to attend the Bid opening).	Annexure- 6		
6.	List of Major Customers of the Bidder and References	Annexure- 7		
7.	Office Details	Annexure- 8		
8.	Compliance Statement	Annexure- 9		
9.	Scope of Work	Annexure- 10		
10.	Tender fee and bid security declaration	Annexure-11		
11.	Escalation Matrix	Annexure- 12		
12.	Non-Disclosure Agreement	Annexure-13		
13.	Make in India Certificate	Annexure-14		
14.	Letter to return EMD	Annexure-15		
15.	Copy of Power of Attorney or Authorization letter from the Company designating the authorized representative of the company for signing the bid document should be furnished along with the bid document.			

Note: Failure to produce the necessary proof may render the applicant in-eligible for empanelment.

Internal

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

Sl. No.	Annexure-1: Other Clauses	Vendor Response [Yes/No]
1.	Whether Bidder has to submit Declaration as per **Annexure-11** in lieu of waiver of Tender fee & EMD?	
2.	Whether the Bid is authenticated by authorized person? Copy of Power of Attorney or Authorization letter from the company authorizing the person to sign the bid document to be submitted in Conformity to Eligibility Criteria?	
3.	Whether all pages are authenticated with signature and seal (Full signature to be affixed and not initials). Erasures/ Overwriting/ Cutting/ Corrections authenticated Certification/ Undertaking is authenticated?	
4.	Whether address of Office on which communication/ order has to be placed is indicated in **Annexure-5.**	
5.	Whether ensured that the offer is in sealed envelope and super scribed as **Expression of Interest for Empanelment of IT/ Cyber Security Auditors from CERT-In Empaneled Auditors under Group A category for period of three (03) years in Canara Bank** The EOI No., Name of the Bidder and Due date of the EOI is specified on the top of the envelope.	
6.	Whether ensured Indexing of all Documents submitted with page numbers?	

Bidders to verify the above checklist and ensure accuracy of the same before submission of the bid.

Checked for accuracy

Date

Signature with seal
Name :
Designation :

Note: The Authorization letter as per format Annexure-6 is to be carried in person and shall not be placed inside any of the bid covers.

Internal

केनरा बैंक Canara Bank

Annexure-2

Bid Covering Letter Format

(Covering Letter has to be submitted in company's letter head)

Offer Reference No:

Date: _____

To

The Deputy General Manager,
Canara Bank,
Centralized Procurement and Vendor Management Wing,
Naveen Complex, 14 M G Road,
Bengaluru - 560 001, Karnataka.

Dear Sir,

Sub: Expression of Interest for Empanelment of IT/ Cyber Security Auditors from CERT-In Empaneled Auditors under Group A category for period of three (03) years in Canara Bank

Ref: EOI 03/2024-25 dated 31/08/2024.

We have examined the above-mentioned tender document including all annexures, the receipt of which is hereby duly acknowledged and subsequent pre-bid clarifications/modifications /amendments, if any, furnished by the Bank and we, the undersigned, offer to get short listed for Expression of Interest for Empanelment of IT/ Cyber Security Auditors from CERT-In Empaneled Auditors under Group A category for period of three (03) years in Canara Bank with the said EOI.

The undersigned is authorized to sign on behalf of the Bidder Company and the necessary supporting documents delegating this authority is enclosed to this letter.

If our offer is accepted, we undertake to participate in the RFP/RFQ process to Security Auditors & Forensic Analyst for the below mentioned IT Audit Services but not limited to:

a. Vulnerability Assessment
b. Penetration Testing
c. Source Code Audit
d. Application /web/ mobile security Audit
e. Ethical Hacking
f. Forensic Audit
g. Incident Response
h. Cloud Security Assessment
i. Secure Configuration Review & Audit
j. API Functionality and Information Security Review
k. Gateway Audit (API Gateway, Payment Gateway etc.)
l. BCP / DR (Preparedness / Readiness) Audit

m. Network Audit including Virtualization, wireless, IoT & Mobile Technologies

n. Secure Architecture review

o. Software Composition Analysis

p. Network Security Audit

q. Database Audits

r. Migration Audit

s. ATM Infra Audit- Switch/ATM Terminals/ ATM Network

t. Vendor Security Risk Assessment

u. Open-Source Software /Tools Security Assessments

v. Comprehensive cyber-Security Audit

w. Any other activity including regulatory audit / assessment such as Advanced /New IT Technology, Cloud Technology, AI & ML Technology, Developing /Reviewing of Policies/ Procedure, Audit of Critical Infrastructure etc. as decided by the Bank during the empanelment period.

We agree to abide by and fulfill all the terms and conditions of the EOI and in default thereof, to forfeit and pay to you or your successors, or authorized nominees such sums of money as are stipulated in the conditions contained in EOI.

We enclose a list of Public Sector/ Private Sector Banks/BFSI in India (giving their full addresses of IT Department) to whom we have provided services of IT/Cyber Security Auditors.

We will not sub-contract works to any contractor from a country which shares a land border with India unless such contractor is registered with the Competent Authority (refer: F/No.6/18/2019-PPD dated 23/07/2020 of Public Procurement Division, Department of Expenditure, Ministry of Finance). We further understand that any false declaration and non-compliance of the above would be a ground for immediate termination of the contract and further legal action in accordance with the laws.

All the details mentioned by us are true and correct and if Bank observes any misrepresentation of facts on any matter at any stage, Bank has the absolute right to reject the proposal and disqualify us from the selection process. Bank reserves the right to verify /evaluate the claims made by the Bidder independently.

We confirm that we have noted the contents of the EOI and have ensured that there is no deviation in filing our response to the EOI and that the Bank will have the right to disqualify us in case of any such deviations.

We hereby undertake that we have not been blacklisted/debarred by any Scheduled Commercial Banks/Public Sector Undertakings/Government Entities in India as on date.

We hereby declare that the information submitted above is true to the best of our knowledge. We understand that in case any discrepancy is found in the information submitted by us, our Bid is liable to be rejected.

Date:
Place:

Signature with seal:
Name:
Designation:

Annexure-3

Qualification Criteria

(Eligibility Criteria Declaration has to be submitted in Company's letter head)

Sub: Expression of Interest for Empanelment of IT/ Cyber Security Auditors from CERT-In Empaneled Auditors under Group A category for period of three (03) years in Canara Bank

Ref: EOI 03/2024-25 dated 31/08/2024.

We have carefully gone through the contents of the above referred EOI and furnish the following information relating to Eligibility Criteria:

Sl. No.	Qualification Criteria	Documents to be submitted In compliance with Qualification Criteria
1.	The bidder (including OEM and OSD/OSO, if any) should either be Class-I or Class-II local supplier as defined in Public Procurement (Preference to Make in India) Revised Order (English) dated 16/09/2020.	Certificate of local content to be submitted as per Annexure-14 as applicable.
2.	The Company operating should be legally compliant company and can be: a. A partnership firm or a Limited Liability Partnership duly registered under the Limited Liability Partnership Act, 2008. (OR) b. Company duly registered in India as per Indian Companies Act, 1956 or Indian Companies Act, 2013. (OR) c. Proprietorship firm duly registered under the applicable shops and commercial Establishments Act and should be compliant to all the applicable laws.	Copy of Certificate of FIRM/LLP registration. (OR) Copy of Certificate of Incorporation and Certificate of Commencement of business in case of Public Limited Company or Certificate of Incorporation in case of Private Limited Company, issued by the Registrar of Companies. (OR) Copy of Certificate of registration under and Certificate of Commencement of business in case of Public Limited Company or Certificate of Incorporation in case of Private Limited Company, issued by the Registrar of Companies. For (c) Documentary proof for confirming registration of Proprietorship firm (e.g. Copy of Certificate of registration under shops and commercial Establishments Act., GST etc.)

