REQUEST FOR EXPRESSION OF INTEREST

FOR

EMPANELMENT OF IT / CYBER SECURITY AUDITORS

Issued by: Canara Bank,
Asset Procurement & Management Group,
Department of Information Technology Wing,
1st Floor, Naveen Complex,
14, M G Road,
Bengaluru - 560 001.
Email : hoditapm@canarabank.com
Phone No: 080-25590070

Bid Details in Brief Description

Sl. No.	Description	Details
1.	EOI No.	EOI 01/2017-18 dated 24/01/2018
2.	Brief Description of the EOI	Request for Expression of Interest for Empanelment of IT/Cyber Security Auditors
3.	Bank's Address for Communication and Submission of Tender	Deputy General Manager Canara Bank, AP&M Group, DIT Wing, 1st Floor, Naveen Complex, 14, MG Road, Bengaluru -560 001 Tel - 080-25590070, 25584873 Fax- 080-25596539 Email: hoditapm@canarabank.com Senior Manager, Asset Procurement & Management Group
4.	Date of Issue	24/01/2018, Wednesday
5.	Last Date of Submission of Queries for Pre Bid Meeting	01/02/2018, Thursday, 03.00 PM
6.	Date of Pre Bid Meeting	02/02/2018, Friday, 03.00 PM
7.	Last Date of Submission of Bids	14/02/2018, Wednesday up to 3.00 PM
8.	Date of Opening of Bid	14/02/2018, Wednesday at 3.30 PM
9.	Application Fees (Non Refundable)	Rs. 5,900/- (Inclusive 18% GST)
10.	Earnest Money Deposit(Refundable)	Rs. 50,000/-

This document can be downloaded from Bank's website http://www.canarabank.com/english/announcements/expression-of-interest. In that event, the bidders should pay the Application Fee for EOI document by means of DD drawn on any scheduled Commercial Bank for the above amount in favour of Canara Bank, payable at Bengaluru and submit the same along with the EOI.

D.I.T. Wing, A.P. & M. Group CANARA BANK HO, Bengaluru - 560 001

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 http://www.canarabank.com/english/announcements/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.

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.	CVC	Central Vigilance Commission
5.	DC	Data Centre
6.	DD	Demand Draft
7.	DIT	Department of Information Technology
8.	DRC	Disaster Recovery Centre
9.	IFSC	Indian Financial System Code
10.	IT	Information Technology
11.	NEFT	National Electronic Fund Transfer
12.	NI ACT	Negotiable Instrument Act
13.	PAN	Permanent Account Number
14.	RFP	Request for Proposal
15.	RFQ	Request for Qualification
16.	RTGS	Real Time Gross Settlement
17.	SOC	Security Operation Centre
18.	DISA	Diploma in Information System Audit
19.	CISA	Certified Information Systems Auditor
20.	CISM	Certified Information Security Manager
21.	CISSP	Certified Information Systems Security Professional
22.	PCIDSS	Payment Card Industry Data Security Standard
23.	CEH	Certified Ethical Hacker
24.	ISO	International Organization for Standardization
25.	COBIT	Control Objectives for Information and Related Technologies
26.	CCNA	Cisco Certified Network Associate
27.	CCNP	Cisco Certified Network Professional
28.	CHFI	Computer Hacking Forensic Investigator
29.	GIAC	Global Information Assurance Certification
30.	CRISC	Certified in Risk and Information Systems Control
31.	SSCP	Systems Security Certified Practitioner
32.	ECSA	EC-Council Certified Security Analyst
33.	ECIH	EC-Council Certified Incident Handler
34.	CRISC	Certified In Risk and Information Systems Control

