REQUEST FOR PROPOSAL
FOR

INFORMATION SYSTEMS AUDIT OF CORE BANKING / NET BANKING / MOBILE BANKING / ATM / DATA CENTRE / D R SITE / NETWORKING INFRASTRUCTURE AND OTHER INTEGRATED SYSTEMS

Indian Bank
Information Systems Audit Cell
Inspection Department, Corporate Office
254-260, Avvai Shanmugam Salai, Royapettah, Chennai – 600 014
E-mail: hoinspection@indianbank.co.in
Website: www.indianbank.in

RFP No	: **CO:INSP: 1 /2017-18**
Porting of RFP in Bank website	: 1st June 2017
Last Date for submitting queries	: 12th June 2017 : 20:00 Hrs
Last date for submitting bids	: 28th June 2017 : 15.00 hrs
Opening of technical proposals	: 28th June 2017 : 15.30 hrs
Fees for RFP document (non-refundable)	: Rs 10,000/-
Bid Security (Bank Guarantee)	: Rs 200,000/-

TABLE OF CONTENTS

1. INTRODUCTION

1.1 - BACKGROUND

Indian Bank is a premier Nationalised Bank with over 2678 Branches and having a business of over Rs. 3,00,000 Crores. The Bank is a forerunner in absorption of technology and has many firsts to its credit in implementation of IT in banking. The Bank has overseas presence through Branches in Singapore, Colombo & Jaffna and has reciprocal arrangements with various Foreign Banks across the globe. Core Banking Solution has been implemented in all the Branches. Bank has introduced Debit Cards, Credit Cards, RuPay cards and Exclusive Credit Card "Bharat Card" for common man – first of its kind in the Banking industry. Banking services are offered through Multiple Delivery Channels like ATM, Internet Banking, Telebanking, Mobile Banking etc. Bank is also partnering various e-governance initiatives of Govt of India and State Governments. The organizational structure of the Bank consists of three tiers, Corporate Office (CO), Zonal Offices (ZO) and Branches. The bank is having a customer base of 360 lakhs and volume of transactions to the tune of 15 lakhs per day with peak time transactions up to 30 lakhs and is expected to increase by 20-25 % per year. Bank has been certified with ISO27001:2013 standard for Information Systems & Security processes and is amongst very few Banks certified worldwide.

1.2 - PURPOSE

This RFP seeks to engage an Information Systems Audit Firm, which has the capability and experience to conduct a comprehensive Information Systems Audit of Bank's critical IT infrastructure and IT Governance.

- Bank seeks to have an external examination of the IT security to ward off risks in the IT Domain and to appraise the findings thereof to the Management.
- To determine the effectiveness of planning and oversight of IT Activities
- Evaluating adequacy of operating processes and internal controls
- Determine adequacy of enterprise-wide compliance efforts relating to IT Policies and Internal Control Procedures.
- Identifying areas with deficient Internal Controls and recommend corrective action to address deficiencies.

1.3 - I T INFRASTRUCTURE

The details of IT and Security Infrastructure of the bank are as under.

1.3.a – CORE BANKING - (Bancs@24)

- Core Banking (Central Application and Server Infrastructure) - The application and the Oracle database servers are on AIX platform.

- Core Banking Front-end application – Bancs@24 Front-end, with Windows platform for Branch Server application and Oracle as the Database.

1.3.b – OTHER MODULES - The following is the brief list of major modules covered in the Core banking application.

- Trade Finance - EXIM Bills Enterprise - The Web, application and the Oracle database servers are on AIX platform.
- Digital Banking Services - Internet Banking, Utility Bill Payments, Various Tax Collections; The Web, application and the Oracle database servers are on AIX platform.
- Mobile Banking, UPI - External Interfaces - App & Middleware hosted on IBM AIX Server
- BBPS & IMPS Switch - Vendor application hosted on IBM AIX Server

2 - Overview of Scope (for the years 2017-18 and 2018-19)

The overall scope of Information Systems and Security Audit will largely include the following:

- The Auditors shall understand the current IT Setup / processes involved in the Bank and the industry prevailing standards and Regulatory guidelines
- Audit of IT Governance evaluating the Bank's strategic and operational alignment with its enterprise's business strategy, ensuring that IT is supporting the Bank's overall goals
- IS Audit shall cover the entire gamut of computerized functioning including e Delivery Channels, robustness of different functions, such as application systems and subsystems, architecture, infrastructure, network, Logical access control, input, processing and output controls, procedures, data integrity/efficiency, Change Management and effectiveness in implementation of Bank's IT Security Policy & Procedures. This shall include any other new addition/ upgradation in hardware, software, business applications, new deliverables, change in architecture/ Migration during the contract period at Data Centre, DR site, Near-DR, Treasury Division & CO Divisions with the prior approval of Head of Audit.

3. COMPREHENSIVE SCOPE OF AUDIT : (Please refer Annexure II)

3. 1. Vertical 1 –

Information System Audit, Vulnerability Assessment and Penetration Testing of Bank's entire CBS and allied infrastructure including Hardware, Operating System, Database, Application(s), Network, Security Devices, Process & People in following locations/Offices:

- Data Center
- Near Disaster Recovery Site
- Disaster Recovery Site
- Digital Banking Division at Chennai
- Information Technology Division at Chennai
- Information System Security Cell at Chennai
- CO International Division at Chennai
- Treasury Branch at Mumbai
- Other departments Corporate Office / Head Office at Chennai or any other bank's office at any place, where critical application/IT infrastructure is installed or may be installed.
- Premises/activities of any third party/service providers (outsourced activities) to review compliance of services/T&C under service level agreements, both at their Primary Site and DR Site
- Minimum of one Specialised branch under each category (like Service Branch, MSME, Ind-Retail Branch (IRB), CMS Hub etc.)
- Minimum 10 CBS branches (along with onsite and offsite ATMs / Bunch Note Accepters (BNAs) / including systems rendering various types of services like Passbook printing, Cheque acceptance etc.)

3. 2. Vertical - 2

1. I S audit and Vulnerability Assessment of Core Banking Applications including BANCS@24, EXIM Bills, and other modules integrated/interfaced with Core Banking like RTGS/NEFT/SFMS, ATM switch, e-commerce including Utility Payment systems, e-Branch-kiosk, Aadhaar Enabled Payment System (AEPS) interface (like Micro ATMs, Aadhaar Pay App, etc), Unified Payment Interface (UPI), CIBIL etc

2. Report on the overall security aspects of the entire Internet Banking / Mobile Banking / ATM Switch / POS Terminal / Payment systems architecture with recommendation for improving the security, if any.

3. I S audit and Vulnerability Assessment of Bank's website, intranet, web applications facing internet, in-house applications accessed by Bank's internal as well as external systems, cyber-roam facility provided to staff members to access the internet.

4. Vulnerability assessment on critical devices and systems and penetration testing to ensure software resilience to be conducted every quarter as per Bank's IS Security Policy; Review of effectiveness and Automated vulnerability scanning tool (VAS) used periodically on systems in the Bank's networks

5. Audit of SWIFT operations as per the Swift guidance document issued by Alliance including VAPT, on a half-yearly basis.

