CENTRAL BANK OF INDIA

REQUEST FOR PROPOSAL FOR CYBER SECURITY AUDIT AND COMPREHENSIVE AUDIT OF CBS PROJECT & OTHER APPLICATIONS
CENTRAL AUDIT & INSPECTION DEPARTMENT 3RD FLOOR, SIR SORABJI BHAVAN, EWART HOUSE FORT- MUMBAI 400 023

Tender No	CO:CA&ID:PUR:2021-22: 02
Date of Commencement of sale of tender document	From 19.07.2021 (MONDAY)
Queries, if any, to be sent by mail by	26.07.2021 (MONDAY) up to 17.00 Hrs
Pre-Bid meeting with bidders	02.08.2021 (MONDAY) at 15.00 Hrs
Last Date and Time for receipts of Tender Offer	09.08.2021 (MONDAY) up to 15.00 Hrs

TABLE OF CONTENTS

1. Invitation for Tender Offers

Central Bank Of India invites sealed tender offers (Technical bid and Commercial bid) from eligible, reputed firms who are committed to the Information Security & Audit business and have the capability and experience in auditing IT infrastructure consisting of hardware, software, CBS & other related applications, network, cyber security, database, operating system, storage, event correlation and analysis etc besides other details as specified in this RFP.

Evaluation criteria: evaluation of the responses to the RFP and subsequent selection of the successful bidder(s) will be entirely at Bank's sole discretion. Banks decision shall be final and no correspondence about the decision shall be entertained.

The brief scope of Audit is as under:-

1. **Application Audit:** Complete review of applications and security audit of all major applications including Core Banking Application (CBS-B@ncs24) and Delivery Channels i.e. Internet Banking, Mobile Banking (SMS/ WAP), RTGS/ NEFT / SWIFT Transactions, Treasury, Financial Inclusion (FIGS) etc. In-house developed applications. (Approximate 42 applications).

   - Top 10 OWASP Vulnerabilities: Compliance review of top 10 OWASP (Open Web Application Security Project) vulnerabilities, especially for public facing applications viz. Internet Banking, Mobile Banking, Corporate Website, Financial Inclusion (FIGS) etc.
   - VAPT (Vulnerability Assessment & Penetration Testing) : VA (Vulnerability Assessment) of all major applications including CBS & Delivery Channels, and Penetration Testing of public facing applications viz. Internet Banking, Mobile Banking, Corporate Website, Financial Inclusion (FIGS) etc.

2. **DC/ DRC Audit**: Thorough Audit of bank's Data Centre (DC) at Navi Mumbai, Disaster Recovery Centre (DRC) at Hyderabad and Near Site at Navi Mumbai. Audit of Disaster Recovery and Business Continuity Plans for adequacy and conformance of BCP guidelines. Audit of effectiveness of Anti-virus system.

3. **Network / Cyber Security Audit:-**Network Infrastructure and Security Audit of entire Network infrastructure.
   Configuration Audit: - Configuration audit of various devices, especially for network & network security devices.

4. **Audit of ATM Project: -** Security audit of ATM switch, ATM card related operations.

5. **Outsourcing Audit**:- Covering audit of Information System, functional and operational aspects of Outsourced activities as per Guidelines of RBI. Outsourced activities/ vendor of DIT, ATM Dept., Call Centre, Financial Inclusion, Debit Card, Credit Card and other outsourced activities. (Approximate 41 outsourced activities)

6. Comprehensive System audit of Core Banking Solution (Finacle) of 2 RRBs sponsored by Central Bank of India and having their Data Center at Navi Mumbai, Maharashtra.

A complete set of tender documents may be purchased by eligible bidder upon payment of a non-refundable fee of Rs.10,000/-(Rupees Ten thousand only) by demand draft/ banker's cheque in favour of Central Bank Of India, payable at Mumbai or through online payment, details of which is given below.

Bid Collection & Submission details are as under:–

Tender Reference Number	CO:CA&ID:PUR:2021-22: 02
Tender Document Cost	Rs.10,000/-
Earnest Money Deposit	Rs. 50,000/- (Fifty Thousand Only)
Date of Commencement of sale of tender document Queries, if any, to be sent by mail	From 19.07.2021(Monday) By 26.07.2021 (Monday) up to 17.00 Hrs
Pre-Bid meeting with Bidders	On 02.08.2021 (Monday) at 15.00 Hrs At CENTRAL BANK OF INDIA CENTRAL AUDIT & INSPECTION DEPARTMENT 3RD FLOOR, SIR SORABJI BHAVAN, EWART HOUSE, FORT MUMBAI 400 023.
Last Date and Time for receipts of tender offers	Up to 09.08.2021 (Tuesday) at 15.00 Hrs
Time & Date of Opening of technical bids	On 10.08.2021 at 15.00 Hrs
No. of Envelopes to be submitted (Non window, sealed)	Three (3) Envelopes **Envelope 1 containing:** Technical Bids as per point no. 4.1 **Envelope 2 containing:** Commercial Bid as per point no. 4.1 (Only one bid to be kept) **Envelope 3 containing:** DDs for Tender cost & earnest money
Address for Communication	**Asst General Manager (CA&ID)** CENTRAL BANK OF INDIA CENTRAL AUDIT & INSPECTION DEPARTMENT 3RD FLOOR, SIR SORABJI BHAVAN, EWART HOUSE, FORT. MUMBAI 400 023
Place of Opening tender offers	Same as above
Contact Telephone Numbers	022-6164 8628,022- 6164 8652
Email ID for communication.	agmaid1@centralbank.co.in manageritcaid@centralbank.co.in caassignment@centralbank.co.in

The bidders who are submitting the bid by downloading from the Bank's website will have to pay the non-refundable fee of Rs.10,000/- by way of a demand draft in favor of Central Bank of India payable at Mumbai, ON OR BEFORE THE PRE-BID MEETING. Alternatively the bidder may pay the cost of Tender document online, details of which is given below,

Bank Account details:
Account No. : 1122845035
Type of account : CD
IFSC Code : CBIN0281067
Account Name : Business Support Department
Bank Name :Central Bank of India
Branch Name : Nariman Point, Mumbai

The Bidder will share the Transaction id/ Reference No. of the online transaction for verification & record.

Only the authorized representatives of the bidders who have purchased the RFP /made the payment of Rs.10,000/- will be permitted to attend the Pre-Bid meeting.

Earnest Money Deposit must accompany with tender offers as specified in this tender document. EMD amount should not be mixed with Technical/Commercial Bid; it should be in separate cover to be handed over to the department.

Tender offers will be opened in the presence of the bidders/their representatives who choose to attend the 'opening of tender' on the above-specified date, time and place.

Technical specifications, Terms and conditions, various formats and Performa for submitting the tender offer are described in the tender document.

ASSISTANT GENERAL MANAGER (CA&ID)
CENTRAL BANK OF INDIA
CENTRAL AUDIT & INSPECTION DEPARTMENT
3RD FLOOR, SIR SORABJI BHAVAN, EWART HOUSE, FORT MUMBAI 400023.

PUBLIC TENDER NO. : 02

1) The RFP is available on Central Bank of India's website **www.centralbankofindia.co.in.** Central Bank of India reserves the right to change audit requirements till last day of submission of bid. However, any such changes will also be available on the web site.

2) Bidders are advised to study the tender document carefully. Submission of bids shall be deemed to have been done after careful study and examination of the tender document with full understanding of its implications.

3) The gist of pre-bid meeting will be posted on Central Bank of India's website. Hence before submitting bids, bidder must ensure that such clarifications / changes have been considered by them. Central Bank of India will not have any responsibility in case bidder has omitted the same.

4) In case of any clarification required by Central Bank of India, useful for assisting in the examination, evaluation and comparison of bids, Central Bank of India may, at its discretion, ask the bidder for clarification. The response / Clarification shall be in writing and no change in the price of substance of the bid shall be sought, offered or permitted.

5) Please note that all the information required as per the bid document needs to be provided. Incomplete information in these areas shall lead to rejection.

6) Modification and / or Withdrawal of Bids:
Bids once submitted will be treated, as final and no further correspondence will be entertained. No bid shall be allowed to modify and withdraw after the deadline for submission of bids.

7) Central Bank of India has the right to reject any or all tenders received without assigning any reason whatsoever.

NOTE:
CENTRAL BANK OF INDIA SHALL NOT BE RESPONSIBLE FOR NON-RECEIPT / NON-DELIVERY/ LATE DELIVERY OF THE BID DOCUMENTS DUE TO ANY REASON WHATSOEVER.

2. Background

2.1 About Central Bank of India

Central Bank of India, established in 1911, was nationalized in the year 1969 and today is a leading public sector undertaking.

The Bank has a four-tier organizational structure comprising of the Central Office, Zonal Offices, Regional Offices and Branches. The Bank has a network of approximate 4700 branches, spread across the length and breadth of the country with presence in all the States and Union Territories. The Bank also has specialized branches catering to the specific needs of Retail customers, Industrial units, corporate clients, Forex dealers, Exporters and Importers, Small Scale Industries and Agricultural sector. The Bank has sponsorship in 2 Regional Rural Banks (RRB).

The Bank has international partnership with Indo-Zambia Bank. The Bank deals in ten foreign currencies, namely, US dollar, Euro, Pound sterling, Francs, Hong Kong Dollar, Singapore Dollar, Deutche Mark, Canadian Dollar, Yen and Krone.

2.2 About Core Banking Solution

Central Bank of India has implemented banking software viz. B@ncs24, a core banking solution from Tata Consultancy Services Limited. All branches of the Bank are connected to the CBS. The Data Center of the Bank and the CBS / DIT Department of the Bank are located in Navi Mumbai. The Disaster Recovery site is situated at Hyderabad. The near site is hosted at another location at Navi Mumbai.

The core banking solution has a centralized database. A small part of database related to front-end application/s is also hosted at system at branches. The branches are connected to the Data Center through gateway PCs located at the branches.

Bank is using the anti-virus solution. The distributed servers for ant-virus are installed at C.O. At the branch level clients are updated through a gateway PC installed in Branch.

The CBS also supports Automated Teller Machines (ATMs), Internet Banking, SMS and Mobile Banking, Treasury Management (e-Treasury), RTGS/NEFT.

External gateways such as RTGS are presently connected to the CBS.

Volume *of* Transactions & Current CBS Infrastructure

Volume of transactions: The average daily transactions including enquiry transactions of CBS are approximately 9 millions.

CBS Infrastructure

The Bank's Data Center is located at Navi Mumbai and Disaster Recovery Center is at Hyderabad. The DC is connected to the branches, Regional Offices, Zonal office and Central Office through Bank wide Area Network (WAN). The branches are connected to Network Aggregation Point (NAP) located at various cities across the country. The NAPs in turn are connected to DC / DRC. The entire network uses MPLS and Backup connectivity through ISDN lines, VSAT etc. The ATMs, Mail Messaging System and other applications also use the WAN.

The Disaster Recovery Center has similar setup as that of DC.

At present around 4700 branches, 90 Regional offices, 10 Zonal offices 13 Zonal Audit Offices and 3 Training colleges are connected through WAN.

The following details will be provided to interested bidder during pre-bid meeting separately.

1.Details of IT Infrastructure
2.Details of Outsourced activities / vendors and their locations.

3. Introduction and Disclaimers

3.1 Purpose of RFP

The purpose of RFP is to shortlist IS Auditor/ Firm for audit of activities at Data Center, Disaster Recovery Site and other activities mentioned in the RFP, for providing independent assurance to the management on:

- Robust IT security,
- Help in mitigation of risks where there are significant control weaknesses
- Safeguarding the information assets viz. hardware, network etc.,
- Maintaining security, confidentiality, integrity and availability of data,
- Efficient utilization of resources-IT.
- Ensuring compliance of IT Security Policy and procedures defined by the Bank.
- Ensuring compliance of RBI Information Security Guidelines/recommendation and other applicable external regulations.
- The selection of bidder will be based on

1) Conformity with Minimum Eligibility Criteria 2) Technical bid 3) Commercial bid.

3.2 Information Provided disclaimer

The Request for Proposal document contains statements derived from information that is believed to be relevant at the date but does not purport to provide all of the information that may be necessary or desirable to enable an intending contracting party to determine whether or not to enter into a contract or arrangement with Central Bank of India. Neither Central Bank of India nor any of its employees, agents, contractors, or advisers gives any representation or warranty, express or implied, as to the accuracy or completeness of any information or statement given or made in this document. Neither Central Bank of India nor any of its employees, agents, contractors, or advisers has carried out or will carry out an independent audit or verification exercise in relation to the contents of any part of the document.

3.3 Disclaimer liability clause

Subject to any law to the contrary, and to the maximum extent permitted by law, Central Bank Of India and its officers, employees, contractors, agents, and advisers disclaim all liability from any loss or damage (whether foreseeable or not) suffered by any person acting on or refraining from acting because of any information including forecasts, statements, estimates, or projections contained in this RFP document or conduct ancillary to it whether or not the loss or damage arises in connection with any negligence, omission, default, lack of care or misrepresentation on the part of Central Bank of India or any of its officers, employees, contractors, agents, or advisers.

3.4 Costs to be borne by Bidder

All costs and expenses incurred by Bidder in any way associated with the development, preparation, and submission of responses, including but not limited to; the attendance at meetings, discussions, demonstrations, etc. and providing any additional information required by Central Bank Of India, will be borne entirely and exclusively by the Bidder.

3.5 No Legal Relationship

No binding legal relationship will exist between any of the Bidder and Central Bank of India until execution of a contractual agreement.

3.6 Bidders Obligation to get Informed Itself

The Bidder must conduct its scrutiny and analysis regarding any information contained in the RFP document and the meaning and impact of that information.

3.7 Evaluation of Offers

Each Bidder acknowledges and accepts that Central Bank of India may in its absolute discretion apply selection criteria specified in the document for evaluation of proposals for short listing / selecting the eligible Bidder(s). The RFP document will not form part of any Contract or arrangement, which may result from the issue of this document or any scrutiny or review, carried out by a Bidder.

3.8 Errors and Omissions

Each Bidder should notify Central Bank of India of any error, omission, or discrepancy found in this RFP document.

3.9 Acceptance of Terms

A Bidder will, by responding to Central Bank of India for RFP, be deemed to have accepted the terms of this Introduction and Disclaimer.

3.10 Lodgment of RFP

RFP submission:

RFP document submission is required to be done as stated in this RFP.

1. Faxed copies of any submission are not acceptable and will be rejected by the Bank.
2. All copies of RFPs and attachments must be provided in a **sealed** envelope.
3. If the submission does not include all the information required or is incomplete, the Proposal is liable to be rejected.

All submissions, including any accompanying documents, will become the property of Central Bank of India. Recipients shall be deemed to license, and grant all rights to Central Bank Of India to reproduce the whole or any portion of their submission for the purpose of evaluation, to disclose the contents of the submission to other recipients and to disclose and/or use the contents of the submission to other Recipients and to disclose and/or use the contents of the submission as the basis for any resulting RFP process, notwithstanding any copyright or other intellectual property right that may subsist in the submission or accompanying documents.

Central Bank of India may, in its absolute discretion, seek additional information or material from any Bidder after the RFP closes and all such information and material provided must be taken to form part of that Bidder's response.

Bidder should provide details of their Fax, email and full addresses to ensure that replies to RFP could be conveyed promptly.

If Central Bank of India, in its absolute discretion, deems that the originator of the question will gain an advantage by a response to a question, then Central Bank of India reserves the right to communicate such response to all Bidder.

Central Bank of India may, in its absolute discretion, engage in discussion or negotiation with any Bidder (or simultaneously with more than one Bidder) after the RFP closes to improve or clarify any response.

3.11 Notification

Central Bank of India will notify all short-listed Bidder in writing as soon as practicable about the outcome of their RFP. Central Bank of India is not obliged to provide any reasons for any such acceptance or rejection.

3.12 Disqualification

Any form of canvassing/lobbying/ influence/query regarding short listing, status, etc will be a disqualification.

If the 'successful bidder' backs out at any stage after being declared as 'successful bidder', the Bank reserves the right to blacklist it from participating in further two (02) process, besides having other legal remedies to invoke.

4. Instructions to bidders

4.1 Two Bid System Tender

One hard copy and one soft copy on compact disk (CD), of the Technical Bid and One hard Copy of the masked Commercial Bid must be submitted at the same time, giving full particulars in separate sealed envelopes at the Bank's address given below on or before the schedule given above. All envelopes should be securely sealed and stamped.

In case of difference in information provided in hard copy and soft copy, the signed hard copy shall be treated as binding one and soft copy will be ignored.

The sealed envelope containing Commercial Bid must be submitted separately to the Bank.

Asst General Manager
CENTRAL BANK OF INDIA
Central Audit & Inspection Department
3rd Floor, Sir Sorabji Bhavan, Fort
MUMBAI 400 023

All the envelopes must be super scribed with the following information –

1. Type of Offer- **Cyber Security audit and Comprehensive Audit of CBS Project & other applications** (Technical Bid, Commercial Bid)
2. Tender Reference Number
3. Due Date
4. Name of Bidder
5. Name of the Authorized Person

All schedules, Formats and Annexure should be stamped and signed by an authorized official of the bidder's company. An authorization letter in favor of such person, authorized to sign the documents and submit the bid, should also be submitted in Envelope containing technical bid. In the absence of the said authorization letter, submitted bid shall not be considered for evaluation at any stage.

The bidder will also submit copy of the RFP duly stamped and signed on each page by the authorized official of the bidder's company.

ENVELOPE- I (Technical bid)

The Technical bid should be complete in all respects and contain all information asked for except prices. The TECHNICAL BID should include all items asked for in Annexure-2. The Technical bid should not contain any price information. The TECHNICAL BID should be complete to indicate that all products and services asked for are quoted and should give all required information. A Xerox copy of commercial offer with prices duly masked be submitted along with the Technical Bid to ensure that the commercial bid has been submitted in the bank's format.

ENVELOPE- II (Commercial Bid)

The Commercial bid should give all relevant price information and should not contradict the TECHNICAL BID in any manner. A hard copy of the Commercial Bid duly masking the prices be submitted along with the Technical Bid. An authorization letter in favor of such person, authorized to sign the documents and submit the bid, should also be submitted in Envelope containing commercial bid. In the absence of the said authorization letter, submitted bid shall not be considered for evaluation at any stage.

The prices quoted in the commercial bid should be without any conditions. The bidder should submit an undertaking that there are no deviations to the specifications mentioned in the RFP either with the technical or commercial bids submitted.

ENVELOPE-III (EMD AMOUNT)

This envelope should contain the demand draft for Rupees Fifty Thousand only towards EMD favoring "Central Bank of India-EMD for Tender No. **02** payable at Mumbai.

Bidders are required to give a Demand Draft drawn in favor of Central Bank Of India, payable at Mumbai, (valid for 90 days from the due date of the tender) for Rs.50000/-(Rupees Fifty Thousand only) as Earnest money Deposit (EMD) (non-interest bearing) along with their offer. Aalternatively the bidder may pay the Earnest Money Deposit **online** as per details furnished here below:

Account Name: Business Support Department	Account No. : 1122845035	Type of account: CD
Bank: Central Bank of India	Branch: Nariman Point, Mumbai	IFSC Code: CBIN0281067

(The Bidder will share the Transaction id/ Reference No. of the online transaction for verification & record.

Offers made without E.M.D. will be rejected. Central Bank of India will not pay any interest on the E.M.D.

These three envelopes containing the Technical bids, Commercial bid and EMD amount should be separately submitted. Please note that any envelope containing both technical and commercial bid together will be rejected. However all the three separate envelopes can be submitted in a single large envelope.

All the covers thus prepared should indicate clearly the Name and Address of the Vendor.

The bidder shall bear all the costs associated with the preparation and submission of the bid and Central Bank of India will in no case be responsible or liable for those costs, regardless of the conduct or the outcome of the tendering process.

Bids sent by fax or e-mail will not be considered for evaluation.

4.2 Annexure to the Tender

The tender comprises of following schedules / Annexure-
Annexure 1 – Format of Tender offer cum letter
Annexure 2 – Bidder Information
Annexure 3 – Commercial Bid
Annexure 4 -- Format of Curriculum Vitae
Annexure 8 – Integrity Pact

4.3 Eligibility Criteria

The bidders, who fulfill the eligibility criteria mentioned in para 5.1 "Qualification Criteria" of the tender will only, be eligible for further process i.e. technical evaluation.