LIST OF CONTENTS

Sl. No	Details	Sl. No	Details
1	About Canara Bank	15	Amendment to EOI
2	Definitions	16	Preparation of Bids
3	About EOI	17	EMD
4	Objective	18	Erasures or Alterations
5	Eligibility Criteria	19	Submission of Bids
6	Application Money & EMD	20	Bid Opening
7	Scope of Empanelment	21	Evaluation of EOI
8	Empanelment Procedure	22	Clarifications of Offers
9	De-empanelment of Bidders	23	Modification/Cancellation of EOI
10	Scope of Work of IT Audit Services	24	Responsibility for Completeness
11	Conflict of Interest	25	Intimation to successful Bidders
12	Bid Document & Cost	26	Issuance of RFP
13	Pre bid queries	27	Details of Independent External Monitors
14	Pre bid Meeting		

Sl. No	ANNEXURES
1)	Checklist
2)	Covering Letter Format
3)	Eligibility criteria declaration
4)	Bidder's Profile
5)	Authorization Letter Format
6)	List of major customers

7)	Office Details
8)	Bank Guarantee Format For Earnest Money Deposit
9)	Compliance Statement
10)	Scope of Work of IT Audit Services

1. About Canara Bank

CANARA BANK, a body Corporate and a premier Public Sector Bank established in the Year 1906 and nationalized under the Banking Companies (Acquisition and Transfer of Undertakings) Act, 1970, having its Head office at 112, J C Road Bengaluru-560002 and among others is having Department of Information Technology Wing at Naveen Complex, No.14, M G Road, Bengaluru-560001. The Bank is having Pan India presence of more than 6200 Branches, 21 Circle Offices & 118 Regional Offices situated across the States and presence in abroad. The Bank is working on Core Banking System using Flex cube solutions. As part of initiatives, the Bank has also deployed various IT applications / products like ATMs, Internet & Mobile Banking, UPI, Financial Inclusion, RTGS/NEFT, Depository Services, and Online Trading etc. In addition to these, the Bank proposes to implement several new IT Projects on an on-going basis depending upon the needs. The Bank is a forerunner in implementation of IT related products and 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(EOI) and shall be deemed to include its successors and permitted assigns.

2.2. 'EOI' means this Expression of Interest for Empanelment of Security Auditors for our Bank.

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

3. About EOI

3.1. Bank intends to empanel Security Auditors who can provide suitable and appropriate technical audit services for IT / Cyber Security.

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 **Clause-5** for empanelment of Security Auditors for Information Technology/Cyber Security of ICT infrastructure of CANARA BANK.

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 meet the Eligibility Criteria as per **Annexure-3** may respond.

6. Application Money and EMD:

6.1. The following amount shall be payable towards Application money and EMD.

Application fees for Rs.5,900/- (Non Refundable) (Includes GST @18%)	By way of DD favoring "Canara Bank" payable at Bengaluru.
Non Interest EMD for Rs.50,000/- (Refundable)	By way of DD favoring "Canara Bank" payable at Bengaluru/ Bank Guarantee in lieu of EMD as per ANNEXURE-8.

6.2. MSEs are exempted from paying Application Fee/Cost & EMD.

6.3. MSEs should submit relevant documentary proof for claiming the exemptions.

6.4. Further, all bidders shall have to comply the following:

a. Failure to produce the documents as necessary proof along with the EMD and Application fee while submission of EOI proposal shall render the applicant ineligible for empanelment.
b. The Bidder should submit separate DDs one each for EMD and Application Fee, if DDs are submitted.
c. The Bidder should not provide any commercial proposal with the response to this EOI.

7. Project Scope of Empanelment:

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 invariable 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.

7.1. 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 security Audit
e. Ethical Hacking
f. Forensic Audit
g. Configuration Review Audit
h. BCP / DR Preparedness / Readiness Audit
i. Network Audit including Virtualization, wireless & Mobile Technologies
j. Database Audits / Migration Audit
k. Switch/ATM Terminals Audit/ ATM Network Audit
l. Comprehensive IT and IS Audits including Outsourced Activities and Third Party Audits.
m. Comprehensive cyber Security Audit
n. Any other activity/audit as decided by the Bank during the empanelment period.