Internal

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

Sl. No.	Qualification Criteria	Documents to be submitted In compliance with Qualification Criteria
3.	The bidder should have successfully carried out the services of Information security/Cyber security audit in at least 5 scheduled commercial banks (SCBs) during last 5 years.	Bidder has to submit copy of Purchase order and completion certificate.
4.	The bidder should be a CERT-In Empaneled vendor for continuous period of 5 years i.e., 2019 to 2024 as on date of submission of EOI.	Copy of List of Empaneled Information Security Audit Organizations by CERT-IN containing the name of the bidder.
5.	The bidder is required to ensure active empanelment throughout the 3 years' empanelment period. In the event of being de-empaneled by the CERT-In, the bank will also de-empanel the bidder.	Bidder has to submit an undertaking to this effect.
6.	The bidder should have average annual turnover of Rs.2 Crores during the last three (3) financial years (i.e., 2021-22, 2022-23 and 2023-24). This must be the individual company turnover and not of any group of companies.	Bidder has to submit audited Balance Sheet for last 3 Years i.e., 2021-22, 2022-23 and 2023-24. Bidder must produce a certificate from the Company's Chartered Accountant to this effect. The documents certified by Chartered Accountants should mandatorily contain Unique Document Identification Number.
7.	The bidder should not be owned by or controlled by any director/employee/ex-employee of the Bank or by any of their relatives.	Bidder has to submit an undertaking to this effect.
8.	The Bidder should have positive Net Worth as on 31/03/2024 and also should have not eroded by more than 30% in the last three financial years, ending on 31/03/2024.	The Bidder must produce a certificate from the Company's Chartered Accountant to this effect. The documents certified by Chartered Accountants should mandatorily contain Unique Document Identification Number.
9.	Bank shall not entertain Expression of Interest/ Proposals from Organizations or their subsidiaries who have supplied systems, system development, and maintenance and/ or integration related to IT or networking services or have rendered such services during the preceding 24 months to the Bank.	The Bidder should submit self-declaration on the Company's letter head to this effect.
10.	The bidder should have minimum 100 qualified professional with market standard certification (CISA, CISM, CISSP, CEH, CCNP, OSCP, CCSP, CRISC, CCAK) **Only employees involved in Operation work will be considered. Those employees working in Management or Administrative	HR Certificate (along with list and certifications of the employees and self-declaration forms of employees on their experience and qualifications/certifications)

Sl. No.	Qualification Criteria	Documents to be submitted In compliance with Qualification Criteria
	office will not be considered.	
11.	Bidder to provide undertaking that none of the proprietor/ partners/ directors of the bidder(s) is/are relatives of any member of the Bank's Board of directors.	Letter of Undertaking in company's letter head.
12.	Bidders should not be under debarment/blacklist period for breach of contract/ fraud/ corrupt practices by any Scheduled Commercial Bank/ Public Sector Undertaking/ State or Central Government or their agencies/ departments on the date of submission of this EOI.	The Bidder should submit self-declaration on the Company's letter head to this effect.
13.	Any Bidder (including OEM and OSD/OSO, if any) from a country which shares a land border with India will be eligible to bid, only if the Bidder (including OEM and OSD/OSO) are registered with the Competent Authority. Bidder (entity) from a country which shares a land border with India means: a. An entity incorporated, established or registered in such a country; or b. A subsidiary of an entity incorporated, established or registered in such a country; or c. An entity substantially controlled through entities incorporated, established or registered in such a country; or d. An entity whose beneficial owner is situated in such a country; or e. An Indian (or other) agent of such an entity; or f. A natural person who is a citizen of such a country; or g. A consortium or joint venture where any member of the consortium or joint venture falls under any of the above.	A declaration stating "We have read the clause regarding restrictions on procurement from a Bidder of a country which shares a land border with India. We further certify that we and our OEM are not from such a country or if from such a country, has been registered with Competent Authority. We hereby certify that we and our OEM fulfills all requirements in this regard and are eligible to be considered" to be submitted in Company's letter head. [Where applicable, evidence of valid registration by the Competent Authority shall be attached.]
14.	Authorization Certificate - Whether the Bid is authenticated by authorized person.	Bidder to submit a copy of the Power of Attorney or the Board Resolution and KYC documents evidencing the authority delegated to the authorized signatory.

We confirm that the information furnished above is true and correct. We also note that, if there are any inconsistencies in the information furnished above, the bid is liable for rejection. All documentary evidence/ certificates confirming compliance to Qualification Criteria should be part of the EOI.

Internal

Date:
Place:

Signature with seal
Name:

केनरा बैंक CANARA BANK Tender Processing Section C.P. & V.M. Wing, H.O., Bengaluru - 560 009 सी.पी. एवं वी.एम. विभाग, प्र.का., बेंगलूरु - 560 009

Annexure-4
Technical Eligibility Criteria

Sub: Expression of Interest for Empanelment of IT/ Cyber Security Auditors from CERT-In Empaneled Auditors under Group A category for period of three (03) years in Canara Bank

Ref: EOI 03/2024-25 dated 31/08/2024.

The EOI subject pertains to the Empanelment of IT/ Cyber Security Auditors from CERT-In Empaneled Auditors for the activities mentioned in the Scope of Work.

Activity-wise Weightage is given as below:

Sl. No.	Activities related to Information Security	Maximum Marks	Marks Obtained	Details required as per Clause
1.	Empanelment with Public Sector Banks (PSBs) as IT/Cyber Security Auditors	20		4A
2.	Empanelment in BFSI in India (excluding PSBs) as IT/Cyber Security Auditors	10		4B
3.	Certified & Skilled resources on payroll	15		4C
4.	Experience in handling different kinds of information security assignments	15		4D
5.	Experience in Specialized activities	15		4E
6.	Continuously empanelment with Cert-In for 10 years and above	10		4F
7.	Technical Presentation	15		4G
Total		100		

Bidders will be shortlisted on the basis of score allotted to them by the Bank based on technical evaluation wherein the bidder has to score a minimum of 75% and above.

Bidders who score less than 75% will not be considered for further evaluation. The Bank's decision on the score assigned to bidders during technical evaluation is final and cannot be contested.

After the empanelment process is completed, the Bank will float Request for Quotation (RFQ) among the empaneled vendors according to the specific requirements or activities. Subsequently, the works will be awarded based on the assessment of the commercial aspects involved in the process.

Internal

4A. Empanelment with PSB clients as IT/Cyber Security Auditors

#	Details	Scoring criteria	Maximum Marks	Marks Obtained
1.	Empanelment in Public Sector Banks as IT/ Cyber Security Auditors during last 5 years as on date of EOI.	No. of clients: •3 or more clients- 20 marks •2 clients - 15 marks •1 client - 10 marks	20	
Document to be submitted: Proof of empanelment by the means of Empanelment letter or any related document justifying empanelment.				

NB: The empanelment will be taken into consideration if the empanelment letter /document was issued in last 5 years only as on date of EOI.

4B. Empanelment in BFSI in India (excluding PSBs) as IT/Cyber Security Auditors

#	Details	Scoring criteria	Maximum Marks	Marks Obtained
1.	Empanelment in BFSI in India (excluding PSBs) as IT/Cyber Security Auditors during last 5 years as on date of EOI.	No. of clients: •5 or more clients - 10 marks •4 clients - 6 marks •3 client - 3 marks	10	
Document to be submitted: Proof of empanelment by the means of Empanelment letter or any related document justifying empanelment.				