4.4 Terms and Conditions

Terms and conditions for bidders who participate in the tender are specified in the section called "Terms and Conditions". These terms and conditions will be binding on all the bidders. These terms and conditions will also form a part of the purchase order, to be issued to the successful bidder(s) on the outcome of the tender process.

4.5 Non-transferable Tender Document

This tender document is not transferable. Only the bidder, who has purchased this tender form, is entitled to quote.

4.6 Soft Copy of Tender document

The soft copy of the tender document will be made available on the bank's website.

However Central Bank of India shall not be held responsible in any way, for any errors/omissions/mistakes in the downloaded copy. The bidder is advised to check the contents of the downloaded copy for correctness against the printed copy of the tender document. The printed copy of the tender document shall be treated as correct and final, in case of any errors in soft copy.

The bidders who are submitting the bid by downloading from the Bank's website will have to pay the non-refundable fee of Rs10,000/- by way of a demand draft in favour of Central Bank of India payable at Mumbai while submitting the bid. Alternatively the bidder may pay the cost of Tender document online as per details provided on page no. 7.

4.7 Offer validity Period

The offer should hold good for a period of **210** days from the date of the opening of Commercial bid.

4.8 Address for Communication

Offers should be addressed to the following office at the address given below:

Asst. General Manager (CA&ID)
CENTRAL BANK OF INDIA
Central Audit & Inspection Department
3rd Floor, Sir Sorabji Bhavan (Ewart House), Fort
Mumbai - 400023

4.9 Pre-Bid Meeting

For the purpose of clarification of doubts of the bidders on issues relating to this RFP, Central Bank of India intends to hold a Pre-Bid meeting on the date and time as indicated in the RFP. The queries of all the bidders should reach in writing or by e-mail on or before 26.07.2021 up to 17.00 Hrs. on the address as mentioned above or through mail at agmaid1@centralbank.co.in. It may be noted that no queries of any bidder, received after 17.00 Hrs. on 26.07.2021, shall be entertained. The clarifications given in the Pre-Bid meeting will be available on the Bank's Website.

Only the bidders /authorized representatives of the bidders who have purchased the RFP will be allowed to attend the Pre-Bid meeting.

4.10 Opening of Offers by Central Bank of India

Tender offers received within the prescribed closing date and time will be opened in the presence of bidders/bidders' representatives who choose to attend the opening of the tender on the specified date and time as mentioned earlier in the tender document. The bidders/bidder's representatives present shall sign a register of attendance and minutes and they should be authorized by their respective companies to do so. A copy of the authorization letter should be brought for verification.

4.11 Scrutiny of Offers

Eligibility Criteria:

Central Bank of India will first scrutinize the eligibility of the prospective bidders as per "Eligibility criteria" mentioned in point no. 5 viz. "Qualification Criteria" mentioned in the RFP, based on the documents submitted. The offers of the bidders who fulfill the above eligibility criteria will be taken up for further scrutiny i.e. technical evaluation.

4.12 Clarification of Offers

To assist in the scrutiny, evaluation and comparison of offers, Central Bank of India may, at its discretion, ask some or all bidders for clarification of their offer. The request for such clarifications and the response will necessarily be in writing.

4.13 No Commitment to Accept Lowest or Any Tender

Central Bank of India shall be under no obligation to accept the lowest or any other offer received in response to this tender notice and shall be entitled to reject any or all offers including those received late or incomplete offers, without assigning any reason whatsoever. Central Bank of India reserves the right to make any changes in the terms and conditions of the RFP. Central Bank of India will not be obliged to meet and have discussions with any bidder, and or to listen to any representations.

4.14 Submission of Technical Detail

It is mandatory to provide the technical details in the exact format of **Bidder's Information as per Annexure-2**. The offer may not be evaluated by Central Bank of India in case of non-adherence to the format or non-submission / partial submission of technical details as per the format given in the tender. Central Bank of India will not allow/permit changes in the technical specifications once it is submitted. The relevant information, printed brochure, technical specification sheets etc. should be submitted along with the offer. Failure to submit this information along with the offer can result in disqualification (Please refer to the suggested checklist given in this document)

4.15 Format for Technical bid

The Technical bid must be made in an organized, structured and neat manner. Brochures/leaflets etc. should not be submitted in loose form. This can be divided into

three parts – the first part should contain the documents supporting the eligibility of the vendor to participate in the tendering process as per the eligibility criteria mentioned in the RFP, the second part should contain the technical details of the proposed project and the third part should contain the technical brochures etc.

The suggested format for submission of Technical bid is as follows:

1. Index
2. Covering letter. This should be as per Annexure-1.
3. Details of the bidder, as per Annexure-2.
4. Compliance of eligibility criteria along with support documents in following format:

Sr. No	Short Description of Eligibility Criteria	Support Documents to be submitted	Submitted Yes/ No	Write whenever required(figures)
1	The Bidder must have a minimum turnover of INR 1.5 crores (One crore fifty lacs only) per annum out of its IT / Audit / Security operations for the past 3 years.	Audited Balance Sheets 2017-18 2018-19 2019-20 (If the balance sheet is provisional the CFO of the Company should certify the same under Company's Seal)		
2	Vendor should have the experience of conducting audit from any three of the following core areas: 1.CBS Application Functionality audit and post implementation 2.Audit of DC/DRC/ Near site 3.Networking audit 4. Cyber Security audit 5.IS Audit/System audit of Delivery channel for Two Banks out of which at least one should be Public Sector Bank in India .	Copy of letter of assignment & certification of satisfactory completion of assignment to be submitted from respective Bank/banks		
3	The Bidder should have been in IT Security Management and doing audit related business for at least the past 5 years, i.e. 2016-17, 2017-18, 2018-19, 2019-20 2020-21.	Provide proof, such as Certificate of Constitution issued by relevant authorities.		

Sr. No	Short Description of Eligibility Criteria	Support Documents to be submitted	Submitted Yes/ No	Write whenever required(figures)
4	The bidder's Audit team shall consist of minimum 6 permanent experts/ Certified resource with minimum one each from :- a). ACA/FCA b). CISA c). CISSP/ CISM d). ISO 27001 LA/ ISO 22301 LA e). CCNP/ CCSP f). CEH	Details of minimum six experts / Certified Resources with minimum one each from : a). ACA/FCA b). CISA c). CISSP/ CISM d). ISO 27001 LA/ ISO 22301 LA e). CCNP/ CCSP f). CEH		
5	Bidder must warrant that key project personnel to be deployed in this project, they have been sufficiently involved in the similar project in the past.	Provide along with the proposal, the bio data of the persons doing the audit be submitted indicating their qualifications, professional experience and projects handled etc.		
6	Company/firm should not be appointed as consultant or should not be associated as a sub-agent/business partner of the principal who is system integrator of CBS project running in the Bank. The Bidder should also not be involved directly or indirectly in implementing CBS Project in the Bank.	Self-declaration for not being associated as consultant for CBS project running in the bank.		
7	The bidder should not be blacklisted by any of the institution.	Self-declaration for not being black listed by any Govt. Authority or Organization.		
8	The Bidder (i) should be in existence for at least five years as on 31.03.2021 (In case of mergers/ acquisitions/ restructuring or name change, the date of establishment of earlier/ original Partnership Firm/ Limited Company can be taken into account)	Provide proof, such as Certificate of Constitution issued by relevant authorities. Copy of letter of		

Sr. No	Short Description of Eligibility Criteria	Support Documents to be submitted	Submitted Yes/ No	Write whenever required(figures)
	and **(ii) Should have done audits as above in 2 Banks out of which at least one should be a Public Sector bank in India. Certificate from the bank to that effect to be submitted**	assignment & certification of satisfactory completion of assignment to be submitted.		
9	The Bidder Company should be profit making company for the last three financial years i.e., 2017-18, 2018-19 & 2019-20. A copy of last three financial years' relevant audited balance sheets and profit and loss statements should be submitted with the offer.	The applicant should be a profit making entity. Provide Profit figure **(Net Profit after Tax)** of following years : 2017-18 2018-19 2019-20		
10	The bidder should have executed orders for above Audits totaling to Rs. 50 Lacs during last three financial years.	Necessary Certificates having executed orders of aggregate value of minimum Rs. 50 lacs during last three financial years for Information Systems Audit including that of Cyber Security / CBS Application /Functionality Audit/ Audit of DC / DRC, Networking Audit, IS Audit / System Audit of CBS / Delivery channel Audits (This certification is in addition to the copies of purchase orders enclosed)		
11	Domain Knowledge, technical knowledge and Credentials: -The personnel involved in the audit should possess domain knowledge of retail, corporate, trade finance, corporate banking and other general banking operations. The proof as to his involvement in CBS application	Provide details of domain knowledge, technical knowledge and credentials for professionals involved in the proposed audit.		

Sr. No	Short Description of Eligibility Criteria	Support Documents to be submitted	Submitted Yes/ No	Write whenever required(figures)
	audit project- to be enclosed. -Should have proven methodologies and approach for program governance and project monitoring. The personnel involved should possess technical knowledge of doing the Information security audit of Applications, DC, DRC, networking and Cyber Security audit.			
12	The vendor should be empanelled with CERT-In.	Copy of Certificate of empanelment with CERT-IN		

Additional information for Technical Bid Evaluation Criteria:

Sr No	Particulars	Support documents to be submitted	Submitted Yes/ No	Write whenever required (figures)
1	Period (in years) since the Bidder is empanelled for IT Security auditing with Computer Emergency Response Team – India (Cert-In) Government of India, Delhi	Number of years of empanelment with CERT-IN (Copy of Certificate of empanelment with CERT-IN)		
2	Number of technically qualified auditor/professional as mentioned below on the permanent roll of the organization. The list of Qualifications/ Certifications are as CISA, CISSP, CISM, BS7799 , ISO 27001 LA, CCNP, CCSP,CIEH, CCSE, CVA, CEH	Details and number of technically qualified auditors/professionals on the permanent roll of the organization.		
3	Domain Knowledge and	Details and Number of ACA/FCA on the		

Sr No	Particulars	Support documents to be submitted	Submitted Yes/ No	Write whenever required (figures)
	Credentials – The personnel involved in the audit should possess domain knowledge of retail, corporate, trade finance, corporate banking and other general banking operations. The proof as to his involvement in CBS application audit project to be enclosed. Number of ACA/ FCA on the permanent roll of the organization.	permanent roll of the organization having domain knowledge.		
4	Number of years for which bidder is carrying out Information Security Audit	Details and Number of years for which bidder is carrying out Information Security Audit.		
5	Number of years for which Application system audit of CBS and related application is being carried out by the bidder	Number of years for which Application system audit of CBS and related application carrying out by the bidder.		
6	Number and list of tools used so far by the bidder in the Information Security Audit & application audit. - No. of Licensed / supported version of open source tools - No. of Commercial tools :- - No. of Proprietary tools :-	Name and details of Licensed / Commercial / proprietary tools that will be used in the proposed audit.		
7	Number of completed audit which includes Cyber Security, Network Audit, DC/DRC audit and CBS & other application software	Details & number of such audits completed in last three years.		

Sr No	Particulars	Support documents to be submitted	Submitted Yes/ No	Write whenever required (figures)
	audit in Private Sector Bank/ PSU Banks (Excluding Co-operative banks) in last three years.			

The eligibility criteria will be verified based on above compliance table duly filled by the bidder, submitted along with the supporting documents.

5. The bidder should give undertaking that bidder complies/ accepts all terms and conditions stipulated in the RFP without any deviations.
6. Implementation methodology
7. Name, Qualifications and Domain knowledge of the personnel who are going to audit the various modules from the audit firm. Please submit details for each person as per **Annexure 4: Format of curriculum vitae (CV)**
8. Types and details of Tools that are going to be used for the auditing.
9. Audit period
10. Deliverables
11. Project plan
12. Bidder's Financial Details (audited balance sheets, annual reports etc.) and other supporting documents, as required in the tender document.
13. All documentary evidences, wherever required to be submitted, be properly arranged.
14. Copy of the Commercial Bid duly masking the price column.
15. Integrity Pact, as per attached Annexure 8, on stamp paper of INR 500/-.

Masked Commercial

The bidder should submit a copy of the actual price bid being submitted to the bank by masking the actual prices. This is mandatory. **The bid may be disqualified if it is not submitted.**

4.16 Format for Commercial bid

The Commercial bid must not contradict the Technical bid in any way. The suggested format for submission of Commercial bid is as follows:

a. Index
b. Covering letter
c. Commercial Version of commercial bid document as per Annexure -3
d. A statement that the bidder agrees with Payment terms given in the tender.

The Commercial bids will have to be submitted in the format as per **Annexure-3**. Commercial bids should not have any alteration or overwriting. The bank may reject or load the financial implication of any alteration, if found into the commercial bid submitted by the

respective bidder. The calculation arrived by the Bank will be final and will be binding on the bidders. If any cost items in the commercial bid are found to be blank and not filled with any amount then it shall be considered as zero and the same will be offered to the Bank free of any charges. If quoted amount differs in figures in word, Bank will consider the amount quoted in words.

4.17 Costs & Currency

The offer must be made in Indian Rupees only, and price quoted must include all costs, taxes and levies.

4.18 Fixed Price

The Commercial bid shall be on a fixed price basis, inclusive of all taxes and levies at site as mentioned above. No price variation including those relating to increases in customs duty, excise tax, Service tax, dollar price variation etc. will be permitted.

4.19 No Negotiation except with L1

It is absolutely essential for the bidders to quote the lowest price at the time of making the offer in their own interest, as Central Bank of India will not enter into any price negotiations, except with the lowest quoting bidder, whose offer is found to be fully technically compliant.

4.20 Short-listing of Bidders

Central Bank of India will short-list the bidders on the basis of Technical Evaluation & Commercial evaluation as mentioned in para 5.3 (Bid Evaluation Criteria).

4.21 Right to Alter location.

Central Bank of India reserves the right to alter the proposed locations to be audited.

4.22 Repeat Orders

Central Bank of India reserves the right to place repeat order/s to the successful bidder under the same terms and conditions for next year (maximum one year) also as per need of the Bank, subject to satisfactory performance of the Audit exercise in terms of RFP.

4.23 Cooling period:

There will be a cooling period of one year, in case the same vendor, by virtue of being L1 or otherwise, has been allotted the assignment consecutively for previous three years.

5. Qualification Criteria

5.1 **Eligibility of the Bidder**

Reputed companies/ Firm, who have experience in executing similar projects and who meet the following Eligibility criteria only need to apply:-

5.1.1 The Bidder must have a minimum turnover of INR 1.5 crores (One crore fifty lacs only) per annum out of its IT / Audit / Security operations for the past 3 years & should submit audited financial statements for the year of 2017-18, 2018-19 and 2019-20.

5.1.2 The bidder should be a reputed IT Auditing company / Firm having existence in India and should have the experience of conducting Audit from any three of the following core areas :

- CBS Application functionality audit and Post Implementation review Audit
- Networking Audit
- Cyber Security
- DC/ DRC Audit
- IS Audit / System Audit of Delivery Channels

of at least One Public Sector Bank in India.

5.1.3 The Bidder should have been in IT Security Management and doing audit related business for at least the past 5 years, i.e. 2016-17, 2017-18, 2018-19, 2019-20 & 2020-21.

5.1.4 The bidder's Audit team shall consist of minimum 6 permanent experts/ Certified resource with minimum, one each from :-
a). ACA/FCA
b). CISA
c). CISSP/ CISM
d). ISO 27001 LA/ ISO 22301 LA
e). CCNP/ CCSP
f). CEH

5.1.5 Bidder must warrant that key project personnel to be deployed in this project have been sufficiently involved in the similar project in the past. Along with the proposal, the bio data of the persons doing the audit be submitted indicating their qualifications, professional experience and projects handled

5.1.6 Company/firm should not be appointed as consultant or should not be associated as a sub-agent/business partner of the principal who is system integrator of CBS project running in the Bank. The Bidder should also not be involved directly or indirectly in implementing CBS Project of the Bank.

5.1.7 The bidder should not be blacklisted by any of the institution. Self-declaration to that effect should be submitted along with the technical bid.

5.1.8 The Bidder should be in existence for at least five years as on 31.03.2021 (In case of mergers/ acquisitions/ restructuring or name change, the date of establishment of earlier/ original Partnership Firm/ Limited Company can be taken into account) and **should have done audits as above in 2 Banks out of which at least one in a Public Sector bank in India. Certificate from the bank to that effect to be submitted.**

5.1.9 The Bidder Company should have made profits in the last three financial years i.e. 2017-18, 2018-19 & 2019-20. A copy of last three financial years' relevant audited balance sheets and profit and loss statements should be submitted with the offer.

5.1.10 The bidder should have executed orders for above Audits totaling to Rs. 50 Lacs during last three financial years.

5.1.11 Domain Knowledge, technical knowledge and Credentials

- The personnel involved in the audit should possess domain knowledge of retail, corporate, trade finance, corporate banking and other general banking operations. The proof as to his involvement in CBS application audit project to be enclosed.
- Should have proven methodologies and approach for program governance and project monitoring. The personnel involved should possess technical knowledge of doing the Information security audit of Applications, DC, DRC, networking and Cyber Security audit.

. 5.1.12 the vendor should be empanelled with CERT-In.

5.1.13 Bidder should not be involved in Information System Audit and Security Audit of the Central Bank of India during last three financial years

5.2 Bid Evaluation Criteria

Bidders Selection/Evaluation Process-

The evaluation of technical proposals will be based on the following:

-Bidder's financial stability
-Methodology/Approach proposed for accomplishing the proposed project.
-Professional qualifications and experience of the key staff proposed/ identified for this assignment.
-Previous experience of the bidder in undertaking projects of similar nature.
-Activities / tasks, project planning, resource planning, effort estimate etc.

Technical evaluation:

Central Bank of India will scrutinize the technical offers and will determine whether the technical details along with documents have been furnished as per RFP and whether items/services are quoted as per the schedules / annexure. The technical evaluation will be done on the basis of the information provided in the "Bidder's Information" format along with supporting documents. The bidder will have to give presentation on the following points as a part of the technical evaluation.

1. Implementation of suggested audit methodology
2. Audit tools proposed to be used
3. Audit period for completion of the assignment
4. Deliverables
5. Project plan
6. Audit Team details such as qualifications, experience etc
7. Case study of any of the similar audits carried out in the past
8. Certificate of the public sector bank as a proof for carrying out audit of Cyber Security, Network, CBS project and other applications.

Various stages of technical evaluation are given below:

- Matching the clear eligibility criteria as indicated under Clause 5 (Qualification Criteria)
- Short-listing of the bidders based on the fully matched criteria
- Paper evaluation based on response
- Arriving at the final score on technical proposal

At the sole discretion and determination of the Bank, the Bank may add any other relevant criteria for evaluating the proposals received in response to this RFP.

The evaluation of the response to this RFP will be done on **70-30 techno-commercial evaluation method**. 70% weightage is to the response to Table below – "Technical Bid evaluation criteria" and 30% weightage to the response to Annexure 3 – "Commercial Bid Format". The evaluation will be done on a total score of 100. An illustration of the techno-commercial evaluation methodology has been given below:

Total score = 0.70 x T (s) + 0.30 x F(s)
Where:
T(s) = T(v)/100 x 100
F(s) = (LEC / EC) x 100

Acronyms:
- T(s) stands for percentage of technical evaluation score out of 100
- T(v) stands for sum of the score as per 'Evaluation Criteria- Technical Bid Evaluation Criteria' (refer table below)
- F(s) stands for percentage of a consultant's commercial price compared to the lowest quoted price
- EC stands for Evaluated Cost of the Commercial offer quoted by the bidder
- LEC stands for Lowest Evaluated Cost of the Commercial offer amongst the bidder

The bidder scoring the higher marks based on the criteria given above will be awarded all the assignments given in Scope of work.

Bank may, at its sole discretion, decide to seek more information from the Bidder in order to normalize the bids. However, Bidder will be notified separately, if such normalization exercise is resorted as part of the technical evaluation.

Commercial Bid Evaluation Criteria

It may be noted that commercial bids will be subjected to following evaluation process-
- Only those bidders meeting the eligibility criteria & scoring 60% (60 marks out of 100) in the technical evaluation will be considered for further stages of evaluation and will be short-listed for commercial evaluation.
- Bidder whose commercial quote is found to be lowest (L1) on the basis of score arrived as per 70-30 techno commercial evaluation will be called for negotiation before awarding the contract. It may be noted that Bank will not entertain any price negotiations with any other bidder.