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

7.3. Empanelment would be for THREE 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.

7.4. During Empanelment period, Bank will float limited tenders amongst the qualified empanelled bidders 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. Selected Bidder to submit KYC document.

7.5. 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.

7.6. 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.

8. Empanelment Procedure:

The IT Auditors will be empanelled as per the following process:

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

8.2. 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.

8.3. Based on the documents submitted, and the presentations made and the expertise, the panel shall select the Security Auditors for empanelment.

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. 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.

9.3. 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 empanelled list without giving any notice to the vendor in advance.

9.4. Empanelled 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. Scope of Work of IT Audit Services:

10.1. The Brief Scope of Work for the Thirteen (13) Services is detailed in ANNEXURE-10.

10.2. Bank will float limited tenders amongst the qualified empanelled 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 RFP/RFQ shall be floated by Bank.

11. Conflict of Interest:

11.1. 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.

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

12. Bid Document & Cost

12.1. This document can be downloaded from Bank's website http://www.canarabank.com/english/announcements/expression-of-interest. In that event, the bidders should pay the Application Fee of **Rs.5,900/-** for tender document by means of DD drawn on any scheduled Commercial Bank for the above amount in favour of Canara Bank, payable at Bengaluru and should be kept along with the bid cover. Submission of the cost of the bid document in other than the bid cover is liable to be rejected on grounds of non-payment of the cost of the bid document. MSEs are exempted from payment of Application cost on submission of relevant documentary proof.

12.2. The Bidder shall bear all costs associated with the preparation and submission of the bid and the Bank will not be responsible for the costs, regardless the conduct or outcome of the bidding process. The Bank is not liable for any cost incurred by the bidder in replying to this EOI. It is also clarified that no binding relationship will exist between any of the respondents and the Bank until the execution of the contract.

13. Pre-Bid Queries:

13.1. The bidder should carefully examine and understand the scope and, 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.

13.2. All communications regarding points requiring clarifications and any doubts shall be given in writing to the Deputy General Manager, Canara Bank, DIT Wing, HO(Annexe), 14, M G Road, Bengaluru - 560 001 or an email can be sent to **hoditapm@canarabank.com** by the intending bidders before **03:00 PM on 01/02/2018 (Thursday).**

13.3. No queries will be entertained from the bidders after the above date and time.

13.4. No oral or individual consultation shall be entertained.

14. Pre-Bid Meeting:

14.1. A pre-bid meeting of the intending bidders will be held as scheduled below to clarify any point/doubt raised by them in respect of this EOI.

Date	Day	Time	Venue
02/02/2018	Friday	03.00 PM	Canara Bank, DIT Wing, Conference Hall, II Floor, Naveen Complex, 14 M.G Road, Bengaluru - 560001.

No separate communication will be sent for this meeting. 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.

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

14.3. 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.

14.4. 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

15. Amendment to EOI:

15.1. 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.

15.2. 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.

15.3. 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.

16. Preparation of Bids:

16.1. 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 appended.

16.2. 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.

16.3. The bid must contain EMD/ Bank Guarantee in lieu of EMD as per ANNEXURE-8 of this document. The Conformity to Eligibility Criteria should be complete in all respects and contain all information sought for, as per ANNEXURE-1.

17. Earnest Money Deposit (EMD)/Bank Guarantee In Lieu Of EMD:

17.1. The bidder shall furnish Non interest earning Earnest Money Deposit (EMD) of Rs.50,000/- (Rupees Fifty Thousand Only) by way of Demand Draft drawn on any scheduled bank in favour of Canara Bank, payable at Bengaluru and should be kept along with the bid.

17.2. In Case the EMD is submitted in the form of Bank Guarantee, the same should be valid for the minimum period of 12 months from the last date for submission of offer. The format for submission of EMD in the form of Bank Guarantee is as per ANNEXURE-8.