6. I S Audit of Enterprise Network including Network architecture review, NMS (Network Monitoring system) & Administrative Process with report and recommendations

7. I S audit of Bank's Enterprise wide Security project including SOC, Intrusion Detection/Prevention System (IDPS), Anti-Virus Management etc on a quarterly basis to ensure its effectiveness and efficiency in Cyber Security Preparedness. Audit of Security Information and Event Management (SIEM), Privileged Identity Management Solution (PIM), Vulnerability Assessment Solution (VAS), Database Access Management, with regard to their implementation, integration, maintenance, effective utilization etc

8. Vulnerability assessment of Infrastructure and architecture relating to Core Banking (Data Centre, Project Office, Near DR), Corporate / Head Office, branches, etc. Scan non-production environments actively to identify and address potential problems after corrective actions have been taken, to ensure that vulnerabilities were actually eliminated.

9. Vulnerability assessment & I S Audit of the Information Systems – Standard applications and legacy applications (either integrated with Core Banking Solution or working as stand-alone) such as Credit Card Centre, Treasury Branch – Credence Treasury Domestic / Forex, Anti Money Laundering, Integrated Call Centre, M I S, RTGS/NEFT, H R M S–SAP, Risk Management – RAM /CAM/ CORE, Fraud Risk Management System, Financial Inclusion application, Corporate E-mail system and Active Directory Management, In-house applications.

10. Security testing of applications and code review as per bank's secure coding practices (Sample ten in-house developed applications)

11. Functionality, IS Audit, Vulnerability & Penetration Testing Audit of the ATM Service Centre with regard to reconciliation and settlement within and outside the Bank.

12. Audit of FI application software Solution, infrastructure and database with particular reference to the process of issue of cards, authentication, and authorization of Micro ATM devices and process flow/handling of issuer/acquirer transactions and interfacing with UIDAI/NPCI including visit to atleast one village covered under FI.

13. Audit of Cheque Truncation system/Grid infrastructure including Hardware, Operating System, Database, Application, Network including people and process

14. Audit of Registration Authority, issue/maintenance/retiring of digital signatures to individuals/servers

15. The external Penetration testing of enterprise wide Information systems facing the internet and Internal Penetration Testing of Critical systems including but not

limited to Data Centre, Near-DR Site, Disaster Recovery Site, Corporate Office, Head Office

16. Audit of minimum 10 CBS branches (along with onsite and offsite ATMs / BNAs relating to the identified Branch) with focus on critical areas like operating system security, anti-malware controls, maker-checker controls, segregation of duties, rotation of personnel, physical, logical, environmental and network security, review of critical reports (viz. exception reports, etc)/audit trails, BCP policy and testing, User access controls, etc.

17. Audit of Capacity management and adequacy of performance tuning of Bank's Information and Communication Technology infrastructure

18. Audit of processes / procedures involved in Backup, End Of Day (EOD), Start Of Day(SOD) operations, etc., generation of reports, its distribution to branches, availability, consistency, data integrity, completeness of data

19. Review of the DR drills conducted by the bank during the current year to be done by the auditor

20. Two days intensive training to Indian Bank Inspection (Audit) Team. This will provide skills and knowledge on various aspects of IS Audit, IS Security, Threats, attacks & vulnerabilities and technology for protection of Information Assets. It will also discuss configuration and management of security technologies, system hardening, authentication measures, backup processes and others as applicable in banking environment.

21. Conduct one time review after implementation of recommendations (Bank will intimate the IS Auditor to conduct one time review upon implementation of recommendations deemed feasible at its sole discretion.

22. Presentation to the Top Management on the findings of the Report

4. INSTRUCTIONS TO BIDDERS

4.1 - Qualified professionals to be deployed for the job

The entire Security Audit work has to be got done by qualified CISA/CISSP/ISO 27001 Lead Auditor/Professionals having requisite expertise in Information Security Audit. The Information Security Audit should be completed within the mutually agreed time schedule. Franchise of Information System Auditors will not be permitted under any circumstances.

4.2 - Audit Coverage Period

The proposed Annual I S audit will be for a period of two years. Award of IS Audit assignment will be initially for a period of one year. On satisfactory performance and completion of first year assignment, the same may be extended for another one year.

4.3 - Two Stage Bidding Process

The response to the present tender will be submitted in two parts, Part A containing the General Terms and Conditions including Compliance to Scope of Work and Part B containing the Commercial Bid. The bidder will have to submit the Part A and Part B Portion of the Bids separately in sealed envelopes, duly superscribing

"Information Systems Audit – Bids – Part A Technical Bid" and
"Information Systems Audit – Bids – Part B Commercial Bid" respectively**.**

Both the sealed covers should be put in a sealed outer cover envelope and outer cover should bear the title "Information Systems Audit-BID". All the pages of both Part-A and Part-B of the bid should be signed by authorised person of the Bidding firm.

PART A of the Bid will NOT contain any pricing or commercial information at all.
In the first stage, only Part A of the bids will be opened and evaluated. Those bidders satisfying the requirements as determined by the Bank and accepting the terms and conditions of this document shall be short-listed.

Under the second stage, the Commercial Proposals (Part B) of only those bidders, who have been short listed as above, will be opened in the presence of their authorised representatives. The bidder should arrange for a presentation on IS Audit Methodology and approaches to be adopted and the capabilities of the firm to the accomplishment of the tasks assigned before opening of the bid

4.3. a. PART A- TECHNICAL BID

Part A of the Bid will also contain the Bidders information in the format attached.

Note: The vendor should arrange for producing supporting documents in respect of proof of **having conducted** Information Systems Audit for Internet Banking /Core Banking Services etc and Resume of the qualified professionals on the rolls of the company who will be involved in the audit of our bank.

Contents of document to be submitted - The bidder shall submit the following:

- Bidder's Information as per format.
- Non-refundable fee of Rs. 10,000.00 in the form of a demand draft issued by a scheduled commercial bank favoring Indian Bank
- Acceptance of the terms and conditions as contained in this document.
- Supporting documents in respect of proof of Information Security Audit for Internet Banking /Core Banking Services issued by the Head of the I T Department of the Bank

- Total turnover with break-up towards IS Audit.
- Resume of the qualified professionals on the rolls of the company who will be involved in the audit of our bank.
- Bid security for Rs.2,00,000/- (Rupees Two lakhs only) in the form of Bank Guarantee valid for 120 days from the last date for submission of Tender
- Power of Attorney of the person signing the document
- Articles of Association, Memorandum of Association of the company.
- Audited balance sheets for the last three years.

4.3. b. PART B COMMERCIAL BID

- Commercial offer (as per format) in separate sealed cover

4.4 – BID PROCESS TIME FRAME

The following is an indicative timeframe for the overall selection process. Bank reserves the right to vary this timeframe at its absolute and sole discretion should the need arise. Changes to the timeframe will be relayed to the affected Respondents during the process.

Description	Due Date
Application fee	Rs.10,000/-
EMD (Earnest Money Deposit)	Rs.200,000/-
Date of issue of Tender Notification	01/06/2017
Last date and time of receiving pre-bid queries in writing / thru email to hoinspection@indianbank.co.in	12/06/2017 Time 20:00 Hours
Last date of Tender Submission	28/06/2017 : 15:00 hrs
Date and Time of Technical Bid Opening	28/06/2017 Time 15:30 Hours
Commercial Bid Opening date	Will be intimated to the qualified bidders

* All dates mentioned above are tentative dates and the bidder acknowledges that it cannot hold the Bank responsible for breach of any of the dates.