NB: The empanelment will be taken into consideration if the empanelment letter /document was issued in last 5 years only as on date of EOI.

4C. Certified & Skilled resources on payroll

#	Details	Scoring criteria	Maximum Marks	Marks Obtained
1	Certified Skilled resources with relevant experience of at least 5 years having certifications (CISA / CISM / CISSP / CEH / CCNP / OSCP / CCSP/ CRISC / CCAK) and who are on payroll as on the date of EOI.	No. of certified resources: •≥ 50 - 15 marks • ≥ 40 & < 50 - 12 marks • ≥ 30 & < 40 - 10 marks • ≥ 20 & < 30 - 8 marks •< 20 - 0 marks	15	
Document to be submitted:				

- Supporting documents for above should be HR letter with consolidated list of resources mentioning certificates in force, overall experience, working with the organization since.
- The certified resource should be in the payroll of the organization for a minimum period of 1 year preceding the date of EOI.
- Only such experience should be described in the HR letter which are directly related to Scope of Work of this EOI

4D. Experience in handling various Information Security Assignments in last 5 Years as on the date of EOI.

#	Details	Score for No. of assessments done in India in BFSI/PSU domain (a)	Weightage (in %) (b)	Equivalent Score (c)	Scoring Criteria
1	VAPT		15		No. of assessments (a): •5 or more - 10 marks •4 - 8 marks •3 - 6 marks •2 - 4 marks •1 - 2 marks Formula for equivalent Score (c) = $\frac{\text{Marks obtained (a)}}{\text{Maximum marks (10)}}$ *Weightage (b)
2	Source Code Audit		15		
3	Web Application Security Testing, Mobile Application Security Testing		15		
4	API Assessment		15		
5	Forensic Audit		15		
6	Secure Configuration Audit, Secure Configuration Document review		10		
7	Cloud Security assessment / other IT security assessments		15		
		Total	100		
		Marks after Normalization	15		

Document to be submitted:

- Supporting documents for above should be Purchase Orders along with any of the following documents:
  - Invoice, or
  - Work completion letter or
  - SLA or
  - Letters from clients justifying work undertaken.

Internal

- Only such assignments will be considered which are directly related to Scope of Work of this EOI.

4E. Experience in Specialized activities in last 5 Years as on the date of EOI:

#	Details	Score for No. of assessments done in India in BFSI/PSU domain (a)	Weightage (in %) (b)	Equivalent Score (c)	Scoring Criteria
1	Regulatory security and Compliance audits like IRDAI, Data Localization Audit, PFRDA Audit, PCIDSS, ISO 27001-2013, DPDPA		25		No. of assessments (a): •5 or more - 10 marks •4 - 8 marks •3 - 6 marks •2 - 4 marks •1 - 2 marks Formula for equivalent Score (c): Marks obtained (a) / Maximum marks (10) *Weightage(c)
2	SWIFT infra-audits		20		
3	API Gateway Audit		10		
4	AD Assessment		10		
5	Ransomware Assessment		5		
6	NAC, WAF, Firewall audit/assessment		15		
7	Secure Architecture reviews		15		
		Total	100		
		Marks after normalization	15		

Document to be submitted:

- Supporting documents for above should be Purchase Orders along with any of the following documents:
  - invoice, or
  - work completion letter or
  - SLA or
  - letters from clients justifying work undertaken.
- Only such assignments will be considered which are directly related to Scope of Work of this EOI.

4F. Continuous empanelment with Cert-IN in previous years:

#	Details	Scoring criteria	Maximum Marks	Marks Obtained
1	Number of years continuously empaneled with Cert-In	No. of years: •≥ 10 years - 10 marks •≥ 8 years & < 10 years - 08 marks •≥ 5 years & < 8 years - 06 marks •< 5 years - No marks (Disqualification)	10	
Document to be submitted: • Supporting documents for above should be CERT-IN empaneled document.				

4G. Technical Presentation:

#	Details	Scoring criteria		Maximum Marks	Marks Obtained
1	Presentation and Demonstration of the proposed Audit to the Evaluation Committee	Methodology of audit:	3 Marks	15	
		Framework being followed to cover the scope:	3 Marks		
		Delivery timelines:	3 Marks		
		Recommendation for closure of the gaps:	3 Marks		
		Experience of the bidder and their resource for conducting similar audit:	3 Marks		

We confirm that the information furnished above is true and correct. We also note that, if there are any inconsistencies in the information furnished above, the bid is liable for rejection.

Date:

Place:

Signature with seal
Name :
Designation :

केनरा बैंक Canara Bank

Annexure-5

Applicant's profile

(Bidder's Profile has to be submitted in company's letter head)

Sub: Expression of Interest for Empanelment of IT/ Cyber Security Auditors from CERT-In Empaneled Auditors for period of three (03) years in Canara Bank.

Ref: EOI 03/2024-25 dated 31/08/2024.

Sl. No.	Particulars	Details
1)	Name of the Bidder	
2)	Constitution	
3)	Date of Establishment/ Incorporation	
4)	Whether in technical collaboration with Foreign Company? If so, give details	
5)	Number of Years in the Business	
6)	Number of years of experience in IT/Cyber Security Audit.	
7)	Address for Correspondence: Registered Office: Corporate Office:	
8)	Single Point of contact for this EOI and upcoming RFP/RFQ Name: Designation: Mobile No.: Landline No.: Fax: Email-ID (Any changes in the above should be informed in advance to Bank)	
9)	Domestic Customer Base (Number of Clients for Where Consultancy Service have been provided in India)	
10)	Details of Service Net Work Bengaluru: Mumbai:	
11)	PAN number GSTIN Beneficiary Bank Details Beneficiary Name	Internal

	Beneficiary Account Number Type of Account (OD/OCC etc.) IFSC Name of the Bank and Branch address	

Wherever applicable submit documentary evidence to facilitate verification.

We hereby declare that the information submitted above is true to the best of our knowledge. We understand that in case any discrepancy is found in the information submitted by us our Bid is liable to be rejected.

Date:
Place:

Signature with seal:
Name :
Designation :

Internal

केनरा बैंक Canara Bank

Annexure-6
Authorization Letter Format

(Authorization Letter Format has to submitted in Company's Letter Head)

To
The Deputy General Manager
Canara Bank,
Centralized procurement and Vendor Management Wing,
Naveen complex, 14 MG Road
Bengaluru - 560 001

Date: _____

Dear Sir,

Sub: Expression of Interest for Empanelment of IT/ Cyber Security Auditors from CERT-In Empaneled Auditors under Group A category for period of three (03) years in Canara Bank

Ref: EOI 03/2024-25 dated 31/08/2024.

This has reference to your above EOI for Empanelment of Security Auditors for Information Technology Security in your Bank.

Mr. / Miss/Mrs. _____is hereby authorized to attend the bid opening of the above EOI _____ DT: _____ on _____ on behalf of our organization.

The specimen signature is attested below:

_____
Specimen Signature of Representative

_____
Signature of Authorizing Authority

_____
Name & Designation of Authorizing Authority

_____

Place:

Internal

केनरा बैंक Canara Bank

Annexure-7

List of Major Customers and References

Sub: Expression of Interest for Empanelment of IT/ Cyber Security Auditors from CERT-In Empaneled Auditors under Group A category for period of three (03) years in Canara Bank

Ref: EOI 03/2024-25 dated 31/08/2024.

