Punjab National Bank

REQUEST FOR PROPOSAL

FOR

APPOINTMENT OF IS AUDITOR FOR DATA CENTER, DISASTER RECOVERY SITE, EDW, TREASURY AND OTHER HO DIVISIONS.

Inspection & Audit Division
Rajendra Place, Rajendra Bhawan
New Delhi - 110 008

CONTENTS

Chapter - 1: Introduction

1.1. Background

Punjab National Bank (PNB) has taken many IT initiatives. Bank has computerized 100% of its branches and has implemented a Centralized Banking Solution with Data Centre at New Delhi and Disaster Recovery Site at Mumbai. The Centralized Banking Solution connected to the Data Centre and DRS through a Enterprise Wide Network has networked all (5500 +) of its branches and offices. The modes of connectivity to the branches/offices are a combination of VSATS, leased lines, ISDN Lines, PSTN, Radio frequency and other forms of connectivity, which may emerge in the near future. Remote Access connectivity will also be provided to Identified offices, branches or customers. All the offices and HO Divisions are computerized. Besides this there are interfaces with applications and networks used by different institutions like MTNL, Customs, Reserve Bank of India etc.

Other alternate Delivery channels of services like Internet Banking, ATM, POS etc are also offered by the Bank to customers. An ATM Switch has been installed at New Delhi in the Data Centre and a DR setup is under operation and all the ATMs across the country are connected to the Switch through various modes of communication (both through private network and banks' enterprise Wide Network). Internet Banking Infrastructure is also located and integrated with the Enterprise Wide Network in a secured manner. Payment gateway infrastructure shall be established shortly. Bank also has Exchange server based corporate email setup.

Applications from multiple vendors for different internal requirements of Bank are also in use. Some of these applications are accessed through Enterprise Wide Network by different Branch Offices and also available through Internet and through Dial-up connection.

Bank is also in the process of implementing Data Ware Project to provide better access to information, to foster better and more informed decision-making, besides providing statutory reporting and MIS for the bank. This will also be located at Delhi.

The Operating Systems used in Different applications include different flavors of Unix like Solaris, AIX, SCO etc.), Windows NT, Windows 2000/2003/2008 enterprise Servers,Guardian, IBM AIX, HP Unix, Novell Netware, Tandem, DOS etc. Applications, which use messaging, include SWIFT, SFMS (RBI Infinet), Cash Management Services, Electronic Funds Transfer, and other RBI Projects etc. The Mail Server is on MS Exchange Server 2003. The Data bases include Oracle, MS SQL, DB2, Access, Sybase etc.

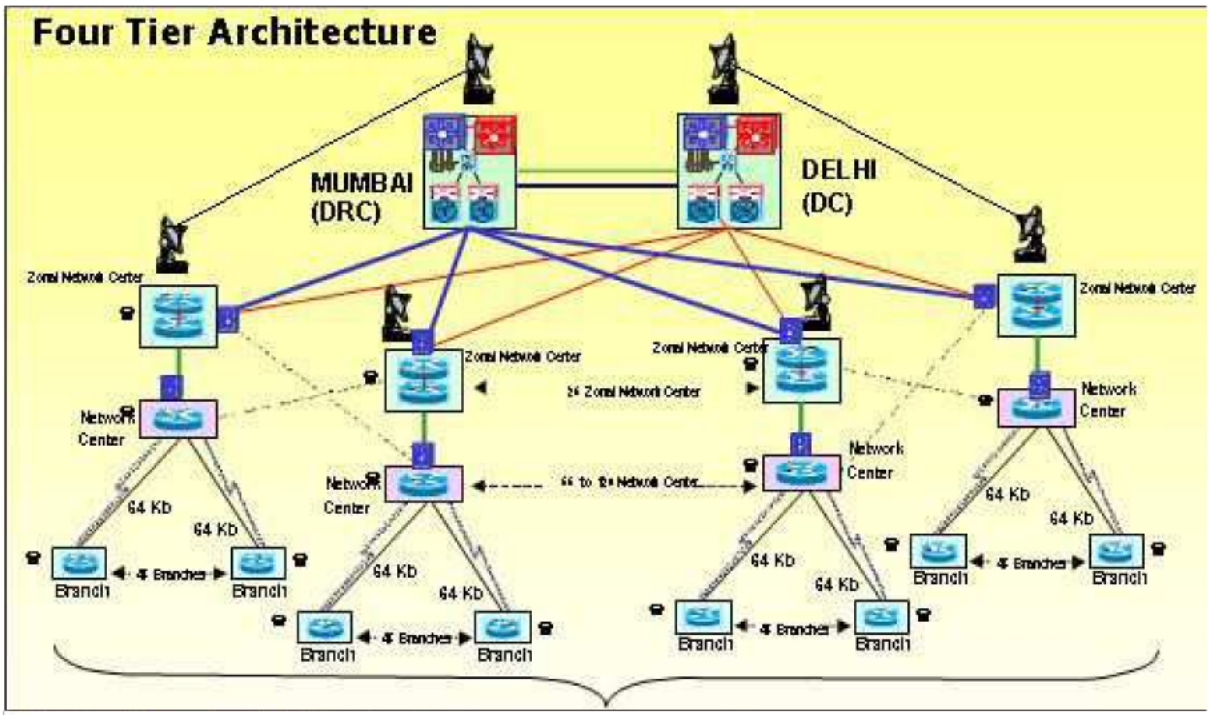
To Secure the Network, Communications, Systems, Application software, Data bases, Data, Information etc and to ensure the availability of resources including the network to authorized users without any disruption or degradation, the bank plans to utilize the services of Information Security.

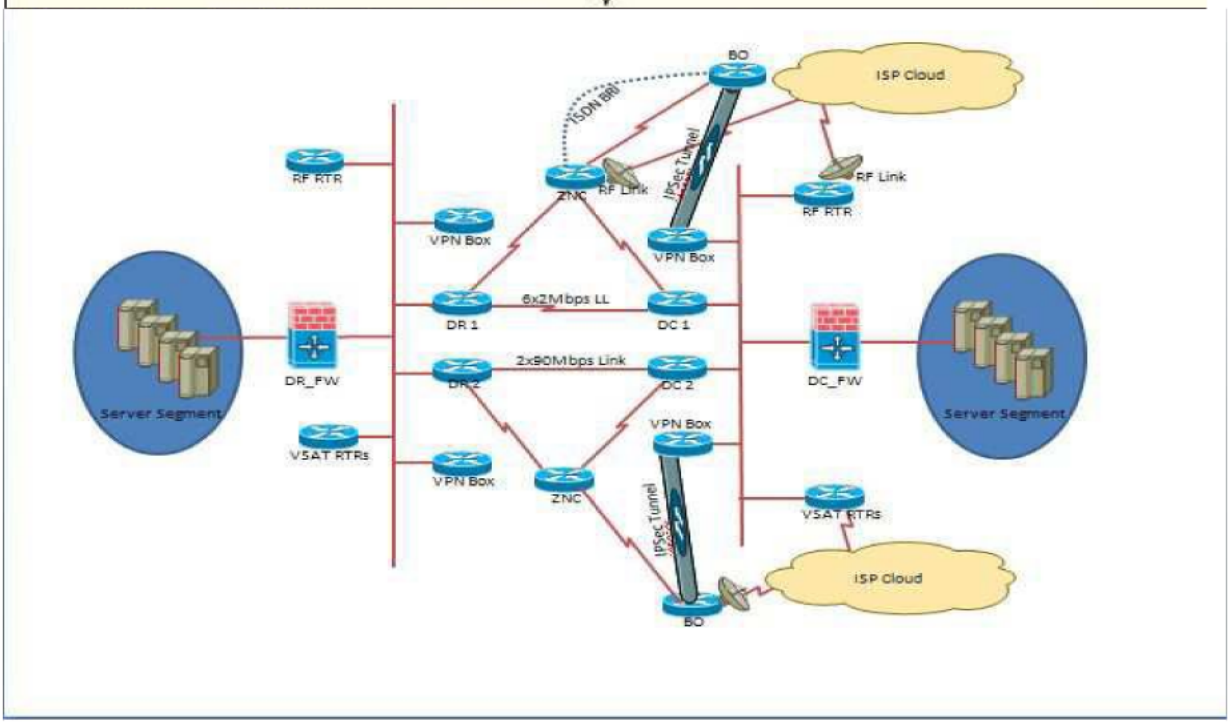
The Enterprise Wide Network is maintained by Bank's Network Integrator and the security measures are already enforced at various levels (Application Security, Network Security, Database Security, OS Security, Access Controls, Physical Security etc.). All these security measures are in place in congruence with the Bank's Information Security Policy, Business Continuity Plan, Disaster Recovery &various other regulatory directives.

The data Center, DRS and NOC have been certified as ISO 27001 compliant.

1.1.1 Technical Environment and Existing Network Architecture at Punjab National Bank

PNB has followed a hierarchical approach. All the locations are divided into Circle Offices. There are multiple Network Centers in each Circle. Network Center is the aggregation point of the branches in and around the city. There can be multiple Network Centers in a city. Some branches can also act as an aggregation point for the small extension counters behind them.





1) Bank has data centre and DRS for core banking application (fully functional). The CBS braches are connected to the centralized banking application, through the enterprise wide network which is a four tier meshed architecture wherein the braches/offices are directly

connected to a Network Center (NC). These NC's are further directly connected to a Zonal networking center (ZNC) which is directly connected to Data center (DC) at Delhi as well as Disaster recovery site (DRS) set up at Mumbai. The branches/offices, NCs and ZNCs are connected with a Leased line as primary link and ISDN dialup as back up link. The branches are generally using bandwidth of 64kbps and NCs are using bandwidth of multiples of 64kbps up to 2 mbps and ZNCs are using bandwidth of 2 mbps. Bank is generally procuring this bandwidth from BSNL/MTNL as it has entered into a MOU with BSNL/MTNL. Presently Bank is using CISCO routers and switches for LAN/WAN at majority of the locations. The equipment is being procured from approved vendor. Bank has installed more than 5553 ATMs which are connected through the WAN or VSAT network. Bank has video conferencing facility at 33 locations connected through an independent ISDN network. Bank WAN is running class A, IP schema 10.x.x.x and is using Dynamic routing protocol (EIGRP).

2) The IT resources of the bank at DC and DRS are protected with perimeter defense appliances/equipments. Checkpoint firewall with Alteon boxes are installed in failover mode. IPS is also installed. Locations like Chennai, Chandigarh and Treasury Division, HO, Delhi, SWIFT network, Mumbai, where the external networks are connected, are provided with CISCO firewalls.

3) Bank has installed an Enterprise Management system (EMS) - Unicenter from Computer Associates, for monitoring, managing and reporting faults, performance and accounting of Bank WAN, servers installed in Data centre, Disaster recovery site and at other locations across the network. Bank has different modules of this solution namely Network system management and Network performance operation, server management, database management, service plus service desk, desktop management, web server management, mail messaging system management and service level management.

4) The data centre of PNB comprises of servers installed with applications like FINACLE, IBS, MMS, HRMS, SFMS, and EMS etc. Besides this, there are base24 switches for ATM connectivity, Layer-3 and Layer-2 switches for ATM connectivity with servers and users. ZNCs are connected with DC and DRS routers with 2 mbps leased line links backed up by ISDN PRI. Besides this, various HO divisions are connected to DC routers through Leased lines backed by ISDN PRI/BRI lines. The DRS is connected to DC routers through Leased lines backed by ISDN PRI/BRI lines. The DRS is connected with the data centre through multiple of 2 mbps leased lines. DRS is a replica of DC containing similar type of servers, routers, switches etc. The network cables of data centre are of 1 gbps fiber and 10/100 mbps UTP. Bank has many web based applications like e-circular, proposal tracking system, PMS etc.

The bank houses various security devices positioned across various locations to protect its infrastructure from internet threats. Approx no is indicated in Annexure A.

1.2. Purpose

For appointment of IS Auditor for audit of activities at Data Center, Disaster Recovery Site and other HO Divisions providing independent reasonable assurance to the management on:

- Robust IT security,
- Mitigation of risks where there are significant control weaknesses
- Safeguarding the information assets viz. hardware, network etc.,
- Maintaining security, confidentiality, integrity and availability of data,

- Efficient utilization of resources-IT.
- Ensuring compliance of IT Security Policy and procedures defined by the Bank.

1.3. Project Scope

Detailed scope is at Annexure A [A1 &A2]. The overall approach of the IS Audit shall be constructive/ contributory. The evaluation shall be comprehensive, clear and IS Auditing shall help rectify the lacunae by concise directions.

1.4. Invitation

This RFP seeks Bidder(s) who are committed to the Information Security business and have the capability and experience in auditing IT infrastructure of PNB's size consisting of hardware, software, operating system, storage, event correlation and analysis etc besides other details as specified in this RFP. Auditor wherever mentioned in RFP means the bidder/ company /firm who will conduct IS Audit of the Bank.

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

1.5. Time Schedule of Various bid related events

1.	**Date of commencement of availability of Bidding Documents for Sale**	**21.10.2011**
2.	**Last date & time for submission of queries (by e-mail).**	**01.11.2011 (Tuesday) 16:00 hrs**
3.	**Last date and time for receipt of Bidding Documents at PNB.**	**16.11.2011 (Wednesday) 14.00 hrs**
4.	**Date and Time of Technical Bid Opening. (Change if any will be communicated to bidders who have submitted RFP in time with cost)**	**17.11.2011 (Thursday) 15.00 hrs**
5.	**Cost of RFP**	**Rs. 10,000/- (non refundable) in the form of Bank Draft/Pay order**
6.	**Earnest Money Deposit Amount**	**Rs.1,00,000/- (Rs. One Lac Only in the form of Bank Draft/Pay order**
7.	**Place of opening of Bids**	**Punjab National Bank, IT Audit Cell, Inspection & Audit Division, Head Office 2nd Floor, Rajendra Bhawan, Rajendra Place, New Delhi – 110008**

Note:

(i) Technical Bids will be opened in the presence of bidders who choose to attend as above

(ii) The schedule is subject to change and notice in writing of any changes will be provided wherever feasible. The PNB reserves the right to cancel the RFP at any time without incurring any financial obligation to any Bidder or potential Bidder.

(iii) Any query regarding the RFP may be sent to iadisaudit@pnb.co.in , vijayagarwal@pnb.co.in and nk_gupta@pnb.co.in addressed to The Chief Manager, IT Audit Cell, Inspection & Audit Division, Head Office, 2nd Floor, Rajendra Bhawan, Rajendra Place, New Delhi – 110008 before the Last date & time for submission of queries by e-mail.

2.1. Confidentiality

The RFP document is confidential and is not to be reproduced, transmitted, or made available or disclosed in any form or manner by the Recipient to any other person. Punjab National Bank may amend or revise the RFP document or any part of it. The Recipient accepts that they will receive any such revised or amended document subject to the same terms and conditions as this original and subject also to confidentiality.

The Recipient will not disclose or discuss the contents of the RFP document with any officer, employee, consultant, director, agent, or other person associated or affiliated in any way with Punjab National Bank or any of its customers, Auditors, or agents without the prior written consent of the Bank. The successful bidder shall execute a Confidentiality & Non Disclosure agreement with the Bank.

