इंडियन बैंक
Indian Bank

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

RFP:INSPN:ISA:133:2011-12

Indian Bank
Information Systems Audit Cell
Head Office, Inspection Department
Chennai – 600 001
E-mail: hoinspection@indianbank.co.in
Website: www.indianbank.in

TABLE OF CONTENTS

1. INTRODUCTION

1.1. BACKGROUND

Indian Bank, a premier nationalised Bank having its Head Office in Chennai has national presence in more than 1800 locations and international presence in Singapore, Jafna and Colombo. It has been serving the nation with a team of dedicated staff for more than 100 years. The Bank is engaged in diversified banking activities. Being a front runner in specialised banking and a leader in Rural development, the Bank is also a pioneer in introducing the latest technology in Banking including introduction of ATMs etc. It has implemented a Centralised Banking Solution /Internet Banking with Data Centre at Chennai and DR site at Hyderabad. The Centralised Banking Solution has already been implemented in all branches covering 100 % of total business and CBS branches are connected to the Data Centre, through a Wide Area Network. Internet Banking Services are offered to customers of all the branches which are covered by the Centralised Banking Solution. The modes of connectivity to the branches will be a combination of leased lines, ISDN Lines, VSATs, GPRS and other forms of connectivity which may emerge in the near future.

This RFP seeks to engage an Information Systems Audit Firm, which has the capability and experience, to conduct a comprehensive Information Systems Audit of its critical IT infrastructure and to make appropriate recommendations, as covered under the Scope of Work. The aim of the RFP is to solicit proposals from qualified bidders for IS Audit assignment. Interested eligible bidders may download the RFP from Indian Bank website **www.indianbank.in - Tenders/Bids/Auction**

The details of Core banking, Internet Banking and Security Infrastructure are as under.

1.2. CORE BANKING

The application and the Oracle database servers are on AIX Unix platform. The Bank has chosen Windows 2000 / 2003 platform for Branch Server application and Oracle 9i /10g /11g / SQL Server 2005 as the Database. IBM RISC based servers are configured under clustering mode for running the application server, database server and WEB Server.

Following is the brief list of modules covered in the Core banking application.

- Core Banking (BANCS@24) – M/s TCS
- Trade Finance (Exim Bills)- M/s China Systems, Taiwan
- Finance One – GL Package- M/s TCS
- Tele Banking -- Fone Bank - M/s TCS
- Credit Analysis – ecredit – M/s TCS
- E-Branch-kiosk – M/s TCS
- Banking Service Center - M/s TCS
- Help Desk Tool
- Internet Banking, Mobile banking, Utility Bills Payments, IMPS - M/s TCS
- Financial inclusion package – M/s TCS

1.3. INTERNET BANKING:

The Internet banking channel offers information and transaction services to both corporate and retail customers. The Internet Banking application from M/S TCS has the following modules:

- Retail Banking
- Corporate Banking
- Bill Payments
- Funds Transfer

1.4. IT SECURITY INFRASTRUCTURE:

The Bank has an IT security policy in place to cater to the Business requirements and to secure I T Assets. Considering its IT Security assets and the vulnerabilities associated with Internet banking, the Bank has designed suitable security architecture.

To Secure the Network, Communications, Systems and Application software, Data bases, Data, Information etc., and ensure the availability of resources to authorised users without any disruption or degradation, the bank plans to put robust security framework as per the Information Security Policy approved by the Bank. In this regard Bank has implemented Enterprise wide Security Project (Security Operation Centre) at Chennai to monitor and protect its IT infrastructure from vulnerabilities.

1. 5. Bank’s Objective for conducting annual I S audit of Information systems and I T infrastructure is to ASSESSS WHETHER

- BANK’S information and data are secure, and will remain complete, current, and accurate
- BANK’S information assets are secured against unauthorized access / usage / damage / changes
- BANK’S business continuity planning is adequate enough to ensure customer service, despite interruption to technology facilities for a significant amount of time
- Precisely identify BANK’S technology infrastructure as well as users at any given time
- BANK’S networks are adequately protected
- that BANK’S computer operations are carried out in a controlled environment
- adequacy of performance tuning to BANK’S I C T (Information and Communication Technology) infrastructure
- Capacity management of BANK’S I C T infrastructure is optimized (right sized) to deliver services effectively and efficiently
- BANK can get independent assurance over effectiveness of controls exercised by out-sourced vendors for technology services
- BANK has appropriate controls in its entire systems development life cycle, project management and implementation activities

2. SCOPE OF WORK {for the years 2011-12 and 2012-13}

1. Vulnerability assessment of Infrastructure relating to CBS Network, Data Centre, CBS-Project office, Head office and D R Site.