17.3. The EMD of bidders will be returned upon the finalization of Empanelment.

17.4. The EMD may be forfeited/ Bank Guarantee may be invoked, if the bidder withdraws or amends the bid during the period of bid validity which is six months from the date of Expression of Interest or date of finalization of the empanelment whichever is later.

18. 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.

19. Submission of Bids:

19.1. The sealed envelope containing the response to EOI along with the required documents shall be super scribed on the top of the envelope " Empanelment of IT / Cyber Security Auditors in response to EOI 01/2017-18 dated 24/01/2018. 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 below:

Last Date of submission of Bid	Day	Time	Venue
14/02/2018	Wednesday	Up to 3.00 PM	Canara Bank, DIT Wing, First Floor, Naveen Complex, 14 M.G Road, Bengaluru - 560 001.

19.2. If the last day of 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.

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

19.4. 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.

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

First Official	Alternate Official
Mr. R S VinayaKumar Senior Manager Canara Bank AP & M Group, DIT Wing, First Floor, Naveen Complex, 14 M G Road, Bengaluru - 560 001. Tel - 080 25590070	Mr. K S Satyanarayana Assistant General Manager Canara Bank AP & M Group, DIT Wing, First Floor Naveen Complex, 14 M G Road, Bengaluru - 560 001. Tel - 080 25590832

19.6. 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 above.

19.7. 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.

20. Bid Opening:

20.1. EOI will be opened in the presence of the Bidder's representative/s who may choose to attend the bid opening as per following schedule.

Date	Day	Time	Venue
14/02/2018	Wednesday	3.30 PM	Canara Bank, Conference Hall,

			2nd Floor, Naveen Complex, 14 M.G Road, Bengaluru 560001.

20.2. 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-5) 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

20.3. 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.

20.4. 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.

21. Evaluation of EOI:

21.1. 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.

21.2. 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.

21.3. EOI submitted by the bidder will be evaluated based on the format mentioned in ANNEXURE-1. Bidders who will qualify under Eligibility Procedure as per clause no 8 of EOI will be empanelled. Period of empanelment will be decided by the Bank. The short listed applicants will be notified in due course. Only shortlisted applicants will be invited to participate in the limited RFP/RFQ. No interim enquiries will be entertained. The decision taken by the Bank shall be final and no representation or correspondence shall be entertained.

22. Clarifications Of Offers

22.1. 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.

22.2. 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.

22.3. 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.

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

23. Modification/Cancellation of EOI:

23.1. 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.

23.2. 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 the in the best interest of the Bank
d. Any other reason

23.3. 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.

24. Responsibility for completeness:

24.1. 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.

24.2. 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.

24.3. 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.

25. Intimation to the selected 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.

26. Issuance of RFP

26.1. Only shortlisted applicants will be invited to participate in the limited RFP/RFQ Process. The shortlisted applicants will be provided with tender documents through E-mail or hand delivery. The vendors are required to respond accordingly.

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

26.3. 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.

26.4. 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.

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

27. Independent External Monitors:

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

Sri. Dilip Mavinkurve Email:dilipmav@gmail.com	Sri. Hari Santosh Kumar Email:hsantoshkumar50@gmail.com

DEPUTY GENERAL MANAGER

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	Complied & Submitted (Yes/No)
1.	Covering Letter.	
2.	A Demand Draft of Rs.5,900/- (Non-Refundable) favouring Canara Bank payable at Bengaluru towards Application Fee.	
3.	EMD for Rs.50,000/- by Demand Draft favouring Canara Bank payable at Bengaluru/Bank Guarantee as per ANNEXURE-8 is enclosed.	
4.	Three (3) Years Audited Balance sheet, P&L account or CA Certificate for the past three years i.e. 2014-15, 2015-16, 2016-17 should be enclosed.	
5.	The documents in support of Eligibility Criteria, wherever required as mentioned in this EOI.	
6.	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.	
7.	Bidder's Profile.	
8.	List of major clients and the quantum of orders with approximate value executed to various organizations including Major PSU Banks and other financial institutions for the last 3 years.	
9.	Compliance Statement	
10.	Authorization letter format for Bid Opening (to be carried by the person who is authorized to attend the Bid opening).	