Sl. No.	Name and complete Postal Address of the Customer	Name, Designation, Telephone, e-mail address of the contact person (customer)	Nature and Description of the assignments/audit conducted during last 3 years	Satisfactory Letter from customer to be Enclosed or Purchase Orders to be enclosed
1	2	3	4	5

(Enclose necessary documentary proof)

Date:
Place:

Signature with seal:
Name:
Designation:

Internal

Annexure-8

Office Details

(Office Details has to be submitted in Company's Letter Head)

Sub: Expression of Interest for Empanelment of IT/ Cyber Security Auditors from CERT-In Empaneled Auditors under Group A category for period of three (03) years in Canara Bank

Ref: EOI 03/2024-25 dated 31/08/2024.

Sl. No.	Name of the Office/ Location	Postal Address and Telephone No's	E-mail ID of office	Service Facilities Available (Describe)	Number of Employees
1.					
2.					
...					

Date:
Place:

Signature with seal:
Name :
Designation :

केनरा बैंक Canara Bank

Annexure-9
Compliance Statement

(Compliance Statement has to submitted in Company's Letter Head)

To
The Deputy General Manager
Canara Bank,
Centralized Procurement and Vendor Management Wing,
Naveen complex, 14 MG Road
Bengaluru - 560 001

Date: _____

Dear Sir,

Sub: Expression of Interest for Empanelment of IT/ Cyber Security Auditors from CERT-In Empaneled Auditors under Group A category for period of three (03) years in Canara Bank

Ref: EOI 03/2024-25 dated 31/08/2024.

We understand that any deviations mentioned elsewhere in the bid will not be considered and evaluated by the Bank. We also agree that the Bank reserves its right to reject the bid, if the bid is not submitted in proper format as per subject

Sl. No.	Description	Complied (Yes/No)
1	Scope of Empanelment	
2	Empanelment procedure	
3	Instructions to the Applicants	

We hereby declare that the information submitted above is true to the best of our knowledge. We understand that in case any discrepancy is found in the information submitted by us our tender is liable to be rejected.

Date:

Signature with seal
Name :
Designation :

Internal

Annexure-10
Scope of Work

Sub: Expression of Interest for Empanelment of IT/ Cyber Security Auditors from CERT-In Empaneled Auditors under Group A category for period of three (03) years in Canara Bank

Ref: EOI 03/2024-25 dated 31/08/2024.

Types of present and future activities and services required by Bank are defined broadly in this EoI and are illustrative and indicative but not exhaustive. The Audit requirements and scope may also undergo changes/updates due to implementation of new products, technology, projects, configuration requirements, business needs, legal and regulatory requirements etc. Bidders are expected to update and include additional relevant items in these activities to conform to global best practices and currently available knowledge base. The detailed scope of each of the security audit services along with deliverables/reports would be provided during RFQ process

1. Common Deliverables:
   - 1.1. Clarifications
   - 1.2. Discussion
   - 1.3. Recommendations
   - 1.4. References / Rationale for recommendations
2. Reports would be in:
   - 1.1. Soft copies
   - 1.2. Hard copies - Two nos.
   - 1.3. Copies of screen shots, Outputs
   - 1.4. Audit evidence
   - 1.5. Soft outputs which are importable into a database, spreadsheet, or GRC platform e.g. XML files, CSV files etc.
   - 1.6. Tracking sheet
   - 1.7. Metrics and Dashboards
   - 1.8. Power point presentation
   - 1.9. Vulnerabilities identified
   - 1.10. Exploit Reports and supporting Evidences
   - 1.11. Vulnerability ratings
   - 1.12. Threat Profile and Threat Report
   - 1.13. Test Plan

1.14. Compliance profile covering compliance with Banks policies, legal and regulatory requirements (inclusive of RBI Guidelines on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds etc.)

1.15. Short Videos and Presentations for awareness sessions

1.16. Compliance requirements where applicable

1.17. Screenshots and code listing or line numbers where feasible in code reviews

1.18. Solutions with details and additional resources.

1.19. Recommendation, suggestions with references

1.20. Testing/Analysis process flow

1.21. The report should include but not limited to Executive Summary, Project Scope, Methodology, Environment testing, findings, severity, impact of risk and tools used for test etc.

1.22. All the reports submitted should be signed by technically qualified persons and accountable for the document/report submitted to the Bank

3. The brief scope, work description and deliverables of required services are given in as below:

3.1. Broadly the audits are conducted in view of applicable Regulatory requirements/ Industry best practices/Bank's internal policies as relevant to existing environment/ ISO 27001 /PCI-DSS/OWASP standards and other national/ international standards that are applicable to the Audit that is being conducted. Methodologies/ tools used should be industry approved; preferably those meeting the requirements of specific relevant standards;

3.2. Since every security audit has the purpose of assurance on the level of Information/cyber security preparedness, every audit should invariably consider the existing risk profile for each of the assets that are being audited, the controls available and deficiencies; the same should be documented along with recommendations for corrections as well as suggestions for improvement along with analysis details and proof of concepts/evidences.

A. Vulnerability Assessment:

A vulnerability assessment is the process of identifying, quantifying, and prioritizing the vulnerabilities in a system. Vulnerability assessment shall attempt to determine vulnerabilities all the systems/Assets to an intruder/attacker who has limited and/ or no previous knowledge of the Bank's network due to the existence of vulnerabilities in operating systems, database, networking and Security Infrastructure and their configurations/authentication systems/ access controls etc. This process may involve automated and manual techniques with varying degrees of rigor and an emphasis on comprehensive coverage. After fixing/rectification of vulnerabilities (which will be found during vulnerability assessment activity) by functional groups, VA Auditor has to do validate and check for all the reported observations for closure report. Quality audit has to be carried out on the observations, which are appearing repeatedly in VA Audit reports.

B. Penetration Testing:

The objective of the assessment is to determine the effectiveness of the security of organization's infrastructure and its ability to withstand an intrusion attempt. This may be achieved by conducting both reconnaissance and a comprehensive penetration test. After fixing/ rectification of vulnerabilities (which will be found during Penetration testing activity) by functional groups, PT Auditor has to do validate and check for all the reported observations for closure report. Quality audit has to be carried out on the observations, which are appearing repeatedly in PT Audit reports.

C. Source Code Audit:

For discovering hidden/unknown bugs, unsecure coding methods, coding flaws etc. which could prove to be potential source of vulnerabilities that could be exploited compromising the security of application leading to further compromise of database or ICT of organization as a whole. The audit includes listing of flaws, bugs etc. discovered, threat profiling for each application, exploiting the vulnerabilities listed out, providing the screen shots of exploitation, grading of the risk etc. Source code audit includes the vulnerabilities which can be detected early, reducing the risk of a security breach and to ensure that your application meets industry standards and regulations, reducing the risk of legal liability. After fixing/ rectification of vulnerabilities (which will be found during Penetration testing activity) by functional groups, Security Auditor has to do validate and check for all the reported observations for closure report. Quality audit has to be carried out on the observations, which are appearing repeatedly in Security Audit reports.

D. Application /web/ mobile security Audit:

The audit should consider the capability of application technical design and process flow to fulfil the requirement of business logic in effective and efficient manner and its security resilience. Testing includes the identification of weaknesses and vulnerabilities and provide fix/recommendation along with compliance with relevant standards like OWASP and other Industry standards for secured application and web services before they can be exploited. After fixing/ rectification of vulnerabilities (which will be found during Penetration testing activity) by functional groups, Security Auditor has to do validate and check for all the reported observations for closure report. Quality audit has to be carried out on the observations, which are appearing repeatedly in Security Audit reports.