2. CBS Project office and Data Centre functional audit covering User / Help Desk / Parameter / Access / Back end corrections /Change Management

3. I S audit of Core Banking Applications including BANCS@24, EXIMBills, ATM interface, e-Credit , e-Branch-kiosk/lounge etc. Broad areas to be covered are as per Annexure –I.

4. Half yearly external and internal Penetration testing of enterprise wide Information systems including internet banking

5. Report on the overall security aspects of the entire Internet Banking /tele banking/ Mobile Banking / IMPS architecture with recommendation for improving the security if any. Broad areas to be covered are as per Annexure – II.

6. Internet banking infrastructure audit - The Auditors will certify that the security architecture of the Bank for Internet banking fulfils the criteria set by Reserve Bank of India

7. Process audit of minimum 10 CBS branches (along with onsite and offsite ATMs relating to the identified Branch) with focus on critical areas like password controls, control of user ids, operating system security, anti-malware controls, maker checker controls, segregation of duties, rotation of personnel, physical security, review of exception reports/audit trails, BCP policy and testing etc.

8. Undertake 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
   Depository participant – Controlling office
   Credit Card Centre
   Treasury Branch – Credence Treasury Domestic / Forex
   Wealth Management System
   Anti Money Laundering
   M I S
   R T G S / NEFT
   H R M S – SAP / Pension / Payroll / P F
   Risk Management – RAM /CAM/ CORE
   Service Branch (in-house clearing software & Cheque Truncation system)
   Overseas Branch – forex related software
   Financial Inclusion application
   E-mail system
9. I S Audit of Enterprise Network including Network architecture review, NMS (Network Monitoring system) & Administrative Process with report and recommendations. Broad areas to be covered are as per annexure – III

10. I S audit of Bank’s Enterprise wide Security project (including SOC) - Broad areas to be covered are as per annexure – VI

11. Audit of Capacity management and adequacy of performance tuning of Bank’s I C T infrastructure - Broad areas to be covered are as per annexure – V
12. ATM Systems Audit (Normal ATM/ Bio-metric ATM / Cash-in-ATM)
    - Application Audit
    - Network Security Audit
    - Switch Functionality Audit
    - Interface Audit
    - Audit Trails
    - Transmission Security
    - Authorization
    - Review of Fallback/ fail over procedures
    - Status Update Review
    - DR Site Audit for ATM.
13. ATM Process Audit
    - ATM Operational controls
    - Consortium issues
    - Reconciliation/ Functional Managerial activities
    - Card / PIN Management cum Security Review
    - RACS with reference to ATM Cash Management
14. DR Site Audit (ATM / CBS / Net banking)
    - Verification of systems/controls at the DR site
    - Assessment of environment and procedures at the BC site
    - Assessment of management parameters
    - Adequacy of infrastructure (capacity to handle full traffic)
    - Review of fallback procedures
    - Assessment of access control
    - Process audit to be carried out during D R drill
15. Record Management
    -Record processes and controls
    - Policies for media handling, disposal and transit
    - Periodic review of Authorisation levels and distribution lists
    - Procedures of handling, storage and disposal of information and media
    - Storage of media backups
    - Protection of records from loss, destructions and falsification in accordance to statutory, regulatory, contractual and business requirement
16. I S audit of Bank’s website, intranet and web applications facing internet

17. Intensive Security training for Indian Bank Inspection (Audit) Team
    This will provide skills and knowledge on various security threats, attacks & vulnerabilities and the security technology for protecting them. It will discuss IS Auditing Process, role, configuration and management of security technologies, system hardening, authentication measures, backup processes and others as applicable in Banking environment. The training will also discuss about the suitable internal audit tools and provide hands on training.