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

Sl. No.	Annexure-1: Other Clauses	Vendor Response [Yes/No]
1.	Whether Cost of the Tender document (Demand Draft payable at Bengaluru) is submitted? If exemption is sought under MSEs, relevant certificate enclosed.	

2.	Whether EMD / Bank guarantee in lieu of EMD Submitted? If exemption is sought under MSEs, relevant certificate enclosed.	
3.	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?	
4.	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?	
5.	Whether address of Office on which communication has to be placed is indicated in ANNEXURE-4.	
6.	Whether ensured that the offer is in sealed envelope and superscribed as "Empanelment of IT/ Cyber Security Auditors", The EOI No., Name of the Bidder firm and Due date of the EOI is specified on the top of the envelope.	
7.	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-5 is to be carried in person and shall not be placed inside any of the bid covers.

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,
Asset Procurement & Management Group,
DIT, Naveen Complex, 14 M G Road,
Bengaluru - 560 001, Karnataka

Dear Sir,

Sub: Empanelment of IT/Cyber Security Auditors.

Ref: EOI 01/2017-18 Dated 24/01/2018.

Having examined the EOI document including **all Annexure** the receipt of which is hereby duly acknowledged, we, the undersigned, offer to get short listed as Consultant for Information Technology Security with the said EOI.

If our offer is accepted, we undertake to participate in the RFP process to Security Auditors for the below mentioned I.T. Audit services but not limited to:

i. Vulnerability Assessment
ii. Penetration Testing
iii. Source Code Audit
iv. Application /web security Audit
v. Ethical Hacking
vi. Forensic Audit
vii. Configuration Review Audit
viii. BCP / DR Preparedness / Readiness Audit
ix. Network Audit including Virtualization, wireless & Mobile Technologies
x. Database Audits / Migration Audit
xi. Switch/ATM Terminals Audit/ ATM Network Audit
xii. Comprehensive IT and IS Audits including Outsourced Activities and Third Party Audits.
xiii. Comprehensive cyber Security Audit
xiv. Any other activity/audit as decided by the Bank during the empanelment period.

We enclose a Demand Draft favouring 'Canara Bank payable at Bengaluru'/Bank Guarantee as per ANNEXURE-8 for Rs.50,000/- as Non-interest Earning refundable deposit/EMD.

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 in India (giving their full addresses of IT Department) to whom we have conducted the IT /Cyber Security Audits.

We accept all the Instructions and Terms and Conditions of the subject EOI.

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

Eligibility Criteria Declaration

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

Sub: Empanelment of Security Auditors for Information Technology Security.

Ref: EOI 01/2017-18 Dated 24/01/2018

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

Sl. No.	Financial and other Requirements to be met by the Bidder.	Documents to be submitted along with the EOI.
1.	The bidder should be a Registered Company under the Companies Act 1956/2013 / Partnership Firm/ LLP in India and should be in existence for minimum period of five (5) years as on the date of RFP.	Copy of Certificate of Incorporation / Certificate of Commence of Business (in case of Companies) and Partnership Deed (in case of Partnership / LLP) to be submitted by the bidder.
2.	The bidder should be a CERT-In Empanelled vendor as on date of submission of EOI.	Copy of List of Empanelled Information Security Audit Organizations by CERT-IN containing the name of the bidder.
3.	The bidder should have minimum annual turnover of Rs.2 Crores during the last three (3) financial years i.e., 2014-15, 2015-16 & 2016-17.	Audited Balance Sheet, P&L account or Chartered Accountant Certificate to that effect.
4.	The Bidder should have positive net worth as on 31/03/2017 or as on 30/09/2017.	Audited Financial statement or CA Certificate to that effect.
5.	The bidder shall have local office in Bengaluru with their Own / Support Centers personnel to liaison various activities.	The Bidders to furnish their details such as Office address, Contact person name, Phone No, Mobile No, Email. Number and Level of Technical working at Bengaluru Office.
6.	The Bidder has not been blacklisted / barred by any Public Sector Bank, Government of India Authority or PSU or any regulatory body in India as on date of the bid submission.	Self-declaration on the letter head of the bidder confirming the criteria.
7.	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.	Self-declaration confirming the criteria.