4.5 – BID SUBMISSION

The response to the present tender will be submitted in two parts, the Technical Bid and the Commercial Bid, in separate sealed covers. The Technical Bid shall be as per the format for Technical Bid specified in the tender document. The Commercial Bid shall be as per the format for Commercial Bid specified in the tender document. Both the bids shall be sealed, enclosed in separate covers and submitted together in a single packet.
Bids duly sealed should be delivered **before 15.00 hours on or before 28/06/2017.** Bids may be sent by registered post or hand delivered so as to be received at the following address:

The Assistant General Manager,
Indian Bank Corporate Office
Expenditure Department
254-260 Avvai Shanmugam Salai
Royapettah, Chennai 600 014
Website: www.indianbank.in
Phone: 2813 4031, 2813 4497
E-mail: hoinspection@indianbank.co.in

4.6 – ACCEPTANCE OF BIDS

Last date for submission of bids is **15:00 hours on 28/06/2017**. Bids received after **15.00 Hrs on 28/06/2017** will not be accepted under any circumstances. The envelope containing **Part A** portion of the bids will be opened immediately thereafter at **15:30 hours on 28/06/2017** in the presence of bidders. All bidders are requested to be present.

Selected bidders will be communicated of the date of opening of the commercial offer to enable them to send their representative in whose presence the bid will be opened.

4.7 -BIDDING

The cost of bidding and submission of tender documents is entirely the responsibility of bidders, regardless of the conduct or outcome of the tendering process.

4.8 –LANGUAGE OF BIDS

All bids and supporting documentation shall be submitted in English.

4.9 –BID CURRENCY

All costs and charges related to the bid shall be expressed in Indian Rupees.

4.10 – PERIOD OF BID VALIDITY

The Bids shall be valid for a period of 90 days from the closing date for submission of the bid.

4.11 – FORMAT AND SIGNING OF BID

Each bid shall be made in the legal name of the Bidder and shall be signed and duly stamped by the Bidder or a person duly authorised to sign on behalf of the Bidder.

4.12 – EVALUATION AND COMPARISON OF BIDS

The Bank reserves the right to modify or relax the eligibility criteria at any time, without assigning any reason, whatsoever. Only bids from Bidders meeting the **eligibility criteria (as described in Annexure-I)** and submitting complete and responsive bids will proceed to the stage of being fully evaluated and compared. The evaluation procedures to be adopted for the bid will be the sole discretion of the Bank and the Bank is not liable to disclose either the criteria or the evaluation report/ reasoning to the bidder(s).

4.13 – RIGHT TO ACCEPT / REJECT

The Bank reserves the right to accept any bid, or to reject a particular bid at its sole discretion without assigning any reason whatsoever.

4.14 – NOTIFICATION OF AWARD

The acceptance of a tender, subject to contract, will be communicated in writing at the address supplied for the bidder in the tender response. Any change of address of the Bidder, should therefore be promptly notified to **Assistant General Manager, Information Systems Audit Cell, Inspection Department, Indian Bank, Corporate Office, 254-260 Avvai Shanmugham Salai, Royapettah, Chennai – 600 014, Tamil Nadu. Contact phone No: 044- 28134031; 28134497 email-id – hoinspection@indianbank.co.in**

4.15 – CONFIDENTIALITY/NON-DISCLOSURE AGREEMENT

As the successful bidder(s) will have access to the data/information of the bank while auditing the security, bank will require the bidder(s) and their representatives to sign a confidentiality/non-disclosure agreement undertaking not to disclose or part with any information relating to the bank and its data to any person or persons, as may come into possession of the bidder(s) during course of the I S Audit. The bidder shall also give a declaration stating that he does not have any vested interest in applying for this audit. They are also prohibited from transmitting any information through personal email IDs and cloud storage. The successful bidder should ensure removal of any data/

information of the bank after the completion of the audit period, shall give a commitment to the effect, prior to the commencement of the audit and a confirmation immediately after removal of the same.

4.16 – COMPLIANCE TO LAWS IN INDIA

The Information Security Auditor will undertake to comply with all the prevailing laws and regulations in India relevant for Information System Audit.

4.17 – COMPLIANCE TO REGULATIONS OF RESERVE BANK OF INDIA/OTHER REGULATORY AGENCIES

The Information Security Auditor will also undertake to comply with all the requirements of the guidelines of Reserve Bank of India or other appropriate agencies as regards Information Systems Security Standards issued from time to time.

Bank reserves the right to inform IBA/GOI/RBI in case any major vulnerability is noticed after Security Audit within 6 months from the date of security audit.

4.18 – SIGNING OF CONTRACT

The successful bidder(s) shall be required to enter into a contract with Indian Bank, within 10 days of the award of the tender or within such extended period as may be specified by **Deputy General Manager, Information Systems Audit Cell, Indian Bank, Corporate Office, Inspection Department, 254-260 Avvai Shanmugham Salai, Royapettah, Chennai – 600014, Tamil Nadu,** on the basis of the Tender Document, the Tender of the successful bidder, the letter of acceptance and such other terms and conditions as may be determined by the Bank to be necessary for the due performance of the work

4.19 - BROAD TERMS & CONDITIONS OF THE CONTRACT

The Information System Auditors will have to audit the Security, Architecture, infrastructure, application and various audits as defined in the scope at the designated locations within the time period specified for this purpose by the bank. Three months after submission of the IS Audit Report, the auditors have to conduct a compliance review audit, to assess the impact of their recommendations.

The award of the I S audit assignment initially will be for a period of one year and on satisfactory performance and on completion of the compliance audit for the first year, audit assignment may be extended for another one year at the sole discretion of the Bank.

4.20 - ARBITRATION

The Bank and the IS Auditor 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 (30) days from the commencement of such informal negotiations, the Bank and the IS Auditor have been unable to resolve amicably a Contract dispute, either party may require that the dispute be referred for resolution to the formal mechanisms. These mechanisms may include, but are not restricted to, conciliation mediated by a third party, adjudication in an agreed national forum.

The dispute resolution mechanism to be applied shall be as follows:

(a) In case of dispute or difference arising between the Bank and the IS Auditor relating to any matter arising out of or connected with this agreement, such dispute or difference shall be settled in accordance with the Arbitration and Conciliation Act, 1996. The arbitral tribunal shall consist of 3 arbitrators one each to be appointed by the Bank and the IS Auditor; the third Arbitrator shall be chosen by the two Arbitrators so appointed by the Parties and shall act as Presiding Arbitrator. In case of failure of the two arbitrators appointed by the parties to reach upon a consensus within a period of 30 days from the appointment of the Arbitrator appointed subsequently, the Presiding Arbitrator shall be appointed by the Chairman, Indian Banks' Association, India which appointment shall be final and binding on the parties.

(b) If one of the parties fails to appoint its arbitrator in pursuance of sub-clause (a) above, within 30 days after receipt of the notice of the appointment of its Arbitrator by the other party, then the Chairman, Indian Banks' Association,(IBA) shall appoint the Arbitrator. A certified copy of the order of the Chairman, Indian Banks' Association (IBA) making such an appointment shall be furnished to each of the parties.

(c) Arbitration proceedings shall be held at Chennai, India, and the language of the arbitration proceedings and that of all documents and communications between the parties shall be English.

(d) The decision of the majority of arbitrators shall be final and binding upon both parties. The cost and expenses of Arbitration proceedings will be paid as determined by the Arbitral Tribunal. However, the expenses incurred by each party in connection with the preparation, presentation etc. of its proceedings as also the fees and expenses paid to the arbitrator appointed by such party or on its behalf shall be borne by each party itself.