Table: Technical Bid Evaluation Criteria

Sr no	Particulars	Max. Marks	Min. Marks	Marks Allotted	Scoring Mechanism
1	Period (in years) since the Bidder is empanelled for IT Security auditing with Computer Emergency Response Team – India (Cert-In) Government of India, Delhi	**10**	**5**		**Maximum Marks – 10** 1) More than 3 years – **10 marks** 2) More than 1 and upto 3 years- **8 marks** 3). Upto 1 year – **5 marks**
2	Number of technically qualified auditor/ professional as mentioned below on the permanent roll of the organization. The list of Qualifications / Certifications are as CISA, CISSP, CISM, BS7799 , ISO 27001 LA, , CCNP, CCSP,CIEH, CCSE, CVA, CEH	**20**	**15**		**Maximum Marks – 20** 1) More than 20 qualified professionals – **20 Marks** 2)More than 10 and upto 20 qualified professionals – **18 Marks** 3) 5 to 10 qualified professionals – **15 Marks**
3	Domain Knowledge and Credentials - The personnel involved in the audit should possess domain knowledge of retail, corporate, trade finance, corporate banking and other general banking operations. The proof as to his involvement in CBS application audit project to be enclosed. Number of ACA/ FCA on the permanent roll of the organization.	**10**	**5**		**Maximum Marks – 10** 1) More than 10 audit professionals – 1**0 Marks** 2)More than 3 and upto 10 audit professionals – **8 Marks** 3) 1 to 3 Audit professionals (Domain Knowledge) – **5 Marks**
4	Number of years for which bidder is carrying out Information Security Audit	**10**	**5**		**Maximum Marks – 10** 1) More than 10 years – **10 marks** 2) 6 years to 10 5 years- **8 marks** 3). 5 years – **5 marks**
5	Number of years for which Application system audit of CBS and related application carrying out by the bidder	**10**	**5**		**Maximum Marks – 10** 1) More than 10 years – **10 marks** 2) 6 years to 10 years - **8 marks**

Sr no	Particulars	Max. Marks	Min. Marks	Marks Allotted	Scoring Mechanism
					3). 5 years – **5 marks**
6	Number and list of tools used so far by the bidder in the Information Security Audit & application audit. - No of Licensed / supported version of open source tools - No of Commercial tools :- - No of Proprietary tools :-	**10**	**5**		**Maximum Marks – 10** 1) No of commercial / proprietary tools more than 6 – **10 marks** 2) No of commercial / proprietary tools 4 to 6 - **8 marks** 3). No of commercial / proprietary tools 1 to 3 – **5 marks**
7	Number of completed audit which includes Cyber Security, Network Audit, DC/DRC audit and CBS & other application software audit in Private Sector Bank/ PSU Banks (Excluding Co-operative banks) in last three years.	**30**	**20**		**Maximum Marks – 30** 1. More than 5 audits **– 30 marks** 2.More than 2 and upto 5 audits – **25 marks** 3. 2 audits –**20 marks**
	TOTAL	**100**	**60**		

Minimum Qualifying Score will be 60% subject to fulfilling minimum marks criteria for each of the parameter.

Note:

- All references have to be from commercial banks in India only
- Banks exclude Cooperative Banks.
- The SP is required to provide documentary evidence for each of the above criteria and the same would be required on the client's letter head in case of credentials

6. Scope Of Work

The IS Audit should comply the various guidelines issued by RBI time to time. A few of them are as follows:-

-**Report of the Committee on Computer Audit (dated: April 2, 2002) Circular on Information System Audit–A Review of Policies and Practices (dated: April 30, 2004 (RBI/2004/191 DBS.CO.OSMOS.BC/ 11 /33.01.029/2003-04)**

-**Guidelines issued by RBI on 'Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds. Chapter 5 – IS Audit vide their letter No. RBI/2010-11/494 DBS.CO.ITC.BC.No. 6 /31.02.2008/2010-11 dated 29.04.2011.**

-**RBI guidelines on 'ATMs - Security and Risk Mitigation Measures for Card Present (CP) Transactions' vide their letter no. RBI/2015-2016/ 413 DPSS.CO.PD.No./2895/02.10.002/2015-2016 dated May 26, 2016**

-**RBI guidelines issued on "Cyber Security Frameworks' vide their letter no RBI/2015-16/418/ DBS.CO/ CSITE/ BC.11 /33.01.001/2015-16 dated 02.06.2016.**

-**RBI guidelines on 'Issuance and Operation of Pre-paid Payment Instruments in India' vide their letter no RBI/2016-2017/16/ DPSS.CO.PD.PPI. No.01/02.14.006/2016-17 dated July 01, 2016**

-**RBI guidelines on 'Mobile Banking transactions in India – Operative Guidelines for Banks' vide their letter no. RBI/2016-17/17 DPSS.CO.PD. Mobile Banking. No./2/02.23.001/2016-2017 dated July 1, 2016**

-**RBI guidelines on 'Security and Risk Mitigation Measures for Card Present and Electronic Payment Transactions – Issuance of EMV Chip and PIN Cards' vide their letter no RBI/2016-17/63 DPSS.CO.PD No.812/02.14.003/2016-17 dated September 15, 2016**

-**RBI guidelines on 'Security and Risk Mitigation measure - Technical Audit of Prepaid Payment Instrument issuers' vide their letter no.RBI/2016-17/178 DPSS.CO.OSD.No.1485/06.08.005/2016-17 dated December 09, 2016**

-**RBI guidelines on 'Master Direction on Digital Payment Security Controls' vide their letter no. RBI/2020-21/74 DoS.CO.CSITE.SEC.No.1852/31.01.015/2020-21 Dated February 18, 2021**
Compliance of various IT/ security related circulars/advisories/alerts issued by RBI during the period (say 01.04.2020 to audit completion date) should also be included.

IS Audit should include:-

- Determining effectiveness of planning and oversight of IT activities
- Evaluating adequacy of operating processes and internal controls
- Determining adequacy of enterprise-wide compliance efforts, related to IT policies and internal control procedures.
- Identifying areas with deficient internal controls, recommend corrective action to address deficiencies and follow-up, to ensure that the management effectively implements the required actions

6.1 Project Overview

To achieve the Banks objectives in the areas of Cyber Security, IT Risk Management, IT assets safeguarding, Data security, Data integrity, IT systems efficiency and effectiveness

and internal control systems. The Bank intends that the IS Security audit and Information systems audit of CBS & related systems should be according to the standards / Best practices prescribed by ISACA / ISO 27001.

6.2 Project Objective

The Bank wishes to make a comprehensive audit for Cyber Security , Centralized Banking Solution ("CBS'"), Security audit of its Data Center, Disaster Recovery Center, network infrastructure, delivery channels like Internet and Mobile (SMS/WAP) banking etc.

6.3 Purpose of the Comprehensive audit:

- To ensure the core Banking system :
  Actually meet business requirements, as intended by Bank
  - Operates appropriately and
  - Assists the user in performing their roles efficiently and effectively.
  - Ensure IT assets safeguards against threats & hazards and ensure data accuracy, integrity and protection.
  - Application meets the industry best practices securities standards
  - Find the bottlenecks in application which may lead to frauds.
  - Find the bottlenecks in CBS project to protect against threats & hazards.
- To ascertain whether the processes as desired by the Bank and controls implemented actually function as intended to do so in normal and also in exceptional circumstances and cases.
- To understand and appreciate the :
  - Strengths
  - Flexibility and
  - Weakness of the core Banking system as implemented and constraints imposed by system on user
- To ensure appropriate testing of various controls including input, process and output controls which wouldresult in :
  - Greater Comfort &
  - Enable the banks management to place reliance on the new solution being deployed

  Audit of Data Centre & Disaster Recovery & Network infrastructure and its compliance with industry best security standards & practices .

6.4 <u>Detailed Scope Of Work</u>

The detailed scope of work is enclosed as Annexure-6 . Scope of work for RRBs is given separately.

Bank however, reserves its right to give all modules or partial modules to the firm selected for the Audit.

6.5 Locations for audit:

Location of audit will be DC Navi Mumbai, Near Site Mumbai, DRC Hyderabad, and various departments of Central Office at Mumbai. Site/ locations of Outsourced vendors will be provided separately to interested / selected bidder.

6.6 Deliverables:

- **Pre Audit** – Prior to starting the groundwork on the audit, the successful bidder shall provide Audit plan and procedure for Cyber Security audit, application and security review of CBS and other applications, DC/DRC audit, Network audit, audit of ATM project and audit of Outsourcing activities. Detailed test cases and plans for the items as per scope of audit.

  Selected vendor has to submit the details of tool(s)to be used for VAPT including name of tool.
  Selected vendor has to submit the copy of license of the tool to be used for VAPT

- **Project Management** :- As a part of the project management monthly reports on status of audit vis-à-vis finalized audit plan shall be submitted to the Bank.

- Vendor will involve the bank's staff during audit. All the audit reports/deliverables during & at the end of audit will be property of the bank.
- The vendor will furnish the audit report (Interim/Final/Compliance) in different parts i.e 1. Report on audit of Application audit, 2. DC,DRC audit 3. Report on audit of Network & Cyber security 4. Report on Audit of ATM project 5. Audit of Outsourcing activities. The audit reports/findings on these five areas should not be intermixed.
- Selected vendor has to submit location-wise reports i.e. separate reports for technical and functional observations.
- All reports should be submitted in soft as well as hard copy.
- Interim reports should be submitted first and would be discussed with Bank and after that final reports would be submitted.
- In Final/ review of compliance report comments/remarks/ compliance of auditee should be included.
- After the audit, reports are to be provided at par with "International Standard' and risk category wise.
- All Checklist and – used during the audit should be provided to the Bank.

7. Terms and Conditions

7.1 Project Timeline

The bidder has to adhere to the following time lines.

Stages	Particular	Period
Stage 1	Commencement of Audit work after acceptance assignment letter / contract	One week
Stage 2	Submission of audit plan, procedure and methodology as per scope of work	Two weeks
Stage 3	Submission of Interim report-after Stage 2	Six weeks
Stage 4	Submission of Final report after Stage 3	Ten weeks

Stage 5	Submission of final compliance review report – after Stage 4	Ten weeks

The total Project should be completed within Seven months of placing of order.

7.2 Payment Terms

The successful bidder will have to give Performance Bank Guarantee for 10% of the total project cost, while submitting the acceptance of order. The validity of the Performance Bank Guarantee should be for 8 months, if required, it should be renewed till completion of the audit.

Payment will be made as follows:

25%	On submission of Interim Audit report
50%	On submission of Final audit report
25%	On submission of final review of compliance report covering all the points as per the scope of audit and its acceptance by the bank

7.3 Delay in conducting assignment

The successful bidder must strictly adhere to the audit schedule, as specified in the Contract, executed between the bank and the successful bidder, pursuant hereto, for performance of the obligations arising out of the contract and any delay will enable the Bank to resort to any or all of the following at sole desecration of the bank.

(a) Claiming Liquidated Damages
(b) Termination of the agreement fully or partly

In addition to the termination of the agreement, Central Bank Of India reserves the right to appropriate the damages from the earnest money deposit (EMD) given by the bidder or invoke the Bank Guarantee given in lieu of EMD and/or invoke the bank guarantee given by the bidder against the advance payment. The Bank also reserves the right to black list the bidder and inform the same to appropriate forums.

Penalty:

Delayed start of audit, delayed completion of audit and delayed submission of report as per agreed terms defined in the RFP will attract penalty of 0.5% per week on delay of total amount payable for audit assignment (maximum up to 15% of the fees), if the delay was solely the auditor's fault and reasons not attributable to Bank.

The Bank also reserves right to charge penalties and to claim damages for improper or incomplete execution of the assignment.

7.4 Liquidated Damages

The liquidated damages will be an estimate of the loss or damage that the bank may have suffered due to delay in performance of the obligations (under the terms and conditions of

the contract) by the successful bidder and the successful bidder shall be liable to pay the Bank as liquidated damages at the rate of 0.25% of total contract value for delay of every week or part thereof. Without any prejudice to the Bank's other rights under the law, the Bank shall recover the liquidate damages, if any, accruing to the Bank, as above, from any amount payable to the successful bidder either as per the Contract, executed between the Bank and the successful bidder pursuant hereto or under any other Agreement/Contract, the Bank may have executed/shall be executing with the successful bidder.

7.5 Indemnity

The successful bidder shall, at their own expense, defend and indemnify the Bank against any claims due to loss of data / damage to data arising as a consequence of any negligence during CBS Application/Functionality Audit, Network, DC, DRC audit, Cyber audit etc.

7.6 Publicity

Any publicity by the bidder in which the name of Central Bank Of India is to be used should be done only with the explicit written permission of Central Bank Of India.

7.7 Force Majeure

The successful bidder or the Bank is not responsible for delays or nonperformance of any contractual obligations, caused by war, blockage, revolutions, insurrection, civil commotion, riots, mobilizations, strikes, blockade, acts of God, plague or other epidemics, fire, flood, obstructions of navigation by ice of port of dispatch, acts of Govt. or public enemy or any other event beyond the control of either party which directly, materially and adversely affect the performance of any contractual obligation.

If a force majeure situation arises, the successful bidder shall promptly notify the Bank in writing of such conditions and the change thereof. Unless otherwise directed by the Bank, in writing, the System Auditor / Firm shall continue to perform his obligations under the contract as far as reasonably practiced and shall seek all reasonable alternative means for performance not prevented by the force majeure event.

7.8 Resolution of Disputes

Central Bank of India and the successful bidder shall make every effort to resolve amicably, by direct informal negotiation, any disagreement or dispute arising between them under or in connection with the contract. If after thirty days from the commencement of such informal negotiations, Central Bank Of India and the Bidder are unable to resolve amicably a contract dispute; either party may require that the dispute be referred for resolution by formal arbitration.

All questions, disputes or differences arising under and out of, or in connection with the contract, shall be referred to two Arbitrators: one Arbitrator to be nominated by Central Bank of India and the other to be nominated by the Bidder. In the case of the said Arbitrators not agreeing, then the matter will be referred to an umpire to be appointed by the Arbitrators in writing before proceeding with the reference. The award of the Arbitrators, and in the event of their not agreeing, the award of the Umpire appointed by them shall be final and binding

on the parties. THE ARBITRATION AND CONCILIATION ACT 1996 shall apply to the arbitration proceedings and the venue & jurisdiction of the arbitration shall be Mumbai.

7.9 Privacy and Security Safeguards

The successful Bidder shall not publish or disclose in any manner, without the Bank's prior written consent, the details of any security safeguards designed, developed, or implemented by the successful Bidder under this contract or existing at any Bank location. The successful Bidder shall ensure that all subcontractors who are involved in audit process shall not publish or disclose in any manner, without the Bank's prior written consent, the details of any security safeguards designed, developed, or implemented by the successful Bidder under this contract or existing at any Bank location.

7.10 Confidentiality

Successful bidder will be required to execute a Non-Disclosure and Confidentiality Agreement and similar other documents as may be desired by the Bank.

7.11 Independent External Monitor:

Bank has appointed Two Independent External Monitors (hereinafter referred to as IEM) for this pact, whose name and e-mail ID are as follows:

1. Dr. Kishore Kumar Sansi [mail: kishoresansi1@gmail.com]
2. Sri Trivikram Nath Tiwari [mail: trivikramnt@yahoo.co.in

- IEM"s task shall be to review –independently and objectively, whether and to what extent the parties comply with the obligations under this pact
- IEM shall not be subjected to instructions by the representatives of the parties and perform his functions neutrally and independently.

Both the parities accept that the IEM has the right to access all the documents relating to the project/procurement, including minutes of meeting.

8. Annexure

8.1 List of abbreviations

List of abbreviations used in this RFP

ACA	**Associate Chartered Accountant**
CBS	**Core Banking Solution**
CCNP	**Cisco Certified Network Professionals**
CCSE	**Checkpoint Certified Security Expert**
CCSP	**Cisco Certified Security Professional**
CEH	**Certified Ethical Hacker**
CERT-IN	**Computer Emergency Response Team-India**
CIHE	**Certified Incident Handling Engineer**
CISA	**Certified Information System Auditor**
CISSP	**Certified Information System Security Professional**
CISM	**Certified Information Security Manager**
CA&ID –	**Central Audit & Inspection Department**
CV	**Curriculum Vitae**
CVA	**Certified Vulnerability Assessment**
CVC	**Central Vigilance Commission**
DC –	**Data Centre**
DR	**Disaster Recovery**
DRC –	**Disaster Recovery Centre**
EMD –	**Earnest Money Deposit**
I S Audit	**Information System Audit**
I S Security	**Information System Security**
LAN	**Local Area Network**
NAP	**Network Aggregation Point**
NEFT	**National Electronic Fund Transfer**
OWASP	**Open web Application Security Project**
PBG –	**Performance Bank Guarantee**
PT	**Penetration Testing**
RFP –	**Request for Proposal**
RTGS	**Real Time Gross Settlement**
WAN	**Wide Area Network**
VA	**Vulnerability Assessment**

8.2 Annexure 1: Format of Tender offer cover letter

Date: _____2021
Tender Reference No.:_____

To:

_____
_____
_____

Having examined the tender documents including all annexure, the receipt of which is hereby duly acknowledged, we, the undersigned, offer to perform Cyber Security audit and comprehensive audit of CBS project and other applications at DC,DRC & branches / ATM locations as mentioned in scope of work in conformity with the said tender documents in accordance with the Commercial bid and made part of this tender.

We understand that the RFP provides generic specifications about all the items and it has not been prepared by keeping in view any specific bidder.

If our tender offer is accepted, we undertake to commence the audit work within_____ (Number) days and to complete audit work as specified in the Contract within _____ (Number) days calculated from the date of receipt of your Notification of Award/Letter of Intent.

We agree to abide by this tender offer till 210 days from the date of tender opening and our offer shall remain binding upon us and may be accepted by the Bank any time before the expiration of that period.

Until a formal contract is prepared and executed, this tender offer, together with the Bank's written acceptance thereof and the Bank's notification of award, shall constitute a binding contract between us.

We understand that the Bank is not bound to accept the lowest or any offer the Bank may receive.

Dated this _____ day of _____2021

Signature: _____

(In the Capacity of:) _____

Duly authorized to sign the tender offer for and on behalf of

8.3 Annexure 2: Bidder's Information

1. Name
2. Constitution and year of establishment
3. Registered Office/Corporate office/Mailing Address
4. Names & Addresses of the Partners if applicable
5. Contact Person(s):
6. Telephone, Fax, e-mail
7. Number of CISA/ CISSP Qualified persons who would be involved in the Audit work along with names and experience.
8. Number of BS7799 lead auditors / ISO 27001 who would be involved in the Audit work along with the names and experience.
9. Qualified network/ Cyber security professionals who would be involved in the Audit work.
10. Proof of experience in Cyber Security audit and CBS System Audit. Please give details of the same including the details of services and the scope.
11. Describe Project Management methodology for the proposed Cyber Security audit and CBS System Audit assignment, clearly indicating about the composition of various teams.
12. Describe Audit Methodology and Standards to be used for Cyber Security audit & CBS System Audit.
13. Indicate Project Plan with milestones and the time frame of completion of different activities of the project.
14. List of Deliverables .
15. Specify that technical consultants who would be involved in the Audit work be certified on types of tools used for audit.
16. Details of the biggest Information Security Audit including the scope, service cost and details of services in last 3 years.
17. Any other related information, not mentioned above, which the audit firm wish to furnish.

DECLARATION

We hereby declare that the information submitted above is complete in all respects and true to the best of our knowledge. We understand that in case any discrepancy or inconsistency or incompleteness is found in the information submitted by us, our application is liable to be rejected.

Date: Authorised Signatory.

Note:

The Technical Bid shall include the detailed project plan corresponding to the deliverables as required by Central Bank of India for the Project. The project plan should indicate the milestones and time frame of completion of the different activities of the project. The audit firm is required to give details of the project management methodology, Audit Standards and methodology along with the quantum of resources to be deployed for the project, in the technical bid. Resources and support required from the Bank may also be clearly defined.

8.4 Annexure 3: commercial bid

The Commercial Bid should contain the Total project cost, on a fixed cost basis. Central Bank of India will not provide any reimbursement for traveling, lodging / boarding, local conveyance or any other related expenses.