8.	The bidder should have minimum 10 employees which each employee having at-least one of the following certificate: i) CISA ii) CISSP iii) CISM **Only those employees will be considered who is involved in Operation work. Those employees working in Management or Administrative office will not be counted.	HR Certificate (along with list and certifications of the employees and self-declaration forms of employees on their experience and qualifications/certifications)

9. Service-wise eligibility is given as below:

Sl. No	Service	Required Certificate (in addition to the certification put in eligibility criteria)	Minimum Experience Required	Document to be provided
9.1.	Vulnerability Assessment	CISA, CISSP, CEH The personnel conducting the subject audit should have at-least three years of experience.	Empanelled bidder would have carried out such activities/audit at least in two different organization, one of which should be in BFSI sector in the last three years from the date of EOI.	**Relevant Credential letters/ Certificate/Agreement/Purchase Order/s to that effect.**
9.2.	Penetration Testing	CISA, CISSP, CEH The personnel conducting the subject audit should have atleast three years of experience.	Empanelled bidder would have carried out such activities/audit at least in two different organization, one of which should be in BFSI sector in the last three years from the date of EOI.	
9.3.	Source Code Audit	CISA, CISSP, CSSLP, CPT The personnel conducting the subject audit should have atleast three years of experience.	Empanelled bidder would have carried out such activities/audit at least in two different organization, one of which should be in BFSI sector in the last three years from the date of EOI.	
9.4.	Application /web security	CISA, CISSP, CSSLP, CPT The personnel conducting	Empanelled bidder would have carried out such activities/audit at least	

	Audit	the subject audit should have atleast three years of experience.	in two different organization, one of which should be in BFSI sector in the last three years from the date of EOI.	
9.5.	Ethical Hacking	CISA, CISSP, CEH The personnel conducting the subject audit should have atleast three years of experience.	Empanelled bidder would have carried out such activities/audit at least in two different organization, one of which should be in BFSI sector in the last three years from the date of EOI.	
9.6.	Forensic Audit	CHFI The personnel conducting the subject audit should have atleast two years of experience.	Empanelled bidder would have carried out such activities/audit at least in two different organization, one of which should be in BFSI sector in the last three years from the date of EOI.	
9.7.	Configuration Review Audit	CISA, CISM The personnel conducting the subject audit should have atleast two years of experience.	Empanelled bidder would have carried out such activities/audit at least in one BFSI sector in the last three years from the date of EOI.	
9.8.	BCP / DR Preparedness / Readiness Audit	CISA, CISM The personnel conducting the subject audit should have atleast two years of experience.	Empanelled bidder would have carried out such activities/audit at least in one BFSI sector in the last three years from the date of EOI.	
9.9.	Network Audit including Virtualization, wireless & Mobile Technologies	CCNP-Security, CEH The personnel conducting the subject audit should have atleast two years of experience.	Empanelled bidder would have carried out such activities/audit at least in one BFSI sector in the last three years from the date of EOI.	
9.10.	Database Audits / Migration	CISA, CISM The personnel conducting	Empanelled bidder would have carried out such activities/audit at least in one BFSI sector in the	