4.21 – GOVERNING LANGUAGE

All correspondence and other documents pertaining to the contract shall be written in English only.

4.22 - NOTICES

Any notice given by one party to the other pursuant to this contract shall be sent to the other party in writing or by cable or facsimile or email and confirmed in writing to the

sender's address (the address as mentioned in the contract). A notice shall be effective when delivered or on the notice's effective date, whichever is later.

4.23 – USE OF CONTRACT DOCUMENTS AND INFORMATION

The Information System Auditor shall not, without the Bank's written consent, disclose the Contract or any provision thereof, or any specification or information furnished by or on behalf of the Bank in connection therewith, to any person(s) other than a person(s) employed by the Information Security Audit or in the performance of the Contract. Disclosure to any such employed person(s) shall be made in confidence against Non-disclosure agreements completed prior to disclosure and disclosure shall extend only so far, as may be necessary for purpose of such performance.

Any document, other than the Contract itself, shall remain the property of the Bank and all copies thereof shall be returned to the Bank on termination of the Contract.

The Information System Auditors shall not, without the Bank's prior written consent, make use of any document or information except for purposes of performing the Contract.

4.24 - INDEMNIFICATION

The Information System Auditor 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 Information System Audit.

4. 25 – PROFESSIONAL FEES / CHARGES

The price charged by the Information System Auditor for the services performed shall not vary from the contracted schedule of fees. Taxes as applicable will be deducted from the fees, as per prevailing rules on the date of payments.

4.26 - DELAYS IN THE INFORMATION SYSTEM AUDIT

The Information System Auditor must strictly adhere to the audit schedule, as specified in the Contract, executed between the bank and the Information System Auditor, 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:

(a) Claiming Liquidated Damages

(b) Termination of the agreement fully or partly

4.27 - 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 Information System Auditor and the Information Security Auditor shall be liable to pay the Bank as liquidated damages at the rate of 0.5% 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 Information System Auditor either as per the Contract, executed between the Bank and the Information System Auditor pursuant hereto or under any other Agreement/Contract, the Bank may have executed/shall be executing with the information System Auditors.

4.28 - FORCE MAJEURE

The Information System Auditor or the Bank is not responsible for delays or non-performance 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 despatch, 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 Information System Auditor shall promptly notify the Bank in writing of such conditions and the change thereof. Unless otherwise directed by the Bank, in writing, the Information System Auditor 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.

4.29. PAYMENT TERMS

Payments for the job of Information System Auditor will be milestone payments after completion of each assignment.

The IS Audit Service Provider's fees will be paid in the following manner for each year:

10%	Of the IS Audit Service Provider's fees after two weeks of commencement of the audit work and on submission of audit plan/procedures and methodology covering all the points as per Scope of Work for IS Audit
25%	of the IS Audit Service Provider's fees on submission of Interim report
25%	of the IS Audit Service Provider's fees on submission of final report
25%	On submission of final review Audit (compliance audit) report covering all the points as per the Scope of Work.
15%	On final Sign-off

5. BIDDER'S INFORMATION AND FORMATS

5. 1 TECHNICAL BID (PART A)

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. Whether empanelled by CERT-IN for providing I T Security Auditing Service and empanelment is currently valid or not (date of empanelment and period to be specified)

8. Number of CISA Qualified persons working in your firm along with names and experience.

9. Number of CISSP Qualified Persons working in the firm along with the names and experience.

10. Number of BS7799/ISO27001 lead auditors working in the firm along with the names and experience.

11. Number of Qualified network professionals and Ethical Hackers working in the firm along with names and experience

12. Number of years of experience in Information System Audit.

13. Describe Project Management methodology for the proposed IS Audit assignment, clearly indicating about the composition of various teams.

14. Describe Audit Methodology and Standards to be used for IS Audit.

15. Indicate Project Plan with milestones and the time frame of completion of different activities of the project.

16. List of Deliverables as per the 'Scope of Work'

17. Role and responsibility of Indian Bank and the Audit firm; explain other requirements from Indian Bank, if any.

18. Please give details of Information System Audit of Core Banking System carried out for Scheduled Commercial Banks in the past 3 years. The details of services and the scope to be indicated.

19. Please give details of Information System Audit of Internet Banking, SWIFT, Mobile Apps, etc. carried out for any Banks in India, Overseas Audit assignments if any may be specified separately.

20. Please give brief financial particulars of your firm for the last 3 years along with the volume of business handled.

    (The information will be kept confidential)

    1. Net Profit/Loss

    2. Total Turnover

    3. Revenue earned from Information Security Audit.

21. The team must have experience in I S audit of Security Technologies with multiple certifications such as RSA, CISCO Pix, Check Point, ISS, Trend etc.

22. Details of Location and infrastructure of Security Operations Centre from where services such as external vulnerability analysis and penetration testing are to be conducted/managed.

23. Capability on security remote management for security checking and device management.

24. Details of Internal expertise in networking, application development, security integration with application.

25. 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 Indian Bank 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.

5.2 FORMAT OF CURRICULUM VITAE (CV)

For Key Personnel likely to be associated with the IS Audit

(To be furnished on a separate sheet for each employee)

Name of the Person		
Profession		
Date of Birth		
Nationality		
Qualifications (Technical and Academic with year of passing):		
Membership of Professional Societies		
Service in this firm from		
Previous employment record	Organization	From to
Details of Key assignments handled in the past three years		
Organization	Month & Year	Details of assignment done

Give an outline of person's experience and training most pertinent to assigned tasks, describing the degree of responsibility held by the person on relevant previous assignments

5. 3 COMMERCIAL BID (PART B)

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

1. The format for the commercial bid is given below :

S. NO.	Name of the Project	Cost [Rs.] per year	Taxes, if any[Rs.]	Total Cost [Inclusive of all taxes, etc] per year [Rs.]
	IS Audit pertaining to Core Banking Solutions (data centre/project office/ network)			
	IS Audit of Internet Banking, e-commerce, mobile banking, payment systems, UPI etc			
	IS Audit of to Enterprise Network, network monitoring system			
	IS Audit of Bank's Security Operations Centre, IDPS, Anti-virus Management			
	IS Audit of ATM switch and infrastructure			
	Audit of SWIFT operations as per Swift guidance document			
	Vulnerability Assessment and Penetration Testing on all Bank's critical/non-critical assets			

	IS Audit, VA and PT of D R Site/near on-site			
	Performance and capacity management audit of ICT infrastructure			
	Audit of FI Application, infrastructure and process			
	All other items referred in the scope			
Total				

6. Annexure –I

Eligibility Criteria

1. The bidder should be a Government Organization (Central or State)/PSU/PSE/ partnership firm/LLP or a limited company. Should be in existence for at least five years as on 31.03.2017 and should have three years experience in Information System Audit of Banks.

2. The bidder should have a minimum turnover of **Rs. 2 (Two) Crores per year** in the last three years (**from operations in India**). The bidder should have made net profits in succession for the last 2 years. The relevant documents to be submitted as part of the proposal are the last three financial years audited Balance Sheets and Profit & Loss Account reports shall be submitted along with the technical BID.