2.2. Non Disclosure Clause

i) The bidder (and his employees) shall not, unless the bank gives permission in writing, disclose any part or whole of this RFP document, of the proposal and/or contract, or any specification, plan, drawing, pattern, sample or information furnished by the bank, in connection therewith to any person other than a person employed by the bidder in the pursuance of the proposal and/or contract. In case of consortium proposals, all members of the consortium shall also be bound by this clause. Disclosure to any such employed person shall be made in confidence and shall be to the extent only so far as may be necessary for purposes of such performance. The employees engaged by the bidder will maintain strict confidentiality.

ii) The bidder, his employees and agents shall not without prior written consent from the bank make any use of any document or information given by the Bank, except for purposes of performing the contract award.

iii) In case of breach, the bank shall take such legal action as it may deem fit.

2.3. RFP TERMINOLOGY

Definitions

Throughout this RFP, unless inconsistent with the subject matter or context, the following terms will have the meaning as under:

i. Agreement:

Any written contract to be entered into between Punjab National Bank and the successful Bidder, including prime bidder, with respect to providing for any deliverables or services contemplated by this RFP. Any Agreement shall be deemed to incorporate, as schedules, this RFP and all supplements issued by the Bank, the bid of the Successful Bidder and any negotiated modifications thereto.

ii. Bidder/Vendor/Auditor:

A firm/ Company submitting a bid in response to this RFP. "Bidder" definition for this specific RFP for appointment of auditor shall include bidder(s) who directly possesses capabilities of conducting such assignments.

iii. Bank:

Reference to "the Bank", "Bank", "PNB" and "Punjab National Bank" shall be determined in context and may mean without limitation "Punjab National Bank", a Nationalized Bank in India.

iv. Proposal/Bid:

The Bidder's written reply or submissions in response to this RFP.

v. RFP:

The Request for Proposal document in its entirety, inclusive of any supplement that may be issued by the Bank.

vi. ITB:

Instructions to Bidders as Contained in Chapter – 3.

2.4. Disclaimer

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

Chapter – 2: Bidding Process

2.1. Bidding

Bidder who decides to bid will have to purchase RFP from the Bank at a cost of Rs. 10000/-. Only those bidders can bid who have purchased RFP from the Bank. Bidders shall submit their Bids in two separate parts, i.e. the Technical Bid and the Commercial Bid at the same time in separate sealed envelopes. The "Technical Bid" will contain the details to prove that it meets the eligibility criteria, whereas the "Commercial Bid" will contain the pricing information. The 'Technical Bid' will NOT contain any pricing or commercial information at all.

Technical Bids will be opened and evaluated first. Those Bidders who meets the eligibility criteria, as per the requirements and the terms and conditions of this document, shall be short-listed.

Commercial Bids will be opened only for the short-listed Bidders who have qualified in the Technical Bid. Bank reserve the right to opt for manual negotiation or Reverse Auction. Reverse Auction may be adopted in case two or more bidders are technically eligible.

2.2. Minimum Eligibility Criteria for Bidder(s)

To become eligible to respond to this RFP the vendor should fulfill the following minimum eligibility criteria:-

a) Bidder must prove that it is a current legal entity in India and must be financially solvent.

b) Should not be a vendor for Software and Hardware components of the Bank at Data Center, EDW, Treasury & DRS level.

c) Should not be involved in implementing Security and network infrastructure of the Bank at Data Center, EDW, Treasury & DRS level.
(For b & c) If involved in any specific activity which does not affect auditor's independence for current audit assignment may be considered at the discretion of the Bank.

d) Should be a Company /Firm /Organization /independent subsidiary with an average annual turnover of Rs.5 (five) crore or more for the last three financial years and should be in net profit during all three financial years.

e) Should have conducted minimum 2 Information System Security audits of data center connected with a minimum 200 offices, in last three years, out of which one audit should be in a bank in India.

Conduct of Information System Security audit shall constitute (but not limited to):

I. IT risk exposures throughout the Bank, including the areas of IT management & strategic planning, data centre (DC & DRS) operations, client/server architecture, local & wide area networks, telecommunication, physical & information security, electronic banking, system development and business continuity planning.
II. Vulnerability assessment and penetration test [VAPT] of servers /security equipment/ network equipment/ Applications through intranet.
III. External attack and penetration test [EAPT] of equipments & applications exposed to outside world through internet.
IV. Verification of compliance of system and procedures as per Organization's IT Security Policy/ guidelines.
(conduct of audit of any one activity will not be considered as complete IS Audit of data center etc.)

f) Should have implemented BS 7799/ISO 27001 security framework in any organization in India. After implementation, that organization should have been certified.

g) Should have capable to depute at a time minimum 10 qualified professionals with degree from Govt. recognized reputable Universities / Institutions as BE (CSE / IT) / B.Tech (CSE / IT) / ME (CSE / IT) / M.Tech(CSE / IT) / MCA / C.A.(ICAI) and certifications as CISA / DISA / CISM / CISSP / CEH / Sun Certified Security Administrator (SCSECA) / OCE (Oracle Certified Expert - Security Administrator), Cisco CCIE-security along with 3 or more years of IS Audit experience including at least one IS Audit for any organization defined at (e) above and should be on permanent roll of the organization.

h) Should not have been blacklisted by any nationalized Bank/ RBI/IBA or any other Government agency from offering such audit services/solutions to them. Bidder must give an Undertaking to this effect.

i) Should be able to depute adequate auditors (minimum 5) to cover given scope with due professional care & to provide deliverables as per clause 3 of "Detailed Scope" - Annexure A (A1& A2) of RFP.

j) Should be on the empanelment of Cert-In, Govt of India for Security Auditors with a certificate of empanelment valid up to 31/03/2012.

Bidder must submit a detailed statement of facts and profile of company including year of commencement of business, Internet site details and name and title of the authorized signatory for their Bid and their contact numbers and e-mail address.

Bidder should provide the documents in support of their eligibility in terms of above minimum eligibility criteria.

2.3. Scope of Bid

The scope of the bid shall be to appoint Information System Auditor to conduct audit as per detailed scope as per Annexure A [A1 & A2].

2.4. Amendments/Supplements to Bidding Documents

At any time prior to the deadline for submission of bids, the bank may, for any reason, modify the Bidding Document by amendments at the sole discretion of the bank. All amendments will be in writing and shall be delivered by hand / post / courier / email or faxed to all prospective bidders who have purchased/ received the physical copy of the bidding document directly from the Bank and will be binding on them. For this purpose bidders must provide name of the contact person, mailing address, telephone number and FAX numbers on the covering letter sent along with the bids/ request for bidding document.

In order to provide, prospective bidders, reasonable time to take the amendment into account in preparing their bid, the bank may, at its discretion, extend the deadline for submission of bids.

2.5. Rights of PNB

PNB reserves the right to :-

- Modify any terms, conditions and specifications of the RFP.
- Obtain revised price Bids from the Bidders with regard to modifications/ changes in RFP.
- Negotiate with Bidders.
- Accept any Bid in whole or in part.
- Split orders in favor of more than one Bidder.
- Release order, part order or more than one order.
- Finalize the bill of material and repeat orders.
- Issue the amendments to the RFP at anytime, prior to the deadline for the submission of Bids. From the date of issue, amendments to Tender Document shall be deemed to form an integral part of the Tender Document.

The Bidders shall, at their own cost, arrange to give a presentation/demonstration on their capabilities after submitting their Bid, if required by PNB. PNB shall communicate the venue, duration, date and time of presentation/demonstration to the Bidders at a later stage.

The Bids received and accepted will be evaluated by PNB to ascertain the best and lowest Bid in the interest of PNB. However, PNB does not bind itself to accept the lowest or any Bid and reserves the right to reject any or all Bids at any point of time prior to the placing of order without assigning any reasons whatsoever. PNB reserves the right to re-tender. PNB shall

not incur any liability to the affected Bidder(s) on account of such rejection. PNB shall not be obliged to inform the affected Bidder(s) of the grounds for PNB's decision of rejection. It is to be understood clearly by the Bidders that the selection process requires them to have adequate expertise in the audit domain.

2.6. Site Visits

Site visits may be sought at the discretion of PNB. Bidders shall provide, in addition to their customer sites, an invitation to the Bank to visit Bidder's own work site.

2.7. Governing Law and Disputes

The Bid and the resulting Contract with the successful Bidder shall be governed in accordance with the Laws of India for the time being in force and will be subjected to the exclusive jurisdiction of Courts at Delhi.

All disputes or differences whatsoever arising between PNB and the Bidders out of the meaning and operation or effect of this Tender Document or breach thereof, shall be settled amicably. If, however, the parties, as above, are not able to resolve them amicably, the matter shall be referred to the Sole Arbitration of General Manager, Inspection & Audit Division of Punjab National Bank, HO New Delhi, who as a Sole Arbitrator shall settle the dispute in accordance with the Arbitration and Conciliation Act 1996, and the award made in pursuance thereof shall be binding on the parties.

Any appeal will be subject to the exclusive jurisdiction of the courts at Delhi (India). In such instances, the Successful bidder shall continue to work under the Contract during the arbitration proceedings unless otherwise directed in writing by PNB or unless the matter is such that the work cannot possibly be continued until the decision of the Arbitrator is obtained.

The venue of the arbitration shall be Delhi, India. The arbitration proceedings will be held in English language.

Chapter – 3: Instructions To Bidders (ITB)

3.1. The Bidding Documents

3.1.1. Cost of Bidding

The cost of bidding and submission of tender documents in response to this RFP is entirely the responsibility of bidders, regardless of the conduct or outcome of the tendering process. PNB will not be liable for any costs incurred by the Bidder in replying to this RFP. It is also clarified that no binding relationship will exist between any of the Respondents and the Bank until execution of a contractual agreement.

3.1.2. Content of Bidding Document

The bidding document provides overview of the requirements, bidding procedures and contract terms. It includes Introduction, eligibility criteria, Instruction to Bidders, Broad terms and conditions of Contract, Technical Bid, Financial Bid. The bidder must conduct its own investigation and analysis regarding any information contained in the RFP document and the meaning and impact of that information.

The Bidder is expected to examine all instructions, statements, forms, terms and specifications in the bidding documents. Failure to furnish all information required by the bidding documents or submission of a bid not responsive to the bidding documents in every respect will be at the Bidder's risk and may result in rejection of the bid. While the Bank has made considerable effort to ensure that accurate information is contained in this RFP, the information contained in this RFP is supplied solely as a guideline for Bidders. Furthermore, during the RFP process, the Bank has disclosed or will disclose in the RFP and supplement (a), as applicable, available information relevant to the Work to the extent, detail, and accuracy allowed by prevailing circumstances. Subject to the provision in the previous sentence, the Bank has used or will use its best judgment and assessment to fairly and reasonably represent the nature and scope of the Work in order for Bidders to submit viable Proposals. However, the Bank shall not be deemed to give any guarantees or warranties of accuracy of any of the information in this RFP or any supplement, nor of its being comprehensive or exhaustive. Nothing in this RFP or any supplement is intended to relieve Bidders from forming their own opinions and conclusions in respect of the matters addressed in this RFP or any supplement, as applicable.

3.1.3. Clarification on RFP

The Bidder shall carefully examine and understand the specifications / conditions of RFP and seek written clarifications, if required, to ensure that they have understood all specifications / conditions of RFP. Written requests for clarification may be submitted to PNB before last date specified for queries (through email) in this regard.

Both questions and responses (including an explanation of the query but without identifying the source of the inquiry) will be circulated to all prospective Bidders, i.e. those that have purchased the Tender Document from the Bank.

Thereafter, no more clarification other than that asked by the last date specified for this purpose shall be entertained. No oral consultation either shall be entertained thereafter. The Bid should not carry any sections like clarifications, 'as orally told', 'to be discussed', interpretations and assumptions. With the submission of the Bid, the Bidder acknowledges that he/she has carefully studied and understood the RFP in totality.

Any questions concerning this RFP must be submitted through email at iadisaudit@pnb.co.in, vijayagarwal@pnb.co.in, nk_gupta@pnb.co.in on or before the last date to:
Chief Manager,
Punjab National Bank,
IT Audit Cell, Inspection & Audit Division,
Head Office, 2nd Floor,
Rajendra Bhawan, Rajendra Place,
New Delhi – 110008

No requests for clarification will be accepted by over telephone.

If a Bidder discovers any significant ambiguity, error, conflict, discrepancy, omission, or other deficiency in this RFP, the Bidder should immediately notify to the above official of such error and request modification or clarification of the RFP document, which (modification/clarification) shall be at the sole discretion of the Bank.

3.1.4. Correction of errors

Arithmetic errors in Bids will be corrected as follows:

i) Where there is a discrepancy in amounts in figures and in words, the amount in words shall govern.

Accordingly, The amount stated in words in the tender shall be considered as binding.

3.2. Preparation of Bids

3.2.1. Language of Bid

The bid prepared by the Bidder, as well as all correspondence and documents relating to the bid exchanged between the Bidder and the Bank shall be written in English language only.

3.2.2. Document Constituting the Bid

The bid prepared by the Bidder shall comprise the following components:

i). Technical Bid

a) **Minimum Eligibility criteria** – Details establishing the qualification of the bidder as per Minimum eligibility criteria (see Chapter-2) for the Bidders.

b) Point wise compliance of the terms and conditions enumerated in Tender Document. Any technical/commercial deviation with the Tender Document should be clearly stated with the reasons thereof.

c) Documentary evidence established in accordance with ITB Section 3.2.6 that the Bidder is qualified to perform the contract if its bid is accepted and that the bidder has financial, technical capability necessary to perform the contract and meets the criteria outlined in the Qualification Requirement and fulfill all the conditions of the Contract.

k) Bid security furnished in accordance with ITB Section 3.2.8.

l) An undertaking from the bidder (As per Annexure D) that the bidder is complying with all the conditions of the Contract and Technical Specifications of the Bidding Document as no deviation will be acceptable to the Bank.

m) All information called for as per above points should be submitted in two separate sealed envelopes.

Technical Bid should not contain any commercial / pricing details

ii) Financial Bid – Financial Bid will comprise of Bid Form as per Annexure I.

3.2.3. Bid Form

The Bidder shall complete the Bid Form and the appropriate Price Schedule furnished in the bidding documents.

3.2.4. Bid Prices

The Bidder shall indicate on total bid prices of the services it proposes to provide under the Contract in Indian National Rupee (INR).

Prices indicated on the Price Schedule shall be entered separately in the following manner:

Price will be quoted including all costs except duties and taxes. However, all applicable Taxes and Duties should be indicated in the Commercial Bid.

Fixed Price - A bid submitted with an adjustable price quotation will be treated as non-responsive and rejected.

In the event of third-party software products being incorporated in or forming part of the services rendered, the bidder(s) shall warrant that the software has been procured by the bidder(s) under valid licenses from the relevant intellectual property right owners of such software.

The bidder(s) further warrants that they possess a legal right to use the software under such licenses, in terms set out under any relevant license or sub-license agreement. The bidder(s) will indemnify the Bank for any and all costs that may arise out of the use of software, in which it is alleged that any rights of the owners of such software have been infringed.