	Audit.	the subject audit should have atleast two years of experience.	last three years from the date of EOI.	
9.11.	Switch/ATM Terminals Audit/ ATM Network Audit.	PCIDSS The personnel conducting the subject audit should have atleast two years of experience.	Empanelled bidder would have carried out such activities/audit at least in one BFSI sector in the last three years from the date of EOI.	
9.12.	Comprehensive IT and IS Audits including Outsourced Activities and Third Party Audits.	CISA, CISM, ISO 27001 LA/L1, GIAC, CRISC, DISA The personnel conducting the subject audit should have atleast two years of experience.	Empanelled bidder would have carried out such activities/audit at least in one BFSI sector in the last three years from the date of EOI.	
9.13.	Comprehensive cyber Security Audit	CISA, CISM, CISSP, ISO 27001 LA/L1, GIAC, CRISC, DISA The personnel conducting the subject audit should have atleast three years of experience.	Empanelled bidder would have carried out such activities/audit at least in one BFSI sector in the last three years from the date of EOI.	

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 :

ANNEXURE-4

Bidder's Profile

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

Sl. No.	Particulars	Details
a.	Name of the Bidder	
b.	Constitution	
c.	Date of Establishment/ Incorporation	
d.	Number of Years in the Business	
e.	Number of years of experience in IT/Cyber Security Audit.	
f.	Address for Correspondence: Registered Office: Corporate Office:	
g.	Single Point of contact for this EOI and upcoming RFP Name: Designation: Mobile No.: Landline No.: Fax: Email-ID (any changes in the above should be informed in advance to Bank)	
h.	Annual Turnover during the last three financial year. 2014-15 2015-16 2016-17 Net worth as on 31/03/2017 or as on 30/09/2017.	

i.	Domestic Customer Base (Number of Clients where IT/Cyber Security Audit Service have been provided in India).	
j.	Our PAN number for Income Tax is _____. We are registered with the GST authorities and our registration numbers are as follows. GST Registration Number is _____. <u>Our Bank Details</u> Name and Style of Bank Account Name of the Bank and Branch address Account Number RTGS / NEFT (IFSC) Code	

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 :

ANNEXURE-5

Authorization Letter Format

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

Date: _____

The Deputy General Manager
Canara Bank,
Asset Procurement & Management Group
DIT Wing
Naveen complex, 14 MG Road
Bengaluru - 560 001

Dear Sir,

Sub: Empanelment of IT/Cyber Security Auditors.

Ref: EOI 01/2017-18 Dated 24/01/2018

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:

ANNEXURE-6

List of Major Customers of the Bidder in Last 3 Years and References in IT/Cyber Security Audit

Sub: Empanelment of IT/Cyber Security Auditors.

Ref: EOI 01/2017-18 Dated 24/01/2018

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	6

(Enclose necessary documentary proof)

Date :
Place :

Signature with seal:
Name :
Designation :

ANNEXURE-7

Office Details

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

Sub: Empanelment of IT/Cyber Security Auditors.

Ref: EOI 01/2017-18 Dated 24/01/2018

Sl. No.	Name of the Office	Address and Telephone No's	E-mail ID of office	Number of Consultant
1.	Head Office			
2.	Bengaluru			
3.	Others(specify)			

Date :
Place :

Signature with seal:
Name :
Designation :

ANNEXURE-8

BANK GUARANTEE FORMAT FOR EARNEST MONEY DEPOSIT

To

.....

.....

.....

.....

WHEREAS _____(Name of Bidder) (hereinafter called "the Bidder" has submitted its Bid dated _____ (Date) for the execution of (Name of Contract)_____(hereinafter called "the Bid") in favour of _____hereinafter called the "Beneficiary";

KNOW ALL MEN by these presents that we, _____(name of the issuing Bank), a body corporate constituted under the _____having its Head Office at _____amongst others a branch/office at _____ (hereinafter called "the Bank" are bound unto the Beneficiary for the sum of Rs_____(Rupees_____only) for which payment well and truly to be made to the said Beneficiary, the Bank binds itself, its successors and assigns by these presents;

THE CONDITION of this obligation is:

If the bidder withdraws or amends their offer of empanelment before finalization of empanelment by the Beneficiary.