3. The bidder Organisation must have been empanelled by CERT-In for providing IT Security Auditing Service and the empanelment should currently be valid. Documentary evidence of the same to be enclosed with the technical Bid

4. The firm should have never been blacklisted / barred / disqualified by any regulator / statutory body or the bidder/firm is otherwise not involved in any such incident with any concern whatsoever , where the job undertaken / performed and conduct has been questioned by any authority , which may lead to legal action. Self –declaration to that effect should be submitted along with the technical Bid. On a later date if self declaration is found to be void it may entail disqualification.

5. Should have prior experience in application functionality, security and controls review of the core banking solution for at least 2 scheduled commercial banks in India in the past 3 years.

6. Should have successfully conducted penetration testing and vulnerability testing in at least 2 Scheduled Commercial banks in India and should have sufficiently trained resources to conduct the tests.

7. Should have resources that are having sufficient domain knowledge of Core Banking solution and other banking applications

8. To ensure audit independence, the bidder should not be a vendor/consultant for supply/installation of Hardware/Software components of the Bank or involved in implementing Security & Network infrastructure of the Bank, either directly or indirectly through a consortium, in the past three years to Indian Bank and should not have conducted the IS Audit of the ICT infrastructure of Indian Bank during the preceding two years. However, the Bank reserves the right to decide if any of the activities mentioned above affects the auditor's independence or not for the current audit assignment at its own discretion.

9. **The Core Audit team assigned for I.S. Audit of the Auditee, should have** at least Four qualified professionals **with qualifications such as** CGEIT (Certified in the Governance of Enterprise IT),CISA, CISSP, CCNA, CCNP, ISO 27001/BS7799 Lead Auditor, OCM & OCP, out of which at least 3 persons should be CISA qualified (including team leader)**.** Bidder must warrant that these key project personnel to be deployed in this project have been sufficiently involved in similar projects in the past. Bidders should provide information about such key project personnel who are proposed to be part of the IS Audit team along with the Bid Document. Bidder should ensure that the members of Core Audit team are actively involved in the conduct of the Audit throughout the period of the contract

10. The Audit engagement manager should have been with the firm for at least a period of 2 years

11. All members of audit team proposed by the bidder should be employees on the rolls of the bidding organization. No part of the engagement shall be outsourced by the selected bidder to third party vendors

12. The bidder should have conducted minimum three IS audit of Data Centre/ DR Site etc. connected with minimum 1000 branches /Offices during last 3 years out of which at least two audit should be for Scheduled Commercial banks in India . The proposal should include certificates stating successful completion of the mentioned audit engagements. The conduct of IS Audit as mentioned above should include :-

I. Vulnerability assessment of servers/security equipment/ network equipment

II. External attack and penetration test of equipments exposed to outside world through internet.

III. Verification of compliance of systems and procedures as per Organization's IT Security Policy/ guidelines.

IV. I S Audit of Core Banking Application suite, Net Banking module, SWIFT, Mobile applications etc.

(Conduct of audit of any one activity will not be considered as complete IS Audit of Core Banking /Data Centre/DR Site)

7. ANNEXURE - II

Detailed scope of IS Audit applicable for all locations (as mentioned in Vertical 1 and Vertical 2) :-

IS Audit will cover entire gamut of computerized functioning including e Delivery Channels & functional areas with specific reference to the following:

1. Policy, Procedures, Standard Practices & other regulatory requirements:

1.1 IT Governance and alignment of Bank's IT strategy with Business goals, Information Security Governance, effectiveness of implementation of Bank's IT Security Policy & Procedures.

1.2 Compliance to National Critical Information Infrastructure Protection Centre guidelines (NCIIPC), guidelines/instructions from RBI/IDRBT, Gopalakrishna Committee recommendations on Information Security, Internet Banking & other delivery channels.

1.3 E-Commerce based on UNCITRAL; VISA, Ru-PAY, Master Card, and other regulatory guidelines; ISO 8583 standards for communication

1.4 CERT-In, PCI-DSS, NPCI and DSCI Guidelines.

1.5 IT Act 2000, IT Act 2008 (amendment) act.

1.6 Best practices of the industry including ISACA's Guidelines / COBIT / ISO standards.

2. Physical and Environmental Security:

2.1 Access control systems, Surveillance systems of Data Centre/ DR Site and Near-DR, Premises management

2.2 Assessment of risks and vulnerabilities due to natural calamities; Air-conditioning, humidity control systems, etc. of DC/ DR Site/ NDR etc.

2.3 Fire protection systems, their adequacy and state of readiness.

2.4 Electrical supply, Redundancy of power level, Generator, UPS capacity

2.5 Assets safeguarding, handling of movement of Man /Material/ Media/ Backup / Software/ Hardware / Information.

2.6 Pest prevention / rodent prevention systems, Water leakage detection systems.

3. IT Architecture – Audit of procedures, security

a. Operating Systems Audit of Servers, Systems and Networking Equipment:

3.a.1 Setup & maintenance of Operating System Parameters; OS Change Management Procedures– Version maintenance, hot-fixes &Service packs

3.a.2 Vulnerability assessment & hardening of Operating Systems

3.a.3 User account management including maintenance of sensitive User accounts - Use of root and other sensitive passwords;

3.a.4 File systems security of the OS; Review of Access rights and privileges, role based access control

3.a.5 Use of administrative shares, default login /passwords, remote access / Net meeting or any other such tool

3.a.6 Use of sensitive system software utilities

3.a.7 Remote access polices including Remote Desktop Management.

3.a.8 Users and Groups created, including all type of users' management ensuring password complexity, periodic changes etc.

3.a.9 Profiles and log-in scripts

3.a.10 Services and ports accessibility; validate the process for creating, deploying, managing and making changes to virtual machines and VSAN

3.a.11 Review of Log Monitoring, its' sufficiency, security, preservation and backup; Registry settings, including registry security permissions

3.a.12 Implementation of ADS (Active Directory Services) or Group Policy

3.a.13 Antivirus update and effectiveness of Big-Fix in patch updation

3.a.14 SAN Security ie., data encryption and integrity; SAN Management including performance optimization, scalability, migration

3. b. Application level Security Audit:

3.b.1 Logical Access Controls- To review all types of Application Level Access Controls including proper controls for access logs and audit trails to ensure the

Sufficiency & Security of Creation, Maintenance, monitoring and Backup of the same

3.b.2 Input controls, Processing controls, and Output controls for all critical Bank's systems

3.b.3 Interface controls - Interfacing of software with ATM switch, EDI, Tele banking server, Web Server and Other interfaces at Network level, Application level and security in their data communication

3.b.4 Authorization controls such as Maker Checker, Exceptions, Overriding exception & Error condition

3.b.5 Audit trail / Audit log generation, storage, retrieval and management

3.b.6 Data integrity & File Continuity Controls

3.b.7 User ID / Password Management; Hard coded user-ids and password, Segregation of duties, access control over development, test and production regions

3.b.8 Review of Parameter maintenance process and controls implemented therein

3.b.9 Change management / Patch management procedures including change request, unit/integration testing, impact analysis documentation, adequacy of user acceptance tests, roll-back procedure and version control. Availability of documentation pertaining to change requests with all changes traceable.

3.b.10 Exceptional procedures and approval mechanism for emergency changes viz. Backend Updations in the Bank's systems including CBS, Exim Bills, etc., Parameter Relaxations, Single Sided transactions, etc.