The format for the commercial bid is given below:-

Sr No	Particulars	No of Man Months (a)	Rate per Man Months (b)	Total Cost (Rs) (a*b)
1	**Application Audit:** The complete review and audit of the Core Banking Application (CBS B@ncs24) and other applications. Audit of Delivery Channels i.e. Internet Banking, Mobile Banking (SMS/ WAP), NEFT etc. As per Annexure-C			
2	**DC/DRC/ Near Site Audit**:-Thorough Audit of bank's Data Centre (DC) at Navi Mumbai, Disaster Recovery Centre (DRC) at Hyderabad and Near Site at Sify Technologies Ltd, Airoli, Navi Mumbai. Audit of Disaster Recovery and Business Continuity Plans & Anti-virus system			
3	**Network Audit / Cyber Security Audit :-**Network Infrastructure and Security Audit of Network. Vulnerability Assessment (VA) of all Servers and Penetration Testing (PT) of public facing application like Internet Banking, Mobile Banking & SMS Banking including SMS Alerts on.			
4	**Audit of ATM Project:-** ATM switch, ATM card related operations, General review, Cash Management.			
5	**Outsourcing Audit**:-I S Audit of Outsourcing activities (as per list given) as per Guidelines of RBI. 1. DIT 2. ATM / Debit Card 3. Central Card 4. Financial Inclusion 5. Operation 6. Recovery 7. Others			
6	**A. Comprehensive System Audit of Core Banking Solution (Finacle) of RRB-1 including audit of DC/ DRC, Vendor's responsibilities as per SLA**			
	B.Comprehensive System Audit of Core Banking Solution (Finacle) of RRB-2 including audit of DC/ DRC, Vendor's responsibilities as per SLA			
7	Any other expenses to be specified			
	TOTAL			

8.5 Annexure 4: Format of curriculum vitae (CV)

(Separate sheets for each person)

Name of Firm :

Name of personnel :

Date of birth :

Qualifications: Technical and Academic with year of passing

Nationality :

Profession :

Position :

Years with firm :

Details of Domain Knowledge :-

Membership of Professional Societies:

Detailed Tasks Assigned : (past 5 years i.e. 2016-17, 2017-18, 2018-19, 2019-20 & 2020-21.**)**

(Giving an outline of person's experience and training most pertinent to task on assignment. Describe degree of responsibility held by the person on relevant previous assignments and give dates and locations)

Employment Record:
(Starting with present position, list in reverse order)

8.6 Annexure 5: checklist of documents to be submitted

1.Eligibility Criteria
2.Technical Bid
3.Security Deposit / EMD
4.Masked commercial Bid
5.Format of CV for the professionals to be involved in the CBS System Audit
6.Commercial Bid
7. Integrity Pact

8.7 ANNEXURE- 6: SCOPE FOR CYBER SECURITY AUDIT, COMPREHENSIVE IS AUDIT OF CBS PROJECT AND OTHER APPLICATIONS-

Scope Of Work

The IS Audit should comply the various guidelines issued by RBI time to time. A few of them as mentioned below :-

Report of the Committee on Computer Audit (dated: April 2, 2002) Circular on Information System Audit–A Review of Policies and Practices (dated: April 30, 2004 (RBI/2004/191 DBS.CO.OSMOS.BC/ 11 /33.01.029/2003-04)

Guidelines issued by RBI on 'Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds. Chapter 5 – IS Audit vide their letter No. RBI/2010-11/494 DBS.CO.ITC.BC.No. 6 /31.02.2008/2010-11 dated 29.04.2011 (Annexure A & B- enclosed).

RBI guidelines on 'ATMs - Security and Risk Mitigation Measures for Card Present (CP) Transactions' vide their letter no. RBI/2015-2016/ 413 DPSS. CO. PD. No./ 2895/ 02.10.002/2015-2016 dated May 26, 2016

RBI guidelines issued on "Cyber Security Frameworks' vide their letter no RBI/2015-16/418/ DBS.CO/ CSITE/ BC.11 /33.01.001/2015-16 dated 02.06.2016.

RBI guidelines on 'Issuance and Operation of Pre-paid Payment Instruments in India' vide their letter no RBI/2016-2017/16/ DPSS.CO.PD.PPI.No.01/ 02.14.006/2016-17 dated July 01, 2016

RBI guidelines on 'Mobile Banking transactions in India – Operative Guidelines for Banks' vide their letter no. RBI/2016-17/17 DPSS.CO.PD. Mobile Banking. No./2/02.23.001/2016-2017 dated July 1, 2016

RBI guidelines on 'Security and Risk Mitigation Measures for Card Present and Electronic Payment Transactions – Issuance of EMV Chip and PIN Cards' vide their letter no RBI/2016-17/63 DPSS.CO.PD No.812/02.14.003/2016-17 dated September 15, 2016

RBI guidelines on 'Security and Risk Mitigation measure - Technical Audit of Prepaid Payment Instrument issuers' vide their letter no.RBI/2016-17/178 DPSS.CO.OSD.No.1485/06.08.005/2016-17 dated December 09, 2016 etc.

Bank's policies & procedures related IT, IT Security , Cyber Security, BCP etc.

IS Audit should include following :-

- Determining effectiveness of planning and oversight of IT activities
- Evaluating adequacy of operating processes and internal controls
- Determining adequacy of enterprise-wide compliance efforts, related to IT policies and internal control procedures
- Identifying areas with deficient internal controls, recommend corrective action to address deficiencies and follow-up, to ensure that the management effectively implements the required actions

Project Scope:

1) **Application Audit : C**omplete review of applications and security audit of all major applications including Core Banking Application (CBS-B@ncs24) and Delivery Channels i.e. Internet Banking, Mobile Banking (SMS/ WAP), RTGS/ NEFT, Financial Inclusion (FIGS) etc. In-house developed applications. (Approximate 42 applications)

   - Top 10 OWASP Vulnerabilities: Compliance review of top 10 OWASP (Open Web Application Security Project) vulnerabilities, especially for public facing applications viz. Internet Banking, Mobile Banking, Corporate Website, Financial Inclusion (FIGS) etc.. ISO 27001, Web-application security and other related security practices are to be observed.

   - VAPT (Vulnerability Assessment & Penetration Testing) : VA (Vulnerability Assessment) of all major applications including CBS & Delivery Channels, and Penetration Testing of public facing applications viz. Internet Banking, Mobile Banking, Corporate Website, Financial Inclusion (FIGS) etc.

2) **DC/ DRC Audit** : Thorough Audit of bank's Data Centre (DC) at Navi Mumbai, Disaster Recovery Centre (DRC) at Hyderabad and Near Site at Sify Technologies Ltd, Airoli, Navi Mumbai. Audit of Disaster Recovery and Business Continuity Plans for adequacy and conformance of BCP. Audit of effectiveness of Anti-virus system.

3) **Network / Cyber Security Audit :-**Network Infrastructure and Security Audit of entire Network infrastructure.

   Configuration Audit :- Configuration audit of various devices, especially for network & network security devices.

4) **Audit of ATM Project :-** Security audit of ATM switch, ATM card related operations.

5) **Outsourcing Audit** :- Covering audit of Information System, functional and operational aspects Outsourcing activities as per Guidelines of RBI. Outsourced activities/ vendor of DIT, ATM Deptt, Call Centre, Financial

Inclusion, Debit Card, Credit Card and other outsourced activities. (Approximate 41 outsourced activities)

6) **EOD Process:** EOD Process of CBS to be audited.

7) Comprehensive System audit of Core Banking Solution (Finacle) of 2 RRBs sponsored by Central Bank of India and having their Data Center at Navi Mumbai, Maharashtra.

Purpose of the audit :

- To ensure the core Banking system :
  - Actually meet business requirements, as intended by Bank
  - Operates appropriately and
  - Assists the user in performing their roles efficiently and effectively.
  - Ensure IT assets safeguards against threats & hazards and ensure data accuracy, integrity and protection.
  - Application meets the industry best practices securities standards
  - Find the bottlenecks in application which may lead to frauds.
  - Find the bottlenecks in CBS project to protect against threats & hazards.
- To ascertain whether the processes as desired by the Bank and controls implemented actually function as intended to do so in normal and also in exceptional circumstances and cases.
- To understand and appreciate the :
  - Strengths
  - Flexibility and
  - Weakness of the core Banking system as implemented and constraints imposed by system on user
- To ensure appropriate testing of various controls including input, process and output controls which would result in :
  - Greater Comfort &
  - Enable the banks management to place reliance on the new solution/ initiatives being deployed

- Audit of Data Centre & Disaster Recovery, Network infrastructure & cyber security and its compliance with industry best security standards & practices .

The below mentioned areas have been broadly referred to as General Banking Business

- Retail Deposits and Advances.
- Corporate Deposits and Advances
- Credit monitoring & NPA management
- General ledger & Trial Balance ,Balance Sheet
- Transaction and teller maintenance
- Lockers
- Off-Balance Sheet Items
- Credit Card business
- Ancillary Business - Bills and remittances
- Management Information System (MIS)

- Interest, commission, charges set up and computations
- Clearing and service branch operations.
- Inter branch operations
- Any other banking area

The Scope of work is broadly as under

Sr No	Business Area		Major Aspects to be covered
1	General Banking	Legal Compliance	• To ensure that the application/s conforms to the applicable provisions of any Act or Law in force with special emphasis on the following acts as amended up to date • Banking Regulation Act • RBI Act • Negotiable Instruments Act • Information Technology Act • Income Tax Act (emphasis on TDS) • FEMA • Contract Act • Transfer of Properties Act • Company Law • PMLA • Any other Applicable Act/ Law/ Rules Regulations
2.	General Banking	Compliance to Government **/ Regulators' guidelines**	To ensure that the application/s conforms • Government Guidelines more particularly Sponsored Schemes •Deposit Schemes e.g. Pension ,PPF •Advances Schemes e.g. PMRY MPBCDC etc. •To ensure that the application/s conforms to Government guidelines for •Classification of Priority Sector Advances. •reporting of Govt's / RBI's / Bank's guidelines / instructions as per Jilani Working Group, Risk & Control measures in computers and telecommunication system Vasudevan Committee report (to ensure ESCROW arrangements with the vendor),Working Group Report on Electronic Banking- Gopalakrishnan Committee, Report of Working Group on Internet Banking etc. as circulated by RBI •Any other relevant Central Government Guidelines.
	General Banking	Compliance to regulatory Guidelines	To ensure that the application/s conforms to the applicable regulatory guidelines e.g. R.B.I. Government of India, FIU-IND etc.
3.	General Banking	Accounting Standards	•To ensure that the application/s conforms to the accounting standards as applicable (General Ledger

Sr No	Business Area		Major Aspects to be covered
			application) •Account / BGL subhead - GL head mapping •Process of BGL creation, CGL head creation •Maker-checker control in GL administration •Review of integrity of B@ncs24 - GL application / interface. •Ability to modify/ update data directly in GL and availability of audit trails •Reconciliation – DD, PO, C2C, CHR/ CHP, Govt. Business, OLRR, Technical Contra, IMPS, ABPS, FI, IB
4.	General Banking	Compliance to Bank's Policies & Procedures / Guidelines	a. To ensure that the application/s conforms to the Bank's Policies Procedures / Guidelines e.g. I S Policy , Credit Policy, I.R.M Policy etc. b. Correctness of functionality of each module and all modules in totality with reference to the extant guidelines of the bank. c. Special Emphasis on Compliance to the relevant Information Security Policy of the Bank. d. **Conformity with Bank's operating procedures with procedures in Application software.** **e. Conformity of business processes with process architecture in Application software.**
5.	Income Recognition & Asset Classification	Income Recognition & Asset Classification	1.Verification of select accounts in Deposits and Advances (to be selected by the Auditor from various products). a. For Term Deposit products, interest calculation on maturity, periodical interest payouts and accruals interest calculation in case of pre-mature payments shall be verified. b. For Loan products, verification of interest Computation (should include calculation of penal interest and back-valuation.) Computation and application of interest, fees and charges for transactions of various types in Trade Finance. 2.Understand the logic and flow of the automated calculation of all income heads (interest, exchange, commission, discount) and re-perform the calculation outside the system to ensure that calculations are performed accurately by the system 3.Understand the logic and flow of the automated calculation of interest accruals and interest expense and re-perform the calculation outside the system to ensure that calculations are performed accurately by the system 4.Understand the logic and flow of the automated calculation of interest, fees and charges in Trade Finance application and re- perform the calculation outside the system to ensure that calculations are

Sr No	Business Area		Major Aspects to be covered
			performed accurately by the system 5.Verify that logics are built in accordance with the Bank's requirements. 6.Verify that all the above types of income/expense booked are accounted for properly and are reflected accurately in the General Ledger (by reference to balances under the relative heads as shown in the Finance 1 application) 7.Functionality of NPA tracking: Understand the logic and flow of the automated NPA Tracking in Core Banking System and verify that the classification of assets & Provisioning by the system is accurate.
6.	Information Systems	Management controls	To ensure proper controls are in place in the area of System development, programming management, data management, security management, operations management and quality assurance management. Industry Best Practices are observed wherever possible.
7.	Information	Information Security	1.Security features including user management. **2.Evaluation of controls prescribed by Bank's IS Policy and BC Policy (ISMS and BCMS) and conformity with ISO 27001 and ISO 22301 respectively.**
8.	Systems Information Systems	Application controls	1. Evaluation of existence and effectiveness of the following controls boundary, input, communications, processing, database 2. Evaluation of safeguarding of assets, data integrity, efficiency and effectiveness of the system 3. Evaluation of system documentation and user manuals and interface with menus, submenus and reports 4. Special emphasis on – a. Sufficiency / accuracy of all types of reports, b. Backups and recovery procedures, c. Audit trails, d. Version control, patch management, rollover, e. Setting of various parameters, f. Areas of income leakage, g. Generation of exception reports and their coverage.
9.	Information Systems	System Generated Transactions	Evaluate the Correctness ,Completeness, Confidentiality Integrity & Availability of System Generated Entries, BGL, CGL including ORACLE Apps and reconciliation thereof
10.	Information Systems	SLA	Compliance with Service Level Agreement (SLA) for Core Banking System. To ensure Monitoring of Service Level Agreements is done by the bank and vendors.
11.	Information	Bulk	Correctness , Completeness , Confidentiality ,Integrity,

Sr No	Business Area		Major Aspects to be covered
	Systems	Transaction Posting Utilities	Availability of transactions posted through bulk transaction posting utilities e.g. Trickle Feed Utility etc.
12.	Business Process Reengineering	Change Management	• Evaluation of the Procedures adopted by the bank for the Business Process Re-engineering and controls thereof with a special emphasis on the processes reengineered since 01/04/2014 Gap Analysis for the Processes Reengineered • **Evaluation of Change management process**
13.		Interfaces- Internal & External	Review process and controls over interface of TCS B@ncs24 application, including validation of interface files and handling of rejections, with the other applications
14.	Information Systems	Core Banking System Control Reports generation	Identify module wise modifications required to achieve the above.
15.	Information Systems	Disaster recovery Plan	• Ascertain DRP if documented, its adequacy, components, awareness, related provisions in software, testing, training needs, recovery alternative and suggest changes / modifications if any. • **Evaluation and review of RTO (Recovery Time Objective), RPO (Recovery Point Objective), MAO (Maximum Acceptable Outage) and MBCO (Minimum Business Continuity Objective) as per ISO 22301 standard.**
16.	Information Systems	Review Of hardware and software to Suggest measures if any for better control	•Maintenance, monitoring, effective and efficient usage of resources Access to Operating System (O.S.), Version control, O.S. security and compliance with essential and desired functionality for Transaction Processing and its support in areas of RDBMS, TCP/IP, distributed transactions managements, audit services etc. •Terms and conditions specified in Annual Maintenance Contracts of Hardware and Software to safeguard bank's interest •**Evaluation of Minimum Base Line Security documents and their implementation.** •**Evaluation of exceptions and their conformity to business requirements.**
17.	Miscellaneous	Audit of other areas	Procedures / guidelines vis-à-vis practice as regards generation / maintenance of record, access control and methods adopted for checking and verification Accounting procedure and control Any other area / aspect relevant to the assignment with mutual understanding
18.	Miscellaneous	Manual Interventions	In addition, the auditor will be required to verify 1.The risk that is posed by the manual interventions that are allowed in all the applications. This will be examined for the need to keep this and restrict it or the need to eliminate it. This decision will be conveyed by the auditor based on the critical nature of the manual control and availability of the system control to manage.
			2. Possibility of any wrong figures / misrepresentation or

Sr No	Business Area		Major Aspects to be covered
			misstatement in financial statement due to system generated entries.
			3. Auditor shall suggest any modification or addition to the existing report structure or addition of any report/s to existing reports to highlight major exception for better management control 4. The auditor is also expected to verify the correctness of any auto reconciliation process in the Core Banking System 5. The auditor shall also evaluate the System adopted by the Bank to verify the Background, competency and trustworthiness of vendor employees
19	IS Audit	IS Audit Controls	ISACA IS Auditing Guidance

1. SCOPE OF WORK FOR CBS & OTHER APPLICATIONS AUDIT

1.1 Application review of the software for Core banking solution and other applications

1. Study & review the implemented functionality of Core Banking Solution (B@ncs24) & allied modules/ applications in all the areas and to ensure correctness of functionality of each module & all modules in totality including parameterization with reference to the specifications given in the CBS RFP & other applications RFP floated and the procedure of the bank for all the modules like Retail deposits, advances, Trade Finance, Bills, Lockers, MIS etc.
2. Study the Core banking application for adequate input, processing and output controls and conduct various tests to verify existence and effectiveness of the controls.
3. Perform a test of controls and functionality setup in the Core Banking application and to ensure that all the functionalities and controls as stated in RFP for CBS are implemented properly and completely.
4. Review/audit the presence of adequate security features in CBS application to meet the standards of confidentiality, reliability and integrity required for the application supporting business processes.
5. Identify ineffectiveness of the intended controls in the software and analyze the cause for its ineffectiveness. Review adequacy and completeness of controls
6. Identify key functionalities not supported by the application.
7. Review effectiveness and efficiency of the Application.
8. Review of all controls including boundary controls, input controls, communication controls, database controls, output controls, interfaces controls from security perspectives.
9. Review of all Interface of application with other system OR interface of other system with applications for Security, accuracy, consistency and safety.
10. Review of EOD process of CBS.
11. Identifying critical risk areas, control weakness in application systems and recommended corrective actions from security prospective.
12. Review of data submitted to other systems for accuracy, completeness, timeliness and consistency of data submitted.
13. Identify and quantify revenue leakage due to IT bugs in the system
14. Identify the fee, charges, commission etc. which can be made system driven to reduce the revenue loss due to manual intervention.

1.2 Application Security and Controls for CBS and Other applications

Review of the application security features built within CBS and other application (list mentioned below) and also the Security and controls built in and around the operating system and data base used by the Core Banking Application (B@ncs24) both at the central level and at the client level. ISO 27001 guidelines, Web application security and other security related guidelines are to be observed.

Top 10 OWASP Vulnerabilities : Compliance review of top 10 OWASP (Open Web Application Security Project) vulnerabilities, especially for public facing applications viz. Internet Banking, Mobile Banking, Corporate Website, Financial Inclusion (FIGS) etc.

VAPT (Vulnerability Assessment & Penetration Testing) : VA (Vulnerability Assessment) of all major applications including CBS & Delivery Channels, and Penetration Testing of public facing applications viz. Internet Banking, Mobile Banking, Corporate Website etc.

– Application Security Controls

1.Review the application security setup supported by the Core Banking Solution and other applications to ensure:

- Access level controls are appropriately built and implemented into the Application
- Only authorized users should be able to edit, input or update data in the application or carry out activities as per their role and/or functional Requirements.
- user maintenance and password policies being followed are as per Bank's Information security policy
- Access on a „need-to-know" and „need to-do basis"

2.Identify gaps in the application security parameter setup in line with Bank's Information security policy and leading applicable practices

3.Review should include threat identification, assessment of threats, exposure analysis and control adjustment in respect of CBS application

- Review of operating system and Data Base Controls:

Review of Operating System Controls

1.Review specific operating system security features used and the parameters set

2. Identify security weaknesses and recommend solutions

3. Review sample user profiles against job roles

4.Minimum Base Line Security documents defined in IS Security Policy

Review of Data Base Controls

1Review specific database system security features used and the parameters set

2Check the database for optimal performance

3Procedure being adopted for data base updations through backend and documentation done in this regard

4Minimum Base Line Security documents defined in IS Security Policy

- Review of other Controls:

1.Review of user manuals, operating manuals and systems manuals and interface with menus, submenus and reports related to CBS, Trade Finance Module, GBM, AML and all other applications.