2.1 Deliverables Under IS Audit

I S Auditor will deliver detailed reports as below:

1. I S Audit (Technical & Process) Report for Core Banking application suite (including Bancs@24, Exim Bills, Finance One, Colombo CBS, e-VVR, E-branch-kiosk etc.,)
2. I S Audit (Technical & Process) Report for Internet Banking (including net banking, telebanking, mobile banking, IMPS, Utility Bills Payments, Banking service centre, financial inclusion etc.)
3. Auditors certification to the effect that the security architecture of the Bank for Internet banking fulfils the criteria set by Reserve Bank of India
4. I S audit report of 10 selected CBS branches and onsite and offsite ATMs relating to the identified 10 Branches
5. CBS Project office and Data Centre functional audit report covering User / Help Desk / Parameter / Access / Back end corrections /Change Management
6. I S Audit reports for standard and legacy applications listed under point no.8 of Scope of work
7. I S Audit report of ATM systems & process
8. Functionality Audit Report of the ATM Switch, Network and Interfaces with CORE Banking & Tie-Up Banks
9. Network Architecture Review Report
10. Network Management and Security Audit Report
11. External & Internal Penetration Testing Report
12. DR Site audit report
13. Capacity management and Performance tuning audit report
14. Vulnerability Assessment Report covering all network components like,
    - Network devices , Operating Systems , Application servers , Database servers available in Data center, CBS-Project Office and Head office
    - Vulnerabilities analysis of ATM interface
    - Vulnerability analysis of Branch CBS infrastructure
    - Vulnerability analysis of CBS interface to other applications
15. Enterprise wide Security Project(SOC) – I S Audit Report
16. I S Audit report of Bank’s Record Management process and controls
17. I S Audit report of Bank’s website, intranet and web applications facing internet
18. Screen Dumps of testing and testing reports
19. Risk Analysis Report
20. Recommendations for Risk Mitigation
21. Presentation to the Top Management on the findings of the Report
22. Prioritized Implementation Schedule of recommendations based on the impact and criticality on Bank’s business.

2.2 Qualified professionals to be deployed for the job

The entire Security Audit work has to be got done by qualified CISA/CISSP Professionals having requisite expertise in Information Security Audit. The Information Security Audit should be completed within the mutually agreed time schedule.

2.3 Audit Coverage period.

The proposed Annual I S audit will be for a period of two years.

3. TWO STAGE BIDDING PROCESS

For the purpose of the present job, a two-stage bidding process will be followed. 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 System Audit-BID" and "Do not open before 27TH JULY 2011" . 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 and Part-B are to be submitted in original, duly signed by the authorised signatories under the seal of the company in every page. Any correction should be authenticated by the same signatory. Documents/brochures showing the compliance to our specifications are to be attached to Part-A form. No enclosures to be sent along with Part-B form of the quotation.

Part A of the Bid will also contain the Bidders information in the format attached. Application fee of Rs.5000/- (Rs. Five thousand only) by Demand Draft(non-refundable) favouring "Indian Bank" payable at Chennai should be submitted along with Part A.

Note:

The vendor should arrange for producing supporting documents in respect of proof of Information Security Audit for Internet Banking /Core Banking Services, total turnover with break up towards IS Audit and Resume of the qualified professionals on the rolls of the company who will be involved in the audit of our bank.

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, which have been short listed as above, will be opened in the presence of their authorised representatives.

If insufficient or false information is furnished and/or if there is any deviation or non-compliance of the stipulated terms and conditions, the quotations will be summarily rejected without any reference to you. The price quoted should be unconditional and should not contain any strings attached thereto. Quotes which do not conform to our specifications will be summarily rejected

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 Part-B of bid.

3.1. Contents of document to be submitted

The bidder shall submit the following:

Part A (along with application fee of Rs.5000/-)

1) Bidder's Information as per format
2) Acceptance of the terms and conditions as contained in this document.

3) 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.
4) Total turnover with break-up towards IS Audit.
5) Resume of the qualified professionals on the rolls of the company who will be involved in the audit of our bank.
6) Bid security for Rs.1,50,000/- in the form of Bank Guarantee valid for 150 days from the last date for submission of Tender.
7) Power of Attorney of the person signing the document.
8) Articles of Association, Memorandum of Association of the company.
9) Audited balance sheets for the last three years 2007-08, 2008-09 & 2009-10

Part B

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

4. INSTRUCTIONS TO BIDDERS

4.1. Bid Process Timeframe

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
Date of issue of Tender Notification	29th June 2011
Pre – bid meeting	15.30 hours on 11th July 2011**
Replies to pre-bid queries will be uploaded on Indian Bank website/tenders by	16th July 2011
Last date and time for Bid Submission	15.00 hours on 27th July 2011
Date and Time of Technical Bid Opening	15.30 hours on 27th July 2011
Date of Completion of Technical Bid Evaluation	Within 10 days from the date of opening technical bid
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 date

**** Pre-bid meeting will be held at IMAGE, M R C Nagar, Raja Annamalaipuram, Chennai 600028, Tamil Nadu Tel No.24955607 At 15.30 hours on 11th July, 2011. Bidder's designated representative (one person only) may attend the pre-bid meeting. It is essential that all clarification/queries related to this RFP be submitted to the Bank at least three days before the date of pre-bid meeting.**

4.2. 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 and submitted separately. **The respective envelopes must have marking "Tender– I S Audit PART – A" and "Tender – I S Audit PART-B"**

Bids duly sealed should be delivered before 1500 hours on or before 27th July, 2011. 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 HO: Expenditure Cell,
8, Jehangir Street, “Govindu Maligai”,
Chennai – 600 001, Tamil Nadu.
Website: www.indianbank.in
Phone: 25260152/25270796
E-mail: hoinspection@indianbank.co.in

Last date for submission of bids is **1500 hours** on **27th July, 2011**. Bids received after **1500 hours** on **27th July, 2011** will not be accepted under any circumstances. The envelope containing Part A portion of the bids will be opened immediately thereafter at **1530 hours on 27th July, 2011** 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.

4.3.Bidding

A complete set of Bidding Documents will be ported in our bank’s website. The cost of Bid document is Rs. 5000/- (Rs. Five thousand only) Non-refundable. The amount has to be paid by way of DD favouring Indian Bank, payable at Chennai. The bidders have to download the bid document from our website. The cost of bid documents can be paid at the time of submission of bid.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.

4.2.Language of Bids & Bid currency

All bids and supporting documentation shall be submitted in English. All costs and charges related to the bid shall be expressed in Indian Rupees.

4.3.Period of bid validity

The Bids shall be valid for a period of 120 days from the closing date for submission of the bid.

4.4.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.

4.5.Acceptance of Bids

Bids shall be accepted up to 1500 hours on 27th July, 2011. No Bid will be accepted after the deadline.

4.6.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-4)** 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).

4.7. Acceptance or rejection of bid

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

4.8. 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 **The Deputy General Manager, Information Systems Audit Cell, HO: Inspection Department, Indian Bank, Head Office, NO.8 Jahangir Street, Chennai – 600 001, Tamil Nadu. Contact phone No:044-25260152; 044-25270796 email-id – hoinspection@indianbank.co.in**

4.9. 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) 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.

4.10. 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.

4.11. Compliance to Regulations of Reserve Bank of India / other Regulatory bodies and 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.

4.12. Signing of Contract

The successful bidder(s) shall be required to enter into a contract with Indian Bank, within 7 days of the award of the tender or within such extended period as may be specified by **The Deputy General Manager, Information Systems Audit Cell, Indian Bank, Head Office, Chennai – 600 001, 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

5. BROAD TERMS & CONDITIONS OF THE CONTRACT

The Information Security Auditors will have to audit the Security Architecture and various audit as defined in the scope at the designated locations within the time period specified for this purpose by the bank.

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.

Only Persons having **CISA/CISSP /GIAC(SANS)/ BS7799** qualifications and with adequate experience will be utilised by the Information Security Audit firm for auditing the Information Systems security architecture. Franchise of Information Security Auditors will not be permitted under any circumstances.

- **A Team containing Minimum of 4 CISA/CISSP /GIAC(SANS)/ BS7799 qualified resources to be deployed for minimum of 360 man days (90 x 4) per year.**

5.1. 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.

5.2. Governing Language

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

5.3.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 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.

5.4.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, if so required by the Bank.

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.

5.5. 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.

5.6. 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.

5.7. 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

5.8. 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.

5.9. 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.

5.10. 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

6. BIDDERS INFORMATION (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 if so, empanelment is currently valid or not

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 lead auditors working in the firm along with the names and experience.

11. Qualified network professional

12. Qualified Ethical hackers

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

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

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

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

17. List of Deliverables as per the ‘Scope of Work’.

18. Role and responsibility of Indian Bank and the Audit firm. Explain other requirements from Indian Bank, if any.

19. 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.

20. Have you done Information System Audit for Internet Banking for any Bank in India. If yes, please give details of the same including the complete details of services and the scope. Overseas Audit assignments if any may be specified separately.

21. Please give brief financial particulars of your firm for the last 3 years (1st April 2008 to 31st March 2010) 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.

22. 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.

23. Capabilities for offering automated penetrative checks.

24. Specify that technical consultants are certified on types of tools to be used for audit.

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

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

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

28. Details of largest Information System Audit executed including the scope, service cost and details of services.

29. 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.

7. FORMAT OF CURRICULUM VITAE (CV)

For Key Personnel likely to be associated with the IS Audit of CBS

(Separate sheets for each person)

Position:

Name of Firm:

Name of Personnel:

Profession:

Date of Birth:

Years with Firm:

Nationality:

Membership of Professional Societies:

Detailed Tasks Assigned: (past 5 years)
(Giving an outline of person's experience and training most pertinent to tasks 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 reversed order)

Qualifications : Technical and Academic with year of passing:

8. 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 traveling, 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.]
1	IS Audit - Core Banking Solutions(datacentre /project office /network)			
2	IS Audit –Internet Banking Application			
3	I S Audit – Networking			
4.	I S Audit of ATM infrastructure			
5	Software audit of Core Banking application software suite			
6	D R Site audit			
7	Performance and capacity management audit of Core Banking System			
8	All other items referred in the scope			
	Total			

i) Cost for the first year 2011-12 Rs.

ii) Cost for the second year 2012-13 Rs.

Total cost for a period of 2 years **Rs ___________.**

- Only the total amount inclusive of taxes will be reckoned for selecting L1 Vendor.
- TDS will be deducted from the amount at the rates prevailing as on the date of payment

Date: Authorised Signatory

9. ANNEXURE - I

SCOPE FOR IS AUDIT OF CORE BANKING SOFTWARE

1. Input controls
2. Processing controls
3. Output controls
4. Logical access control
5. Controls over automated processing /updation of records, review or check of critical calculations such as interest rates, etc., review of the functioning of automated scheduled tasks, output reports design, reports distribution, etc.
6. Auditability both at client side and server side including sufficiency and accuracy of event logging, SQL prompt command usage, Database level logging etc.
7. Extent of parameterization.
8. Functionality.
9. Internal control built in at application software level, database level, server and client side
10. Backup/Fallback/Restoration procedures and contingency planning.
11. Suggestion on segregation of roles and responsibilities with respect to application software to improve internal controls.
12. Review of documentation for formal naming standards, design process for job roles, activity, groups and profiles, assignment, approval and periodic review of user profiles, assignment and use of super user access
13. Manageability with respect to ease of configuration, transaction roll backs, time taken for end of day, day begin operations and recovery procedures
14. Special remarks may also be made on following items

    Hard coded user-id and password

    Interfacing of software with ATM switch, EDI, Tele banking server, Web Server and Other interfaces at Network level, Application level

    Recovery and restart procedures

    Sufficiency and coverage of UAT test cases, review of UAT defects and tracking mechanism deployed by vendor and resolution including re-testing and acceptance

    Review of customizations done to the software and the SDLC policy followed for such customization .

    Proposed change management procedure during conversion, migration of data, version control etc.
15. Suggest any application specific Audit tools or programs
16. Review of Software benchmark results and load and stress testing of IT infrastcture performed by the Vendors
17. Adequacy of Audit trails and meaningful logs
18. Adherence to Legal and Statutory Requirements.
19. Configuration of System mail
20. Adequacy of anti virus measures at CBS environment.
21. Adequacy of hardening of all Servers(data center and branches) and review of application of latest patches supplied by various vendors for known vulnerabilities as published by CERT ,SANS etc.
22. Apart from the IS Audit of the application software, IS Audit should be carried out at Data Center and at least Ten branches.

10. ANNEXURE -II

SCOPE OF IS AUDIT OF INTERNET BANKING APPLICATION

- The auditors will certify that the security architecture of the Bank for internet banking fulfils the criteria set by Reserve Bank of India.

- Review and report on the overall Information Systems Security Framework for internet banking including security aspects of the entire internet Banking Architecture with recommendation for improving the security if any

- Review and suggestions for improvement in the security policy, security/vulnerability patches, adequacy of tools for monitoring systems and network against attacks

- Review of risk control measures on legal requirements and privacy policy with special reference to internet banking scenario.

.

- Review of risk control measures in net banking interfaces like interface in CBS/RRB access for RTGS/NEFT, Interfacing with NSDL for ASBA, Interface for PAN/TAN validation, Access to external sites like IRCTC, from branches/offices

Web Server / Application Server / D B Server

- Review and report on
  1.Security settings with reference to security policy
  2.Security patches applied are current/latest
  3.Exposure of sensitive data on public area
  4.Ports on need to have basis, with special thrust on disabling unnecessary ports or ports that are potentially risky.
  5.Usage of super user account.
  6.Adequacy of control for activities to be done at System Console only

Logs of activity

- Review and report on adequacy of audit logs and procedures for review of audit logs as a preventive, detective and corrective control.

De-militarized zone and Firewall

- Review and report on
  1. Firewall policy, firewall configuration and deployment.
  2. Demilitarized zone

Security Review of all Servers used for Internet Banking

- Review and report on
  1. Adequacy of Operating system security
  2. Report on Parameterisation and its built-in controls.

Database and System Administration

- Review and report on
  1.Roles and responsibilties of DBA and System Administrator.
  2.Process flow documentation

3.Adequacy of controls to monitor activities of super users

4.Menu options in different modules as per the intent of the policy

Operational Activities

- Procedures for opening and operating accounts with thrust on legal aspects in internet banking scenario
- Maintenance of records in internet banking scenario

Application Control Review of Internet Banking Application

- Review and report on adequacy of logical access control procedures

Application Security

- Review and report on adequacy of testing of security infrastructure at various stages of acquisition process
- Undertake penetration tests of the information system. It should include
  1. Attempt to guess passwords using password cracking tools.
  2. Search for back door trap in the program
  3. Attempt to overload the system using DDoS(Distributed Denial of Services) and DoS(Denial of Service) attacks.
  4. Check for commonly known holes in the software, especially the browser and the application compliance to standards like OWASP.
  5. Conduct penetration testing keeping in view of the prevailing RBI guidelines, IT Act and other applicable regulations in India and check for following common vulnerabilities like IP Spoofing, Buffer overflows, Session hijacks, Account spoofing, Frame spoofing, Caching of web pages, Cross-site scripting, Cookie handling, sql injection etc.
- Secured Server Authentication procedures
- General computer control's review like logical access to the internet banking application, OS, Database and network and Physical access control, Backup and program change management.
- Review and report on security controls in RM Module.

11. ANNEXURE III

The Scope of the IS Audit of Networking covers the following aspects:

- Net Scanning – Threat and Vulnerability Assessment
  - It is the process of measuring and prioritizisng the risks associated with network- and host based systems and devices to allow rational planning of technologies and activities that manage business risk.
- Penetration Testing (Includes Both Internal and External in the presence of Indian Bank representatives) comprises of following testing:
- Password Cracking
- Intrusion Detection System / Intrusion prevention system Testing
- Firewall
- Router Testing
- Denial of Service (DOS) Testing
- Distributed DOS Testing
- Containment Measures Testing
- While doing the penetration test on Servers in live environment the ISA should ensure optimum performance of the systems.

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, 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. These functional capabilities need to be reviewed and audited.

Network Infrastructure Review

Network infrastructure at Branch, CBS-Project office, Data centre, D R site, offsite ATM and NAP(network Aggregation Points)

Network Management Review

The key management control aspects like standards for equipment, application, capacity planning, performance, reporting, problem resolution, costing and accounting are to be reviewed.

Network Administrative Review

The domains that are to be reviewed for the effective administration of network:
Monitoring of Structured Cabling and network usage
Optimization of setup,
Resolution of bottlenecks
Bandwidth allocation (requirement/utilisation especially during peak hours for big/service branches)
Standard reports and
Corrective action for the issues
Data Transmission Efficiency & Security:

Data Transmission.

- The Packet size of the message to be transmitted,
- The speed of transmission of message
- Security of message packets to be transmitted whether it is Tamper Proof Adequacy of Procedures for Encryption of Data to be transmitted
- File transfer protocols FTP & SFTP

Network Security Audit

- Physical and logical security measures, tools and processes implemented to protect unauthorized entry into corporate network are to be reviewed. Configuration of Firewalls & Routers, effectiveness of Intrusion Detection system and / automated audit trial of all the users of network are the key areas that should undergo review. Check if adequate security is available in the various Net work connectivity provided to ensure only authorized users are accessing the system.
- Check if remote logon is enabled and if so, whether it is identifiable by terminal IDs / IP addresses.
- Check if remote logon through services such as ftp, telnet, etc., is disabled. If not, ensure that the same has been implemented as instant guidelines.
- In case of WAN (Wide Area Networks), are the Router maintained securely to ensure efficient Information Security Administration.
- Focus should be on detecting the system vulnerabilities arising out of multiple access levels. Standard tools to scan various entry points to the network are to be used and an exhaustive analysis of security targets are to be provided. The scope includes operating system, databases, firewalls, routers, remote access devices and switches.
- Review the activities of Network Administrator/System Administrator and suggest Improvements and controls, if any, required.

12.Annexure –IV

Evaluation/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 31.03.2011 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 (2008-09 and 2009-10). 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 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 trained on the Core Banking solution preferably in FNS/BANCS@24

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, but excluding IS Audit Services, either directly or indirectly through a consortium, in the past three years to Indian Bank. 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 Five qualified professionals **with qualifications such as** CGEIT (Certified in the Governance of Enterprise IT),CISA, CISSP,CCNA, CCNE ,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/ DRS etc. connected with minimum 500 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 and Net Banking module

    (Conduct of audit of any one activity will not be considered as complete IS Audit of Core Banking /data center/DRSite)

14. ANNEXURE V

The Scope of the IS Audit of Capacity Management and performance tuning covers the following aspects:

The goal of Audit of capacity Planning and Management is to provide satisfactory service levels to users in a cost effective manner.

The basic steps for capacity planning & Management Audit:

1. Determine Service Level Requirements for old servers.
2. Analyse Current Capacity
3. Also analyse network bandwidth availability at peak level.
3. Planning for the future.
4. Analyse periodically Workloads and Service.
5. Measure overall resource usage.
6. Determine a process to measure the incoming work.
7. Establish service level requirements Vs performance.
8. Check whether the organization will be prepared for the future.
9. Identification of unauthorized programs/tools for removal

Thus ensuring that service level requirements will be met using an optimal configuration. This will also help us to identify when the old servers / PCs are required to be changed.

Prepare a framework that will help the bank instantly acquire the information necessary to purchase only what it need, avoiding over-provisioning while at the same time assuring adequate service

15. ANNEXURE VI

The Scope of the IS Audit of Enterprise-wide security project (SOC) covers the following aspects:

Security Device Audit

Configuration, policy/rule sets, signatures, Stateful Inspection, Logging, Location, redundancy, port restrictions, patches & updates, Administration & Management

- Firewalls (CISCO PIX (2 Nos), Checkpoint on SPLAT (6 Nos), Checkpoint on NOKIA (4 Nos)
- Network Intrusion Prevention Systems (IBM-ISS Proventia – 8 nos)
- Host Intrusion Detection Systems (IBM-Real Secure Server Sensor – 47 nos)

Architecture & placement of security devices

SOC Processes

- Change Management Processes – Deployment of rules, policies and adequacy of change management through Trouble Ticketing tool
- Incident Management Processes
- Documentation
- Backup processes
- Storage of logs
- Adequacy of Phishing Monitoring/Antiphishing services
- Adequacy of Security Monitoring
- Failover/Fallback processes and testing of failover/fallback processes

Adequacy of Reporting & Escalation Mechanisms

BigFix

Patch Management