3.b.11 Review adequacy and completeness of controls; Identification of gaps in application security parameters

3.b.12 Audit of management controls including system configuration/ parameterization

3.b.13 Audit of controls over operations including communication network, data preparation and entry, production, documentation and program library, Help Desk and technical support, capacity planning and performance, availability of user & operation manuals

3.b.14 Monitoring of outsourced operations, Adequacy of Vendor support and whether in line with Service Level Agreements

3.b.15 Manageability with respect to ease of configuration, transaction roll backs, time taken for end of day, day begin operations and recovery procedures

3.b.16 Review of Software customization and adherence to SDLC Policy for such customization

3.b.17 Adherence to Legal & Statutory Requirements

3.b.18 Application level Recovery & Restart procedures; Backup/Fallback/Restoration procedures and contingency planning

3.b.19 If outsourced, escrow arrangement with application owner

3.b.20 Auditing, both at client side and server side, including sufficiency and accuracy of event logging, SQL prompt command usage, Database level logging etc

3.b.21 Adequacy of hardening of all Servers and review of application of latest patches supplied by various vendors for known vulnerabilities as published by CERT, SANS etc

3.b.22 Bank's IT Department will take necessary action to protect information contained on a server / storage device that is no longer in use e.g. erase and reformat disks. The Auditors shall examine instances of any lapses on this score.

3.b.23 Application-level risks at system and data-level including system integrity risks, system-security risks, data risks and system maintainability risks

3.b.24 Review of Software benchmark results and load and stress testing of IT infrastructure performed by the Vendors

3.b.25 Special remarks may also be made on following items- Hard coded user-id and Password, system mail retrieval and storage

3. c. Audit of DBMS and Data Security:

3.c.1 Logical access controls which ensure access to data is restricted to authorized users; authorization, authentication and security are in place; Segregation of duties

3.c.2 Audit of data integrity controls including master table updates; integrity is ensured to avoid concurrency problem

3.c.3 Confidentiality requirements are met; Physical access and protection

3.c.4 Use of Data Repository Systems, Data Definition Language, Data Manipulation Language (DML) and Data Control Language, Audit of log of changes to Data Definitions

3.c.5 Protection of Sensitive Information during transmission between applications/databases

3.c.6 Availability of Catalog Server, Synchronization of control file and catalog server

3.c.7 Database Backup Management, storage, retrieval, restoration procedures from older version to newer versions

3.c.8 Purging -Policy, procedures and process of purge of data

3.c.9 Security of oracle systems files viz. control files, redo log files, archive log files, initialization file, configuration file, Table space security, utilization, modifications, etc

3.c.10 Password check-up of Systems and Sys Users

3.c.11 Checking of database privileges assigned to DBAs and Users (privilege like ALTER SESSION, ALTER SYSTEM and BECOME USER etc.

3.c.12 To examine and review different types of Logs generated from users/ background/ memory process etc. and to examine the controls ensuring sufficiency & security of creation, maintenance and backup of the same

3.c.13 Procedures to ensure that all data are classified in terms of sensitivity by a formal and explicit decision by the data owner and necessary safeguards for its confidentiality, integrity and authenticity are taken as per IT Security Policy

3.c.14 Patches and new versions are updated as and when released by vendor/ Research and Development team

4. Network – Audit of Network Security architecture, Management, network devices, traffic and Performance analysis, review of NW monitoring software

4.1 Network Security architecture of the entire network including understanding traffic flow in the network at LAN & WAN level

4.2 Review of appropriate segregation of network into various trusted zones. Analysis of Network Security controls including logical locations of Security components like firewall, IDS/IPS, proxy server, antivirus server, email Systems, VSAT IDUs etc. in various zones

4.3 The Auditors shall review to ensure that access to Bank's Corporate e-mail facility is granted to authorized users

4.4 Review of redundancy for Links and Devices in CBS Setup both at central level and branch level

4.5 Review of security measures at the entry and exit points of the network

4.6 Checking Inter-VLAN Routing and Optimization, Study of incoming and outgoing traffic flow among web servers, application servers, database servers, DNS servers and Active Directory

4.7 Audit of VLAN segregation, access to servers, encryption mechanisms for connectivity and access, remote access provisioning etc

4.8 Review of Routing policy, Route path and table audit; Review of placement of security devices and DMZ's; Routing protocols and security controls therein

4.9 Audit of network architecture from disaster recovery point of view

4.10 Access control for DMZ, WAN, and for specific applications of the respective zones

4.11 Firewall policy, configurations, deployment and effectiveness

4.12 Review of all types of network level access controls & logs, for ensuring sufficiency & security of creation, maintenance and backup of the same, delegation of rights to users in accordance with job functions.

4.13 Secure Network Connections for CBS, ATM and Internet Banking including Client / browser based security

4.14 Review of Methodology adopted in maintenance of Network devices, their performance, replacement at all locations, DC/DR/NDR/ Branches/ offices.

4.15 Evaluation of centralized controls over Routers installed in Branches, DC/DR/NDR & their Password storage and Management

4.16 Audit of VSAT & Wireless connectivity infrastructure

4.17 Internet access management including cyber-roam - creation, maintenance, authentication procedures, access rights, deletion etc as per Bank's security policy

4.18 Active directory management – creation, maintenance, allocation of access rights and user groups, restrictions etc

4.19 Incident management: Audit of Incident Management and handling processes, roles and responsibilities, alerting and incident response procedures, verification of incident reports and effectiveness measurement, awareness of security incidents and events, Adherence to SLA

4.20 Privileges available to outsourced vendors

4.21 Review of

- Network documentation policy
- Network topology diagram
- nomenclature of server names, labelling, roles and allocation of IP Addresses
- Creation of change log for each server
- Documentation of software versions and proof of licence
- Documentation of hardware /firmware components, mode of connectivity of device, configuration, back up for configuration, password management for each device
- Documentation of backup procedure
- Violation logging management

4.22 Session Management

4.23 Configuration to defy security attacks like IP spoofing, ICMP redirects, banner grabbing using Telnet/FTP/HTTP etc, IP directed broadcasts

4.24 Verification of network devices for security threats including but not limited to DoS, DDoS, Spoofing, DNS poisoning, SYN flood etc

4.25 Checking for all known Viruses, Trojans, Root kits, Worms

4.26 Open TCP/UDP ports

4.27 Review of traffic & performance through

- LAN/WAN link utilisation/quality analysis/bandwidth availability/usage etc
- Capacity planning analysis including scalability
- Congestion area at various topology layer and traffic pattern analysis
- Analysis of latency/response time in traffic across various links
- Analysis of load balancing mechanism

4.28 Security audit of Wireless networking infrastructure deployed by the Bank including but not limited to Encryption technique, Authentication mechanism etc. of endpoints using technology like WLL, VSAT, RF, CDMA etc. for connectivity

5. Backup, Storage Media Management, Handling and Recovery Testing:

5.1 Audit of

- Backup & recovery/restoration testing procedures

- media maintenance procedures, definition of standards for external identification of magnetic media
- access controls, movement and storage of backup media to support accountability
- Consistency in handling and storing of information in accordance to its classification
- Sufficiency checks of backup process to ensure data integrity/restorability from earlier versions, validity of the data to the present environment, periodicity of backup storage and retrieval, etc.
- Controls for Prevention of Data Leakage through removable media or other means
- Synchronization between DC/NDR & DR Site databases

5.2 Adherence to Policies for media handling, disposal and transit

5.3 Protection of records from loss, destruction and falsification in accordance to statutory, regulatory, contractual and business requirement