E. Secure Configuration Review and Audit:

- Review and creation of the Bank defined Secure configuration documents which underline the Baseline security and industry best benchmarks such as CIS for the Bank's IT Assets.
- Audit for identification and ensuring that IT assets including operating systems, applications, databases and network devices are compliant with

Bank's Defined Secure Configuration Documents/Industry Benchmarks such as CIS etc. and Bank policies & guidelines. After fixing/ rectification of vulnerabilities (which will be found during Penetration testing activity) by functional groups, Security Auditor has to do validate and check for all the reported observations for closure report. Quality audit has to be carried out on the observations, which are appearing repeatedly in Security Audit reports.

F. Ethical Hacking:

Ethical Hacking should include systematic attempts to penetrate the application/ Assets to find the security vulnerabilities that a malicious hacker can exploit. The scope of Ethical Hacking should include but not limited to:

- Attempts to penetrate the application/ Assets and find the vulnerabilities in the application.
- Attempt to guess passwords using Password Cracking tools.
- Attempt to overload the systems using DOS and DDoS Techniques. The attempt should be limited to the application only and should not impact other infrastructure of the Bank.
- Attempt to search for backdoor traps in programs.
- 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.
- A test plan should be shared with the Bank including the methodology, tools used and prerequisites for conducting the test.
- Only licensed version of reputed software/ tools should be used for conduct the test.
- Ethical hacking of the web applications/ Assets should also cover commonly available vulnerability index such as OWASP Top 10 and SANS Top 25.

G. Forensic Audit:

The audit involves identifying, preserving, recovering, analyzing and presenting facts and opinions about the digital information on specific or across various IT systems, applications, Databases, Websites, interfaces etc. providing the chain of evidence with verifiable documents; provide inputs to the Bank on forensic preparedness.

H. API Functionality and Information Security Review:

The audit should consider the capability of application technical design and process flow to fulfil the requirement of business logic in effective and efficient manner and its security resilience. Testing includes the identification of weaknesses and vulnerabilities and provide fix/recommendation along with

compliance with relevant standards like OWASP and other Industry standards for secured application, API and web services before they can be exploited. After fixing/ rectification of vulnerabilities (which will be found during Penetration testing activity) by functional groups, Security Auditor has to do validate and check for all the reported observations for closure report. Quality audit has to be carried out on the observations, which are appearing repeatedly in Security Audit reports.

I. **BCP/DR preparedness/Readiness Audit:**

- Review existing BCP policy of Bank and the implementation; Review against requirements of relevant ISO and other standards; identify the deficient processes and procedures and recommend measures to correct and improve the systems and procedures for ensuring Business continuity without compromising the requirement for confidentiality, integrity and authenticity/audit- ability.
- Backup procedure Review

J. **Network Audit including Virtualization, wireless IoT & Mobile Technologies:**

The audit should include at minimum analysis of Network (wired/wireless) architecture for adequacy/appropriateness of the technologies deployed, capacity planning and redundancies, review of traffic flow, network performance, Configuration of network devices and network security devices, intranet/internet/extranet policies/controls, review of layered defense, routing policies, access controls, review of baseline security configurations/practices of architecture, devices in line with industry standards and relevant to Bank's environment etc. provide the deficiencies, flaws in terms of availability, confidentiality and authenticity, threat profiling, risk assessment and proportionate controls/ compensatory controls; recommendations for improvement.

K. **Database Audit and Migration Audit:**

The database audit should broadly review authentication, access controls, audit, logging and tracing, patch management, remote access policies, configurations, encryption mechanisms, redundancy and back up procedures etc. The migration audit involves auditing the completeness and accuracy of migrating the legacy data to new solutions; verifying and tallying the legacy environment with newer environment to which data is migrated to as and when the migration takes place; review that the controls that existed in legacy data are in place in new environment and the controls that are specific for new environment are also addressed.

L. **Comprehensive Cyber Security Audit:**

The audit includes verifying the Cyber Security preparedness of the Bank against the Gap assessments conducted (internal/external), the regulatory requirements in terms of policy and practices; the regulatory requirements include both Indian and US Information/Cyber Security laws as applicable.

M. Comprehensive IT and IS Audits including Outsourced Activities and Third-Party Audits:

Evaluating the effectiveness/adequacy of planning and oversight of IT activities that include operating processes, internal controls, Security policies; verifying the Risk assessment processes and whether the controls are in proportion to the risk assessed. IS Audits on the Bank assets, complying with the regulatory/Bank Guidelines & policies.

N. Software Composition Analysis (SCA) Assessment:

A Software Composition Analysis (SCA) Assessment is crucial for identifying and managing risks associated with the use of open-source and third-party components in software development. Below is a brief outline of the scope of work but not limited to below:

- Identify all open-source and third-party components used within the software.
- Assess the licensing compliance of the software components.
- Detect known vulnerabilities and security risks associated with the components.
- Scanning the identified components against known vulnerability databases (e.g., NVD, CVE databases).
- Evaluation of the legal, security, and operational risks associated with each component.
- Prioritization of risks based on the severity and potential impact on the software.
- Identification of outdated components or components with known vulnerabilities.
- Examination of the licenses of all identified components.
- Identification of any non-compliant, conflicting, or high-risk licenses.
- Provide remediation recommendations to address identified risks.

O. API Gateway Audit:

The scope of work for an API Gateway Security and Risk Audit involves a thorough evaluation of the API gateway's security posture, identifying potential risks, and ensuring that it aligns with industry best practices and compliance requirements. Below is a brief outline of the scope of work but not limited to below:

- Assess the security controls and configurations of the API gateway.
- Identify vulnerabilities and potential risks that could impact the confidentiality, integrity, and availability of APIs.
- Ensure compliance with relevant industry standards and regulatory requirements.

- Authentication, authorization, and encryption mechanisms.
- Logging, monitoring, and alerting configurations.

- Identify applicable regulatory frameworks (e.g., GDPR, PCI-DSS) and industry standards (e.g., OWASP API Security Top 10) relevant to the API gateway.
- Access Control and Authentication
- Evaluate the effectiveness of authentication mechanisms (e.g. Ensure that all sensitive data transmitted through the API gateway is encrypted using strong encryption protocols (e.g., TLS 1.2/1.3).
- Evaluate the encryption of sensitive data at rest within the API gateway infrastructure.
- Review the implementation of role-based access control (RBAC) and least privilege
- Verify that proper authorization mechanisms are in place to restrict access based on user roles and permissions.
- Review input validation mechanisms to prevent injection attacks (e.g., SQL injection, XML external entity injection).
- Assess how the API gateway handles untrusted input and sanitizes data before processing.
- API Rate Limiting and Throttling
- Security Monitoring and Logging
- Review the API gateway configuration for security best practices, including secure defaults, least privilege access, and disabling unnecessary services.
- Check for misconfigurations that could expose sensitive data or allow unauthorized access.
- Review the API gateway configuration for security best practices, including secure defaults, least privilege access, and disabling unnecessary services.
- Conduct a threat modelling exercise to identify potential threats and vulnerabilities in the API gateway and associated APIs.
- Perform automated and manual vulnerability scans on the API gateway to identify known security issues.
- Map identified threats to relevant security controls to determine the effectiveness of existing measures.
- Review the API gateway's adherence to relevant regulatory requirements (e.g., GDPR).
- Identify any gaps in compliance and provide recommendations for remediation.
- Compare the API gateway's security posture against industry best practices and standards (e.g., OWASP API Security Top 10).
- Recommend improvements based on identified deviations from best practices.