2.Review of

- Sufficiency/accuracy of all types of data extracts,
- Audit trails,

- Setting of various parameters, updation thereof and actual working of them as intended and accurately,
- Turn around time required for each transaction,
- Backups and recovery procedure / controls,

3.Review of management controls including systems development, data management, security management, operations management and quality assurance management and change management control.

System development – Problem / opportunity definition, Management of Change process, analysis of existing system, formulation of requirement, application Software development, procedure development, acceptance testing.

Data management Control– Users must be able to share data, data must be available to users when it is needed, in the location where it is needed and in the form, in which it is needed, it must be possible to modify data fairly easily in the light of changing user requirements, integrity of data must be preserved.

Security management - review of physical concerning personnel, hardware, facilities, supplies and documentation. Logical security control over malicious threats, review of security program.

Operations management to cover daily running of hardware, software, facilities, Production application system can accomplish their work, Segregation of duties and accesses of production staff and development staff with access control over development, test and production regions. Review of controls over computer operations, communication network control, data preparation and entry, production control, file library, documentation and program library, help desk and technical support, capacity planning and performance monitoring and outsourced operations.

Quality assurance management– ensuring achievement of certain quality goals and their development, implementation, operation and maintenance of system with a set of quality standards.

Review of hardware and software to suggest measures if any for better control.

Review of procedures for delivery channels i.e. ATM, NEFT, CPSMS, Internet and Mobile Banking from security prospective.

Verification/review of compliance with regulatory requirements including Guidelines/directives of Reserve Bank of India and CERT-IN, statutory agencies etc

Change Management control: Review of change management control procedure. Review of procedure/methodologies being adopted for carrying out the changes in application.

- Check & review application up & down time
- In application audit following audit points are to be included :-

1.Software Release Control Register
2.Standard instruction charge (Global)
3.Stop payment instruction charges (Global)
4.Cheque book charges (Global)
5.Account closing charges (Global)
6.Password Change parameters (Global)
7.Penal interest parameters

- **Evaluation and conformity of development / test activities as per IS Security policy of the bank.**
- **Evaluation of Regression testing and conformity as per IS Security policy of the bank.**
- **Vulnerability assessment of all the critical servers/ devices.**

2. <u>Scope of audit for Data Centre , Disaster Recovery Centre (DRC) & Near Site</u>

2.1 Physical security of Data Centre , Disaster Recovery Centre and Near Site

- Access control system
- Fire / flooding / water leakage / gas leakage etc.
- Handling of movement of man /material in /out of DC / DRC
- Air-conditioning of DC / DRC
- Electrical supply to DC/ DRC , Raw power / UPS / Genset
- Surveillance system of DC / DRC
- Redundancy of power level, UPS capacity at DC , DRC
- Physical & environmental controls at DC & DRC
- Assets safeguarding
- Incident handling procedures
- Parameters

2.2 Server system

The servers consists of WINDOWS & SUN servers, storage, tape library etc. installed at DC & DRC

- Physical / logical access to the servers
- Review of hardware installed in DC/DRC
- Inventory management / movement
- Configuration setting , parameterization
- Performance monitoring vis –a – vis RFP and SLA
- Audit logs / trails
- User / privilege management, default / build-in account management
- File system, directory & free space management
- Domain control / administration
- Backup and recovery policy and procedure

- Cross check between the primary server at DC and standby server at DRS with special attention to : Configuration / file system set-up and system change management
- Check & review application up & down time and various interfaces up time and down time

2.3 Database system

- Segregation of duties of database administrators
- Password policies
- User maintenance process
- User access privileges
- Authorization profiles
- Database security functionality
- Backup & Restore procedures
- Archival & Purge Procedures
- Backup security
- Check the database for optimal performance
- Monitoring the health of the database.
- Synchronization between DC and DRC databases

2.4 Operating System Security

The Auditor will review the operating system configuration and perform a preliminary assessment of its controls at DC, DRC. The review of the operating system will address:

- Operating System Installation
- Operating Systems Access controls
- Privilege Management
- Domain Account Policies
- Built In Accounts
- User Accounts Properties
- Groups
- Domain Administration
- Directory and File Security
- Back up & Recovery

2.5 Identity management

Auditing of identity management. The Auditor shall examine sensitive and critical IT systems and data files. The Auditor shall develop a list for review of data security techniques and Methods, which shall include the following :

I. Access control, integrity controls, and backup procedures
II. Media Storage, Handling, Disposal, cryptography
III. Sensitive data procedures and implementation

IV. Existing privacy policies and protections
V. Information access (authorization and implementation)
VI. Developmental systems and how systems are moved into production
VII. Written user responsibilities for management of information and systems.

Check application up/down time (and various interfaces too) as there may be instance due to one reason or other the server and database may be up and application may be down and our user are not able to access the CBS system

- Review & audit of DR Drill activity between DC & DRC
- Review & audit of Business continuity & disaster recovery procedure of CBS project
- Securities vulnerabilities at DC and DRC
- **Vulnerability assessment of all the critical servers/ devices.**

3. NETWORK INFRASTRUCTURE AND CYBER SECURITY AUDIT

3.1. Networking Infrastructure Audit

The scope of this audit is the complete review of the Local Area Network at Data Centre, Disaster Recovery Centre and Wide Area Network and is to conduct an intensive diagnostic and planning service designed to check the critical components of our network for Security, Reliability, Performance .The broad parameters, which are required to be reviewed by the auditor, are :

Configuration Audit :- Configuration audit of various devices, specially for network devices.

Review of security architecture and security policy

Assess all security vulnerabilities of the Local Area network (Data Centre, DR) and WAN, and to recommend solutions for identified vulnerabilities Assessments of Data Center LAN and WAN of the bank to meet the performance requirements related to traffic and transactions carried over it and to recommend solutions for improving the performance.

To verify the adequacy, configuration and parameters of various security equipment's such as Firewalls, IDS, IPS etc. deployed at Data Center, DRC for ensuring secured transactions.

External and internal vulnerability assessment of Bank's network.

IS security environment, including procedural controls, IS security management structure and documentation review

- Audit of Network Architecture from security prospective

- Audit of WAN, VLAN, VPN etc. being used for CBS project from security prospective
- Audit of anti virus protection at host and at desktop levels
- Audit on methodology / procedure of anti virus updates. Evaluate updation policies and identified gaps
- Network performance Vis-à-vis CBS RFP

3.2 . Network Vulnerability Assessment (VA)

i). The vendor identified will conduct Vulnerability Assessment (VA) against Servers and network infrastructure components to identify services in use and potential vulnerabilities present. Our requirements under VA are:

- Provide accurate network discovery detail.
- Identify network risks and prioritize issues.
- Enable efficient network-wide remediation.
- **Black Virus vulnerabilities**
- **Ransomware Virus Vulnerabilities**
- **Heartbleed Vulnerabilities**

ii). Configuration of all Network Equipment installed at DC, DRC & CBS Branches should be verified for any Security threats which include the following like :

- Smurf and SYN Flood
- DOS (Denial of Service), DDoS (Distributed Denial of Service) Attacks
- Protection against well know Viruses like Nachi, Slammer, and Trojans etc.
- Communication Controls
- TCP Ports
- Firewall/ACLs (Access Control List)
- Whether LAN Access policy are well defined.
- Whether Redundant Configuration of Ethernet ports of the servers.
- Whether the redundant power source are connected to different power sources?
- Redundancy at power levels UPS and capacity, and recommendations.
- Port Scan
- Checking for Trojans, root kits, Nachi, and Slammer
- Checking of VLAN architecture and Security measures.
- Servers Security Policies
- Mis-configuration related to access lists, account settings
- Validate the key registry settings & group policies / local policies.
- Scanner should be run to check and verify for only application specific ports are open.
- Un patched holes in the operating system of the critical and important Servers specially Proxy Servers, database Servers, DNS Servers, DHCP servers.

- Does the Server setup conducts proper authentication to suit the risk associated with their access?
- Checking the High Availability of the Enterprise Servers like CBSs critical Application Servers, Proxy server and DC.
- Desktop Security at branches, DC & DRC.
- Vulnerability scanning of desktop systems
- Observe, analyze and assess the operations being performed from desktop system
- Analyze the vulnerability scanning report
- Detailed report on findings with suggestions and recommendations. etc.

iii) The assessment should check for various categories of threat to the network like :

- Unauthorized access into the network and extent of such access possible
- Unauthorized modifications to the network and the traffic flowing over network
- Extent of information disclosure from the network
- Spoofing of identity over the network
- Possibility of denial of services
- Possible threats from malicious codes (viruses and worms)
- Effectiveness of Virus Control system
- In E-mail gateways
- In usage of other media – Floppies/CD/USB – ports
- Control over network points
- Can visitor plug in laptops / devices ?
- Control over access Time, station, dial-up and so on
- Possibility of traffic route poisoning
- Configuration issues related to access lists, account settings
- Whether the IOS has been latest not been in the Security Advisories etc.

iv) Access Control

Every router / Switches/firewalls at DC,DRC should be checked for the following configuration standards:

- Whether routers/ Switches are using AAA model for all user authentication.
- Whether enable password on the routers/ Switches are secure encrypted form.
- Whether it meets the password policy with minimum Characters in length.
- Whether local and remote access to the Networking devices are limited & restricted.

Validate following services for security, effectiveness and efficiency on all Network devices:

- IP directed broadcasts
- Incoming packets at the router sourced with invalid addresses such as RFC1918 address
- TCP small services
- UDP small services
- All source routing
- All web services running on router
- What standardized SNMP community strings used
- Logging & Auditing

v) Penetration Testing of public facing applications viz. Internet Banking, Mobile Banking, Corporate Website etc.

- Penetration Testing of public facing application like Internet Banking, Mobile Banking & SMS Banking including SMS alerts on quarterly basis
- Attempt to guess passwords using password cracking tools
- Search for back door trap in the application
- Attempt to overload the system using DDoS & DoS
- Check for commonly known holes in the software like browser, email application.
- Check for common vulnerabilities like – IP Spoofing, Buffer overflows, session hijacks, account spoofing, frame spoofing, caching of web pages, cross site scripting, SQL injection etc.
- Secured Server authentication procedures
- Review logical access to Internet Banking (IB), Mobile Banking & SMS Banking applications, OS, database, network, Physical access control.
- Review logical access to bank's web application, OS, database, network, physical access control hosted at ISP's premises.
- Back up of Internet Banking (IB), Mobile Banking & SMS Banking data
- Program change management
- Check for vulnerabilities that could be exploited for website defacement & unauthorized modification of Internet Banking website.

3.3 Network Architecture Audit:

Network Architecture review should be carried out for security and performance which include the following:

- Review the appropriate segregation of network into various trusted zones
- Review the traffic flow in the network
- Review the existing routing policy
- Review the route path and table audit
- Review of routing protocols and security controls therein
- Review the security measures at the entry and exit points of the network

- Obtaining information about the architecture and address scheme of the network
- Checking Routing and Inter-Vlan Routing and Optimization.
- Checking of HSRP Configurations if any, and its working.
- Checking redundancy and Load Balancing as per the requirement
- Routing Protocol Analysis
- Analyze protocols used and traffic generated and means to optimize traffic
- Analysis of load balancing mechanism
- Analysis of latency in traffic across various links

3.4 Network Performance Analysis (NPA)

An analysis of the performance of the network needs to be carried out by the vendor to ascertain the ability of the network to meet current and future needs of users and to identify any bottlenecks. Network Performance Audit analysis should include the capacity planning analysis, LAN/WAN link utilization and quality analysis, Existing load pattern for network device and Uplink, packet flow performance, Congestion area at various topology layer and traffic pattern analysis.

3.5 Capacity Planning

Audit may consist of network device audit for existing capacity requirement and scalable factor, existing load and capacity of physical layer topology and logical layer architecture, audit on type of equipment required for specific task (Core Network device, Perimeter device and Aggregating devices are at least needed to be consider for SOW).

Following minimum should be Collected during the audit.

- Bandwidth utilization at links
- Availability of bandwidth
- Current utilization levels (normal and non-peak hours)
- Scalability of bandwidth & utilization
- Network device performance related to CPU and memory utilization of devices During peak traffic
- Memory
- Performance (Ping response time)
- Queue/buffer drops
- Broadcast volumes, Collisions, Giants, Runts, traffic-shaping parameters
- Netflow statistic
- RMON

3.6 Performance Audit

The most important task of this exercise is the performance audit.

i) Link Level

A detailed analysis of link usage patterns is to be prepared. This should include, for each link, average and peak utilization over the time period. Latency (round-trip response time) of each link at various load conditions should also be obtained. Throughput to also be measured (using dummy applications- such as ftp for example) for as many critical segments as possible.

ii) Application level

A break down by each category of traffic (i.e. which application is generating how much data) should be obtained for as many links as possible. This should be analyzed for any anomaly and suggestions given for reducing/controlling any unnecessary traffic.

iii) Real-Time Monitoring/Analysis/Control Mechanisms

An exhaustive list of reports to be generated regularly (every few minutes, hourly, daily, weekly) such as the following :

- Degradation in performance of any link below a threshold.
- Health of all services and generate alarms on failures.
- Throughput on all critical paths (using dummy applications if needed).
- Usage patterns (number of transactions) per application should be prepared.

Suggestions for suitable state-of-the art tools for pro-active real time monitoring, analysis and control of the network traffic should also be given.

3.7 Process Management Audit

i) Review of key processes related to the Network

- Configuration Management Process
- Change Management Process
- Account Management Process
- Anti Virus
- Backup
- SLA Management

ii) Accounts / Identity Management

- Policy for usernames / passwords, shared documents
- Guest users, adding new staff, removing old staff access.
- User access to outsourced staff and other outside consultants appointed by the bank

iii) Help Desk, Complaint & Incident Handling Procedures

An audit of the current network management procedures, including complaint registrations and call handling should be done with recommendations for improvement. This should also address the manpower and expertise currently available and projected requirements.

iv) Software License Compliance

- How are software / hardware acquisition / disposals controlled?
- How well security procedures are documented, understood and followed?

3.8 Network Monitoring Software (NMS)

Review of Network Monitoring Software (NMS) installed to monitor critical servers of the entire network including the branches for sizing etc., to monitor the network components of LAN & WAN, Fault Management, Performance Management of the network and the servers, Inventory Management, automatic discovery of network components etc. NMS is also implemented for Proactive Monitoring, Reporting and to Generate Performance Reports of Core Banking Network and for Desktop Management which includes Asset Recovery, Automated Software Delivery and Remote Diagnosis. The functional capabilities and effectiveness of NMS software need to be reviewed and audited. Availability of tools to generate ad-hoc reports from the system logs also to be confirmed.

3.9 Physical and Environmental Controls

1. Assessment of vulnerability towards natural calamities.
2. Assessment of any systems and delivery channels not available to end users due to external factors.
3. Fire protection systems, their adequacy and state of readiness.
4. General failure of systems as a whole due to external factors, and the related threat perception.
5. Working environment vis-à-vis adequacy of air conditioning and other infrastructure related setup.
6. Physical security and access control to server room/data centers areas where N/w devices reside.
7. Premises management.
8. Access card management.
9. Other security systems, their adequacy and monitoring.
10. Adherence to provisions of RRB's Information Security Policy.
11. Physical verification of Hardware inventory and configuration of hardware items vis-à-vis Bank's Records and documents at DC and DRC.

3.10 Audit of Security Operation Centre (SOC).

Audit of Security Operation Centre (SOC) implemented by the bank for monitoring Critical Servers, databases and Network devises.

4. SCOPE FOR AUDIT OF ATM PROJECT

4.1 Review of Operations at Switch

- Terminal driving and Switching, routing activities / HSM / VAP review
- Review of Middleware between Switch / HSM
- SLA Monitoring Review
- Switch Review - password administration, access to sensitive data, access to sensitive privileges and utilities, auditing, logging and monitoring, Remote access, Network (ATM router security review) Mapping of Card and Account number, data integrity, Access control review – physical and logical, Interface controls, overall monitoring of Switch activities, Facility management.
- Management of various KEYS by service provider and Bank, Procedures for generating / loading /destruction and ensuring security of various Keys
- Switch database security review – Policies and procedures, confidentiality and data integrity, access controls, Availability and recovery, Audit trails. Review of processes.
- Review of Fraud Risk Management System
- Review of response time setting
- Validation / verification of PIN and Card by Switch
- Compliance of VISA / NPCI requirements for Switch operations
- Review of process of Addition of ATM at switch
- General controls review
- Security review of all operations including various KEYs password controls at switch and HSM and middleware
- Version control and change management for switch software
- Provision of backup for entire switch services
- Backup practices, off-site storage, backup of switch software
- BCP / DRP - DRS Location audit- hot backup, Dual HSM with automatic fallback.
- Compliance in line with Bank's RTO & RPO
- Service Providers Payment Gateway operators are PCI-DSS compliant.

4.2 Review of Card Cell and related operations

- Review of various activities / functions of ATM card cell
- Reconciliation Software - User Rights, Outstanding entries, Handling of Reversal Transactions, Suspect transactions for ATM and POS transactions, ATM Cash reconciliation. Review of reconciliation process including adequacy and accuracy, Interbank and Inter-branch transactions reconciliation/settlement, Mechanism for redressal of complaints – roles of branch/card cell/ Vendor/s, Managing suspense items, Report generation

- Cash Management – Replenishment, Reconciliation, Handling cash/cheques deposited in ATM, Overnight custody of Cash at vault, accounting entries. Risk mitigation - by way of insurance.
- Card Management activities - Software, User Rights, Production, Dispatch, Embossing, Inventory management, Control over card issue, Activation, Renewal, Hot-listing, Re-activation process, card Database Management, Replacement / Duplicate cards, Generation of PIN mailers, Delivery of cards and PIN mailers, Managing non-delivery if any of cards, PIN, Generation of CAF file, Transit insurance of cards and PIN mailers
- Review of data conversion in case of database of existing card holders
- Review of processes for - Cash Replenishment at ATMs & Daily Reconciliation of Cash, Start of Day and End of Day for ATMs, Journal Printer Logs / ATM transaction activity records, ATM Card Captured / Swallowed, Card Activation, ATM Transaction Reconciliation between Switch & TBA s/w, Dealing with ATM transactions like
- Rejections, Partial Cash dispense etc, Handling cash deposited in envelopes at ATMs, Handling Cheques deposited in ATMs, Overnight Vaulting.
- Security and accuracy of flow of application data among branch, card cell and Vendors and confirmation by Switch and card cell about the correctness of all fields. The procedure for receiving the ATM Application forms from the customers by the branch and forwarding the same to Card Cell is to be followed by the branches as per extant guidelines.
- The procedure of data entry at Card Cell in Card Management System (CMS) and verification, personalization, after personalization posting of CAF (Card Authentication File) in to switch. Review of card usage – monitoring of highly active in-active cards.
- Terminal control software

4.3 General Review

- Up-time of ATM, SWITCH, Online monitoring, daily reporting of uptime /downtime, review of method of computing downtime.
- Handling of ATM problems/ complaints
- PIN Security – Encryption in EPP, Transmission of PIN, regeneration of PIN
- Confirmation of adherence to VISA requirements by service provider and Bank
- (Security of various keys, Responsibilities as Issuer / Acquirer)
- POS Transactions – Daily transactions processing, switching / routing and reporting, Preparation of transaction summary, clearing and settlement reports, Reconciliation
- of disputed transactions, Preparation of daily / weekly / monthly merchant statements
- Reports – MIS, Financial, Non-financial, reversal transactions, interchange fees, authorization charges, settlement charges, Acquirer, Issuer transaction reports, transaction summary, clearing and settlement, posting reports etc., reporting of snaps taken by surveillance camera. The auditor to comment on need for any additional reports.
- Conformance to Triple DES encryption, Mapping

- Review of AMC of Bank with vendor/s
- Ensuring conformance to Banks IS Security Policy including Third Party access policy, Equipment Security Policy, Physical Security Policy, Network Security Policy, Incident management policy and BCP Policy
- Complaints handling
- Conformance to terms of order / Service Level Agreement (SLA) – to cover each point, along with specification for Hardware, Software, Performance and upgrades, and fulfillment of various obligations by vendors and their service providers /sub-contractors if any.
- Review of project documents prepared by vendors e.g. Cash Management, Card Management, and Reconciliation.
- Review of various documents to be submitted by vendors as per contract and actual submission of these documents including their adequacy and authenticity.
- Review of adequacy of various systems and procedures set up by Bank and vendor
- Review of various applicable guidelines from RBI, Government, Regulators, Bank, various committees

4.4. CASH MANAGEMENT

- Cash retracted/not delivered by ATMs.
- Software - The entire process of cash management i.e. cash replenishment request to adjustment of POB should be duly managed through the WAN-based software to be provided by C.O. IT department.
- Report submission by vendors such as EJ, others.
- Confirmation of daily cash position from the transaction log files (TLF) provided by vendors.
- Reconciliation – pending entries in ATM reconciliation
- Exact time of reckoning of closing cash balance on a particular day
- Daily statement of ATM wise cash balances
- Insurance of cash

5. SCOPE FOR AUDIT OF OUTSOURCING ACTIVITIES

The scope of audit of outsourced activities should be as per Bank's Outsourcing Policy and guidelines issued by RBI in this regards. Some of the RBI guidelines are as under :-

RBI Circular no RBI/2008-09/449 Ref : DBS.CO.PPD.BC.5/11.01.005/2008-09 dated 22.04.2009 on 'Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Bank's- Compliance Certificate'.