We undertake to pay to the Beneficiary up to the above amount upon receipt of his first written demand without the Beneficiary having to substantiate his demand, provided that in his demand the Beneficiary will note that the amount claimed by him is due to him owing to the occurrence the above condition.

Notwithstanding anything contained herein

i) Our liability under this Bank Guarantee shall not exceed Rs._____ (Rupees _____only)

ii) This Bank Guarantee is valid up to _____ and

iii) We are liable to pay the guaranteed amount or any part thereof under this Bank Guarantee only and only if you serve upon us a written claim or demand on or before _____(mention period of guarantee as found under clause (ii) above plus claim period)

Dated _____day of _____2018

SIGNATURE OF THE BANK

Annexure-9

Compliance Statement

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

Sub: Empanelment of IT/Cyber Security Auditors.

Ref: EOI 01/2017-18 Dated 24/01/2018

The Deputy General Manager
Canara Bank,
Asset Procurement & Management Group
DIT Wing
Naveen complex, 14 MG Road
Bengaluru - 560 001

Date: _____

Dear Sir,

Sub: Empanelment of IT/Cyber Security Auditors.

Ref: EOI 01/2017-18 Dated 24/01/2018.

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 :

Annexure-10

Scope of Work of IT Audit Services

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:**

   9.13.1. Clarifications
   9.13.2. Discussions
   9.13.3. Recommendations
   9.13.4. References / Rationale for recommendations

2. **Reports would be in:**

   a. Soft copies
   b. Hard copies - Two nos.
   c. Copies of screen shots, Outputs
   d. Audit evidence
   e. Soft outputs which are importable into a database, spreadsheet, or GRC platform e.g. XML files, CSV files etc.
   f. Tracking sheet
   g. Metrics and Dashboards
   h. Power point presentation
   i. Vulnerabilities identified
   j. Exploit Reports and supporting Evidences
   k. Vulnerability ratings
   l. Threat Profile
   m. Test Plan
   n. 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.)
   o. Short Videos and Presentations for awareness sessions
   p. Compliance requirements where applicable
   q. Screenshots and code listing or line numbers where feasible in code reviews
   r. Solutions with details and additional resources.

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

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 invariable 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.

a. **Vulnerability Assessment:** Vulnerability assessment shall attempt to determine vulnerabilities that may enable unauthorized logical access to protected systems to an intruder 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. After fixing/rectification of vulnerabilities (which will be found during vulnerability assessment activity) by functional groups, VA Auditor has to do check for all critical observations and minimum 20% of remaining observations on random basis. 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 check for all critical observations and minimum 20% of remaining observations on random basis. 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.

d. **Application security /Web security Audit:** The audit should consider the capability of application technical design and process flow to fulfill

the requirement of business logic in effective and efficient manner and its security resilience. Compliance with relevant standards like OWASP and other Industry standards for secured application and web services.

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

1. Attempts to penetrate the application and find the vulnerabilities in the application.
2. Attempt to guess passwords using Password Cracking Tools
3. 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.
4. Attempt to search for backdoor traps in programs.
5. 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.
6. A test plan should be shared with the Bank including the methodology, tools used and prerequisites for conducting the test.
7. Only licensed version of reputed software/ tools should be used for conduct the test.
8. Ethical hacking of the web applications should also cover commonly available vulnerability index such as OWASP Top 10 and SANS Top 25.

f. **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.

g. **Configuration Review Audit:** Review of configuration items (CIs) against applicable recommended baselines (keeping in view the environment in which the CIs are operating); procedures for management of changes to configurations;

h. **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.

i. **Network Security Audit:** 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.

j. **Database Audit/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 to

k. **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.

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. **IT and IS audit:** 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

n. **Any other activity as decided by the Bank during the empanelment period:** In view of various guidelines for varying Audits of ICT infrastructure, 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.

4. Bank will float limited tenders amongst the qualified empanelled 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.