P. Payment Gateway Audit

The scope of work for Payment Gateway Audit is mentioned below (but not limited to):

1. Conduct security assessments like VAPT, Secure Configuration, System Hardening, etc. for the PG Infrastructure.
2. Assess the security posture and controls of the PG architecture and application.
3. Review of the Network Architecture of PG Infrastructure.
4. Review the compliance to the various regulatory guidelines & bank policies (For ex. Backup Policy, Encryption Standards, Data Tokenization, Key Management, etc.).
5. Evaluation of compliance with relevant industry regulations or guidelines such as RBI, PCI DSS, SOC, Data Localization etc.
6. Review data retention, consent management, and user rights processes.
7. Review as per the industry best practices such as NIST, ISO, CIS Benchmark, etc.
8. Review Vulnerability management and patching processes, Incident Response Procedures.
9. Review IAM & access control measures (authentication, authorization).
10. Review the effectiveness of fraud detection and prevention mechanisms.
11. Review processes for monitoring and responding to suspicious activities.
12. Review the accuracy of transaction records, including logging, error handling, and reconciliation processes.
13. Review the effectiveness of disaster recovery and business continuity plans related to the payment gateway.
14. Review of testing and validation of backup and recovery processes.
15. Review policies and procedures for handling cardholder data.
16. Review of any exceptions in the PG infrastructure.
17. Identify vulnerabilities, weakness, risk in the PG infrastructure/ architecture, along with the criticality for the same.

Q. Secure Architecture Review

The scope of work for Secure Architecture Review (SAR) is mentioned below (but not limited to):

1. Thorough analysis of the banking and associated setup infrastructure to ensure that it is secure, working efficiently and complying to the regulatory guidelines and the industry best practices.
2. Assess the security posture and controls of the organization's architecture and application.
3. Review of the Network Architecture incl. network topology, network components, ports & protocols, network segregations, security controls, etc.
4. Review of the application architecture & design principals of the bank incl. 3 Tier Architecture, secure data flow between different components of the applications, etc.

5. Review of the Cloud infrastructure/architecture incl. integration with on-prem setup, secure configuration, etc.
6. Review of the Security Architecture of the bank incl. IAM, security solutions etc.
7. Evaluation of compliance with relevant industry regulations or guidelines such as RBI, PCI DSS etc.
8. Review as per the industry best practices such as NIST, ISO, CoBIT, CIS Benchmark, etc.
9. Review of any exceptions in the organization infrastructure.
10. Identify vulnerabilities, weakness, risk in the infrastructure/ architecture, along with the criticality for the same.

R. ATM Infra Audit- ATM Switch/Terminal/Network Audit:

The Audit should aim at discovering the vulnerabilities in ATM switch, Terminals and Network covering the Operating system, configurations, interfaces etc. including the access controls and process flow.

An ATM infrastructure Audit (ATM terminal and network audit) involves a comprehensive review of the entire ATM system to ensure it operates efficiently, securely, and in compliance and regulator standards. Below is a detailed scope of work for such an audit:

- Analyze the architecture of the ATM network, including connectivity to the Bank's core systems.
- Check the configuration and effectiveness of firewall and Intrusion detection systems / Intrusion prevention system.
- Verify that communications between the ATM and the bank's data centre are encrypted and secure.
- Review the procedures in place for detecting and responding to security incidents involving the ATM network.
- Assess the physical security of ATM locations, including CCTV coverage, lighting, alarm systems, and access controls.
- Evaluate the security measures of the ATM terminals themselves, including locks, tamper-evident seals, and anti-skimming devices.
- Review the processes and protocols for cash replenishment and storage at ATMs.
- Inspect the physical condition and specifications of ATM hardware, including the dispenser, card reader, keypad, screen, and receipt printer.
- Verify that the ATM software is up-to-date with the latest security patches and compliant with industry standards.
- Review data encryption protocols and assess how sensitive customer information is handled during transactions.
- Ensure that all ATMs and network components comply with relevant regulations (PCI-DSS, EMV, etc.).
- Assess the compliance with data protection regulations, including GDPR (if applicable).
- Verify that proper logging is in place for all ATM transactions and that audit trails are securely stored and accessible for review.

- Review logs to determine the frequency and causes of ATM downtimes and assess the effectiveness of the response.
- Compare ATM transaction times and performance against industry standards or benchmarks.
- Review the disaster recovery plans related to ATM operations and ensure backups are in place for critical data.
- Review the SLAs in place with vendors to ensure they are being met and are adequate.
- Assess risks associated with third-party access to the ATM network and data.
- Identify any gaps by performing VA & PT for the all assets (servers, network devices and applications) involved in ATM infrastructure.
- Detect the checks by secure configuration audit on Servers, databases, network devices and Middleware.
- Provide a risk assessment based on the audit findings and recommend mitigation strategies.
- Check ATM malware traces in ATM machines by selecting random 5-10 ATM locations.

S. Network Security Audit:

A Network Security Audit involves a systematic review and evaluation of an organization's network infrastructure, practices, and security controls to identify vulnerabilities, ensure compliance with policies and standards, and recommend improvements. Below are the brief Scope of Work for a Network Security Audit but not limited to that:

- Assess the current network security posture, identify vulnerabilities, ensure compliance with industry standards and regulations, and provide actionable recommendations for improvements which includes , Network Architecture Review, Perimeter Security review, Endpoint Security review, Access Control review, Data Protection, Patch Management and Vulnerability Management, Firewall review, Third-Party and Remote Access Security review, Compliance and Policy Review, Physical Security, Network Security, Configuration Review, Secure Device Configuration review etc.
- Conduct a comprehensive examination of the network's design, including all LAN, WAN, wireless, and cloud components.
- Advanced Segmentation Analysis: Evaluate network segmentation down to the micro-segmentation level, ensuring that even the smallest network segments are properly isolated and secured.
- Traffic Flow Analysis: Analyze network traffic patterns to identify any unusual or potentially malicious activity, using both real-time monitoring and historical data.
- Deep Configuration Analysis: Perform an in-depth assessment of firewalls, IDS/IPS, VPNs, and DMZs, including detailed rule set reviews and testing for configuration errors.

- Advanced Penetration Testing: Conduct sophisticated penetration testing, simulating advanced persistent threats (APTs) and zero-day attacks to test perimeter and internal defenses.
- behavioral analysis tools to detect anomalies and potential insider threats.
- Analyze access control mechanisms in detail, focusing on least privilege principles, RBAC policies, MFA enforcement, and identity and access management (IAM) practices.
- Evaluate the controls around privileged accounts, including PAM (Privileged Access Management) solutions, audit trails, and access review processes.
- Perform proactive threat hunting exercises, using advanced tools and techniques to identify hidden threats and compromise indicators within the network.
- Firewall access review controls, rules review.
- Evaluate the encryption mechanisms for data at rest, in transit, and during processing, ensuring compliance with industry best practices and Create a detailed map of data flows within the organization, identifying potential risks associated with data storage, transmission, and processing.
- Review the physical security measures in place to protect network infrastructure, including access controls, surveillance systems, and environmental controls
- Perform advanced network vulnerability scans, deep packet inspection, and detailed configuration reviews.
- Utilize machine learning and AI-based tools for anomaly detection and behavioral analysis.
- Conduct in-depth forensic analysis of logs, network traffic, and endpoint data.
- Review of Unrestricted access to network systems, devices, etc.

T. Open-Source Tool/Software Assessment:

Conducting a cybersecurity assessment specifically focused on open-source software (OSS) and tools involves evaluating the security posture of the OSS components used within an organization.

- Compile a comprehensive list of all open-source software and tools used within the organization, including direct and transitive dependencies.
- Identify the versions of all OSS components in use to determine their currency and relevance to security.
- Review the licenses associated with each OSS component to ensure they are compatible with the organization's policies and legal requirements.
- Ensure that the use of OSS complies with licensing terms, particularly with regard to distribution, modification, and commercialization.
- Identify and document any known vulnerabilities associated with the OSS components by cross-referencing with public vulnerability databases (e.g., CVE, NVD).

- Conduct vulnerability scans on OSS components to detect unpatched security flaws.
- Analyse vulnerabilities in the dependencies of OSS components, as they can indirectly affect the security of the primary software.
- Perform static analysis of the OSS codebase to identify potential security issues such as insecure coding practices, buffer overflows, or injection flaws.
- Conduct dynamic analysis (e.g., fuzz testing) to detect runtime vulnerabilities, memory leaks, or unexpected behaviour.
- In high-risk areas, perform a manual review of the source code to detect complex security issues that automated tools may miss.
- Assess the default and current configurations of OSS components to ensure they are securely configured.
- Provide recommendations or follow existing hardening guides to improve the security posture of the OSS components.
- Evaluate the feasibility and security implications of automated update mechanisms for OSS components.
- Review the patch status of OSS components and ensure all critical patches have been applied.
- Review logs for signs of security incidents or unusual behaviour related to OSS components.
- Ensure that adequate logging is enabled for OSS components to capture security-relevant events for future forensic investigation.
- Review the access control mechanisms in place for OSS components, ensuring that least privilege principles are applied.
- Assess the implementation of authentication and authorization processes within the OSS components. Evaluate how well OSS components integrate with existing security infrastructure (e.g., firewalls, IDS/IPS, DLP).
- Prioritize OSS components based on their risk profile, considering factors such as exposure, criticality, and likelihood of exploitation. Implement continuous monitoring of OSS repositories for changes, new vulnerabilities, or security advisories.
- Verify the integrity and authenticity of the source code for OSS components, including checks for tampering or malicious code insertion.
- Assess the security of the supply chain for OSS components, particularly the risks associated with third-party dependencies.
- Review or develop incident response plans that include specific procedures for dealing with security incidents involving OSS components.
- Deliver a detailed report outlining the findings of the security assessment, including identified vulnerabilities, compliance issues, and configuration weaknesses.

U. Incident Response and Management

1. Review the Incident Management policies, processes and procedures.

2. Review Incident detection capability.
3. Review Incident handling process, SOC team structure and skillset.
4. Review Incident handling timelines against the defined processes.
5. Review the general Incident Response Preparedness
6. Review information Security related user awareness training
7. Review the Effectives of Communication and Decision Making during Incidents
8. Find the gaps in the Incident Response Process
9. Evaluate SOC Metrics

V. Vendor Security Risk Assessment

- **Vendor Profile:** Asses vendor's background, financial stability, reputation, available resource, history of compliance etc.,
- **Compliance:** Ensure the Vendor complies with relevant rules & regulations and industry specific standards and Data Protection Laws as applicable.
- **Security Measures:** Evaluate Vendor's Cyber Security practices and data protection measures to prevent breaches or data leaks. Industry standard certifications like ISO 27001, ISO 22301, ISO 31000 etc., Also assess Physical and Operational Security aspects.
- **Cloud Services Management and Security Considerations:** Verify implementation of Industry best cloud security practices like The Open Group, IDRBT-Cloud Security Framework, ISO 27017.
- **Contingency Planning:** Ensure the vendor has adequate business continuity and disaster recovery plans in place. (DR Drills, BIA, Scenario & Stress Testing activities).
- **Performance Metrics:** Monitor and assess the vendor's performance against the agreed upon service levels and deliverables.
- **Audit and Monitoring:** Ongoing monitoring an auditing process to continuously assess vendor risk.
- **SLAs/NDAs:** Incorporate clauses like during Onboarding assess inherent risk before granting access to critical assets/data. During Offboarding, ensure that access is terminated and data has been protected or destroyed.
- **Incident Management:** Verify if any incidents occurred in the history and assess the impact and recovery of the vendor from the incident. Incident Management Mechanism should be defined and the same to be in place.

W. Any other activity/audit such as Advanced /New IT Technology, Cloud Technology, AI & ML Technology, Developing /Reviewing of Policies/Procedure, Audit of Critical Infrastructure etc. as decided by the Bank during the empanelment period.

a. <u>Cloud Assessment:</u>

Evaluation the Cloud and infrastructure and security controls. Assess all workloads and performance in IT environment - both physical and virtual, including VMs, historical use data, core network infrastructure, servers, and data centers. Evaluating and provide recommendations for the access controls, misconfigurations, vulnerability management, identity and access permissions, and compliance standards, security controls implementation and Improve safety and complying with the regulatory/Bank Guidelines & policies.

b. **Review of policy/procedures:**

Evaluating the effectiveness/adequacy of planning and oversight of IT activities that include operating processes, internal controls, Security policies. Assistance with the implementation of the new or modification/review of process and procedures.

c. **Regulatory audit/Risk assessment:**

Various system / functional audits mandated by regulatory bodies such e.g. RBI, SEBI, NABARD, UIDAI / governing bodies / Government etc. An illustrative list of such audits is given below:

- Cyber security and cyber resilience audit of Treasury
- Special audit of dealing room and the System in operation (As per guidelines of RBI)
- Storage of Payment data in India
- Annual System Audit of Depository
- Kiosk Banking Solution audit of Canara Bank and sponsored RRB as per UIDAI guidelines
- Tokenization's/SAR Report of Cards
- Audit of Customer service program for SWIFT
- Audit of implementation of Information & Cybersecurity Guidelines for Insurance intermediaries
- SWIFT's Customer Security Program (CSP)
- Assessing the VPN Connectivity and WFH Setup configuration and parameters
- Active Directory Assessments
- Assisting in assessing Incident response readiness and preparing a robust Incident Response Plan.
- Any other audit directed by regulatory bodies, governing bodies / Government etc.

d. **Others:**

In view of various guidelines for varying Audits of ICT infrastructure, End to End Assessment of Applications, Blockchain technology related, SAST or Software Composition Analysis (SCA) Scan, DAST (Dynamic Application Security Testing), Red Team - Blue Team Exercise, activities offering implementation of complex architecture, Advance/New IT technology, Cloud technology, AI & ML technology, Audit of critical infrastructure etc. or similar kind of activities.

4. Bank may, during the empanelment period may require specific audit services as and when the same are mandated by applicable Regulatory authorities. The requirement for such new audits may also arise out of introduction of new technologies in to the existing environment. Bank may avail such services which should be completed in timely manner as required/stipulated by the Bank.
5. Vendor has to use standard procedures like comply with Bank's information security policy while conducting the assessment and should take adequate security measures to ensure confidentiality of the information.
6. Bank will float limited tenders amongst the qualified empaneled vendors and seek responses for various requirements. Individual tender/s will contain detailed terms and conditions, instructions, location details and scope of work. Such limited tenders shall be floated by Bank.

We hereby comply with the above Scope of Work without any deviations. Non-compliance to any of the scope of work will lead to disqualification of the bidder for empanelment.