The auditor is required to look into the following at the time of audit of outsourced activities:-

A). Procedural & Operational aspects:-

1. Whether the process of outsourcing is complied as per Outsourcing Policy of the Bank.

2.Compliance to instructions/ guidelines issued by Regulator, time to time on outsourcing.
3.Whether due diligence is taken into consideration for the qualitative and quantitative, financial, operational and reputational factors of service provider. Such due diligence review should highlight any deterioration or breach in performance standards, confidentiality and security and business continuity preparedness.
4.To assess the ability of the service provider to continue to meet obligation/(activity outsourced by the Bank).
5.Ensuring due diligence by service provider of its employees
6.Whether the agreement with vendor is vetted by legal department.
7.Whether periodic due diligence review of service provider done to identify new material outsourcing risk as they arise.
8.Review of the outsourcing contracts.
9.Whether proper records of the outsourced activities are maintained.
10.Whether SLA monitoring mechanism is adopted.
11.Ensure the preservation and protection of the security and confidentiality of Bank's customer information, in the custody or possession of the service provider.
12.Conducting Risk Assessment of outsourcing arrangements
13.Verify completeness of outsourcing agreement, as per Bank's Outsourced Policy and RBI guidelines on outsourcing activities.

B). Technology aspects:-

1.Ensuring that contingencies plans, based on realistic and probable disruptive scenarios, are in place and tested by Service Provider. Contingency plan to ensure business continuity.
2.Security of infrastructure facility
3.Review and monitor the security practices and control processes of the service provider by Bank on a regular basis and require the service provider to disclose security breaches
4.For outsourced technology operations, specific metrics is defined for the service availability, business continuity and transaction security, in order to measure services rendered by the external vendor organization.
5.Understanding and monitoring the control environment of service providers that have access to the Bank's systems, records or resources.
6.Review of adherence of outsourced information systems and operations with the Information Security policy of the Bank.
7.Review of ACS (Access Control System) for physical and logical security

6. **Scope of System and VAPT audit of Financial Inclusion Gateway Server (FIGS):** The audit shall cover domains such as Client and Server end penetration, security framework, base line security policies, auditing and logging, specifications of application programming interface used for authentication, specifications of biometric devices for all type of versions such as Windows, Android and Web application. In addition scope also include 1) End Point security 2) Harding of hardware 3) OWASP Top 10 Vulnerabilities.

7. **Scope of System Audit of Core Banking Solution(Finacle) RRBs at DC/DRC will be the same as referred above for audit of CBS project of Central Bank of India (B@NCS24) including Networking, VAPT,**

ANNEXURES

(RBI Guidelines)

ANNEX –A

An Illustrative Information Security Check List

Security Policy - Governance, Implementation & Review

Whether there exists a well-documented Information security policy	Yes/ No
When was the policy last approved by the Board of directors/ Management	mm/dd/yy
What is the review frequency of the policy	Quarterly/ Half-yearly/ Yearly
When was the last review conducted	mm/dd/yy
What was the last review purpose	a. Periodic
	b. Incident driven
	c. Infrastructure changes
Whether the policy addresses legal and regulatory requirements	Yes/ No
Who is the security policy owner for maintenance and review	a. Board of directors
	b. Security Committee
	c. CISO
Whether IS committee is constituted comprising of representatives from all verticals	Yes/ No
What is the meeting frequency of the IS committee	quarterly/ half-yearly/yearly
Whether the role and responsibilities of IS committee is clearly defined	Yes/ No
Whether the role and responsibilities of CISO is clearly defined	Yes/ No
Whether the policy is communicated to	Yes/ No

relevant users	
What is the medium of communication	a. Email
	b. Intranet
	c. In-house Periodic trainings
	d. Induction training for new recruits
	e. Undertaking
Whether supporting procedures/ sub-policies have been developed for organizational security	Yes/ No
Who reviews the supporting procedures/ sub-policies	a. CISO
	b. IS Committee
Whether security policy is in line with global best practices guidelines like ISO 27001 (and other frameworks like COBIT etc) and/or as per requirements of RBI circular	Yes/ No
Whether every procedure/ sub-policy has a designated owner	Yes/ No
Whether the policy takes into consideration the long-term business strategy of the organisation	Yes/ No
Whether the organisation has considered IS security for budgetary allocation	Yes/ No
Whether independent audit is conducted to ensure adherence to security policy	Yes/ No
Frequency of internal audit	Quarterly/ Half-yearly/ Yearly
Frequency of external audit	Quarterly/ Half-yearly/ Yearly/ Bi-annually

Asset classification and control -*Accountability of assets*

Whether the organization has distinguished its information assets	Yes/ No
Whether an inventory database is maintained for all information assets	Yes/ No
Whether there is a designated owner for each distinguished asset	Yes/ No
How is the inventory database maintained	Centrally/ Locally
Whether a separate asset inventory exists for datacentre and DR site	Yes/ No
Whether there is a designated owner for the datacentre asset inventory	Yes/ No
Whether a process exist for updation of asset inventory	Yes/ No
Whether each information asset is labeled	Yes/ No
Whether information classification guidelines exist and are enforced	Yes/ No
Whether the classification level of information asset is reviewed periodically	Yes/ No
Who is responsible for deciding the asset classification level	a. IS Committee
	b. CISO
	c. Asset owner
Whether classification level for each asset is recorded in inventory database.	Yes/ No

Human resource security

How do you communicate individual security roles and responsibilities to employee end users	a. Employment contract
	b. Induction trainings
	c. Periodic IS awareness trainings
Is there a training calendar for IS awareness trainings	Yes/ No
Number of IS awareness trainings conducted in a year	_____
Number of induction trainings conducted in a year	_____
Whether a background verification check is part of the recruitment process of the organisation	Yes/ No
How the background verification check is conducted	a. In-house
	b Outsourced
Whether employment contract covers non-disclosure/ confidentiality clause	Yes/ No
Whether written acknowledgement w.r.t understanding and acceptance of employment contract is obtained	Yes/ No
Whether employment contract covers appropriate controls to address post employment responsibilities	Yes/ No

Third Party Security/ Vendor Management

How do you communicate individual security roles and responsibilities to third party users	a. Third party contract
	b. Periodic IS awareness trainings

	c. Both
Whether a background verification check is a mandatory requirement in third party contracts	Yes/ No
What process there is to ensure background verification check is performed	a. SLA review
	b Third party audit
Whether third party contract mentions adherence to security policy and procedures of the organization	Yes/ No
Whether third party contract covers non-disclosure/ confidentiality clause	Yes/ No
Whether written acknowledgement w.r.t understanding and acceptance of third party contract is obtained	Yes/ No
Do you conduct due diligence for third parties/ vendor before outsourcing	Yes/ No
Do you conduct onsite security audit of third party/ vendor before outsourcing	Yes/ No
Have you identified the risks associated with third party contractors working on-site	Yes/ No
Do you conduct periodic reviews of all accesses provided to third parties/ vendor	Yes/ No
What is the frequency of such reviews	Monthly/ Quarterly/ Yearly
Whether the CISO reviews all security controls w.r.t third party contracts	Yes/ No

Physical and Environmental Security

What physical border security facility has been implemented to protect the Information processing facilities	a. Electronic access control (access cards)
	b. Biometric system
	c. Security guards
	d. Perimeter walls
	e. All of the above
What entry controls are in place to allow only authorised personnel into various areas within the organisation	a. Electronic access control (access cards)
	b. Biometric system
	c. Manned reception
	d. All of the above
Whether access to information processing facilities is limited to approved personnel only	Yes/ No
Whether the physical access control procedures differentiate employees, vendors, equipment & facility maintenance staff	Yes/ No
Whether potential threats to information processing facilities like fire, flood, earthquake, theft are taken into consideration in the risk assessment exercise	Yes/ No
Whether separate security controls are in place for third party/ vendor personnel working in secure areas	Yes/ No
Whether goods delivery area and secure area are isolated from each other to avoid any unauthorized access	Yes/ No
Whether appropriate controls are deployed to minimize the risk from heat,	Yes/ No

smoke, adverse environmental conditions, explosives, dust, chemical effects, electrical supply interfaces, electromagnetic radiation, vibrations, water leakages, rodents etc.	
What is the frequency of conducting fire drill and training	Quaterly/ Half-yearly/ Yearly
Whether evacuation plan with clear responsibilities is in place in case of a disaster	Yes/ No
Whether there is a policy dealing with eating, drinking and smoking in proximity to information processing services	Yes/ No
Whether appropriate signages are displayed with reference to above	Yes/ No
Whether the power and telecommunications cable carrying data or supporting information services are protected from interception or damage	Yes/ No
Whether information processing facility is equipped with all of the following: multiple feed power supply; UPS, generator backups	Yes/ No
Whether the equipment is maintained/ upgraded as per the supplier's recommended service intervals and specifications	Yes/ No
Who carries out the maintenance/ upgradation of critical information processing systems and facilities	a. Third party support personnel
	b. Equipment manufacturer
	c. In-house personnel
Whether logs are maintained with all suspected or actual faults and all preventive and corrective measures	Yes/ No
Who reviews the above logs	a. CISO
	b. Datacentre Head
	c. IT Head

Whether appropriate controls are implemented while sending equipment off premises	Yes/ No
Whether the equipment insurance requirements are satisfied	Yes/ No
Whether secure disposal policy is in place for sensitive information	Yes/ No
How many workstations and servers exist	_____
Whether the organisation maintains a network diagram that includes IP addresses, room numbers/ location and asset owners/ responsible parties	Yes/ No
Whether clear desk and clear screen policies exist	Yes/ No
Whether screen saver time out is implemented	Yes/ No

Information Security Incident Management

Is there a well-documented Incident Management process to handle security incidents	Yes/ No
Whether end users are aware of incident management process	Yes/ No
Whether the process clearly spells out responsibilities, steps for orderly response to a security incident	Yes/ No
Whether the procedure separately addresses different types of incidents like denial of service attacks, breach of confidentiality etc., and ways to handle them	Yes/ No
What kind of monitoring system/ forensic investigation capability is in place so that proactive action is taken to avoid security incidents and malfunctions	a. Audit trail
	b. Log Correlation

	c. Intrusion Prevention/ Detection System
	d. Any other system, please specify
Whether appropriate contacts with law enforcement authorities, regulatory bodies, information service providers and telecommunication operators are maintained to ensure that appropriate action can be quickly taken and specialist advice obtained, in the event of a security incident (Eg. CERT-IN, IDRBT, IBA etc.)	Yes/ No
Whether an escalation reporting procedure exists to report security incidents, security weakness, software malfunctions, threats to systems and processes through appropriate management channels as quickly as possible	Yes/ No
Has the security escalation matrix been defined and documented	Yes/ No
Whether CISO periodically reviews the security incidents	Yes/ No
What is the frequency of such reviews	Monthly/ Quarterly
Whether such incidents are brought to the notice of the Security Steering Committee	Yes/ No
What kind of mechanism is in place to analyse the type of damage and quantify the volume and cost of malfunctions and incidents. Please specify	_____
Number of security incidents in the last six months	_____
Whether there is a formal disciplinary process in place for employees who have violated organisational security policies and procedures	Yes/ No
Do you have contacts with the cybercrime cell/ investigation agencies	Yes/ No

Communications and Operations Management

Whether operating procedures have been documented for critical processes like Back-up, Capacity planning, Equipment maintenance, Application monitoring, Network monitoring, Server monitoring, Security monitoring etc.	Yes/ No
Whether a documented change request procedure exist for all of the above critical processes	Yes/ No
Whether process owner reviews and endorses every change request	Yes/ No
Whether business approval is required for every change request	Yes/ No
Whether audit logs are maintained for any change made to the production programs	Yes/ No
Whether segregation of duties is clearly spelt out for the above critical processes	Yes/ No
Whether the development and testing facilities are isolated from operational facilities	Yes/ No
Whether any of the Information processing facility is managed by third party/ vendor	Yes/ No
Whether the risks associated with such outsourced management are addressed by deploying appropriate controls	Yes/ No
Whether necessary approval is obtained from business owners for such engagement	Yes/ No
Whether the performance is monitored and projections for upgrade requirements are made to ensure that adequate processing power and storage are available. Example: Monitoring Hard disk space, RAM, CPU on critical servers	Yes/ No
Whether suitable User Acceptance tests (UAT) are carried out prior to	Yes/ No

acceptance of new information systems, upgrades and new versions	
Which of these controls exist against malicious software usage	a. Desktop firewall
	b. Endpoint security solutions
	c. Active Directory group policies
	d. Anti-virus software
	e. All of the above
Have you subscribed to warning bulletins/ alerts with regards to malicious software usage	Yes/ No
Whether Anti-virus software is installed on end user desktops, internet gateway and mail gateway	Yes/ No
Total number of desktops in the organisation	_____
Total number of dekstops updated with today's Anti-virus Definition	_____
How many regional servers are there for Anti-virus updates in the organisation	_____
Whether a dedicated Virus Helpdesk is established	Yes/ No
Is there a defined procedure to connect vendor/consultant/support personnel laptops to the organization network	Yes/ No
Who reviews daily Anti-virus coverage reports	_____
Whether comprehensive Back-up schedule of essential business applications is in place	Yes/ No
Whether comprehensive Back-up schedule is also implemented at DR Site	Yes/ No
Whether the backup media along with the procedure to restore the backup are stored securely	Yes/ No
Whether the backup media are stored at	Yes/ No

off-site location	
Whether dedicated media liabrary is created for backup media	Yes/ No
Whether the backup copies of critical applications/databases are available on SAN Storage	Yes/ No
Whether the backup media are regularly tested for restoration within the time frame allotted in the operational procedure for recovery	Yes/ No
When was the restoration last tested	mm/dd/yy
Whether daily operations log sheet is maintained for Database housekeeping tasks	Yes/ No
Who reviews the operations log sheets for Database housekeeping tasks	_____
Whether operations logs sheets are randomly compared with system generated operator logs	Yes/ No
Whether a defined fault logging mechanism is in place for Database related issues	Yes/ No
Which technique is used to grant network access to the user	a. AD Authentication
	b. Single Sign-on
	c. Identity Management
	d. Workgroup Environment
Which Network Monitoring tool is used by the organisation	_____
Whether Network/System Administration task is isolated (Network Isolation) from End User Network Segments	Yes/ No
Whether central authentication tools like TACACS/RADIUS are used for Network Device Authentication	Yes/ No
Whether all routers (Branch/WAN) have	Yes/ No

ACLs	
Who reviews the ACLs periodically	_____
Whether clear guidelines exist for remote management of critical equipment (Servers/Routers etc.)	Yes/ No
Whether VPN is used for remote management/administration of critical equipment	Yes/ No
Which type of VPN is being used	_____
Whether VPN Access Authorization process is established	Yes/ No
Whether Media handling guidelines are established	Yes/ No
Whether secure disposal process for media is in place	Yes/ No
Whether the media is transported in a secured manner	Yes/ No
Whether disposal of sensitive items are logged where necessary in order to maintain an audit trail	Yes/ No
Whether System Documentation is stored in a secure manner and protected from unauthorised access	Yes/ No
Whether a list of individuals having access to System Documentation is maintained	Yes/ No
Whether all exchanges of information, for business purposes, are governed by formal agreements	Yes/ No
Whether such agreements adequately address Security issues	Yes/ No
Whether e-commerce transactions are SSL enabled	Yes/ No
Whether multi-factor authentication mechanism is in place for e-commerce environment	Yes/ No

Which of the following additional factors is used for authentication	a. Hardware Token
	b. OTP
	c. MobiToken
	d. IVR Callback
Whether controls are in place to guard e-commerce systems against phishing attacks	Yes/ No
Whether e-commerce systems are under periodic VA/PT cycles	Yes/ No
Whether standard defensive techniques like IPS, Malware Scanning etc. are deployed for e-commerce systems	Yes/ No
Whether the use of the organisation's electronic mail system is governed by acceptable use policy or guidelines	Yes/ No
Whether all e-mails are archived centrally	Yes/ No
Whether gateway level anti-virus, anti-spam protection is enforced for E-mail system	Yes/ No
Whether data leakage prevention system is implemented to maintain confidentiality of the information	Yes/ No
Whether the e-mail traffic is encrypted	Yes/ No
Whether use of all electronic office systems is governed by acceptable use policy	Yes/ No
Whether there is any formal authorisation process in place for the information to be made publicly available	Yes/ No
Whether there are any policies, procedures or controls in place to protect the exchange of information through the	Yes/ No

use of voice, facsimile and video communication facilities	
Whether continuous education/ awareness is imparted to employees w.r.t Information Security best practices while exchanging the information over phone/fax/video etc.	Yes/ No

Access Control

Whether business requirements are documented for access control	Yes/ No
Whether there is any formal user registration and de-registration procedure for granting access to multi-user information systems and services	Yes/ No
Whether privileges are allocated on need-to-use basis and after formal authorisation process	Yes/ No
Whether there exists a process to review user access rights at regular intervals. Eg. Special privilege review every 3 months, normal privileges every 6 months	Yes/ No
Frequency of user access review	Quarterly/ Half-yearly/ Yearly
Whether clear password policy is in place and communicated to all users	Yes/ No
Whether the users and contractors are made aware of the security requirements and procedures for protecting unattended equipment	Yes/ No
Whether networks and network services access policy is in place for the organization	Yes/ No
Which of these authentication mechanisms is used for challenging external connections	a. Cryptography based technique
	b. Hardware Tokens

	c. Software Tokens
	d. Challenge Response protocol
	e. Any other
Whether all external connections have proper Management and Security approvals	Yes/ No
Whether accesses to diagnostic ports are securely controlled and have Security approvals	Yes/ No
Whether Perimeter and Internal Firewalls are distinctly installed in the organization	Yes/ No
Whether ftp is allowed across the organization	Yes/ No
Whether NIDS/NIPS controls are deployed in the organization	Yes/ No
Whether access to information systems is attainable only via a secure log-on process	Yes/ No
Whether unique identifier is provided to every user such as operators, system administrators and all other staff including technical	Yes/ No
Whether there exists a password management system that enforces various password controls such as: individual password for accountability, enforce password changes, store passwords in encrypted form, not display passwords on screen etc.	Yes/ No
Whether Inactive terminal in public areas are configured to clear the screen or shut down automatically after a defined period of inactivity	Yes/ No
Whether sensitive systems are provided with isolated computing environment	Yes/ No

such as running on a dedicated computer, share resources only with trusted application systems, etc.	
Whether there exist any restrictions on connection time for high-risk applications	Yes/ No
Whether procedures are set up for monitoring the use of information processing facility	Yes/ No
Whether the results of the monitoring activities are reviewed regularly	Yes/ No
Whether audit logs recording exceptions and other security relevant events are enabled	Yes/ No
What is the retention period for audit logs	_____
Whether NTP is implemented and clock for all servers/ devices is in sync with NTP	Yes/ No
Whether a formal policy is in place to address the risks of working with computing facilities such as notebooks, palmtops etc. especially in unprotected environments	Yes/ No
Whether there is any policy, procedure and/ or standard to control teleworking activities	Yes/ No
Whether suitable protection of teleworking site is in place against threats such as theft of equipment, unauthorised disclosure of information etc.	Yes/ No

Systems acquisition, development and maintenance

Whether security requirements and controls are incorporated as part of business requirement statement for new systems	Yes/ No
Whether risk assessments are conducted before commencement of system development	Yes/ No
Whether data input to application system	Yes/ No

is validated to ensure that it is correct and appropriate	
Whether areas of risks are identified in the processing cycle and validation checks included	Yes/ No
Whether appropriate controls are identified based on nature of application and business impact in case of data corruption to mitigate risks during internal processing	Yes/ No
Whether Message authentication mechanism is in place, if necessary	Yes/ No
Whether the data output of application system is validated to ensure that the processing of stored information is correct	Yes/ No
Whether there is a policy in use of cryptographic controls for protection of information is in place	Yes/ No
Whether a risk assessment was carried out to identify the level of protection the information should be given	Yes/ No
Whether encryption techniques are used to protect the data.	Yes/ No
Whether assessments are conducted to analyze the sensitivity of the data and the level of protection needed	Yes/ No
Whether Digital signatures are used to protect the authenticity and integrity of electronic documents	Yes/ No
Whether non-repudiation services are used to resolve disputes	Yes/ No
Whether there is a management system in place to support the organization's use of cryptographic techniques like Secret	Yes/ No
key technique and Public key technique	
Whether the Key management system is based on agreed set of standards and secure methods	Yes/ No
Whether there are any controls in place	Yes/ No

for the implementation of software on operational systems	
Whether system test data is protected and controlled	Yes/ No
Whether strict controls are in place over access to program source libraries so as to reduce the potential for corruption of computer programs	Yes/ No
Whether there are strict control procedures in place over implementation of changes to the information system so as to minimize the corruption of information system	Yes/ No
Whether there are any restrictions in place to limit changes to software packages	Yes/ No
Whether there are controls in place to ensure that the covert channels and Trojan codes are not introduced into new or upgraded system	Yes/ No
Whether there is any process in place to ensure application system is reviewed and tested after operating system changes like installation of service packs, patches etc.	Yes/ No

Compliance

Whether relevant regulatory and contractual requirements are documented for each information system	Yes/ No
Whether responsibilities of individuals concerned to meet these requirements are well defined and communicated	Yes/ No
Whether there exist procedures to ensure compliance with legal restrictions on use of material like intellectual property rights, trademarks, copy rights etc.	Yes/ No
Whether important records of the organisation is protected from loss destruction	Yes/ No
Whether there is a management	Yes/ No

structure and control in place to protect data and privacy of personal information	
Whether at the log-on security banner or a warning message is presented on the computer screen indicating that the	Yes/ No
system being entered is private and that unauthorised access is not permitted	
Whether the process involved in collecting the evidence is in accordance with legal best practices	Yes/ No
Whether all areas within the organisation are considered for regular review to ensure compliance with security policy, standards and procedures	Yes/ No
Whether information systems are regularly checked for compliance with security implementation standards	Yes/ No
Whether the technical compliance check is carried out by, or under the supervision of, competent, authorised persons	Yes/ No
Whether all computers, systems and network devices like routers and switches within your organization regularly tested for exploitable vulnerabilities and illegally copied software	Yes/ No
Whether audit requirements and activities involving checks on operational systems are planned and agreed upon to minimise the risk of disruptions to business process	Yes/ No
Whether access to system audit tools such as software or data files are protected to prevent misuse	Yes/ No
Whether there is a designated compliance officer for the organization	Yes/ No

ANNEX–B

(RBI Guidelines)

IS Audit Scope

Indicative scope of IS Audit is given below:

The indicative scope of IS Audit is given below:

- Alignment of IT strategy with Business strategy
- IT Governance related processes
- Long term IT strategy and Short term IT plans
- Information security governance, effectiveness of implementation of security policies and processes
- IT Architecture
  - Acquisition and Implementation of Packaged software
    - Requirement Identification and Analysis
    - Product and Vendor selection criteria
    - Vendor selection process
    - Contracts
    - Implementation
    - Post Implementation Issues
  - Development of software- In-house and Out-sourced
    - Audit framework for software developed in house, if any
    - Software Audit process
      - Audit at Program level
      - Audit at Application level
      - Audit at Organizational level
    - Audit framework for software outsourcing
  - Operating Systems Controls
    - Adherence to licensing requirements
    - Version maintenance and application of patches
    - Network Security
    - User Account Management
    - Logical Access Controls
    - System Administration
    - Maintenance of sensitive user accounts
  - Application Systems and Controls
    - Logical Access Controls
    - Input Controls
    - Processing Controls
    - Output Controls
    - Interface Controls
    - Authorization Controls
    - Data Integrity/ File Continuity controls

Review of logs and audit trails

- – Database Controls Physical access and protection
- ferential Integrity and accuracy Administration and Housekeeping

– Network Management audit
  - Process
  - Risk acceptance (deviation)
  - Authentication
  - Passwords
  - Personal Identification Numbers ('PINS')
  - Dynamic password
  - Public key Infrastructure ('PKI')
  - Biometrics authentication
  - Access Control
  - Cryptography
  - Network Information Security
  - E-mail and Voicemail rules and requirements
  - Information security administration
  - Microcomputer/ PC security
  - Audit trails
  - Violation logging management
  - Information storage and retrieval
  - Penetration testing

- Physical and environmental security
- Maintenance
  – Change Request Management
    - Software developed in-house
  – Version Control
  – Software procured from outside vendors
  – Software trouble-shooting
    - Helpdesk
  – File/ Data reorganization
  – Backup and recovery
    - Software
    - Data
    - Purging of data
  – Hardware maintenance
  – Training
- Internet Banking
  – Information systems security framework
  – Web server
  – Logs of activity

– De-militarized zone and firewall
– Security reviews of all servers used for Internet Banking
– Database and Systems Administration
– Operational activities
– Application Control reviews for internet banking application
– Application security

•Privacy and Data Protection

– Controls established for data coversion process

– Information classification based on criticality and sensitivity to business operations
– Fraud prevention and Security standards
– Isolation and confidentiality in maintaining of Bank's customer information, documents, records by banks
– Procedures for identification of owners
– Procedures of erasing, shredding of documents and media containing sensitive information after the period of usage.
– Media control within the premises

- Business Continuity Management
  – Top Management guidance and support on BCP
  – The BCP methodology covering the following:
    - Identification of critical business
    - Owned and shared resources with supporting function
    - Risk assessment on the basis of Business Impact Analysis ('BIA')
    - Formulation of Recovery Time Objective ('RTO') and Identification of Recovery Point Objective('RPO')
    - Minimising immediate damage and losses
    - Restoring of critical business functions, including customer-facing systems and payment settlement systems
    - Establishing management succession and emergency powers
  – Addressing of HR issues and training aspects
  – Providing for the safety and wellbeing of people at branch or location at the time of disaster
  – Assurance from Service providers of critical operations for having BCP in place with testing performed on periodic basis.
  – Independent Audit and review of the BCP and test result
  – Participation in drills conducted by RBI for Banks using RTGS/ NDS/ CFMS services
  – Maintaining of robust framework for documenting, maintaining and testing business continuity and recovery plans by Banks and service providers
- Asset Management
  – Records of assets mapped to owners
  – For PCI covered data, the following should be implemented:

- Proper usage policies for use of critical employee facing technologies
- Maintenance of Inventory logs for media

– Restriction of access to assets through acceptable useage policies, explicit management approval, authentication use of technology, access control list covering list of employees and devices, labeling of devices, list of approved company products, automatic session disconnection of remote devices after prolong inactivity
– Review of duties of employees having access to asset on regular basis.

- Human Resources
  – Recruitment policy and procedures for staff
  – Formal organization chart and defined job description prepared and reviewed regularly
  – Proper segregation of duties maintained and reviewed regularly
  – Prevention of unauthorized access of Former employees
  – Close supervision of staff in sensitive position
  – People on notice period moved in non-sensitive role
  – Dismissed staff to be removed from premises on immediate effect

- IT Financial Control
  – Comprehensive outsourcing policy
  – Coverage of confidentiality clause and clear assignment of liability for loss resulting from information security lapse in the vendor contract
  – Periodic review of financial and operational condition of service provider with emphasis to performance standards, confidentiality and security, business continuity preparedness
  – Contract clauses for vendor to allow RBI or personnel authorized by RBI access relevant information/ records within reasonable frame of time.
- IT Operations
  – Application Security covering access control
  – Business Relationship Management
    - Customer Education and awareness for adoptation of security measures
    - Mechanism for informing banks for deceptive domains, suspecious emails
    - Trademarking and monitoring of domain names to help prevent entity for registering in deceptively similar names
    - Use of SSL and updated certification in website
    - Informing client of various attacks like phishing
  – Capacity Management
  – Service Continuity and availability management
    - Consistency in handling and storing of information in accordance to its classification
    - Securing of confidential data with proper storage

- Media disposal
- Infrastructure for backup and recovery
- Regular backups for essential business information and software
- Continuation of voice mail and telephone services as part of business contingency and disaster recovery plans
- Adequate insurance maintained to cover the cost of replacement of IT resources in event of disaster
- Avoidance of single point failure through contingency planning

– Service Level Management

- Project Management
  – Information System Acquisition, Development and Maintenance
    - Sponsorship of senior management for development projects
    - New system or changes to current systems should be adequately specified, programmed, tested, documented prior to transfer in the live environment
    - Scrambling of sensitive data prior to use for testing purpose
  – Release Management
    - Access to computer environment and data based on job roles and responsibilities
    - Proper segregation of duties to be maintained while granting access in the following environment
      – Live
      – Test
      – Development

      Segregation of development, test and operating environments for software
- Record Management
  – Record processes and controls
    - Policies for media handling, disposal and transit
    - Periodic review of Authorization levels and distribution lists
    - Procedures of handling, storage and disposal of information and media
    - Storage of media backups
    - Protection of records from loss, destruction and falsification in accordance to statutory, regulatory, contractual and business requirement
- Technology Licensing
  – Periodic review of software licenses
  – Legal and regulatory requirement of Importing or exporting of software
- IT outsourcing related controls
- Detailed audit delivery channels and related processes like ATM, internet banking, mobile banking, phone banking, card based processes
- Data centre operations and processes

  Review relating to requirements of card networks (for example, PIN security review)

Annexure-C

LIST OF APPLICATIONS SOFTWARE TO BE AUDITED

Sr.No.	Application Name
1	Core Banking Solutions (B@ancs24)
2	Trade Finance (Exim Bills)
3	E-Treasury
4	AML (AmLock)
5	Mobile Banking System (along with IMPS)
6	Internet Banking System (along with IMPS)
7	ATM including Switch
8	Credit Card System
9	RTGS
10	NEFT
11	NDS-OM,NDS-Call,FX-CLEAR,FX-SWAP,CROMS, CBLO Dealing Room
12	Biometric Authentication System
13	SWIFT
14	CMS
15	Online Share Trading
16	ASBA
17	DP Secure Software for Demat
18	HRMS
19	SDR
20	CLASS/ LLMS
21	Privilege Identity Management (PIM)
22	SAS Risk Management System
24	CTS
25	E-Mail
26	Financial Inclusion
27	Bank's Website
28	Call Centre
29	CPPS
30	CPSMS
31	OFF Site Monitoring
32	eTDS (Saral TDS)
33	KIOSK
34	FTM
35	UPI
36	Prepaid Instruments (PPI)
37	Mobile App- Performatrix
38	Help desk-CA
39	Mobile App- Retiral Benefit
40	Mobile APP - NPA tracker
41	M- Passbook
42	Document Management System

** The list of Application software will/may include any future regulatory/ statutory /RBI requirements, further application if developed/used by bank before the completion of the audit project, at no additional cost.

8.8 Annexure- 7: Scope of IS Audit of RRBs

Central Bank of India has sponsored two Regional Rural Banks which shall be be covered under present assignment. Details of these RRBs are as under:

1) **Uttar Bihar Gramin Bank**,
   Head Office,
   Kalambagh Chowk,
   Muzaffarpur,
   BIHAR – 842001

2) **Uttarbanga Kshetriya Gramin Bank,**
   Head Office,
   Sunity Road,
   Coochbehar
   West Bengal- 736101.

The Scope is broadly categorized into following Audits as per RFP

1.Comprehensive audit for its deployed RRB's Centralized Banking Solution ("RRB-CBS'"), Security audit of RRB's Data Center, Disaster Recovery Center, network infrastructure and 2 RRB's Branches (one from each RRB), delivery channels like Internet/Mobile (SMS/WAP) banking, FI,AEPS,HSM, BHIM-Aadhaar.

2.The complete review and audit of the Core Banking Application of RRB

3.Audit of bank's Data Centre (DC) at Navi Mumbai, Disaster Recovery Centre (DRC) at Hyderabad

4. Information Security Audit of Network

5. Audit of Disaster Recovery and Business Continuity Plans & Anti-virus

6.Vulnerability Assessment (VA) of all Servers and Penetration Testing (PT) of public facing application like Internet Banking, Mobile Banking & SMS Banking including SMS Alerts on quarterly basis.If required (Please note at present INB\Mobile banking is not live in both RRBs)

7. Audit of Delivery Channels – Internet Banking, Mobile Banking (SMS/WAP), NEFT, FI, AEPS, BHIM-Aadhaar,IMPS etc.

Scope of Work for CBS Application Audit

Application Review Scope

Application Review covers all the applications implemented in the RRB as a part of the CBS turnkey project covering functionalities under:

8.General Banking

9.SB and Current Account

10. Term Deposits
11. Advances
12. OD / CC/CKCC
13. Term Loan
14. Office Accounts
15. General Ledger
16. PMSSS (JBY,SBY,APY)
17. DBTL (ACH,APBS)
18. Locker
19. Anti-Money Laundering
20. Asset – Liability Management
21. Financial Inclusion, AEPS,EKYC,BHIM-Aadhaar
22. Interfaces with ATM, NEFT, FI, Rupay, Debit Card
23. PFMS
24. Unclaimed deposit
25. Accounts maintained in other banks

Under these domains following functional activities are to be covered for the Audit:

26. Functionality implemented vis-à-vis the Bank's requirements
27. Input, processing and output controls across various schemes across the bank.
28. Accuracy, adequacy and integrity of data in reports.
29. Sufficiency of Audit Trails and Logs

Application review of the software for Core banking solution i.e. Finacle

1. Study & review the implemented functionality of Finacle core banking solution & allied modules in all the areas and to ensure correctness of functionality of each module & all modules in totality including parameterization with reference to the specifications given in the RRB's CBS RFP floated and the procedure of the bank for all the modules like Retail deposits, advances, Bills, Lockers, MIS etc.

2. Study the Finacle Core banking application for adequate input, processing and output controls and conduct various tests to verify existence and effectiveness of the controls.
3. Perform a test of controls and functionality setup in the Finacle Core Banking application and to ensure that all the functionalities and controls as stated in RFP for RRB-CBS are implemented properly and completely.
4. Review/audit the presence of adequate security features in RRB-CBS application to meet the standards of confidentiality, reliability and integrity required for the application supporting business processes.
5. Identify ineffectiveness of the intended controls in the software and analyze the cause for its ineffectiveness. Review adequacy and completeness of controls
6. Identify key functionalities not supported by the application.
7. Review effectiveness and efficiency of the Application.
8. Review of all controls including boundary controls, input controls, communication controls, database controls, output controls, and interfaces controls from security perspectives.
9. Review of all Interface of application with other system OR interface of other system with applications for Security, accuracy, consistency and safety.
10. Identifying critical risk areas, control weakness in application systems and recommended corrective actions from security prospective

CBS Application Security and Controls

Review of the application security features built within RRB-CBS application and also the Security and controls built in and around the operating system and data base used by the Finacle - Core Banking Application both at the central level and at the client level

Application Security Controls

1. Review the application security setup supported by the Finacle - core banking solution to ensure:
   - Access level controls are appropriately built and implemented into the Application
   - Only authorized users should be able to edit, input or update data in the application or carry out activities as per their role and/or functional Requirements.
   - User maintenance and password policies being followed are as per RRB's Information security policy

2. Identify gaps in the application security parameter setup in line with RRB's Information security policy and leading applicable practices
3. Review should include threat identification, assessment of threats and exposure analysis and control adjustment in respect of RRB-CBS.

Review of operating system and Data Base Controls

Review of Operating System Controls

1. Review specific operating system security features used and the parameters set
2. Identify security weaknesses and recommend solutions
3. Review sample user profiles against job roles

Review of Data Base Controls

1. Review specific database system security features used and the parameters set
2. Check the database for optimal performance
3. Procedure being adopted for data base updations through backend and documentation done in this regard

Review of other Controls

1. Review of user manuals, operating manuals and systems manuals and interface with menus, submenus and reports related to RRB-CBS, Trade Finance Module, GBM, ALM & AML.
2. Review of -
    - Sufficiency/accuracy of all types of data extracts,
    - Audit trails,
    - Setting of various parameters, updations thereof and actual working of them as Intended and accurately.
    - Turnaround time required for each transaction,
    - Backups and recovery procedure / controls,
3. Review of management controls including systems development, data management, security management, operations management and quality assurance management and change management control.

System development to include – Problem / opportunity definition, Management of Change process, analysis of existing system, formulation of requirement, application Software development, procedure development, acceptance testing.

Data management Control– Users must be able to share data, data must be available to users when it is needed, in the location where it is needed and in the form, in which it is needed, it must be possible to modify data fairly easily in the light of changing user requirements, integrity of data must be preserved.

Security management - review of physical concerning personnel, hardware, facilities, supplies and documentation. Logical security control over malicious threats, review of security program.

Operations management to cover daily running of hardware, software, facilities, Production application system can accomplish their work, Segregation of duties and accesses of production staff and development staff with access control over development, test and production regions. Review of controls over computer operations, communication network control, data preparation and entry, production control, file library, documentation and program library, help desk and technical support, capacity planning and performance Monitoring and outsourced operations.

Quality assurance management review to include – ensuring achievement of certain quality goals and their development, implementation, operation and maintenance of system with a set of quality standards.

Review of hardware and software (at branches selected) to suggest measures if any for better control:

Review of procedures for ATM, NEFT, CPSMS, USB, Internet and Mobile Banking from security prospective.

Verification/ review of compliance with regulatory requirements including Guidelines/ directives of Reserve Bank of India and CERT-IN, statutory agencies.

Change Management control: Review of change management control procedure. Review of procedure/methodologies being adopted for carrying out the changes in application.

30.Check & review application up & down time

Scope of audit for Data Centre & Disaster Recovery Centre (DRC)

Physical security of Data Centre and Disaster Recovery Site

31.Access control system

32.Fire / flooding / water leakage / gas leakage etc.

33.Handling of movement of man /material in /out of DC / DRC

34.Air-conditioning of DC / DRC

35.Electrical supply to DC/ DRC , Raw power / UPS / Genset

36.Surveillance system of DC / DRC

37.Redundancy of power level, UPS capacity at DC , DRC

38.Physical & environmental controls at DC & DRC

39.Assets safeguarding

40.Incident handling procedures

41.Parameters

42.AMC and Insurance

Server system

The servers consists of WINDOWS & SUN servers, storage, tape library etc. installed at DC & DRC

43.Physical / logical access to the servers

44.Review of hardware installed in DC/DRC

45.Inventory management / movement

46.Configuration setting , parameterization

47.Performance monitoring vis –a – vis RFP and SLA

48.Audit logs / trails

49.User / privilege management, default / build-in account management

50.File system, directory & free space management

51.Domain control / administration

52.Backup and recovery policy and procedure

Cross check between the primary server at DC and standby server at DRS With special attention to: Configuration / file system set-up and system change management

53. Check & review application up & down time and various interfaces up time and down time

Database system

54. Segregation of duties of database administrators
55. Password policies
56. User maintenance process
57. User access privileges
58. Authorization profiles
59. Database security functionality
60. Backup & Restore procedures
61. Archival & Purge Procedures
62. Backup security
63. Check the database for optimal performance
64. Monitoring the health of the database.
65. Synchronization between DC and DRC databases

Operating System Security

The Auditor will review the operating system configuration and perform a preliminary assessment of its controls at DC, DRC. The review of the operating system will address:

66. Operating System Installation
67. Operating Systems Access controls
68. Privilege Management
69. Domain Account Policies
70. Built In Accounts
71. User Accounts Properties

72.Groups

73.Domain Administration

74.Directory and File Security

75.Back up & Recovery

Identity management

The Auditor shall examine sensitive and critical IT systems and data files. The Auditor shall develop a list for review of data security techniques and Methods, which shall include the following:

76.Access control, integrity controls, and backup procedures

77.Media Storage, Handling, Disposal, cryptography

78.Sensitive data procedures and implementation

79.Existing privacy policies and protections

80.Information access (authorization and implementation)

81.Developmental systems and how systems are moved into production

82.Written user responsibilities for management of information and systems.