5.4 Review of Retention periods and storage terms, as per regulatory requirements for documents, data, programs, reports, messages (incoming & Outgoing), keys/certificates used for encryption and authentication, log files for various activities

6. Privacy, Data Protection & Fraud Prevention:

6.1 Policy on implementation and Assurance to the management regarding proper controls and periodic updation of the same to prevent Cyber Frauds / IT Frauds and detection mechanism

6.2 Isolation and confidentiality in maintaining bank's customer information, documents, records by the bank including information available to Call Centre vendors, related sub-systems, Hardware, Software, applications, infrastructure used by the vendors involved in development/testing

6.3 Prevention of unauthorized access of former employees; People on notice period moved to non-sensitive role; Retired/Dismissed staff to be removed from the Active User List on immediate basis; Close supervision of staff in sensitive position

6.4 Review of documents / media retention policy; Media control within the premises

6.5 Procedures to prevent access to sensitive information and software from Computers, disks and other equipment or media when they are disposed of or transferred to another user are defined and implemented

6.6 Such procedures guarantee that data marked as deleted or to be disposed cannot be retrieved by any internal or third party

7. Business Continuity Methodology and Management and effectiveness of DR Drill process

7.1 Review of methodology adopted in identification of critical business process, systems and establish its ownership

7.2 Escalation procedure and policy with reference to efficacy of Emergency Response team/ Recovery team/Salvage Team/Incidence Reporting team

7.3 Review the adequacy of processes for conducting business impact analysis, risk assessment on the basis of Business Impact Analysis (BIA); Review and assess the adequacy of recovery strategies deployed by bank including cryptographic disaster

7.4 Participate in the DR Drill conducted by the bank every half year, once from the DR site and the other from the Data Centre and review DR Drill activity with respect to documented procedures, highlight any deviations from such procedures or improvements, if any, thereupon, including the effectiveness and efficiency of the automated tool for Switch over / Switch back activities

7.5 Adherence to Recovery Time Objective ('RTO') and Identification of Recovery Point Objective ('RPO') based on policies/guidelines

7.6 Data Backup – periodic media verification for its readability, offsite storage and movement of backups at the time of DR Drill; restoration of backup at DR Site

7.7 Assurance from Service providers for critical operations for having BCP in place with testing performed on periodic basis

7.8 Maintaining of robust framework for documenting, maintaining and testing business continuity and recovery plans by Bank and service providers

7.9 Adequate insurance maintained to cover the cost of replacement of IT Resources in event of disaster.

7.10 Time delay in transmission and restoration of daily data at DRS

7.11 Comment on success of Drill exercises

7.12 Review of escalation procedure adopted during disaster in branches, as per RTO & RPO of BCP Policy of the Bank

8. Addressing of HR issues and training aspect including:

8.1 Providing for the safety and wellbeing of people at branch or location at the time of disaster

8.2 Participation in drills conducted by RBI for Banks using RTGS/ NDS/ CFMS services

8.3 Security awareness training to staff; Communication of individual security Roles & Responsibilities to Employees

9. Asset Inventory Management:

9.1 Records of assets maintained - Existence of Inventory Database & Controls, which identify and record all IT assets and their physical location, and a regular verification schedule which confirms their existence, review and updating including remarks on under-utilization, if any

9.2 IT assets classification, ownership definition & Labelling of Assets

9.3 List of approved software and its license, Modality for Checking and restriction of usage of unauthorized software, Approved Software storage controls

9.4 Proper usage policies for use of critical technologies by Outsourced Vendor/Employee

9.5 Maintenance of Inventory logs for media

9.6 Proper utilization of infrastructure of IT Assets, license and Warranty / AMC details and overloading of resources

10. Outsourcing policy and review of risks –

10.1 Compliance to Outsourcing Policy/IS Security policy

10.2 Review of Coverage of confidentiality clause/Non-disclosure Agreement and clear assignment of liability for loss resulting from information security lapse in the vendor contract

10.3 Service levels are defined and managed; review of financial and operational condition of service provider with emphasis to performance standards, imposing penalties wherever deviations are observed, business continuity preparedness

10.4 Review of monitoring of vendors activities as per SLAs

10.5 Review of physical / logical access provided to third party contractors working onsite

10.6 Service Level Agreements (SLAs); audit of SLA management for all kinds of services like Data Centre, DR site, ATM Switch, Internet Banking, Physical Security, Facility Management, etc.

10.7 Review of formal agreements executed to take care of all the risks associated with outsourcing

11. IT Operations:

11.1 Business Relationship Management

11.2 Customer Education and awareness for adaptation of security measures; Mechanism for informing for deceptive domains, suspicious emails within the organisation/to customers

11.3 Review of monitoring of domain names to help prevent Entity for registering in deceptively similar names

11.4 Personnel scheduling - Shift hand-over process

11.5 Day begin and Day end process, Audit of SOD / EOD procedures, controls, control of transactions affecting intermittent accounts, control of systems generated transactions, re-posting of night region transactions, Job schedulers and execution/rollback of standing instructions.

11.6 Reviews of console log activity during system shutdown and hardware/ software initialization

11.7 Processes documentation; Operational procedure/documentation for Data Centre/Near-DR/ DR Site

11.8 Review of monitoring of operator log to identify variances between schedules and actual activity

11.9 Duty / Role segregation mechanisms/ procedures

12. Capacity Management:

12.1 Review of monitoring of system performance and resource usage to optimize Computer resource utilization and whether the same is as per Bank's policies

12.2 Service Continuity and availability management ; Avoidance of single point failure through contingency planning

13. Project Management:

13.1 Process & Procedure involved in Information System Acquisition, Customization, Maintenance including version control, SW Library, ESCROW arrangement

13.2 Development, modification, maintenance and enhancements to In-house applications including version control, maintenance of SW library

13.3 Changes to current systems should be adequately specified, programmed, tested, documented prior to transfer in the live environment

13.4 Scrambling of sensitive data prior to use for testing purpose

13.5 Release Management

13.6 Segregation of development, test and operating environments and review of segregation of duties while granting access in Development, test and live environment

14. Audit of Help Desk activities :

14.1 Review of functioning of centralized help-desk and the policy/procedure adopted

14.2 Review of methodology adopted in incident reporting, handling, resolution, and escalation to prevent recurrence with proper documentation including root cause analysis

14.3 Review of methodology adopted in prioritization/timely resolution of reported problems;

14.4 Audit trails and centralised archival of communication to and from helpdesks

14.5 Trend analysis and reporting

14.6 Development of knowledge base

15. Anti-Virus and Big-Fix, NTP server monitoring and implementation:

15.1 Proactive virus prevention and detection procedures are in place and implemented Virus definitions are updated regularly.

15.2 Review of monitoring of antivirus servers and clients located at branches, Zonal/Corporate Office in various locations for having updated latest versions and definitions.