Date:
Place:

Signature with seal
Name :
Designation :

केनरा बैंक Canara Bank

Annexure-11

Tender Fee and Bid Security Declaration

(To be provided on letter head)

To,

The Deputy General Manager
Canara Bank,
Centralized Procurement and Vendor Management Wing,
Naveen complex, 14 MG Road
Bengaluru - 560 001

Date: _____

Sub: Expression of Interest for Empanelment of IT/ Cyber Security Auditors from CERT-In Empaneled Auditors f under Group A category for period of three (03) years in Canara Bank.

Ref: EOI 03/2024-25 dated 31/08/2024.

Dear Sir

We declare that if we withdraw or modify our Bids during the period of validity, or if we are awarded the contract and we fail to sign the contract, or to submit a performance security before the deadline defined in the EOI, we note that we will be suspended for the period of three years from being eligible to submit Bids for contracts with Canara Bank.

Place:
Date:

[Signature of Authorized Signatory]
Name:
Designation:
Seal:

Internal

केनरा बैंक Canara Bank

Annexure-12

Escalation Matrix

(Should be submitted on Company's letter head with company seal and signature of the authorized person)

SUB: Expression of Interest for Empanelment of IT/ Cyber Security Auditors from CERT-In Empaneled Auditors under Group A category for period of three (03) years in Canara Bank

Ref: EOI 03/2024-25 dated 31/08/2024.

For Service Related Issues
Name of the Bidder Firm:

Sl. No.	Name	Level of Contact	Office Postal Address	Phone No.	Mobile No.	Fax	Email address
a.		First Level Contact					
b.		Second level contact (If response not received in 4 Hours)					
c.		Regional/Zonal Head (If response not received in 24 Hours)					
d.		Country Head (If response not received in 48 Hours)					

Any change in designation, substitution will be informed by us immediately.

Date:
Place:

Signature with seal
Name:
Designation:

Internal

केनरा बैंक Canara Bank

Annexure-13

Non-Disclosure Agreement

(Should be submitted on Company's letter head with company seal and signature of the authorized person)

SUB: Expression of Interest for Empanelment of IT/ Cyber Security Auditors from CERT-In Empaneled Auditors under Group A category for period of three (03) years in Canara Bank

Ref: EOI 03/2024-25 dated 31/08/2024.

WHEREAS, we, _____, having Registered Office at _____, hereinafter referred to as the Bidder, are agreeable to the provide services/ deliverables as per terms mentioned in the EOI to Canara Bank, having its office at 14, Naveen complex, HO(annex), M.G Road Bengaluru -560001 hereinafter referred to as the BANK and,

WHEREAS, the Bidder understands that the information regarding the Bank's IT Infrastructure shared by the BANK in their EOI/RFP/RFQ is confidential and/or proprietary to the BANK, and

WHEREAS, the Bidder understands that in the course of submission of the offer for the subject EOI/RFP/RFQ and/or in the aftermath thereof, it may be necessary that the Bidder may perform certain jobs/duties on the Banks properties and/or have access to certain plans, documents, approvals or information of the BANK; NOW THEREFORE, in consideration of the foregoing, the Bidder agrees to all of the following conditions, in order to induce the BANK to grant the Bidder specific access to the BANK's property/information. The Bidder will not publish or disclose to others, nor, use in any services that the Bidder performs for others, any confidential or proprietary information belonging to the BANK, unless the Bidder has first obtained the BANK's written authorization to do so.

The Bidder agrees that notes, specifications, designs, memoranda and other data shared by the BANK or, prepared or produced by the Bidder for the purpose of submitting the offer to the BANK for the said solution, will not be disclosed during or subsequent to submission of the offer to the BANK, to anyone outside the BANK.

The Bidder shall not, without the BANKs written consent, disclose the contents of this Request for Proposal (Bid) or any provision thereof, or any specification, plan, pattern, sample or information (to be) furnished by or on behalf of the BANK in connection therewith, to any person(s) other than those employed/engaged by the Bidder for the purpose of submitting the offer to the BANK and/or for the performance of the Contract in the aftermath. Disclosure to any employed/engaged person(s) shall be made in confidence and shall extend only so far as necessary for the purposes of such performance.

Date:
Place:

Signature with seal
Name:
Designation:

Internal

केनरा बैंक Canara Bank

Annexure-14

Make in India Certificate

(Should be submitted on Company's letter head with company seal and signature of the authorized person)

Bidder's Reference No._____ Date.....

To,
The Deputy General Manager
Canara Bank,
Centralized Procurement and Vendor Management Wing,
Naveen Complex,
14 M G Road,
Bengaluru - 560 001, Karnataka.

SUB: Expression of Interest for Empanelment of IT/ Cyber Security Auditors from CERT-In Empaneled Auditors under Group A category for period of three (03) years in Canara Bank

Ref: EOI 03/2024-25 dated 31/08/2024.

Dear Sir/Madam,

(To be certified by statutory auditor or cost auditor of the company (in the case of companies) for a tender value above Rs.10 crores giving the percentage of local content.)

1. In line with Government Public Procurement Order No. P-45021/2/2017-PP (BE-II) dated 16.09.2020 and its amendments, we hereby certify that we M/s _____ are local supplier meeting the requirement of minimum local content i.e., _____% against Canara Bank Tender No..... dated..... We qualify as a _____ (Class-I or Class II) local supplier. Details of location at which local value addition will be made as follows: _____.

2. We also understand, false declarations will be in breach of the code of integrity under rule 175(1)(i)(h) of the General Financial Rules for which a bidder or its successors can be debarred for up to two years as per Rule 151(iii) of the General Financial Rules along with such other actions as may be permissible under law.

3. We have submitted the details indicating total cost value of inputs used, total cost of inputs which are locally sourced and cost of inputs which are imported, directly or indirectly with the commercial proposal.

Place:
Date:

[Signature of Authorized Signatory of Bidder]
Name:
Designation:
Seal:

Internal

केनरा बैंक CANARA BANK Tender Processing Section C.P. & V.M. Wing, H.O., Bengaluru - 560 001

केनरा बैंक Canara Bank

Annexure-15

Letter to Return EMD (if applicable)

[On Firm's / Company's letter head]

To,
The Deputy General Manager
Canara Bank,
Centralized Procurement and Vendor Management Wing,
Naveen Complex,
14 M G Road,
Bengaluru - 560 001, Karnataka.

SUB: Expression of Interest for Empanelment of IT/ Cyber Security Auditors from CERT-In Empaneled Auditors under Group A category for period of three (03) years in Canara Bank

Ref: EOI 03/2024-25 dated 31/08/2024.

We _____ (Company Name) had participated in the EOI for **Empanelment of IT/ Cyber Security Auditors from CERT-In Empaneled Auditors under Group A category for period of three (03) years in Canara Bank.**

Details of EMD submitted are as follows:

Sl. No.	Bidder Name	BG/DD/NEFT/RTGS Ref No.	Drawn on Bank Name	Date of BG/DD/NEFT/RTGS	Amount in Rupees

Bank details to which the EMD amount to be returned via NEFT/RTGS are as follows:

Account Title/Name	
Account Number	
IFSC Code	
Account Type	
Name of the Bank with Branch Address	

Declaration:

1. We here by note that the EMD submitted will be returned as per the terms and conditions of the EOI.

2. We hereby confirm that the information submitted above is true to the best of our knowledge. We understand that in case any discrepancy is found in the information submitted by us Bank is not liable under any circumstances.

Date:
Place:

Signature with seal
Name:
Designation:

Internal

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