3.2.5. Bid Currencies

All Costs indicated in the Commercial Bids should only be in Indian Rupees.

3.2.6. Document Establishing Bidder's Qualification.

Pursuant to ITB section 3.2.2., the Bidder shall furnish, as part of its Technical Bid, documents establishing the Bidder's qualification to perform the Contract if the bid is accepted.

The documentary evidence of Bidder's qualification to perform the Contract if the bid is accepted should establish to the Bank's full satisfaction that the bidder has the financial, technical and performance capability necessary to perform the Contract and meets the criteria outlined in the Minimum eligibility Criteria specified in this RFP. Bids that do not fully comply with minimum eligibility criteria will be rejected.

3.2.7. Documents establishing Solution Conformity to Bidding Documents

All the documents must accompany the response to this RFP as per Annexure O

Willful misrepresentation of the facts will lead to the cancellation of the contract without prejudice to any other action that the Bank may take.

All the submissions, including any accompanying documents, will become property of Punjab National Bank. The bidders shall be deemed to have license, and grant all rights to, Punjab National Bank, to reproduce the whole or any portion of thereof for the purpose of evaluation, to disclose the contents of submission to other bidders and to disclose and/or use the contents of submission as the basis for RFP process.

3.2.8. Bid Security

(i) Pursuant to ITB Section 3.2.2., the Bidder shall furnish, as part of its bid, a **bid security of INR 1 Lacs (Rupees one Lac only**).

(ii) The bid security is required to protect the Bank against the risk of Bidder's misconduct, which would result in the forfeiture fo the bid security.

(iii) The bid security shall be in Indian Rupees and shall be in the form of a Draft / Banker's cheque, in favour of Punjab National Bank, IT Audit Cell, payable at Delhi.

(iv) Any bid, not secured in accordance with above will be rejected by the Bank as non-responsive.

(v) Unsuccessful bidder's bid security will be discharged/returned as promptly as possible but not later than 30 days after the expiry of the period of bid validity

prescribed by the Bank. Bank will not be liable for any delay beyond 30 days as aforesaid and no claim for delayed interest will be allowed

(vi) The successful bidder's bid security will be discharged upon the Bidder signing the Contract, and furnishing the Performance Guarantee.

(vii) The bid security may be forfeited, if a Bidder

a) Withdraws its bid during the period of bid validity specified by the Bidder on the Bid Form; **or** does not accept the correction of errors ; **or**

b) In case of a successful Bidder, if the Bidder fails:

- To sign the Contract in accordance with Section 3.4.6; or
- To furnish Performance Guarantee in accordance with Section 3.4.7.

(viii) The Bid Security should not be placed in the Commercial Bid envelopes. Submission of Bid Security in the Commercial Bid envelope shall render the Bid liable to be rejected outright on the ground of non-submission of Bid Security.

(ix) The Bid Security shall be returned to the successful Bidder on his/her submission of Contract Performance Guarantee. For other Bidders, the Bid Security shall be returned on placement of order on the successful Bidder.

3.2.9. Period of Validity of Bids

The bids shall be valid for a period of 180 days from the date of closure for submission of the bid. The bid valid for shorter period shall be rejected as non-responsive.

In exceptional circumstances, the Bank may solicit the Bidder's consent to an extension of the period of validity. The request and the response thereto shall be made in writing (or by fax). The bid security validity period shall also be suitably extended. A Bidder may refuse the request without forfeiting its bid security. A Bidder granting the request of extension will not be required nor permitted to modify its bid.

3.2.10. Format and Signing of Bid

(i) The Bidder shall prepare the Technical Bid and Financial Bid separately, clearly marking each "Technical Bid" and "Financial Bid", as appropriate.

(ii) The bid shall be typed or written in indelible ink, numbered and shall be signed by the Bidder or a person or persons duly authorized to bind the Bidder to the Contract. The authorization shall be indicated by a written power-of-attorney or a board resolution accompanying the bid. The person or persons signing the bid shall sign all pages of the bid, except for an un-amended printed literature.

(iii) Any interlineations, erasures or overwriting shall be valid only if the person or persons signing the bid sign them.

(iv) Bid should be typed and submitted on A4 size paper and bound securely. Bidders responding to this RFP must comply with the following format requirements:

COVER LETTER/BIDDER CERTIFICATIONS:

Attach any covering letter included with the bid and those certifications required for submission of proposal.

Proposals submitted in response to this RFP must be signed by the person working in the bidder's organization who is responsible for the decision as to the prices being offered in the

bid or by a person who has been authorized in writing to act as agent for the person responsible for the decision on prices. Each bid shall stipulate that it is predicated upon the terms and conditions of this RFP and any supplement or revision thereof. By submitting a signed proposal, the bidder's signatories certify that in connection with this assignment:

- The bidder's organization or an agent of the bidder's organization has arrived at the prices in its bid without consultation, communication or agreement with any other respondent or with any competitor for the purpose of restricting competition,
- The prices quoted in the bid have not been knowingly disclosed by the bidder's organization or by any agent of the bidder's organization and will not be knowingly disclosed by same, directly or indirectly, to any other respondent or to any competitor, and
- No attempt has been made or will be made by the bidder's organization or by any agent of the bidder's organization to induce any other person or firm to submit or not to submit a bid for the purpose of restricting competition.

REFERENCE DATA SHEET:

For the services offered, Bidder must furnish a list of minimum of two (2) references that will be capable of verifying information supplied by the Bidders in proposal. Bidders should submit additional Reference Data Sheet forms if they have more than two (2) references.

The Bank reserves the right to contact and/or visit any party listed as a reference, which has previously utilized or is presently utilizing service(s) identical or similar to those being proposed by the bidder. The Bank may also utilize other sources of information about the product(s) and/or service(s) proposed by the Bidder where these sources are publicly available and are equally available for all competing bidders. The Bidder should not be present during site visits.

FINANCIAL STABILITY DOCUMENTATION:

Bidders responding to this RFP must be able to substantiate their financial stability. Audited Financial statements along with additional supporting documentation must be submitted with the bid.

RESPONSE TO GENERAL, TECHNICAL, PERFORMANCE AND SUPPORT REQUIREMENTS:

Provide a point-by-point response to each and every requirement specified in this RFP. Responses must indicate that either bidder's bid "does comply" with specifications or that it "does not comply." A succinct explanation of how each requirement can be met or cannot be met must be included.

ADDITIONAL INFORMATION:

Include additional information, which will be essential to an understanding of the proposal. This might include diagrams, excerpts from manuals, or other explanatory documentation, which would clarify and/or substantiate the bid. Any material included here should be specifically referenced elsewhere in the bid.

GLOSSARY:

Provide a glossary of all abbreviations, acronyms, and technical terms used to describe the services or products proposed. This glossary should be provided even if these terms are described or defined at their first use in the bid response.

PRESENTATION:

Bidders may be required to make presentations to supplement their bids, if requested by the Bank. The Bank will make every reasonable attempt to schedule each oral presentation at a time and location that is agreeable to the bidder. Failure of a Bidder to complete a scheduled oral presentation to the Bank before the date established in the above calendar of events may result in rejection of that Bidder's proposal.

3.2.11. Sealing, Marking and Submission of Bids

Bidders should provide their 'Minimum Eligibility Criteria', 'Technical' and 'Commercial' responses in one original and two additional copies and shall be labeled as "Original" or "Copy" as appropriate. Each of these shall then be sealed in a separate envelope labeled "Original Tender" or "Copy Tender" as appropriate. All the sealed envelopes containing Technical responses shall then be sealed in one envelope marked "Technical Bid for appointment of IS Auditor for data center and allied activities" in the top left hand corner. Similarly all the sealed envelopes containing Commercial responses shall be sealed in another envelope marked "Commercial Bid for appointment of IS Auditor for data center and allied activities " in the top left hand corner.

The Bids, which are not sealed as indicated above, are liable to be rejected. PNB will not be liable for Postal/Courier delay, non-receipt/non-delivery of documents, loss of documents in transit, etc., if any, in the Bidder receiving the RFP and/or in submitting the Bid before the scheduled time.

Bidders are requested to submit a "softcopy" version of their Technical and Commercial responses on a CD in Microsoft Office 2000/2003 format. Softcopies are to be sealed within the respective Technical and Commercial Bid envelopes.

All pages of the Bid including Brochures are to be numbered as Page --- (current page) of --- (total pages). The numbering shall be done for the whole Bid and not section-wise.

The envelopes shall be dated with the current date in the top right hand corner and addressed to as below:

The Chief Manager,
Punjab National Bank,
IT Audit Cell, Inspection & Audit Division,
Head Office, 2nd Floor,
Rajendra Bhawan, Rajendra Place,
New Delhi – 110008

If the envelope is not sealed and marked, the Bank will assume no responsibility for the bid's misplacement or premature opening.

Telex, Email or fax bids will be rejected.

3.2.12. Deadline for Submission of Bids

Bids (Technical and Financial) must be received by the Bank at the address specified under Section 3.2.11. on or before the last date of receipt of the Bid . In the event of the specified date for the submission of Bids being declared a holiday for the Bank, the Bids will be received up to the appointed time on the next working day.

The Bank may, at its discretion, extend this deadline for submission of bids by amending the bid documents in accordance with section 2.5, in which case all rights and obligations of the Bank and Bidders previously subject to the deadline will thereafter be subject to the deadline as extended.

3.2.13. Late Bids

Any bid received by the Bank after the deadline fixed for submission of the bids will not be considered. PNB will not be liable for any delayed receipt due to Postal/Courier delay. Bidder shall ensure timely dispatch so that the same reaches the Bank before deadline.

3.2.14. Modification and Withdrawal of Bids

i) The Bidder may modify or withdraw its bid after the bid's submission, provided that written notice of the modification or withdrawal is received by the Bank prior to the deadline prescribed for submission of bids.

ii) The Bidder's modification or withdrawal notice should be sealed and marked accordingly.

iii) No bid can be modified subsequent to the deadline for submission of bids.

iv) No bid can be withdrawn during the interval period between the deadline for submission of bids and the expiration of period of bid validity. The act of withdrawal of a bid during this interval will result in the forfeiture of the Bidder's bid security. In other words, no withdrawal of the Bid is allowed after the Dead Line fixed for Submission of the Bid.

3.2.15. Acceptance or rejection of bid

Incomplete Bid(s), conditional Bid(s), Bid(s) not conforming to the terms and conditions, Bid without EMD are liable for rejection by PNB.

The Bank reserves the right not to accept any bid, or to accept or reject a particular bid at its sole discretion without assigning any reason whatsoever.

3.2.16. Notification of award

The acceptance of 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 Chief Manager,** Punjab National Bank, IT Audit Cell, Inspection & Audit Division, Head Office, 2nd Floor, Rajendra Bhawan, Rajendra Place, New Delhi – 110008.

3.3. Bid Opening and Evaluation of Bids

3.3.1. Assumptions and Agreements

PNB will generally base its technical evaluation of the proposal on the information compiled by the bidder in accordance with the requested proposal format.

PNB, at its discretion, may make modifications to the selection criteria and the weightage pattern will be disclosed.

PNB reserves the right to accept or reject any proposal without assigning any reason whatsoever.

3.3.2. Opening and evaluation of Technical Bids by the Bank

i) The Bank will open only the Technical bids, in the presence of Bidders' representatives who choose to attend at the date/time and venue specified in section 1.5. The Bidder's representatives who are present shall sign a register evidencing

their attendance. In the event of the specified date of Bid opening being declared a holiday for the Bank, the Bids shall be opened at the appointed time and location on the next working day.

ii) All Bidders, or their authorized representatives, shall be present at the time of the opening of the Technical Bid. Only two persons per Bidder will be allowed to be present at the time of the opening the Technical Bids.

iii) The bidder's names, bid modifications or withdrawals and the presence or absence of requisite bid security and such other details as the Bank at its discretion may consider appropriate will be announced at the time of bid opening.

iv) Bids that are not opened and read out at bid opening shall not be considered for further evaluation, irrespective of the circumstances.

v) The Bank will prepare minutes of the bid opening.

vi) The technical bids would be evaluated by the Technical Committee. Bidders should be ready to give presentation in front of the technical committee in 3-4 days notice, on their capabilities. They are expected to reply to all the queries from the technical committee during the presentation. This presentation would be part of technical evaluation process.

vii) If a bid is not responsive or not fulfilling all the conditions of the Contract or not meeting Technical Specifications and Qualification Requirement, it will be rejected by the bank and may not subsequently be made responsive by the Bidder by correction of the non-conformity.

viii) Proposal will be reviewed to assess compliance with the requirements set out on this RFP. Proposals that do not fully comply with the minimum requirements will be rejected without further consideration.

Commercial bids of those bidders, whose technical bids are found eligible by the bank, shall only be opened.

3.3.3. Opening and evaluation of Commercial Bids

i) After the evaluation of Technical Bid, the Bank shall notify the Bidders whose Technical Bid were considered acceptable to the Bank indicating the date, time and place for opening of the Commercial Bids. The notification may be sent by registered letter, fax, or email.

ii) The Commercial Bid shall be opened in the presence of Bidders who choose to attend.

iii) The Bank will prepare the minutes of the Bid opening.

iv) Price Comparison: Price comparison will take into account all initial payments and all future payments anticipated.

v) Arithmetical errors will be rectified on the following basis. If there is a discrepancy between words and figures, the amount in words shall prevail. If the Successful bidder does not accept the correction of errors, its bid will be rejected and its bid security may be forfeited.

3.3.4. Clarification of Bids

During evaluation of bids, the Bank may, at its discretion, ask the Bidder for a clarification of its bid. The request for clarification and the response shall be in writing.

3.3.5. Technical Evaluation Criteria

i) Preliminary scrutiny of all the bids received will be done and bids not meeting the eligibility criteria would be rejected.

ii) Only those bids fulfilling each of the above mentioned criteria would be considered for final short-listing.

iii) In the process of scrutiny of the proposals, Bank may seek additional inputs and clarifications as may be needed and also may request the service providers to make a presentation.

3.3.6. Contacting the Bank

No Bidder shall contact the Bank or its employees on any matter relating to its bid, from the time of the bid opening to the time the Contract is awarded. If the bidder wishes to bring additional information to the notice of the Bank, it should do so in writing.

Any effort by a Bidder to influence the Bank in its decisions on bid evaluation, bid comparison or contract award may result in rejection of the Bidder's bid.

3.4. Award of Contract

3.4.1. Post qualification

The Bank will determine to its satisfaction whether the Bidder that is successful as having submitted the lowest evaluated responsive bid meets the criteria specified in Section 3.2.6., and is qualified to perform the contract satisfactorily. The determination will take into account the Bidder's financial, technical and performance capabilities. It will be based upon an examination of the documentary evidence of the Bidder's qualifications, expertise, capability submitted by the bidder as well as such other information as the Bank deems necessary and appropriate.

Award of contract will be subject to the bidder qualifying all the evaluation criteria decided by the Bank.

3.4.2. Award Criteria

The financial evaluation committee will select L-1 vendor on the basis of the lowest rates quoted by it in its financial bid, for appointment of IS Auditor for Data Center and allied activities as requested vide this RFP and who satisfies all the conditions of the contract and meets the technical specifications and qualification requirement of the bidding document. The financial evaluation committee of the Bank reserves the right to negotiate the price with the qualified L - 1 vendor or conduct the Reverse Auction in case more than 2 bidders are technically eligible.

3.4.3. Dead Line / Critical Dates

The bidder shall complete all activities before last date.

3.4.4. Right to accept any Bid and to reject any or All Bids

(a) The Bank reserves the right to accept or reject any or all Bids without assigning any reasons. Bids may be accepted or rejected in total or in any part or items thereof. Any Bid not containing sufficient information, in view of the Bank, so as to enable a thorough analysis may be rejected.

(b) The Bank reserves the right to verify the validity of bid information, and to reject any bid where the contents appear to be incorrect, inaccurate or inappropriate in the Bank's estimation.

(c) The Bank shall have the right to determine in its own best judgment, the Bidders who will qualify for the short list, if any, and thereafter, the final successful bidder shall undertake the work.

(d) Bids not conforming to the requirements of the RFP may not be considered by the Bank. However, the Bank reserves the right, at any time, to waive any of the requirements of the RFP, if, in the sole discretion of the Bank, the best interests of the Bank would be served.

(e) If, in the opinion of the Bank, any Bidder has clearly misinterpreted the Work and /or underestimated the hours and / or value of the Work to be performed as reflected in the bid content and quoted price(s)/rate(s), then the Bank may reject the bid as unbalanced (i.e. not representative of the Work Scope).

(f) Further, the bank shall have the right to cancel the RFP process at any time prior to award of the contract, without thereby incurring any liability to the affected Bidder or bidders. Reasons for cancellation, as determined by the Bank in its sole discretion, include, but are not limited to, the following:

(i) Services contemplated are no longer required;

(ii) Requirements and terms of reference (scope of work) of the RFP were not adequately or clearly defined due to unforeseen circumstances and /or factors and /or new developments;

(iii) The RFP did not allow for consideration of all significant elements of the Bank for the work (e.g. new/additional matters have arisen);

(iv) Proposed price is unacceptable for the Work; and

(v) The Project is not in the best interest of the Bank

(vi) Any other reason

3.4.5. Notification of Award of Contract

Prior to the expiration of the period of bid validity, the Bank will notify the successful bidder in writing by registered letter / courier/ email or by fax, to be confirmed in writing by registered letter, that its bid has been accepted.

The notification of award will constitute the formation of the Contract.

Upon the successful Bidder's furnishing of Performance Guarantee as specified in Section 3.4.7 thereof, the Bank will promptly discharge the bid security.

3.4.6. Signing of Contract

At the same time as the Bank notifies the successful bidder that its bid has been accepted; the Bank will send the bidder the Contract Form incorporating all agreements between the parties as enumerated in RFP.

Within 7 days of receipt of the Contract Form, the successful bidder shall sign and date the Contract and return it to the Bank. The Bidder will agree to all the terms and conditions as mentioned in this RFP.

3.4.7. Performance Guarantee

Within 7 days of the receipt of notification of award from the Bank, the successful Bidder shall furnish the Performance Guarantee from a scheduled commercial bank, payable on demand for an amount equivalent to Twenty percent (20%) of the contract price for the due performance and fulfillment of the contract by the Successful bidder, in accordance with the conditions of Contract, in the Performance Guarantee Form provided in the bidding documents or in another form acceptable to the Bank.

The Performance Guarantee may be discharged by the PNB upon being satisfied that there has been due performance of the obligations by the Successful bidder under the contract. The Performance Guarantee shall be valid till the end of the contract Period.

Failure of the successful bidder to comply with the requirement shall constitute sufficient grounds for the annulment of the award and forfeiture of the bid security, in which event the Bank may make the award to the next lowest evaluated bidder or call for new bids.

Chapter – 4: Broad Terms and Conditions

This chapter describes the general terms and conditions of the Contract. However, the terms and conditions are not conclusive and PNB reserves the right to add, delete, modify or alter all or any of these terms and conditions in any manner, as deemed necessary by PNB.

The successful Bidder will have to enter into a purchase agreement directly with PNB as per terms and conditions mentioned in this RFP..

If any irregularity is detected anytime in respect of the above, PNB will have the right to take appropriate action against the Bidder, as deemed fit by PNB.

4.1. Standards

The services rendered under the contract shall conform to the industry standards/ best practices.

4.2. Arbitration

All disputes and differences of any kind, whatsoever, between the parties i.e Successful bidder and PNB, arising out of or in relation to the construction, meaning, operation or effect of the Contract, shall be settled amicably. If, however, the parties are not able to resolve any dispute or differences amicably, the same shall be referred to Sole Arbitration of General Manager, Inspection and Audit Division of Punjab National Bank, HO New Delhi who as a Sole Arbitrator shall settle the dispute in accordance with the Arbitration Act, 1996, and the award made in pursuance thereof shall be binding on the parties.

Any appeal will be subject to the exclusive jurisdiction of the courts in Delhi (India). In such instances, the successful bidder shall continue to work under the Contract during the arbitration proceedings unless otherwise directed in writing by PNB, unless the matter is such that the works cannot possibly be continued until the decision of the arbitrator is obtained.

The venue for arbitration shall be at Delhi, India. The Arbitration proceedings will be held in English language.

4.3. Notices

Notice or other communications given or required to be given under the Contract shall be in writing and shall be hand-delivered with acknowledgement thereof, or transmitted by pre-paid registered post or by recognized courier, or by facsimile, provided that where such notice is sent by facsimile, a confirmation copy shall be sent by pre-paid registered post or by recognized courier within five days of the transmission by facsimile, to the address of the receiving party by the other in writing, provided such change of address has been notified at least ten days prior to the date on which such notice has been given under the terms of the contract.

Any notice or other communications shall be deemed to have validly given on date of delivery if hand-delivered; if sent by registered post or by recognized courier, then on the expiration of seven days from the date of posting; and if transmitted by facsimile, then on the next business date after the date of transmission.

4.4. Use of Contract Documents and Information

The Successful bidder shall not, without PNB's prior written consent, disclose the Contract or any provision thereof, or any specification or information furnished by or on behalf of PNB in connection therewith, to any person other than a person employed by the Successful bidder in the performance of the Contract. Disclosure to any such employed person 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 the purposes of such performance. Any document, other than the Contract itself, shall remain the property of PNB and all copies thereof shall be returned to PNB on termination of the Contract.

4.5. Patent and Copyrights

The Successful bidder shall, at its own cost and expenses, defend and indemnify and keep indemnified PNB against all third-party claims including those of the infringement of Intellectual Property Rights, including patent, trademark, copyright, trade secret or industrial design rights, arising from use of the Products or services or any part thereof in India.

If PNB is required to pay compensation to a third party resulting from such infringement, the Successful bidder shall be fully responsible therefore, including all expenses and court and legal fees. PNB will give notice to the Successful bidder of any such claim and shall provide reasonable assistance to the Successful bidder in disposing of the claim.

The Successful bidder shall also be liable to indemnify PNB, at its own cost and expenses, against all losses/damages, which PNB may suffer on account of violation by the Successful bidder of any or all national/international trade laws, norms, standards, procedures etc.

4.6. Deliverables

Schedule of audit and reports required are covered in scope of audit.

4.7. Prices

The bidder shall indicate Price in Annexure I of the commercial bid, total **bid price for one year**. **These price will be applicable for minimum 2 years.** Bidder will have to perform the audit in 2nd year on the same price and terms and conditions if bank management intend & found services satisfactory.

Price will be quoted including all costs except duties and taxes. However, all applicable Taxes and Duties should be indicated in the Commercial Bid.

No escalation in price quoted is permitted for any reason whatsoever. Prices quoted must be firm till the complete execution of the contract.

If the prices quoted in figures and words have any discrepancy, the rates given in words will be considered.

4.8. Payment Terms

a. Advance Payment on acceptance	20% of annual fee.
b. On submission of first quarter report and presentation made.	20% of annual fee.
c. On submission of second quarter report , third EAPT Report and presentation made.	20% of annual fee.
d. On submission of third quarter report and presentation made.	20% of annual fee.
e. On submission of fourth quarter report, sixth EAPT Report and presentation made.	20% of annual fee.

4.9. Taxes and Duties

Price will be quoted including all costs except duties and taxes. However, all applicable Taxes and Duties should be indicated in the Commercial Bid.

4.10.Delays in the Performance

The Successful bidder must strictly adhere to the audit schedule, as specified in the contract in the performance of the obligations and any delay in this regard will enable PNB to resort to any or both of the following:

(a) Claiming Liquidated Damages

(b) Termination of the agreement fully or partly and claim liquidated damages.

(c) Imposing penalty.

4.11.Penalty

Delayed start of audit, Delayed completion of audit and Delayed submission of report as per agreed terms defined in scope of audit will attract penalty of 0.25 % per day of default/delay of total amount payable for that quarter – (maximum up to 15% of the fees of that quarter). If the report is not submitted within 30 days after completion of audit, the bank may cancel the order.

Time is the essence of the Contract. The Successful bidder will be liable to pay PNB liquidated damages (LD) due to any delay in performance or non-performance of any or all the obligations under the contract, 1% of Contract value per week maximum upto10 % of the Contract value will be charged. This condition will not be applicable for reasons attributable to PNB as well as Force Majeure, though the onus of proving the same lies with the Successful bidder.

PNB will have the rights to recover the liquidated damages, if any, from any amount payable to the Successful bidder.

4.12.Force Majeure

The Successful bidder or PNB shall not be responsible for delays or non-performance of any or all contractual obligations, caused by war, revolution, insurrection, civil commotion, riots, mobilizations, strikes, blockade, acts of God, Plague or other epidemics, fire, flood, obstructions of navigation by ice of Port of dispatch, acts of government or public enemy or any other event beyond the control of either party, which directly, materially and adversely affect the performance of any or all such contractual obligations.

Provided either party shall within ten (10) days from the occurrence of such a cause notify the other in writing of such causes. Unless otherwise directed by the Purchaser in writing, the Successful bidder shall continue to perform his obligations under the contract as far as possible, and shall seek all means for performance of all other obligations, not prevented by the Force Majeure event.

4.13. Correspondences

PNB and the successful Bidder shall nominate a Project Manager each immediately on acceptance of the order, who shall be the single point of contact for the project. However, for escalation purpose, details of other persons shall also be given. The project manager nominated by the Bidder should have prior experience in implementing similar systems in the past and should be a qualified professional.

4.14.Successful bidder's Obligations

The following form illustrative obligations of the Successful bidder. These are not exhaustive.

The Successful bidder will abide by the job safety, customs and immigration measures prevalent and laws in force in India, and will indemnify PNB against all demands or responsibilities arising from accidents or loss of life, the cause of which is the Successful bidder's negligence. The Successful bidder will pay all indemnities arising from such incidents and will not hold PNB responsible or obligated.

The Successful bidder is responsible for, and obligated to conduct all contracted activities with due care and diligence, in accordance with the Contract and using state-of-the-art methods and economic principles, and exercising all reasonable means to achieve the performance specified in the Contract.

The Successful bidder is obliged to work closely with PNB's staff, act within its own authority, and abide by directives issued by PNB that are consistent with the terms of the Contract. The Successful bidder is responsible for managing the activities of its personnel, and will hold itself responsible for any misdemeanors.

The Successful bidder shall be solely responsible for the performance of the contract to the satisfaction of PNB.

4.15.Contract Amendments

Any change made in any clause of the contract which shall modify the purview of the contract within the validity and currency of the contract shall be deemed as an Amendment. Such an amendment can and will be made and be deemed legal only when the parties to the contract provide their written consent about the amendment, subsequent to which the amendment is duly signed by the parties and shall be construed as a part of the contract. The details of the procedure for amendment shall be as specified in the contract.

4.16.Extension of Bank Guarantees

The Bidder shall be responsible for extending the validity date and claim period of all the bank guarantees as and when it is due. PNB shall invoke the guarantee before expiry of validity if work is not completed and the guarantee is not extended, accordingly.

Annexure- A [: A1]

1 SCOPE

Comprehensive Information System and Security Audit will be conducted as under:

a) Office covered:
- Data Center at Delhi
- Disaster Recovery Site at Mumbai
- Treasury Division at Delhi
- Transaction Banking Division at Delhi
- Enterprise Data Ware house at Delhi
- Other HO divisions at Delhi, where critical application/IT infrastructure is installed.
- Premises/activities of service providers (outsourced activities) only to review compliance of services/T&C under service level agreements.

b) Compliance testing, Vulnerability Assessment & Penetration Testing (VAPT), process audit, policy/procedure review, WAN Audit etc, four times in a year at a interval of three months.
c) Conducting External Attack and Penetration Test (EAPT) of equipments/applications exposed to outside world once in two months i.e. six times in a year.
d) Comment upon compliance to ISO 27001 standards (or later standard to which bank is certified) & RBI IT/Security guidelines.
e) Evaluate the adequacy of operating processes, internal control procedures / guidelines documents.
f) Evaluate timely review & completeness of IT Security Policy and Guidelines with industry best practices for various IT Infrastructure.
g) Evaluate role, responsibility and accountability of business process owners.
h) A verification that adequate security & business continuity controls governing the connection to other systems, be they telecommunications, Intranet, Extranet & Internet etc., have been put in place, have been fully documented and correspond to the stated requirements of the Bank.
i) If the formal procedures are not in place for any activity, evaluate the process applied, risk associated and give recommendations for improvement as per best practices.

Below table lists a fairly accurate count of Servers/devices in different locations. It may vary in actual scenario.

Equipment/Platform	Data Center & IT Division	DRS at Mumbai	Treasury Division	EDW	IBD-SWIFT/TBD/GBD/other HO Divisions.
Solaris/ Sun	80	36	1		4
Windows Server	73	9	7	9	14
HP Unix	7				
AIX				13	
Tandem Server / ATM switch	1	1			
Firewall/IPS/IDS	29	4	2	2	
Core Router/Switch	63	24	7	7	15
Linux	3				
AAA Server	1				

Note: Any new addition/ up gradation in hardware, software, business applications, new deliverables, change in architecture during the contract period at Data Center, DRS, EDW, Treasury Division & HO Divisions will also be covered in the audit .

2 Schedule of Audit:

The Information System & Security Audit will be done as under:
Successful bidder will have to visit the respective location and no remote access will be given.

S.NO	Activity	Schedule
1	Conducting Information System & Security Audit of Data Center at Delhi and Disaster Recovery Site at Mumbai, Treasury Division- HO in Delhi, EDW at Delhi.	To start in 2nd week of a Quarter. January , April, July, October
2	WAN Audit	To start in 2nd week of a Quarter. January , April, July, October
3	Conducting external attack and penetration test of equipments exposed to outside world [Both internal &External] once in two months i.e. six times in a year	To start in 1st week of every alternate month.

3 DELIVERABLES:

3.1 Time Lines

a) Will provide schedule of audit, 7 working days prior to start of audit along with full credentials of Audit team (consisting minimum 5 auditors with qualification& experience as defined in RFP) who will be conducting the audit at PNB(onsite).
b) IS auditors should develop a questionnaire [Based on bank IT/Security policies, RBI/IDRBT working group guidelines & given IT/IS audit check list- **Annexure- A-'A2'**] to obtain the requisite information from Department/Section/Division for audit/review.
c) Completion of each audit as mentioned above within 12 working days. (Policy & Procedures compliance and VAPT, EAPT)
d) Minutes of daily meeting will be prepared by next day where observations are based on discussion and will be signed by all participants.
e) Giving draft report for discussions with owners within 3 working days after completion of audit
f) Discussion of the issues with owner after 2 working days at respective location (2 working days)
g) Give final report within 3 working days after discussions with owners
(Total 22 working days) (12+3+2+2+3).
a) If recommendation for risk mitigation/ removal could not be implemented as suggested, alternate solutions will be provided over phone/ email or personal visits to department if required. Response over phone/ email should come within 4 hours of receipt of request and personal visit should be made within 4 days.
h) Resources strength with experience as defined in 2.2(g) will be deployed keeping in view the scope of audit and time schedule.

i) No inexperienced / less qualified resource should be deployed for audit. Resume of auditor will be provided to Bank before hand and will be deputed to assignment only after Bank's consent.
j) Single point of contact person who should not be changed frequently.

3.2 REPORTS:

Report should be provided with snap shot / evidence/ documents details from which observation made wherever required by Bank.

Reporting formats should at the minimum include

a) Compliance status of previous quarter report –Found Complied/ Found partially complied/ Found Non complied/ Exception taken
b) Audit report of current quarter with status Repeat/ Exception or New
c) If repeated – since when
d) If exception – expiry date
e) Vulnerability ID
f) Vulnerability Identified (specific to equipments/ resources - indicating name and IP address of equipment with office and department name and should not be generalized)
g) Broad domain categorization of activity (Port/SQL injection/ Services/Physical access control/ Logical access control/ environment etc.)
h) Risk category – High, Medium, Low
i) Servers/ Resources affected with IP address
j) Office to whom relates
k) Department in office to whom relates
l) Risk / Implication
m) Recommendation for risk mitigation/ removal – step wise. If not resolved, alternate solutions will be provided over phone/ email or personal visits to department if required. Response over phone/ email should come within 4 hours of receipt of request.
n) Provision for updating owner's compliance comments.
o) Reports should be department wise with brief about

- Identification of auditee (Address & contact information)
- Date, location &, time span of audit

p) Explicit reference to key policy and procedure documents of the Bank against identified risk/observation.
q) Additional mandatory or voluntary standards or regulations applicable to the banking industry as best practices should be reported under "Improvement /suggestions"
r) Standards followed
s) Summary of audit findings including identification tests, tools used and results of tests performed (like vulnerability assessment, application security assessment

a. Tools used
b. List of vulnerabilities identified.
c. Description of vulnerability

d. Test cases used for assessing the vulnerabilities

Analysis of vulnerabilities and issues of concern

t) Personnel involved in the audit, including identification of any trainees

The auditor may further provide any other required information as per the approach adopted by them and which they feel is relevant to the audit process.

3.3 MIS

Successful bidder will use some tools preferably Web Based (cost if any included in audit fee), shall be capable of providing audit report which should support dashboard format (Major gaps with subsequent details through links). It should be capable of presenting reports sorted on following major domains and presentable in pie chart/ graphs. Bank will have the right to use that tool.

Should be able to view/ print report sorted on following:

a) Compliance status of previous quarter report –Found Complied/ Found partially complied/ Found Non complied/ Exception taken wise
b) Audit report of current quarter with status Repeat/ Exception or New wise
c) Repeated
d) Exceptions
e) Broad domain activity wise
f) Risk category – High, Medium, Low wise
g) Servers/ Resources affected wise
h) Each server/ resources history (activity wise) should be maintained so that trend analysis can be done.
i) Office to whom relates wise
j) Department in office to whom relates wise.
k) It should show the top 5 vulnerabilities for a given period of 3,6 or 12 months for broad domain, server, resources, office, department wise.

- Report will be given in editable and non editable softcopy so that editable can be used in updating compliances by User Department
- Report will be given in signed hard copy also.
- Presentation on findings of audit will be given to Management by the person who audited accompanied by senior consultant after completion of each quarterly audit within a week time of giving final report.

3.4 RISK MOVEMENT

a) Overall risk of each Office – High, Medium, Low
b) Over all risk for Domain and department wise
c) Risk movement as compared to previous audits – broad category wise and department wise on a scale of 10.
d) Will maintain history of all previous audit risks scores conducted by successful bidder.
e) Based on check list - base line standards advised with each previous audit report– for each domain– (1-i) assign compliance level to each domain and department for each audit in terms of percentage and comparison with previous audits conducted by successful bidder.

Successful bidder and Auditee will decide Major domains, departments, activities before start of 1st audit based on which report will be prepared. The same can be reviewed whenever there is a change.

4 DETAILED SCOPE OF AUDIT

Provide a confirmation that functioning of activities audited are in Compliance with all domains of the:

a) Bank's IT Security & Other IT Policies.
b) External regulations i.e. IT Act 2000, IT (Amendment) Act 2008, RBI Information Security guidelines & recommendations, any other legal requirements.
c) Compliance to ISO 27001 standards (or later version) for the activities complied to it.
d) Adherence to Long and short term IT plan.

Successful bidder is supposed to check at the minimum the following aspects detailed below for respective domains. Evaluate and comment on compliance by Bank as per Security Policy/ Procedures, ISO 27001 standards and Industry best practices.

4.1.1 MANAGING FACILITIES

a) Physical surrounding which protects the IT equipment and people against man-made and natural hazards.
b) Installation of suitable environmental and physical controls which are regularly reviewed for their proper functioning
c) Environmental threat protection
d) Access to facilities.
e) Personnel health and safety.
f) Preventive maintenance policies.
g) Uninterrupted Power Supply – its placement, maintenance, capacity etc.
h) Electrical fittings
i) Data Cabling
j) Fire Protection
k) Insurance
l) Inspection and escalation policies

4.1.2 MANAGING OPERATIONS

a) IT support functions are performed regularly and in an orderly fashion
b) Operational procedure for Data Center and DRS.
c) Processes documentation.
d) User management.
e) Day begin and Day end process.
f) Reviews of console log activity during system shutdown and hardware/software re-initialization.
g) Review of operator log to identify variances between schedules and actual activity.
h) Monitoring of system performance and resource usage to optimize computer resource utilization.
i) Personnel scheduling - Shift hand-over process
j) Coordination with change, availability and business continuity management

k) Preventive maintenance
l) Automated operations documentation.
m) Interface controls over other applications interfaced with Finacle i.e ATM, Online Bills/Tax payments, Internet Banking, RTGS, SFMS, Credit Card etc.
n) Issue and maintenance of Digital signatures.
o) Cryptographic Controls.
p) Use of Internet

4.1.3 HARDWARE

a. Hardware acquisition, installation, usage and disposal procedures.
b. Methodology to forecast the resources required for operating new and significantly changed software.

Servers

c. Procurement as per business requirement.
d. Server sizing – hard disk capacity, RAM, Processing power etc as per requirements.
e. Server capacity is sufficient to take work load as per short and long term plan.
f. Efficient utilization of hardware resources.

4.1.4 NETWORK MANAGEMENT (NOC)

a. Overall Network management.
b. Network design – provides scalability, redundancy.
c. Network cabling is structured.
d. IP Sec implementation
e. Evaluate procedures adopted for:
    i. Secured transmission of data through dialup/leased line/VPN/VSATs, wireless etc.
    ii. Bandwidth management
    iii. Uptime of network – its monitoring as per service level agreement.
    iv. Fault management
    v. Capacity planning
    vi. Performance management etc.
    vii. Monitoring of logs.

4.1.5 NETWORKING & SECURITY EQUIPMENTS:

- Selection of Router, Firewall, Proxy, Intrusion Prevention System, Switch, Modems etc are in consonance with business requirement.
- Evaluate their installation, **deployment/ placement**, configuration, security, policies defined in respective equipment for meeting the security requirement of the LAN & WAN and monitoring of their logs.

- Evaluate centralized controls over Routers installed in Branches and their pass word management.

- Review of access control monitoring and logging mechanism through VLAN's, remote accesses, WAN access, internet access, third party access etc.

- Security and network devices management & hardening processes: review of access controls and privileges to the devices, review of network security processes, redundancy & fall back mechanisms

- Other devices interfaces, including service provider link termination [perform tests to check that valid users cannot exceed their privileges], access rights delegation & management in the device software.

4.1.6 VULNERABILITY/THREAT ASSESSMENT & PENETRATION TESTING (INTERNAL)

Testing should not disrupt our services. Test cases should not be selected that are destructive. The techniques, the tools used should have been thoroughly tested and licensed.

Exercise will be carried out from the place where server are placed. The same will also be carried out from a selected branch outlet for selected sample critical application/ servers.

Appropriate updated tools should be used for each phase of test.

a) Vulnerability assessment of all servers, ATM Switch, network equipments, security equipments installed
b) Placement/ Deployment of security equipments, network equipments for securing database, application, web servers of various applications.
c) Configurations and Monitoring of logs of Intrusion Prevention System, firewalls and response capabilities.
d) In Penetration testing on applications through internal network (Intranet).

4.1.7 EXTERNAL ATTACK AND PENETRATION TEST –

Testing should not disrupt our services. Test cases should not be selected that are destructive. The techniques, the tools used should have been thoroughly tested.

Ethical hacking - Test at the minimum cover –

a) To expose security gaps and demonstrates the effectiveness or ineffectiveness of security measures. This should be done by skilled and experienced professionals only.
b) Test should be designed to simulate a real world attack keeping in view prevailing RBI guidelines, IT Act 2000/(Amendment)2008 and other applicable regulations in India.
c) Information Gathering
d) Port Scanning
e) System Fingerprinting
f) Services Fingerprinting
g) Vulnerability Scanning
h) Firewall & Access Control List Mapping
i) Attempt to guess passwords using password-cracking tools.
j) Buffer Overflow
k) Malicious Input Checks
l) Vulnerabilities for defacement and unauthorized modification of corporate web sites.
m) Search for back door traps in the programs.
n) Attempt to overload the system using DDoS (Distributed Denial of Service) and DoS (Denial of Service) attacks.
o) Check if commonly known holes in the software, especially the browser and the email software exist.
p) should cover following or latest “OWASP Top 10 Web Application Security Risks” -

A1: SQL or Command Injection
A2: Cross-Site Scripting (XSS)
A3: Broken Authentication and Session Management
A4: Insecure Direct Object References
A5: Cross-Site Request Forgery (CSRF)
A6: Security Misconfiguration
A7: Insecure Cryptographic Storage
A8: Failure to Restrict URL Access
A9: Insufficient Transport Layer Protection
A10: Unvalidated Redirects and Forwards

NOTE: Penetration testing should include network and application layer testing as well as controls & processes around the networks & applications, and should conduct from both outside the network trying to come in (external testing) and from inside the network (internal testing) .

4.1.8 ATM Switch Application, interfaces, process review

a) ATM base 24 Switches security review including VAPT.
b) Review of setup, configuration, Security and control at ATM Switches & their interface with Master Card, NFS and VISA switches in terms of bank's security guidelines and other regulatory guidelines.
c) Monitoring procedure of ATM's for 24X7 uptime and incident management.
d) Interface with other Bank's ATM setup.
e) Business Continuity Plan.
f) Maintenance of manual records.
g) Process review audit of ATM center management at Bank's identified location (Presently TBD / ITD – HO at Delhi) for
    1) PIN Management
    2) Card Management
    3) Time Management in delivering ATM Cards/PINs to customers.
    4) Hot listing of cards.
    5) Transactions & Reconciliation Management.

4.1.9 INTERNET & MOBILE BANKING APPLICATION SYSTEM

a) Bank's internet & mobile banking product line, transaction flow.
b) Those adequate internal controls are in place to minimize errors, discourage fraud.
c) Interface with other organizations for utility payments
d) Interface with other applications.
e) Review Process of creation/management of internet & mobile banking IDs / 3D security management / 2nd factor authentication / IBS Shield etc additional security features.
f) PINS/Password management
g) Authentication controls
h) Applications Security & Control Review
i) Compliance of RBI guidelines ON Internet Banking, Mobile Banking.
j) Review to ensure strong access control measures & Confidentiality in the transmission, processing or storing of customer data.

4.1.10 OPEARATING SYSTEM (OS)

i. Set up and maintenance of operative system parameters.
ii. All the Security features available in the OS are enabled/taken advantage of as far as possible.

iii. Vulnerabilities in OS are being taken care off. Compensatory controls for known vulnerabilities are in place.
iv. Security configuration of devices with respect to OEM latest released patches and software versions.
v. Changes in system software are controlled in line with the organisation's change management procedures. Proper record is maintained and authenticated regarding installation, its up-gradation, re-installation and maintenance.
vi. Use of sensitive system software utilities is in controlled manner and it is monitored and logged.
vii. Root and sensitive passwords are used in controlled manner. Their use is logged and monitored.

4.1.11 SOFTWARE

i. Release of software is governed by formal procedures ensuring sign-off, through testing, handover, etc.
ii. Formal procedure for change management is adopted.
iii. All request for change are assessed in a structured way for all possible impacts on the operational system and its functionality are reviewed.
iv. Impact analysis of changes made.
v. Associated documents and procedures are updated accordingly.
vi. Maintenance personnel have specific assignments and that their work is properly monitored. Their system access rights are controlled to avoid risks of unauthorized access to automated systems.
vii. Access log is monitored.
viii. Multilevel or duplicate access ID in the system.
ix. Audit trail / Audit log generation and management.
x. Communicating users with new features during version upgradation.
xi. Regular updation of job cards with new version releases.
xii. If outsourced, escrow arrangement with application owner.

4.1.12 DATA BASE MANAGEMENT SYSTEM AND DATA SECURITY

a) Use of Data Repository System (DRS), Data Definition Language (DDL), Data Manipulation Language (DML).
b) Storage of duplicate copy of Data Definition and DRS at off-site.
c) Monitoring of log of changes to the Data Definitions.
d) Data Dictionary and Data Directory System
e) 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.
f) Logical access controls which ensure the access to data is restricted to unauthorized users
g) Confidentiality and privacy requirements are met.
h) Authorization, authentication and access control are in place
i) Segregation of duties is ensured for accessing data.
j) Purging policy-procedures of Data Files.
k) How the database integrity is ensured in case tables are not properly updated by application software due to various reasons, i.e break in link, bug in software, etc. In case of direct Updation /modification of database is done by opening the tables in live environment, evaluate the controls.
l) Protection of Sensitive Information during Transmission and Transport.
m) Separation of duties.
n) Rotation of duties.

o) Patches and new versions are updated as and when released by vendor/ Research and Development team. If not done then comment upon vulnerabilities and availability of services of existing version being used. Evaluate procedure for correct updation of the same and confirmation by user/ Research and Development team.

4.1.13 ANTI VIRUS

a) Proactive virus prevention and detection procedures are in place and implemented. Virus definitions are updated regularly.
b) Monitoring of antivirus servers located at Circles and other locations for having updated latest versions and definitions.
c) Monitoring procedures effectiveness for branch level client's updations.

4.1.14 OUTSOURCING

a) Service levels are defined and managed.
b) Non Disclosure agreement NDA is in place.
c) Responsibility and liability of vendors have been defined.
d) Service Level Agreements (SLAs) covers key performance indicators which formalise the performance criteria with penalty clause against which the quantity and quality of service is measured
e) Monitoring of vendors activities as per SLAs.
f) Imposing penalties wherever there are deviations.
g) Formal agreements are entered which takes care of all the risks associated with outsourcing.

4.1.15 BUSINESS CONTINUITY

a) Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) and their adequacy / completeness including Cryptographic Disasters.
b) Perform one to one mapping of DR and DC equipments (servers, network, security) with respect to configuration, OS version, patch up-dations.
c) Report deviations(if any) in (b) above and risk associated with it.
d) Specify events which could restrict successful shifting to DRS in case of any disruptions at main site.
e) Restoration of backup at DRS
f) Time delay in transmission and restoration of daily data at DRS.
g) Backup storage – system and data
h) Offsite storage and movement of backups.
i) Data Backup – periodic media verification for its readability.
j) Successful bidder shall depute an audit team at DC and DRS during drill and oversee actual execution. (every quarter)
k) Comment on success of Drill exercises.
l) Evaluate timely review of BCP guidelines.

4.1.15 INVENTORY MAINTENANCE

a) Controls, which identify and record all IT assets and their physical location, and a regular verification programme which confirms their existence.
b) IT assets classification
c) Checking for unauthorised software
d) Software storage controls
e) License management

4.1.16 HELP DESK

a) Help desk facility which provides first-line support and advice
b) Prioritisation of reported problems.
c) Timely resolution of reported problems
d) That problems and incidents are resolved, and the cause investigated to prevent any recurrence
e) Incident handling
f) Trend analysis and reporting
g) Development of knowledge base
h) Root cause analysis
i) Problem tracking and escalation with proper documentation
j) Audit trails of problems and solutions
k) Management/ operations of Enterprise Management System (EMS) –Unicenter from Computer Associates, for monitoring, managing and reporting the faults, configuration, performance and accounting of the Bank's Wide Area Network, Servers installed in Data Centre, Disaster Recovery Site and at other locations across the network.

4.1.17 STORAGE MANAGEMENT

Retention periods and storage terms are defined for:

a) Documents
b) Data
c) Programs
d) Reports
e) Messages (incoming and outgoing)
f) Keys, certificates used for their encryption and authentication.
g) Log files for various activities
h) Policy and Procedures for purging of data.

4.1.18 MEDIA STORAGE:

a) Responsibilities for media (magnetic tape, cartridge, disks and diskettes) library management are assigned to specific members of the IT function.
b) Housekeeping procedures are designed to protect media library contents.
c) Standards are defined for the external identification of magnetic media and the control of their physical movement and storage to support accountability.
d) Procedures to assure that contents of its media library containing data are inventoried systematically, that any discrepancies disclosed by a physical inventory are remedied in a timely fashion and that measures are taken to maintain the integrity of magnetic media stored in the library.

4.1.19 PROTECTION OF DISPOSED SENSITIVE INFORMATION

a) 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 use are defined and implemented.
b) Such procedures guarantee that data marked as deleted or to be disposed cannot be retrieved by any internal or third party.

4.2 WIDE AREA NETWORK AUDIT

The successful bidder shall examine and evaluate the following aspects keeping in view the existing and future requirements and recommend ways to build better network & security:

a) Checking Configuration of Routers
b) Current network & security posture of the WAN architecture
c) IP Addressing schemes and their allocations
d) Physical & Logical Separation of the Networks
e) Network & Security Products & technologies deployed – Their adequacy.
f) IP Sec implementation.
g) Network bottlenecks & performance issues
h) Study of Inter-operability of CO/ZNC/CNC/NC LANs with Corporate WAN
i) Availability of the Network
j) SLAs with third parties & monitoring of key performance indicators by bank
k) Scalability & Robustness of Network
l) Entire administration of the Network Management tools & EMS
m) Availability and quality of system documentation

4.3.1 DURING THE COURSE OF REVIEW, THE SUCCESSFUL BIDDER WILL LOOK FOR;

a) Instructions issued and not complied with
b) Adequacy of Instructions vis-à-vis Policy
c) Role & responsibility of Netowrk Integrator at HO /ZNC/ NC and its compliance level
d) IS Guidelines on Network—implementation & awareness of users.
e) Effectiveness of Monitoring of Logs of Network & Security equipment
f) Capacity utilization of the deployed Network and Security equipments
g) Bandwidth management.

4.3.2 THE SUCCESSFUL BIDDERS WILL SUGGEST:

a) Ways to secure the existing Networks & any new networks being merged / created.
b) Provide re-designed network & security architecture along with technical specifications of network & security solutions (if any suggested during the review of IT infrastructure)based on the operational and business requirements of Punjab National Bank. These technical specifications can be used by PNB for selecting products / solutions.

5. REGISTRATION AUTHORITY

a) Audit of all RA functions
b) Compliance to the requirements of Chief Certifying Authority/ IT act 2000, Rules and Regulations.
c) Compliance of RA functions as per IDRBT checklist.
d) Reconciliation of digital signatures issued/ revoked by RA with IDRBT
e) Digital Certificates details/record maintenance as per IDRBT requirements.

Annexure-A[:A2]

Note: IS auditors should develop a questionnaire [Based on bank IT/Security policies, RBI working group guidelines] and obtain the requisite information or distribute to the IT team in advance of the offsite interviews. A segment wise IT/IS audit check list (but not limited to) is as under-

An Illustrative Information Security Check List

1. > ***Security Policy - Governance, Implementation & Review***

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

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

2. > Asset classification and control - *Accountability of assets*

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

3. > Human resource security

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

4. > Third Party Security/ Vendor Management

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

5. > Physical and Environmental Security

What physical border security facility has been implemented to protect the Information processing facilities	a. Electronic access control (access cards)
	b. Biometric system
	c. Security guards
	d. Perimeter walls
	e. All of the above
What entry controls are in place to allow only authorised personnel into various areas within the organisation	a. Electronic access control (access cards)
	b. Biometric system
	c. Manned reception
	d. All of the above
Whether access to information processing facilities is limited to approved personnel only	Yes/ No
Whether the physical access control procedures differentiate employees, vendors, equipment & facility maintenance staff	Yes/ No
Whether potential threats to information processing facilities like fire, flood, earthquake, theft are taken into consideration in the risk assessment exercise	Yes/ No
Whether separate security controls are in place for third party/ vendor personnel working in secure areas	Yes/ No
Whether goods delivery area and secure area are isolated from each other to avoid any unauthorized access	Yes/ No
Whether appropriate controls are deployed to minimize the risk from heat, smoke, adverse environmental conditions, explosives, dust, chemical effects, electrical supply interfaces, electromagnetic radiation, vibrations, water leakages, rodents etc.	Yes/ No
What is the frequency of conducting fire drill and training	Quaterly/ Half-yearly/ Yearly
Whether evacuation plan with clear responsibilities is in place in case of a disaster	Yes/ No

Whether there is a policy dealing with eating, drinking and smoking in proximity to information processing services	Yes/ No
Whether appropriate signages are displayed with reference to above	Yes/ No
Whether the power and telecommunications cable carrying data or supporting information services are protected from interception or damage	Yes/ No
Whether information processing facility is equipped with all of the following: multiple feed power supply; UPS, generator backups	Yes/ No
Whether the equipment is maintained/ upgraded as per the supplier's recommended service intervals and specifications	Yes/ No
Who carries out the maintenance/ upgradation of critical information processing systems and facilities	a. Third party support personnel
	b. Equipment manufacturer
	c. In-house personnel
Whether logs are maintained with all suspected or actual faults and all preventive and corrective measures	Yes/ No
Who reviews the above logs	a. CISO
	b. Datacentre Head
	c. IT Head
Whether appropriate controls are implemented while sending equipment off premises	Yes/ No
Whether the equipment insurance requirements are satisfied	Yes/ No
Whether secure disposal policy is in place for sensitive information	Yes/ No
How many workstations and servers exist	----------
Whether the organisation maintains a network diagram that includes IP addresses, room numbers/ location and asset owners/ responsible parties	Yes/ No
Whether clear desk and clear screen policies exist	Yes/ No
Whether screen saver time out is implemented	Yes/ No

6. > Information Security Incident Management

Is there a well-documented Incident Management process to handle security incidents	Yes/ No
Whether end users are aware of incident management process	Yes/ No
Whether the process clearly spells out responsibilities, steps for orderly response to a security incident	Yes/ No
Whether the procedure separately addresses different types of incidents like denial of service attacks, breach of confidentiality etc., and ways to handle them	Yes/ No
What kind of monitoring system/ forensic investigation capability is in place so that proactive action is taken to avoid security incidents and malfunctions	a. Audit trail
	b. Log Correlation
	c. Intrusion Prevention/ Detection System
	d. Any other system, please specify
Whether appropriate contacts with law enforcement authorities, regulatory bodies, information service providers and telecommunication operators are maintained to ensure that appropriate action can be quickly taken and specialist advice obtained, in the event of a security incident (Eg. CERT-IN, IDRBT, IBA etc.)	Yes/ No
Whether an escalation reporting procedure exists to report security incidents, security weakness, software malfunctions, threats to systems and processes through appropriate management channels as quickly as possible	Yes/ No
Has the security escalation matrix been defined and documented	Yes/ No
Whether CISO periodically reviews the security incidents	Yes/ No
What is the frequency of such reviews	Monthly/ Quarterly

Whether such incidents are brought to the notice of the Security Steering Committee	Yes/ No
What kind of mechanism is in place to analyse the type of damage and quantify the volume and cost of malfunctions and incidents. Please specify	
Number of security incidents in the last six months	--------
Whether there is a formal disciplinary process in place for employees who have violated organisational security policies and procedures	Yes/ No
Do you have contacts with the cybercrime cell/ investigation agencies	Yes/ No

7. > Communications and Operations Management

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

Have you subscribed to warning bulletins/ alerts with regards to malicious software usage	Yes/ No
Whether Anti-virus software is installed on end user desktops, internet gateway and mail gateway	Yes/ No
Total number of desktops in the organisation	----------
Total number of dekstops updated with today's Anti-virus Definition	----------
How many regional servers are there for Anti-virus updates in the organisation	----------
Whether a dedicated Virus Helpdesk is established	Yes/ No
Is there a defined procedure to connect vendor/consultant/support personnel laptops to the organization network	Yes/ No
Who reviews daily Anti-virus coverage reports	----------
Whether comprehensive Back-up schedule of essential business applications is in place	Yes/ No
Whether comprehensive Back-up schedule is also implemented at DR Site	Yes/ No
Whether the backup media along with the procedure to restore the backup are stored securely	Yes/ No
Whether the backup media are stored at off-site location	Yes/ No
Whether dedicated media liabrary is created for backup media	Yes/ No
Whether the backup copies of critical applications/databases are available on SAN Storage	Yes/ No
Whether the backup media are regularly tested for restoration within the time frame allotted in the operational procedure for recovery	Yes/ No
When was the restoration last tested	mm/dd/yy
Whether daily operations log sheet is maintained for Database housekeeping tasks	Yes/ No
Who reviews the operations log sheets for Database housekeeping tasks	----------
Whether operations logs sheets are randomly compared with system generated operator logs	Yes/ No
Whether a defined fault logging mechanism is in place for Database related issues	Yes/ No

Which technique is used to grant network access to the user	a. AD Authentication
	b. Single Sign-on
	c. Identity Management
	d. Workgroup Environment
Which Network Monitoring tool is used by the organisation	----------
Whether Network/System Administration task is isolated (Network Isolation) from End User Network Segments	Yes/ No
Whether central authentication tools like TACACS/RADIUS are used for Network Device Authentication	Yes/ No
Whether all routers (Branch/WAN) have ACLs	Yes/ No
Who reviews the ACLs periodically	----------
Whether clear guidelines exist for remote management of critical equipment (Servers/Routers etc.)	Yes/ No
Whether VPN is used for remote management/administration of critical equipment	Yes/ No
Which type of VPN is being used	----------
Whether VPN Access Authorization process is established	Yes/ No
Whether Media handling guidelines are established	Yes/ No
Whether secure disposal process for media is in place	Yes/ No
Whether the media is transported in a secured manner	Yes/ No
Whether disposal of sensitive items are logged where necessary in order to maintain an audit trail	Yes/ No
Whether System Documentation is stored in a secure manner and protected from unauthorised access	Yes/ No
Whether a list of individuals having access to System Documentation is maintained	Yes/ No
Whether all exchanges of information, for business purposes, are governed by formal agreements	Yes/ No
Whether such agreements adequately address Security issues	Yes/ No

Whether e-commerce transactions are SSL enabled	Yes/ No
Whether multi-factor authentication mechanism is in place for e-commerce environment	Yes/ No
Which of the following additional factors is used for authentication	a. Hardware Token
	b. OTP
	c. MobiToken
	d. IVR Callback
Whether controls are in place to guard e-commerce systems against phishing attacks	Yes/ No
Whether e-commerce systems are under periodic VA/PT cycles	Yes/ No
Whether standard defensive techniques like IPS, Malware Scanning etc. are deployed for e-commerce systems	Yes/ No
Whether the use of the organisation's electronic mail system is governed by acceptable use policy or guidelines	Yes/ No
Whether all e-mails are archived centrally	Yes/ No
Whether gateway level anti-virus, anti-spam protection is enforced for E-mail system	Yes/ No
Whether data leakage prevention system is implemented to maintain confidentiality of the information	Yes/ No
Whether the e-mail traffic is encrypted	Yes/ No
Whether use of all electronic office systems is governed by acceptable use policy	Yes/ No
Whether there is any formal authorisation process in place for the information to be made publicly available	Yes/ No
Whether there are any policies, procedures or controls in place to protect the exchange of information through the use of voice, facsimile and video communication facilities	Yes/ No
Whether continuous education/ awareness is imparted to employees w.r.t Information Security best practices while exchanging the information over phone/fax/video etc.	Yes/ No

8. > Access Control

Whether business requirements are documented for access control	Yes/ No
Whether there is any formal user registration and de-registration procedure for granting access to multi-user information systems and services	Yes/ No
Whether privileges are allocated on need-to-use basis and after formal authorisation process	Yes/ No
Whether there exists a process to review user access rights at regular intervals. Eg. Special privilege review every 3 months, normal privileges every 6 months	Yes/ No
Frequency of user access review	Quarterly/ Half-yearly/ Yearly
Whether clear password policy is in place and communicated to all users	Yes/ No
Whether the users and contractors are made aware of the security requirements and procedures for protecting unattended equipment	Yes/ No
Whether networks and network services access policy is in place for the organization	Yes/ No
Which of these authentication mechanisms is used for challenging external connections	a. Cryptography based technique
	b. Hardware Tokens
	c. Software Tokens
	d. Challenge Response protocol
	e. Any other
Whether all external connections have proper Management and Security approvals	Yes/ No
Whether accesses to diagnostic ports are securely controlled and have Security approvals	Yes/ No
Whether Perimeter and Internal Firewalls are distinctly installed in the organization	Yes/ No
Whether ftp is allowed across the organization	Yes/ No
Whether NIDS/NIPS controls are deployed in the organization	Yes/ No

Whether access to information systems is attainable only via a secure log-on process	Yes/ No
Whether unique identifier is provided to every user such as operators, system administrators and all other staff including technical	Yes/ No
Whether there exists a password management system that enforces various password controls such as: individual password for accountability, enforce password changes, store passwords in encrypted form, not display passwords on screen etc.	Yes/ No
Whether Inactive terminal in public areas are configured to clear the screen or shut down automatically after a defined period of inactivity	Yes/ No
Whether sensitive systems are provided with isolated computing environment such as running on a dedicated computer, share resources only with trusted application systems, etc.	Yes/ No
Whether there exist any restrictions on connection time for high-risk applications	Yes/ No
Whether procedures are set up for monitoring the use of information processing facility	Yes/ No
Whether the results of the monitoring activities are reviewed regularly	Yes/ No
Whether audit logs recording exceptions and other security relevant events are enabled	Yes/ No
What is the retention period for audit logs	----------
Whether NTP is implemented and clock for all servers/ devices is in sync with NTP	Yes/ No
Whether a formal policy is in place to address the risks of working with computing facilities such as notebooks, palmtops etc. especially in unprotected environments	Yes/ No
Whether there is any policy, procedure and/ or standard to control teleworking activities	Yes/ No
Whether suitable protection of teleworking site is in place against threats such as theft of equipment, unauthorised disclosure of information etc.	Yes/ No

9. > Systems acquisition, development and maintenance

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

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

10. > Compliance

Whether relevant regulatory and contractual requirements are documented for each information system	Yes/ No
Whether responsibilities of individuals concerned to meet these requirements are well defined and communicated	Yes/ No
Whether there exist procedures to ensure compliance with legal restrictions on use of material like intellectual property rights, trademarks, copy rights etc.	Yes/ No
Whether important records of the organisation is protected from loss destruction	Yes/ No
Whether there is a management structure and control in place to protect data and privacy of personal information	Yes/ No
Whether at the log-on security banner or a warning message is presented on the computer screen indicating that the	Yes/ No
system being entered is private and that unauthorised access is not permitted	
Whether the process involved in collecting the evidence is in accordance with legal best practices	Yes/ No
Whether all areas within the organisation are considered for regular review to ensure compliance with security policy, standards and procedures	Yes/ No
Whether information systems are regularly checked for compliance with security implementation standards	Yes/ No
Whether the technical compliance check is carried out by, or under the supervision of, competent, authorised persons	Yes/ No
Whether all computers, systems and network devices like routers and switches within your organization regularly tested for exploitable vulnerabilities and illegally copied software	Yes/ No
Whether audit requirements and activities involving checks on operational systems are planned and agreed upon to minimise the risk of disruptions to business process	Yes/ No
Whether access to system audit tools such as software or data files are protected to prevent misuse	Yes/ No
Whether there is a designated compliance officer for the organisation	Yes/ No

Annexure – B
Performance Guarantee Form

Date :

To,
The Chief Manager ,
Punjab National Bank,
IT Audit Cell, Inspection & Audit Division,
Head Office, 2nd Floor,
Rajendra Bhawan, Rajendra Place,
New Delhi – 110008

Dear Sir,

PERFORMANCE BANK GUARANTEE – Information Systems audit of the Punjab National Bank as per scope in RFP.

WHEREAS

M/s.(name of Auditor), a company/Firm registered under the Companies Act, 1956,(as applicable) having its registered and corporate office at (address of the Auditor), (hereinafter referred to as "our constituent", which expression, unless excluded or repugnant to the context or meaning thereof, includes its successors and assigns), entered into a Agreement dated…….(hereinafter , referred to as "the said Agreement") with you (Punjab National Bank) for conduct of information system audit as detailed in the said Agreement.

We are aware of the fact that in terms of sub-para (…), Section (…), Chapter (…) of the said Agreement, our constituent is required to furnish a Bank Guarantee for an amount Rs…….(in words and figures), being 20% of the Contract Price of Rs……. (in words and figures), as per the saidnh Agreement, as security against breach/default of the said Agreement by our Constituent.

In consideration of the fact that our constituent is our valued customer and the fact that he has entered into the said Agreement with you, we, (name and address of the bank), have agreed to issue this Performance Bank Guarantee.

Therefore, we (name and address of the bank) hereby unconditionally and irrevocably

Guarantee you as under :

I. In the event of our constituent committing any breach/default of the said Agreement, which breach/default has not been rectified within a period of thirty (30) days after receipt of written notice from you, we hereby agree to pay you forthwith on demand such sum/s not exceeding the sum of Rs…….. (in words and figures) without any demur.

II. Notwithstanding anything to the contrary, as contained in the said Agreement, We agree that your decision as to whether our constituent has made any such default/s/ breach/es, as afore-said and the amount or amounts to which you are entitled by reasons thereof, subject to the terms and conditions of the said Agreement, will be binding on us and we shall not be entitled to ask you to establish your claim or claims under this Performance Bank Guarantee, but will pay the same forthwith on your demand without any protest or demur.

III. This Performance Bank Guarantee shall continue and hold good till the completion of the audit (2 years from the date of agreement i.e (date), subject to the terms and conditions in the said Agreement.

IV. We bind ourselves to pay the above said amount at any point of time commencing from the date of the said Purchase Agreement until the completion of the contract.

V. We further agree that the termination of the said Agreement, for reasons solely attributable to our constituent, virtually empowers you to demand for the payment of the above said amount under this guarantee and we have an obligation to honour the same without demur.

VI. In order to give full effect to the guarantee contained herein, we (name and address of the bank), agree that you shall be entitled to act as if we were your principal debtors in respect of your claims against our constituent. We hereby expressly waive all our rights of surety ship and other rights, if any , which are in any way inconsistent with any of the provisions of this Performance Bank Guarantee.

VII. We confirm that this Performance Bank Guarantee will cover your claim/s against our constituent made in accordance with this Guarantee from time to time, arising out of or in relation to the said Agreement and in respect of which your claim is lodged with us on or before the data of expiry of this Performance Guarantee, irrespective of your entitlement to other claims, rights and relief, as provided in the said Agreement.

VIII. Any notice by way of demand or otherwise hereunder may be sent by special courier, telex, fax, registered post or other electronic media to our address, as aforesaid and if sent by post, it shall be deemed to have been given to us after the expiry of 48 hours when the same has been posted.

IX. If it is necessary to extend this guarantee on account of any reason whatsoever, we undertake to extend the period of this guarantee on the request of our constituent under intimation to you (Punjab National Bank).

X. This Performance Bank Guarantee shall not be affected by any change in the constitution of our constituent nor shall it be affected by any change in our constitution or by any amalgamation or absorption thereof or therewith or reconstruction or winding up, but will ensure the benefit to you and be available to and be enforceable by you.

XI. Notwithstanding anything contained hereinabove, our liability under this Performance Guarantee is restricted to Rs……..(in words and figures) and shall continue to exist, subject to the terms and conditions contained herein, unless a written claim is lodged on us on or before the afore-said date of expiry of this guarantee.

XII. We hereby confirm that we have the power/s to issue this Guarantee in your favour and the undersigned is/are the recipient of authority by express delegation of power/s and has/have full power/s to execute this guarantee under the Power of Attorney issued by the bank in his/their favour.

XIII. We further agree that the exercise of any of your rights against our constituent to enforce or forbear to enforce or any other indulgence of facility, extended to our constituent to carry out the contractual obligations as per the said Agreement, would not release our liability under this guarantee and that your right against us shall remain in full force and

effect, notwithstanding any arrangement that may be entered into between you and our constituent, during the entire currency of this guarantee.

Notwithstanding anything contained herein :

a. Our liability under this Performance Bank Guarantee shall not exceed Rs……. (in words and figure) ;
b. This Performance Bank Guarantee shall be valid only up to ……..(and
c. We are liable to pay the guaranteed amount or part thereof under this Performance Bank Guarantee only and only if we receive a written claim or demand on or before ……..(.

This Performance Bank Guarantee must be returned to the bank upon expiry of the claim period as under © above. If the Performance Bank Guarantee is not received by the bank within the above-mentioned period, subject to the terms and conditions contained herein, it shall be deemed to be automatically cancelled.

Dated…….this……day……20…..

Yours faithfully,

For and on behalf of the ……..Bank,

(Signature)
Designation
(Address of the Bank)

Note:

a) This guarantee will attract stamp duty as a security bond.
b) A duly certified copy of the requisite authority conferred on the official/s to execute the guarantee on behalf of the bank should be annexed to this guarantee for verification and retention thereof as documentary evidence in the matter.

Annexure – C

BID SECURITY / EMD FORM FORMAT

Whereas …… *(Name of Bidder)* (Hereinafter called "the Bidder") has submitted its bid dated ……..*(Date of submission of bid)* for the supply of …….. *(name and description of the system/services)* (Hereinafter called "the Bid") KNOW ALL PEOPLE by these presents that WE ……*(name of bank)* carrying a banking business amongst other places at …….. of ……. *(name of country)*, and having our registered offices at ……*(address of bank)* (hereinafter called "the Bank"), are bound unto Punjab National Bank *(name of Purchaser)* (hereinafter called "the PNB "), in the sum of …… for which payment well and truly to be made to the said PNB , the Bank binds itself, its successors, and assigns by these presents. Sealed with the common seal of the said Bank this ……..…. Day of …….. 20…….

THE CONDITIONS of this obligation are:

1. If the Bidder withdraws the bid during the period of bid validity specified by the Bidder on the Bid Form; or Does not accept the correction of errors in accordance with the INSTRUCTIONS TO BIDDER (Chapter 3); or

2. If the Bidder, having been notified of the acceptance of its bid by the PNB during the period of bid validity :

- Fails or refuses to execute the Contract Form if required; or
- Fails or refuses to furnish the Performance Guarantee in accordance with the INSTRUCTIONS TO BIDDER;

We undertake to pay the PNB up to the above amount upon receipt of its first written demand, without the PNB having to substantiate its demand, provided that in the demand the PNB will note that the amount claimed by it is due to it, owing to the occurrence or one or both of the two conditions, specifying the occurred condition or conditions and not withstanding any objections raised by the bidder. The Bank agrees that the liability to pay the amount will be irrecoverable and absolute and bank will not be entitled to inquire whether claim is due or not.

This undertaking to pay will remain in force up to and including forty five (45) days after the period of the bid validity, and any demand in respect thereof should reach the Bank not later than the above date.

……
(Signature of the Bank)

Annexure – D

Technical BID FORM

Date :

To,
The Chief Manager ,
Punjab National Bank,
IT Audit Cell, Inspection & Audit Division,
Head Office, 2nd Floor,
Rajendra Bhawan, Rajendra Place,
New Delhi – 110008

Dear Sir,

Reg: Information Systems audit of the Punjab National Bank as per scope in RFP.
Dear Sir,

Having examined the RFP Documents, the receipt of which is hereby duly acknowledged, we, the undersigned, offer to conduct Information System audit in conformity with the said RFP Documents and hereby undertake that we accept all the conditions of the contract as per the Bidding Document and will audit the complete systems (Hardware, Software etc) as per the Technical Specifications of the bidding documents. We further undertake that we fulfill the Minimum eligibility criteria stated in Chapter 2 clause 2.2 and for this purpose we enclose the details. In addition to this, the particulars of our organization such as legal status, principal place of business, details of experience and past performance, service support details, capability statement and the required bid security in shape of bank draft are furnished with this bid form.

We further undertake, if our bid is accepted, to execute the audit assignment in accordance with the requirements and the delivery schedule as mentioned in the Schedule of Requirements.

If our bid is accepted, we will obtain the guarantee of a bank in the form prescribed by you for a sum equivalent to 20% of the Contract Price for the due performance of the Contract.

We agree to abide by this bid for the Bid validity period specified in section 3.2.9. of the ITB and it shall remain binding upon us and may be accepted at any time before the expiration of that period. Until a formal contract is prepared and executed, this bid, together with your written acceptance thereof and your notification of award, shall constitute a binding Contract between us.

We undertake that, in competing for (and, if the award is made to us, in executing) the above contract, we will strictly observe the laws against fraud and corruption in force in India namely "Prevention of Corruption Act. We understand that you are not bound to accept the lowest or any bid you may receive.

Dated this …….. day of …… 20…..
*(Signature and the capacity of the person d*uly authorized to sign Bid for and on behalf of)

Annexure – E

Commercial BID FORM

Date :

To,
The Chief Manager ,
Punjab National Bank,
IT Audit Cell, Inspection & Audit Division,
Head Office, 2nd Floor,
Rajendra Bhawan, Rajendra Place,
New Delhi – 110008

Dear Sir,

Reg: Information Systems audit of the Punjab National Bank as per scope in RFP.

Having examined the Bidding Documents, the receipt of which is hereby duly acknowledged, we, the undersigned, offer to supply and deliver …… *(Description of System and Services)* in conformity with the said Bidding Documents for the sum of ……..*(Total bid amount in words and figures)* or such other sums as may be ascertained in accordance with the Schedule of Prices attached herewith and made part of this bid, and hereby undertake that we accept all the conditions of the contract of the Bidding Document and will execute the audit work as stipulated in RFP. We further undertake that we fulfill the Eligibility requirement and for this purpose we enclose the details. In addition to this, the particulars of our organization such as legal status, principal place of business, details of experience and past performance, service support details, capability statement and the required bid security in the shape of Bank guarantee/Bank draft are furnished with this bid form.

We further undertake, if our bid is accepted, to deliver the goods in accordance with the delivery schedule finalized. .

If our bid is accepted, we will obtain the guarantee of a bank in the form prescribed by the Purchaser for a sum equivalent to 20% of the Contract Price for the due performance of the Contract.

We agree to abide by this bid for the Bid validity period specified in section 3.2.9 of the ITB and it shall remain binding upon us and may be accepted at any time before the expiration of that period.

Until a formal contract is prepared and executed, this bid, together with your written acceptance thereof and your notification of award, shall constitute a binding Contract between us.

We undertake that, in competing for (and, if the award is made to us, in executing) the above contract, we will strictly observe the laws against fraud and corruption in force in India namely "Prevention of Corruption Act 1998".

We understand that you are not bound to accept the lowest or any bid you may receive.

Dated this …….. day of …… 20…..

_____ _____

(Signature) (in the capacity of Duly authorized to sign Bid for and on behalf of)

Annexure –F

Undertaking- 1

To,

Date

The Chief Manager ,
Punjab National Bank,
IT Audit Cell, Inspection & Audit Division,
Head Office, 2nd Floor,
Rajendra Bhawan, Rajendra Place,
New Delhi – 110008

Dear Sir,

Reg: Information Systems audit of the Punjab National Bank as per scope in RFP.

We understand that

a) You are not bound to accept the lowest or any bid received by you, and you may reject all or any bid.
b) We understand that Bank has option to go for Reverse Auction for finalization of lowest bidder
c) If our Bid for the above job is accepted, we undertake to enter into and execute at our cost, when called upon by the purchaser to do so, a contract in the prescribed form. Unless and until a formal contract is prepared and executed, this bid together with your written acceptance thereof, shall constitute a binding contract between us.
d) If our bid is accepted, we are responsible for the due performance of the contract.
e) You may accept or entrust the entire work to one vendor or divide the work to more than one vendors without assigning any reason or giving any explanation whatsoever.
f) Vendor means the bidder who is decided and declared so after examination of commercial bids/after reverse auction.
g) The names of shortlisted bidders after the completion of first stage (Technical Bid), and the same of successful bidder to whom the contract is finally awarded after the completion of second stage (Commercial Bid), shall be displayed on the Notice Board of the purchaser at Punjab National Bank, IT Audit Cell, Inspection & Audit Division, Head Office, 2nd Floor, Rajendra Bhawan, Rajendra Place, New Delhi – 110008

Dated at_____this _____day of _____20….

*(Signature and the capacity of the person d*uly authorized to sign Bid for and on behalf of)

Annexure –G UNDERTAKING 2

To,
The Chief Manager ,
Punjab National Bank,
IT Audit Cell, Inspection & Audit Division,
Head Office, 2nd Floor,
Rajendra Bhawan, Rajendra Place,
New Delhi – 110008

Date

Dear Sir,

Reg: Information Systems audit of the Punjab National Bank as per scope in RFP.

a) We hereby confirm that all the requirements as enumerated in RFP as per requirement of the Bank have been included in the commercial bid. Further, we hereby undertake and agree to abide by all the terms and conditions stipulated by the Bank in this RFP. We understand that any deviation may result in disqualification of bids.

b) We undertake that adequate number of qualified auditors (minimum 5) will be deployed for audit process to complete the audit within stipulated time as per clause 3.1 of annexure A-A1.

c) We undertake that reporting formats should at the minimum include all the requirements as per clause 3.2 of annexure A-A1.

d) We have the tool (clearly mentioned Web Based / Stand-alone), which is capable of providing audit report that support dashboard format (subsequent details through links). It is capable of presenting reports sorted on major domains and presentable in pie chart/ graphs. Bank will have the right to use that tool. We shall demonstrate the capability of the tool which shall be used for reporting purpose.

e) We undertake that we will have legal right to use any third party software if required for audit and under such licenses, in terms set out under any relevant license or sub-license agreement. We will indemnify the Bank for any and all costs that may arise out of the use of software, in which it is alleged that any rights of the owners of such software have been infringed.

f) We shall provide Risk Movement for various activities as desired.

g) We have not been blacklisted by any nationalised Bank/ RBI/IBA or any other Government agency. No legal action is pending against us for any cause in any legal jurisdiction.

(Deviation to the above if any, the Bidder must provide details of such action (s).)

1)
2)
3)
4)

*(Signature and the capacity of the person d*uly authorized to sign Bid for and on behalf of)

Annexure – H

GUIDELINES FOR REVERSE AUCTION:

Initiation on the Bid Process
Opening bid price and bid decrements will be intimated at the start of the bidding process by the means of on-line messages. In case of not receiving the details, the supplier has to inform PNB system administrator one hour before the scheduled event time through email and request for the details.

Opening Price
Opening price is the upper/ceiling price of the contract value fixed by PNB for the lot/item. Suppliers can bid only lower than the opening price in case of Reverse Auctions (Bid price would be based on the total price arrived at multiplying specified quantities with unit rates and summing up for the entire requirement).

Weightage / Loading Factor
This factor shall be incorporated by the System Automatically during the event. This factor is the effect of financial implication arising out of the deviation taken by the Bidder in his Bid.

Auction Types
Bank may either go for *Price Base Auction* when the price quoted by each bidder is shown to all the participants or *Rank Base Auction* when only rank of the particular bidder is visible instead of price.

Alias Name
Each bidder will be given a unique alias name, generated by the system and informed by system generated email. Bidders can see the bids of other suppliers but the real name will not be visible on the screen. Complete, schedule of the auction will be intimated through a system generated emails to the participating suppliers. Flash messages between the event and at the end of the events. The normal duration of Reverse auction will be 1 hour (60 minutes) with provision of auto extension as per auction rules to be decided by Negotiation Committee before start of auction. The Bid Extension rules shall be governed after the expiry of the Auction Time earlier set & decided before start of Event. In the event a bidder is placing his bid in last 5 minutes of the scheduled end time of the event, the event will get automatically extended for next 5 minutes infinitely. The auction time will get automatically extended so as to allow other the bidder an opportunity to supplier to participate and give better offer to win the bid. In the event of any typographic error while posting the bid, the auction would still get extended so as to allow the bidder an opportunity to correct the mistake. Screen will refresh automatically in every seven (7) second. It is recommended to manually refresh screen by pressing F-5 from keyboard, if no changes are seen on screen for unusual period.

Bid Decrement
Bid Decrement is the minimum fixed amount by which, or by multiples of which, the next bid value can be decreased. Bid decrement is usually calculated 0.25% of the opening price. However PNB reserves the right to decide appropriate bid decrement factor. Bidders should enter the next bid price considering the Bid Decrement, with reference to self bid for Rank Auction and L1 bid with reference to Price Auction. However in no case would the system accept modification to a higher value.

Auto Bid
Auto Bid is disabled from the start time of bidding.

Surrogate Bidding
Surrogate bidding is not allowed.

Price Break Up
Bidders are required to submit the price break up of the final bid price just after the event on to the formats/ price breakup sheet.

Price Variation Factor
If a bidder quoting higher prices, higher by more than **40%** as compared to the average quoted prices (of all technically qualified bidders) for all items in aggregate, the same bidder shall not be called for reverse auction process.

Mistake Proofing
If a bid placed X times below or higher of the bid decrement / increment as decided by PNB, a warning message will be flashed on screen to confirm the placed bid, Bid once placed will not be deleted in any circumstances and the supplier will be bound to deliver the item on the quoted bid.
The following term and conditions are deemed as accepted by vendor on participation in the bid event
Bidders/ participants are deemed to have accepted the auction rules on participation at the bid event. Participation in a bid event is by invitation from PNB. Any other supplier does not automatically qualify for participation. PNB will make every effort to make the bid process transparent. However, the award decision by PNB would be final and binding on supplier.

1. Bidders agrees to non-disclosure of trade information regarding the purchase, identity of PNB, bid process, bid technology, bid documentation and bid details.
2. Bidder cannot change price or quantity or delivery terms (or any other terms that impact the price) post the bid event.
3. Deed to furnish the item rate form within the stipulated time after the bid event.
4. Bidder cannot divulge either his bids or those of other suppliers to any other external party.
5. Technical and other non-commercial queries (not impacting price) can be routed to the respective PNB contact personnel indicated in the RFP.
6. Bidder is advised that he will understand auto bid process is to safeguard them in case of technical failure. Inability to bid due to telephone line glitch, Internet response issues, software or hardware hangs will not be the responsibility of PNB.
7. Bidder should be prepared with competitive price quotes on the day of the bidding event. Participate in the online bidding event as per the schedule. Submit the item wise price break up for all the items as per his last bid price in the stipulated time as per the schedule immediately after the online sourcing event. The bidder has to necessarily quote for all the items listed in the BOQ. In case of incompleteness of the bid, same may be rejected.

8. NOTE –
   1) If two or more bidders are technically eligible, we may also initiate the process of reverse auction
   2) Bank reserves the right to hold Reverse Auction /or call L-1 bidder for negotiation.

Annexure - I

Commercial Bid

To,
The Chief Manager ,
Punjab National Bank,
IT Audit Cell, Inspection & Audit Division,
Head Office, 2nd Floor,
Rajendra Bhawan, Rajendra Place,
New Delhi – 110008

Date

Reg: Information Systems audit of the Punjab National Bank as per scope in RFP.

Dear Sir,

We undertake to conduct Information System and security audit of PNB as per detailed scope of audit in Annexure A of RFP at a cost of:

Audit Fee including all costs Rs (for one year payable as per clause 4.8 of RFP)	. ……
Taxes (PI specify rate and type of tax)	……..
Total	……..

(In words)……..

These price will be applicable for minimum 2 years. Bank may at its discretion, extend the services for 2nd year also. We undertake to perform the audit in 2nd year also on the same price and terms and conditions.

We confirm that cost of all the factors required for IS Audit as per RFP have been included in the commercial bid. Further, we understand that Bank reserve the right to use reverse auction method.

*(Signature and the capacity of the person d*uly authorized to sign Bid for and on behalf of)

Annexure - J

Technical Compliance Sheet

S.No	Criteria	Details
a	Bidder must prove that it is a current legal entity in India and must warrant that it is financially solvent.	Successful bidder's Firm/Company Name: Registered Head office: Offices at other locations: 1 2 Brief Profile: Year of commencement of Business Website: Authorized person: Designation: Phone No Email Address
b	Should not be a vendor for Software and Hardware components of the Bank at Data Center, EDW, Treasury & DRS level.	Provides following hardware and software to the Bank:
C	Should not be involved in implementing Security and network infrastructure of the Bank at Data Center, EDW, Treasury & and DRS level.	Provides following services and support to the Bank:
d	Should be a Company /Firm /Organization /independent subsidiary with an average annual turnover of Rs.5 (five) crore or more during the last three financial years and should be in net profit during all three financial years.	Turn over and profit during last 3 years: (In Indian Rupee) 2010-11 2009-10 2008-09 Turnover Net Profit Attach copy of audited balance sheets of above periods.
e	Should have conducted minimum 2 Information System Security audits of data center connected with a minimum 200 offices, in last three years, out of which one audit should be in a bank in India.	Conducted following IS Audits in last three years: Organisations Fill details in Annexure K
f	Should have implemented BS 7799/ ISO 27001 security framework in any organization.	Implemented BS7799/ ISO 27001 security framework in last three years:

<table>
<tr><td></td><td>After implementation, that organization should have been certified.</td><td>Organization

Fill details in Annexure L</td></tr>
<tr><td>g</td><td>Should have capable to depute at a time minimum 10 qualified professionals with degree from Govt. recognized reputable Universities / Institutions as BE (CSE / IT) / B.Tech (CSE / IT) / ME (CSE / IT) / M.Tech(CSE / IT) / MCA / C.A.(ICAI) and certifications as CISA / DISA / CISM / CISSP / CEH / Sun Certified Security Administrator (SCSECA) / OCE (Oracle Certified Expert - Security Administrator), Cisco CCIE-Security along with 3 or more years of IS Audit experience including at least one IS Audit for any organization defined at 2.2(e) of this document(RFP) and should be on permanent roll of the organization. List all those who will be involved in the assignment.</td><td>No of such Professionals on the permanent roll of the bidding company with certifications
<table><tr><td>1. CISA/CISM</td><td></td></tr><tr><td>2. CISSP</td><td></td></tr><tr><td>3. DISA</td><td></td></tr><tr><td>4. CEH</td><td></td></tr><tr><td>5. SCSECA/OCE</td><td></td></tr><tr><td>6. CCIE-Security</td><td></td></tr><tr><td>7. Others(Specify)</td><td></td></tr></table>
Fill details in Annexure M</td></tr>
<tr><td>h</td><td>Should not have been blacklisted by any nationalized Bank/ RBI/IBA or any other Government agency.</td><td>Signed Undertaking in annexure G</td></tr>
<tr><td>I</td><td>Should be able to provide deliverables as per clause 3 of Annexure A-A1 of RFP.</td><td>a) Time Lines – should be able to deploy adequate number of auditors to complete the audit process within stipulated time. Give details in Annexure N
b) Submit estimated work plan and time schedules for the different items requiring to be audited as specified under the scope of work (Annexure-A(A1,A2)). Please submit the Project plan documents covering the items mentioned under the scope of work (major component wise break-up along with the time chart).
c) Reporting formats - should provide reports as per clause 3.2 of scope of audit.
d) Name of Tool used:

Successful bidder shall also be capable of providing audit report through some tool</td></tr>
</table>

		preferably Web based which should support dashboard format (subsequent details through links). It should be capable of presenting reports sorted on major domains and presentable in pie chart/ graphs. Bank will have the right to use that tool. Tool capabilities will be evaluated on the basis of presentation made by bidder. e) Provide Risk Movement for various activities. (Undertaking in Annexure G)

Place:

Date: **Seal & Signature of Bidder**

ANNEXURE K

IS Audit Assignments:

Organization Website address:	IS Audit scope (Attach copy of order / contract)	Date/ Period when conducted	Data center located at	Number of remote branch/ locations/ offices connected to data center

Place:

Date: **Seal & Signature of Bidder**

ANNEXURE L

BS7799/ ISO 27001 security framework implementation

Organization Website address:	Scope of work (Attach copy of order / contract)	Date/ Period when implemented	Located at	Certification obtained on

Place:

Date: **Seal & Signature of Bidder**

ANNEXURE M

Professional's details : The structure should clearly indicate if the member is part of (a) the Governance Structure or (b) the team proposed to be deployed for the IS Audit. The information should distinguish the teams clearly.

S.NO	Name	Designation	Educational Qualification	Certifications/Accreditations	Total Experience	Since when in the bidder organization	Conducted IS audit of organization(s) with brief scope and when conducted	Role, which may given by bidder in the assignment e.g. Penetration testing, process audit, vulnerability analysis, WAN Audit, policy reviewer etc.	Employee profile (Domain specific and others e.g. Banking, Ethical Hacking, Sun Solaris security, Oracle DB Security, Networking Security etc.).	Whether Member is part of the team proposed to be deployed for the IS Audit (YES/ NO)

Important Note: CVs of Audit team members to be deployed for the IS Audit are **to be furnished on a separate sheet including** their Credential in the specialized qualification and their previous employment record.

Place:

Date: **Seal & Signature of Bidder**

ANNEXURE N

Number of auditors (approx) [having minimum experience as defined under 2.2.(g) & Annexure J(g)] to be deployed for audit at PNB.

S.NO	Activities	Number of team members who will be deployed.		Elapsed Time	Effort in Man days	Remarks
		For Conducting Audit	For Preparation of Draft Report for Discussion			
1	Compliance to System and Procedure [Quarterly]	1. CISA/CISM 2. DISA 3. Others(Specify)				
2	VAPT- Vulnerability Assessment & Penetration Testing from intranet [Quarterly]	1. CISSP 2. CEH 3. CCIE Security 4. SCSECA/OCE 5. Others(Specify)				
3	WAN Audit [Quarterly]	1. CISA/CISM 2. CISSP 3. CCIE Security 4. Others(Specify)				
4.	EAPT- External attack and penetration test from internet [six in a year]	1. CISSP/CCIE 2. CEH 3. Others(Specify)				

Place:

Date: **Seal & Signature of Bidder**

ANNEXURE O

Check list for the Documents to be submitted

Document	Particular	YES/NO
Company Details	Brief Profile	
Audited Balance Sheets	Copy of balance sheets for 2010-11, 2009-10 and 2008-09	
Annexure C	Bid Security Form	
Annexure D	Technical BID FORM	
Annexure E	Commercial BID FORM	
Annexure F	Undertaking 1	
Annexure G	Undertaking 2	
Annexure I	Commercial Bid	
Annexure J	Technical Compliance Sheet	
Annexure K	IS Audit assignments	
Annexure L	BS7799/ ISO 27001 security framework implementation	
Annexure M	Professional's details	
Annexure N	Number of auditors (approx) to be deployed for audit	