Also in DC audit they should also check application up/down time (and various interfaces too) as there may be instance due to one reason or other the server and database may be up and application may be down and our user are not able to access the CBS system

83.Review & audit of Drill activity between DC & DRC

84.Review & audit of Business continuity & disaster recovery procedure of RRB-CBS project

85.Securities vulnerabilities at DC and DRC

Networking Infrastructure Audit

The scope of this audit is the complete review of the Local Area Network at Data Centre, Disaster Recovery Centre and Wide Area Network and is to conduct an intensive diagnostic and planning service designed to check the critical components of our network for Security, Reliability, Performance .The broad parameters, which are required to be reviewed by the auditor, are:

Review of security architecture and security policy

Assess all security vulnerabilities of the Local Area network (Data Centre, DR) and WAN, and to recommend solutions for identified vulnerabilities Assessments of Data Center LAN and WAN of the bank to meet the performance requirements related to traffic and transactions carried over it and to recommend solutions for improving the performance.

To verify the adequacy, configuration and parameters of various security equipment such as Firewalls, IDS etc. deployed at Data Center, DRC for ensuring secured transactions.

External and internal vulnerability assessment of Bank's network.

IS security environment, including procedural controls, IS security management structure and documentation review

86.Audit of Network Architecture from security prospective

87.Audit of WAN, VLAN, VPN etc. being used for RRB-CBS project from security prospective

88.Audit of anti-virus protection at host and at desktop levels

89.Audit on methodology / procedure of antivirus updates. Evaluate updations policies and identified gaps

90.Network performance Vis-à-vis RRB's CBS RFP

Network Vulnerability Assessment (VA)

The vendor identified will conduct Vulnerability Assessment (VA) against Servers and network infrastructure components to identify services in use and potential vulnerabilities present. Our requirements under VA are:

91.Provide accurate network discovery detail.

92.Identify network risks and prioritize issues.

93.Enable efficient network-wide remediation.

Configuration of all Network Equipment installed at DC, DRC & 2 RRB Branches should be verified for any Security threats which include the following like:

94.Smurf and SYN Flood

95.DOS Attacks

96.Protection against well known Viruses like Nachi, Slammer, and Trojans etc.

97.Communication Controls

98.TCP Ports

99.Firewall/ACLs (Access Control List)

100.Whether LAN Access policy are well defined.

101.Whether Redundant Configuration of Ethernet ports of the servers.

102.Whether the redundant power source are connected to different power sources?

103.Redundancy at power levels UPS and capacity, and recommendations.

104.Port Scan

105.Checking for Trojans, root kits, Nachi, and Slammer

106.Checking of VLAN architecture and Security measures.

107.Servers Security Policies

108.Mis-configuration related to access lists, account settings

109.Validate the key registry settings & group policies / local policies.

110.Scanner should be run to check and verify for only application specific ports are open.

111.Unpatched holes in the operating system of the critical and important Servers especially Proxy Servers, database Servers, DNS Servers, DHCP servers.

112.Does the Server setup conducts proper authentication to suit the risk associated with their access?

113.Checking the High Availability of the Enterprise Servers like CBSs critical Application Servers, Proxy server and DC.

114.Desktop Security at branches, DC & DRC.

115.Vulnerability scanning of desktop systems

116. Observe, analyze and assess the operations being performed from desktop system
117. Analyze the vulnerability scanning report
118. Detailed report on findings with suggestions and recommendations. Etc.

The assessment should check for various categories of threat to the network like:

119. Unauthorized access into the network and extent of such access possible
120. Unauthorized modifications to the network and the traffic flowing over network
121. Extent of information disclosure from the network
122. Spoofing of identity over the network
123. Possibility of denial of services
124. Possible threats from malicious codes (viruses and worms)
125. Effectiveness of Virus Control system
126. In E-mail gateways
127. In usage of other media – Floppies/CD/USB – ports
128. Control over network points
129. Can visitor plug in laptops / devices
130. Control over access Time, station, dial-up and so on
131. Possibility of traffic route poisoning
132. Configuration issues related to access lists, account settings
133. Whether the IOS has been latest not been in the Security Advisories etc.

Access Control

Every router / Switches/firewalls at DC, DRC should be checked for the following configuration standards:

134. Whether routers/ Switches are using AAA model for all user authentication.
135. Whether enable password on the routers/ Switches are secure encrypted form.
136. Whether it meets the password policy with minimum Characters in length.
137. Whether local and remote access to the Networking devices are limited & restricted.

Validate following services for security, effectiveness and efficiency on all Network devices:

138. IP directed broadcasts
139. Incoming packets at the router sourced with invalid addresses such as RFC1918 address
140. TCP small services
141. UDP small services
142. All source routing
143. All web services running on router
144. What standardized SNMP community strings used
145. Logging & Auditing

Penetration Testing (if applicable)

146. Penetration Testing of public facing application like Internet Banking, Mobile Banking & SMS Banking including SMS alerts on quarterly basis
147. Attempt to guess passwords using password cracking tools
148. Search for back door trap in the application
149. Attempt to overload the system using DDoS & DoS
150. Check for commonly known holes in the software like browser, email application.
151. Check for common vulnerabilities like – IP Spoofing, Buffer overflows, session Hijacks, account spoofing, frame spoofing, caching of web pages, cross site Scripting, SQL injection etc.
152. Secured Server authentication procedures
153. Review logical access to Internet Banking (IB), Mobile Banking & SMS Banking applications, OS, database, network, Physical access control.
154. Review logical access to RRB's web application, OS, database, network, physical access control hosted at ISP's premises in Mumbai.
155. Back up of Internet Banking (IB), Mobile Banking & SMS Banking data
156. Program change management
157. Check for vulnerabilities that could be exploited for website defacement & unauthorized modification of Internet Banking website.

Network Architecture Audit

Network Architecture review should be carried out for security and performance which include the following:

158. Review the appropriate segregation of network into various trusted zones
159. Review the traffic flow in the network
160. Review the existing routing policy
161. Review the route path and table audit
162. Review of routing protocols and security controls therein
163. Review the security measures at the entry and exit points of the network
164. Obtaining information about the architecture and address scheme of the network
165. Checking Routing and Inter-Vlan Routing and Optimization.
166. Checking of HSRP Configurations if any, and its working.
167. Checking redundancy and Load Balancing as per the requirement.
168. Routing Protocol Analysis
169. Analyze protocols used and traffic generated and means to optimize traffic
170. Analysis of load balancing mechanism
171. Analysis of latency in traffic across various links

Network Performance Analysis (NPA)

An analysis of the performance of the network needs to be carried out by the vendor to ascertain the ability of the network to meet current and future needs of users and to identify any bottlenecks. Network Performance Audit analysis should include the capacity planning analysis, LAN/WAN link utilization and quality analysis, Existing load pattern for network device and Uplink, packet flow performance, Congestion area at various topology layer and traffic pattern analysis. Our requirements under NPA are:

Capacity Planning

Audit may consist of network device audit for existing capacity requirement and scalable factor, existing load and capacity of physical layer topology and logical layer architecture, audit on type of equipment required for specific task (Core Network

device, Perimeter device and Aggregating devices are at least needed to be consider for SOW). Following minimum should be collected during the audit.

172. Bandwidth utilization at links

173. Availability of bandwidth

174. Current utilization levels (normal and non-peak hours)

175. Scalability of bandwidth & utilization

176. Network device performance related to CPU and memory utilization of devices During peak traffic Memory

177. Performance (Ping response time)

178. Queue/buffer drops

179. Broadcast volumes, Collisions, Giants, Runts, traffic-shaping parameters

180. Netflow statistic

181. RMON

Performance Audit

The most important task of this exercise is the performance audit.

182. Link Level

A detailed analysis of link usage patterns is to be prepared. This should include, for each link, average and peak utilization over the time period. Latency (round-trip response time) of each link at various load conditions should also be obtained. Throughput to also be measured (using dummy applications- such as ftp for example) for as many critical segments as possible.

183. Application level

A break down by each category of traffic (i.e. which application is generating how much data) should be obtained for as many links as possible. This should be analyzed for any anomaly and suggestions given for reducing/controlling any unnecessary traffic.

Real-Time Monitoring/Analysis/Control Mechanisms\

An exhaustive list of reports to be generated regularly (every few minutes, hourly, daily, weekly) such as the following:

184. Degradation in performance of any link below a threshold.

185. Health of all services and generate alarms on failures.

186. Throughput on all critical paths (using dummy applications if needed).

187. Usage patterns (number of transactions) per application should be prepared.

188. Suggestions for suitable state-of-the art tools for pro-active real time monitoring, analysis and control of the network traffic should also be given.

Process Management Audit

Review of key processes related to the Network

189. Configuration Management Process

190. Change Management Process

191. Account Management Process

192. Anti-Virus

193. Backup

194. SLA Management

Accounts / Identity Management

195. Policy for usernames / passwords, shared documents

196. Guest users, adding new staff, removing old staff access.

197. User access to outsourced staff and other outside consultants appointed by the bank

Help Desk, Complaint & Incident Handling Procedures

An audit of the current network management procedures, including complaint registrations and call handling should be done with recommendations for improvement. This should also address the manpower and expertise currently available and projected requirements.

Software License Compliance

198. How are software / hardware acquisition / disposals controlled

199. How well security procedures are documented, understood and followed

Network Monitoring Software (NMS)

Review of Network Monitoring Software (NMS) installed to monitor critical servers of the entire network including the branches for sizing etc., to monitor the network

components of LAN & WAN, Fault Management, Performance Management of the network and the servers, Inventory Management, automatic discovery of network components etc. NMS is also implemented for Proactive Monitoring, Reporting and to Generate Performance Reports of Core Banking Network and for Desktop Management which includes Asset Recovery, Automated Software Delivery and Remote Diagnosis. The functional capabilities and effectiveness of NMS software need to be reviewed and audited. Availability of tools to generate ad-hoc reports from the system logs also to be confirmed.

Physical and Environmental Controls

200. Assessment of vulnerability towards natural calamities.
201. Assessment of any systems and delivery channels not available to end users due to external factors.
202. Fire protection systems, their adequacy and state of readiness.
203. General failure of systems as a whole due to external factors, and the related threat perception.
204. Working environment vis-à-vis adequacy of air conditioning and other infrastructure related setup.
205. Physical security and access control to server room/data centers areas where N/w devices reside.
206. Premises management.
207. Access card management.
208. Other security systems, their adequacy and monitoring.
209. Adherence to provisions of RRB's Information Security Policy.
210. Physical verification of Hardware inventory and configuration of hardware items vis-à-vis Bank's Records and documents at DC and DRC.

Note:-----All the reports provided by Auditors must be separate for each RRB along with separate invoice.

8.9 Annexure 8: Integrity Pact to be submitted by Bidders:

Each participating bidder/s shall submit Integrity Pact as per attached Annexure on a stamp paper of INR 500/-. Integrity pact should be submitted by all participating bidders at the time of submission of bid documents or as per satisfaction of the Bank. The Non submission of Integrity Pact as per time scheduled prescribed by Bank may be relevant ground of disqualification to participating in bid process. The format of Integrity pact is given below:

Annexure-8: **Format of Integrity Pact**

INTEGRITY PACT

Between

Central Bank of India hereinafter referred to as **"The Principal"**,

And

…… hereinafter referred to as **"The Bidder/ Contractor"**

Preamble

The Principal intends to award, under laid down organizational procedures, contract/s for…… …… The Principal values full compliance with all relevant laws of the land, rules, regulations, economic use of resources and of fairness / transparency in its relations with its Bidder(s) and / or Contractor(s).

In order to achieve these goals, the Principal will appoint Independent External Monitor/s (IEM), who will monitor the tender process and the execution of the contract for compliance with the principles mentioned above.

Section 1 – Commitments of the Principal

1. The Principal commits itself to take all measures necessary to prevent corruption and to observe the following principles:-

   a. No employee of the Principal, personally or through family members, will in connection with the tender for, or the execution of a contract, demand, take a promise for or accept, for self or third person, any material or immaterial benefit which the person is not legally entitled to.
   b. The Principal will, during the tender process treat all Bidder(s) with equity and reason. The Principal will in particular, before and during the tender process, provide to all Bidder(s) the same information and will not provide to any Bidder(s) confidential / additional information through which the Bidder(s) could obtain an advantage in relation to the tender process or the contract execution.
   c. The Principal will exclude from the process all known prejudiced persons.

2. If the Principal obtains information on the conduct of any of its employees which is a criminal offence under the IPC/PC Act, or if there be a substantive suspicion in this regard, the Principal will inform the Chief Vigilance Officer and in addition can initiate disciplinary actions.

Section 2 – Commitments of the Bidder(s)/ contractor(s)

1. The Bidder(s)/ Contractor(s) commit themselves to take all measures necessary to prevent corruption. He commits himself to observe the following principles during his participation in the tender process and during the contract execution.

   a. The Bidder(s)/ Contractor(s) will not, directly or through any other person or firm, offer, promise or give to any of the Principal's employees involved in the tender process or the execution of the contract or to any third person any material or other benefit which he/she is not legally entitled to, in order to obtain in exchange any advantage of any kind whatsoever during the tender process or during the execution of the contract.

   b. The Bidder(s)/ Contractor(s) will not enter with other Bidders into any undisclosed agreement or understanding, whether formal or informal. This applies in particular to prices, specifications, certifications, subsidiary contracts, submission or non-submission of bids or any other actions to restrict competitiveness or to introduce cartelisation in the bidding process.

   c. The Bidder(s)/ Contractor(s) will not commit any offence under the relevant IPC/PC Act; further the Bidder(s)/ Contractor(s) will not use improperly, for purposes of competition or personal gain, or pass on to others, any information or document provided by the Principal as part of the business relationship, regarding plans, technical proposals and business details, including information contained or transmitted electronically.

   d. The Bidder(s)/Contractors(s) of foreign origin shall disclose the name and address of the Agents/representatives in India, if any. Similarly the Bidder(s)/Contractors(s) of Indian Nationality shall furnish the name and address of the foreign principals, if any. Further details as mentioned in the "Guidelines on Indian Agents of Foreign Suppliers" shall be disclosed by the Bidder(s)/Contractor(s).Further, as mentioned in the Guidelines all the payments made to the Indian agent/representative have to be in Indian Rupees only. Copy of the "Guidelines on Indian Agents of Foreign Suppliers" is placed at (page nos. 6-7).

   e. The Bidder(s) / Contractor(s) will, when presenting his bid, disclose any and all payments he has made, is committed to or intends to make to agents, brokers or any other intermediaries in connection with the award of the contract.

2. The Bidder(s)/ Contractor(s) will not instigate third persons to commit offences outlined above or be an accessory to such offences.

Section 3- Disqualification from tender process and exclusion from future contracts

If the Bidder(s)/Contractor(s), before award or during execution has committed a transgression through a violation of Section 2, above or in any other form such as to put his reliability or credibility in question, the Principal is entitled to disqualify the Bidder(s)/Contractor(s) from the tender process or take action as per the procedure mentioned in the "Guidelines on Banning of business dealings". Copy of the "Guidelines on Banning of business dealings" is placed at
(page nos. 8-17).

Section 4 – Compensation for Damages

1. If the Principal has disqualified the Bidder(s) from the tender process prior to the award according to Section 3, the Principal is entitled to demand and recover the damages equivalent to Earnest Money Deposit/ Bid Security.

2. If the Principal has terminated the contract according to Section 3, or if the Principal is entitled to terminate the contract according to Section 3, the Principal shall be entitled to demand and recover from the Contractor liquidated damages of the Contract value or the amount equivalent to Performance Bank Guarantee.

Section 5 – Previous transgression

1. The Bidder declares that no previous transgressions occurred in the last three years with any other Bank in any country conforming to the anti-corruption approach or with any Public Sector Enterprise in India that could justify his exclusion from the tender process.

2. If the Bidder makes incorrect statement on this subject, he can be disqualified from the tender process or action can be taken as per the procedure mentioned in "Guidelines on Banning of business dealings".

Section 6 – Equal treatment of all Bidders / Contractors / Subcontractors

1. The Bidder(s)/ Contractor(s) undertake(s) to demand from his subcontractors a commitment in conformity with this Integrity Pact.

2. The Principal will enter into agreements with identical conditions as this one with all Bidders and Contractors.

3. The Principal will disqualify from the tender process all bidders who do not sign this Pact or violate its provisions.

Section 7 – Criminal charges against violating Bidder(s) / Contractor(s) / Subcontractor(s)

If the Principal obtains knowledge of conduct of a Bidder, Contractor or Subcontractor, or of an employee or a representative or an associate of a Bidder, Contractor or Subcontractor which constitutes corruption, or if the Principal has substantive suspicion in this regard, the Principal will inform the same to the Chief Vigilance Officer.

Section 8 – Independent External Monitor / Monitors

1. The Principal appoints competent and credible Independent External Monitor for this Pact. The task of the Monitor is to review independently and objectively, whether and to what extent the parties comply with the obligations under this agreement.

2. The Monitor is not subject to instructions by the representatives of the parties and performs his functions neutrally and independently. It will be obligatory for him to treat the information and documents of the Bidders/Contractors as confidential. He reports to the Managing Director & Chief Executive Officer, CENTRAL BANK OF INDIA.

3. The Bidder(s)/Contractor(s) accepts that the Monitor has the right to access without restriction to all Project documentation of the Principal including that provided by the Contractor. The Contractor will also grant the Monitor, upon his request and demonstration of a valid interest, unrestricted and unconditional access to his project documentation. The same is applicable to Subcontractors. The Monitor is under contractual obligation to treat the information and documents of the Bidder(s)/ Contractor(s)/ Subcontractor(s) with confidentiality.

4. The Principal will provide to the Monitor sufficient information about all meetings among the parties related to the Project provided such meetings could have an impact on the contractual relations between the Principal and the Contractor. The parties offer to the Monitor the option to participate in such meetings.

5. As soon as the Monitor notices, or believes to notice, a violation of this agreement, he will so inform the Management of the Principal and request the Management to discontinue or take corrective action, or to take other relevant action. The monitor can in this regard submit non-binding recommendations.

Beyond this, the Monitor has no right to demand from the parties that they act in a specific manner, refrain from action or tolerate action.

6. The Monitor will submit a written report to the Managing Director & Chief Executive Officer, CENTRAL BANK OF INDIA within 8 to 10 weeks from the date of reference or intimation to him by the Principal and, should the occasion arise, submit proposals for correcting problematic situations.

7. If the Monitor has reported to the Managing Director & Chief Executive Officer, CENTRAL BANK OF INDIA, a substantiated suspicion of an offence under relevant IPC/ PC Act, and the Managing Director & Chief Executive Officer, CENTRAL BANK OF INDIA has not, within the reasonable time taken visible action to proceed against such offence or reported it to the Chief Vigilance Officer, the Monitor may also transmit this information directly to the Central Vigilance Commissioner.

8. The word "Monitor" would include both singular and plural.

Section 9 – Pact Duration

This Pact begins when both parties have legally signed it. It expires for the Contractor 12 months after the last payment under the contract, and for all other Bidders 6 months after the contract has been awarded.

If any claim is made / lodged during this time, the same shall be binding and continue to be valid despite the lapse of this pact as specified above, unless it is discharged / determined by Managing Director & Chief Executive Officer of CENTRAL BANK OF INDIA.

Section 10 – Other provisions

1. This agreement is subject to Indian Law. Place of performance and jurisdiction is the Registered Office of the Principal, i.e. Mumbai.
2. Changes and supplements as well as termination notices need to be made in writing. Side agreements have not been made.
3. If the Contractor is a partnership or a consortium, this agreement must be signed by all partners or consortium members.
4. Should one or several provisions of this agreement turn out to be invalid, the remainder of this agreement remains valid. In this case, the parties will strive to come to an agreement to their original intentions.

5. In the event of any contradiction between the Integrity Pact and its Annexure, the Clause in the Integrity Pact will prevail."

(**For & On behalf of the Principal) Bidder** /	**For & On behalf of the Principal Contractor**
(Office Seal)	**(Office Seal)**
Place_____	Place_____
Date_____	Date_____
Witness1:Witness1:	
Name & AddressName & Address	
----------	_____
----------	_____
----------	_____
Witness 2:Witness 2:	
Name & AddressName & Address	
----------	_____
----------	_____
----------	_____