15.3 Audit of anti-virus protection at servers/clients located at Data Centre/Near DR/DR site, Gateway level AV protection etc

15.4 Review of Implementation of automated security/OS updates in DC/NDR/DR/branches through Big-Fix

15.5 Review of implementation of synchronised time throughout network through NTP servers

16. Audit of Internet Banking & Mobile Banking Infrastructure:

16.1 Review of the process of Net Banking/Mobile Banking application, interface, data & Operational Security with reference to the Policy of the bank and regulatory requirement

16.2 Review of the net-banking/mobile banking architecture, connectivity, monitoring; creation, maintenance and modifications through RM Module at Branch level/Central Level

16.3 Review of controls to mitigate the risks due to Phishing / Vishing etc.

16.4 Systems audit of the Unified payments Interface (UPI) mobile application with PCI-DSS / PA DSS testing / Application Security Testing etc., as per NPCI guidelines. The auditors shall also comment on the deviations, if any, in the processes followed from the process flow submitted to the NPCI. (Auditor shall refer RBI Guidelines, NPCI Circulars, Industry Standards like ISO-27001, PCI-DSS etc. while performing an audit exercise)

16.5 Adequacy, generation & availability of Reports for financial, regulatory, statutory, MIS & statistical purpose covering all Mobile/net banking transactions

16.6 Adherence to Operational/Statutory guidelines issued by RBI, NPCI, PCI-DSS & other Regulatory bodies' with reference to Internet/ Mobile Banking Application

16.7 Audit of various functionalities provided in the application like Fund transfer, Transactions & queries, Cheque Book related, PAN/TAN validation etc.

16.8 Review of risk control measures in net-banking interfacing with CBS, access for NEFT/RTGS/ SFMS servers for LCs, payment of taxes, access to external sites like IRCTC, e-commerce transactions through gateway, 3D security management / 2nd factor authentication

16.9 Review of Customer feedback and appropriate resolution and reply communication to customers

16.10 Compliance of License agreement for all software/Hardware/OS

16.11 Adequacy of Operational Security features through Access Control, User Rights, Logging, Data integrity, Accountability, Auditability etc. for the Internet/Mobile Application Solution

16.12 Adequacy of PIN/ Password Management Controls (Generation, Re-generation, Authorization, Verifications etc.) of Internet Banking/ Mobile Banking & Key Management features

16.13 Audit of various security features including but not limited to Transaction level security, Platform Security & reliability includes Database, Network & transmission Security, Registration features, Administration Portal features, Call logging, tracking & Dispute Resolution features etc.

16.14 Analysis/Verification of Audit Logs /Audit Trails of Transactions, Exception List, Incident management report etc

16.15 Review to ensure strong access control measures & Confidentiality in the transmission, processing or storing of customer data both by Service Provider and Bank

16.16 Compliance of SLA provisions with the service provider

17. a) ATM Switch & ATM Facility Management (Outsourced)

17.a.1 Compliance of Service Level Agreement (SLA) with the outsourced ATM Switch Vendor & ATM facility management vendor including PIN Management, card Printing and Management, Hot listing of cards, Time Management in delivering ATM Cards/PINS to customers/ Home branch

17.a.2 Adherence to various limits accepted with the Switch Vendor/Managed Services Vendors in the SLAs w.r.t. Uptime/Availability/Penalties etc.

17.a.3 Process Audit of Debit Card Management System (DCMS) including issue, hot-listing, regeneration and printing of PIN

17.a.4 Audit of Fraud Risk Management Tool deployed in the ATM switch for real time monitoring, process of configuration of policies, rules for real-time detection/ prevention of fraud

17.a.5 ATM Process Audit comprising ATM Operational Controls, Consortium issues, Reconciliation, posting, settlement between Master/VISA/RuPAY Cards & Gateway vendors handling e-commerce transactions, dispute Management, Controls against Skimming, etc

17.a.6 Audit of the Reconciliation activities being carried out w.r.t transactions involving various Acquirer, Issuer, Merchant, Interchange, other stakeholders etc. found in the ATM switch files with the transactions found in Host, Interchange & Partner Bank's switch. Also, Chargeback processing including VISA chargeback, NFS Chargeback etc. to be checked for appropriateness

17.a.7 Connectivity to partner networks and two way authentication between Bank's Server & Third Party's Server (in case of STP Transactions like online bills payment etc. for Customers/ Users)

17.a.8 Adequacy of Operational Security features through Access Control, User Rights, Logging, Data integrity, Accountability, Auditability etc. at the ATM Switch/ATM Service Centre; Verification of the detailed security procedures & processes of the ATM Switch vendor including security controls for remote login of ATM Switch

17.a.9 Adequacy of Physical/environmental Security Controls at the ATM Switch (DC & DR) Presence of Biometric Authentication devices for Access Control, Fire Detection mechanisms & other Safety standards, Video Surveillance Systems/CCTV etc. to be checked

17.a.10 Analysis/Verification of Audit Logs /Audit Trails of Transactions, Exception List, Incident management report, reconciliation between Bank's GL and Vendor's GL

17.a.11 ATM Cash Management including outsourced Cash Management services; Review of daily operations including cash acceptance through Bunch Note Acceptors (BNA), reconciliation, EOD process through ADMIN menu, relevant Journal reports, dispute management, etc

17.a.12 Adequacy of contingency arrangement (Fallback / fail over procedures, Redundancy & Back-up) in the event of System Breakdown/Failure w.r.t Recovery/Restart facilities, Diagnostics for identification, Protection of Data, Backup facilities

17.a.13 Adequacy of Data/Network Security features with respect to the connectivity between ATM Switch (DC & DR Site), Bank's CBS DC/DRS, ATM Back Office etc Review of adequacy/appropriateness of the security protocol implemented (IPsec, SSH, SSL etc.), Network Security System Hardware/Software deployed (Firewall, IDS, Anti-Virus etc.), Adequacy /Reliability /Redundancy of the Bandwidth provided etc.

17.a.14 Adequacy, generation & availability of Reports for accounting, regulatory, statutory, reconciliation, MIS & statistical purpose covering all ATM transactions

17.a.15 Scalability & Interoperability for expanding network in future & sharing arrangements.

17. b) Credit Card Management

17.b.1 Compliance of Service Level Agreement (SLA) with the outsourced Credit Card Vendor inclusive of charging penalties in case of non-adherence to acceptable level of service

17.b.2 Review of security involved in sharing confidential customer details with the vendor, mutual sharing of reports, payment reconciliation etc

18. Project Management:

The Bank and the vendor will nominate a Project Manager immediately on acceptance of the order, who will be the single point of contact for the Project. However, for escalation purpose, details of other persons will also be given.

8. RFP Response Format

(Letter to the Bank on the Bidder's letterhead)

To
Indian Bank,
Information Systems Audit Cell
Corporate Office, Inspection Department
Chennai – 600 014

Dear Sir,

Sub : Response to RFP in connection with outsourcing IS Audit
Ref : RFP No CO:INSP: 1/2017 dated 01/06/2017

With reference to the above RFP, having examined and understood the instructions, terms and conditions, we hereby enclose our offer for conducting IS Audit of the systems, as detailed in your above referred inquiry.

We confirm that the offer is in conformity with the terms and conditions as mentioned in your above referred RFP. We further confirm that the information furnished in the proposal, annexures, formats, etc is correct. Bank may make its own inquiries for verification and we understand that the Bank has the right to disqualify and reject the proposal, if any of the information furnished in the proposal is not correct.

We also understand that the Bank is not bound to accept the offer either in part or in full. If the Bank rejects the offer in full or in part, the Bank may do so without assigning any reasons thereof.

We further understand that the finalized prices will be frozen for a period of two years from the date of entrustment of assignment and that the Bank, at its discretion may entrust the assignment again in full or parts at the same price and terms as per its requirements.

Yours faithfully,

Authorized Signatories
(Name, Designation and Seal of the Company)

Date: