



Punjab National Bank

REQUEST FOR PROPOSAL

**FOR
APPOINTMENT OF IS AUDITOR FOR
INFORMATION SYSTEM AUDIT
AND
SECURITY CUM FUNCTIONAL AUDIT OF
APPLICATION SOFTWARES**

Inspection & Audit Division
Sector-32, Plot No. 5
Gurugram - 122001



CONTENTS

1 INTRODUCTION

- 1.1 Background
- 1.2 Purpose
- 1.3 Project Scope
- 1.4 Invitation
- 1.5 Time Schedule of Various bid related events
- 1.6 Confidentiality
- 1.7 Non-Disclosure Clause
- 1.8 RFP Terminology
- 1.9 Disclaimer

2 BIDDING PROCESS

- 2.1 Bidding
- 2.2 Minimum Eligibility Criteria for Bidder(s)
- 2.3 Scope of Bid
- 2.4 Amendments/Supplements to Bidding Documents
- 2.5 Rights of PNB
- 2.6 Governing Law and Disputes

3 INSTRUCTIONS TO BIDDER

- 3.1 The Bidding Documents
 - 3.1.1 Cost of Bidding
 - 3.1.2 Content of Bidding Document
 - 3.1.3 Clarification on RFP
 - 3.1.4 Correction of errors

3.2 Preparation of Bids

- 3.2.1 Language of Bid
- 3.2.2 Document Constituting the Bid
- 3.2.3 Bid Form
- 3.2.4 Bid Prices
- 3.2.5 Bid Currencies
- 3.2.6 Document Establishing Bidder's Qualification.
- 3.2.7 Documents establishing Solution Conformity to Bidding Documents
- 3.2.8 Bid Security
- 3.2.9 Period of Validity of Bids
- 3.2.10 Format and Signing of Bid
- 3.2.11 Sealing, Marking and Submission of Bids
- 3.2.12 Deadline for Submission of Bids
- 3.2.13 Late Bids
- 3.2.14 Modification and Withdrawal of Bids
- 3.2.15 Acceptance or rejection of bid
- 3.2.16 Notification of award

3.3 Bid Opening and Evaluation of Bids

- 3.3.1 Assumptions and Agreements
- 3.3.2 Opening and evaluation of Technical Bids by the Bank
- 3.3.3 Opening and evaluation of Commercial Bids
- 3.3.4 Clarification of Bids
- 3.3.5 Technical Evaluation Criteria
- 3.3.6 Contacting the Bank



3.4 Award of Contract

- 3.4.1 Post qualification
- 3.4.2 Award Criteria
- 3.4.3 Dead Line / Critical Dates
- 3.4.4 Right to accept any Bid and to reject any or All Bids
- 3.4.5 Notification of Award of Contract
- 3.4.6 Signing of Contract
- 3.4.7 Performance Guarantee

4 Broad Terms and Conditions

- 4.1 Standards
- 4.2 Arbitration
- 4.3 Notices
- 4.4 Use of Contract Documents and Information
- 4.5 Patent and Copyrights
- 4.6 Deliverables
- 4.7 Prices
- 4.8 Payment Terms
- 4.9 Taxes and Duties
- 4.10 Delays in the Performance
- 4.11 Penalty
- 4.12 Force Majeure
- 4.13 Correspondences
- 4.14 Successful bidder's Obligations
- 4.15 Contract Amendments
- 4.16 Extension of Bank Guarantees
- 4.17 Adherence to Standards & Right of Audit/Visit
- 4.18 Extension of contract period
- 4.19 Variation
- 4.20 Subcontracting
- 4.21 Course of Audit

Annexure	A	Detailed Scope of Audit
Annexure	B	Performance Guarantee Form
Annexure	C	Technical BID FORM
Annexure	D	Commercial BID FORM
Annexure	E	Undertaking 1
Annexure	F	Undertaking 2
Annexure	G	Reverse Auction Guidelines
Annexure	H	Compliance Statement
Annexure	I	Technical Compliance Sheet
Annexure	J	IS Audit assignments
Annexure	K	BS7799/ ISO 27001 security framework implementation
Annexure	L	Professional's details
Annexure	M	Number of auditors (approx) to be deployed for audit
Annexure	N	Performa for Integrity Pact
Annexure	O	Check list for the Documents to be submitted



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. Bank has more than 12000 SOLs (Service Outlets i.e. Branches / Extension Counters / Service Branches / Administrative Offices) in India. The Centralized Banking Solution connected to the Data Centre and DRS through a Enterprise Wide Network has networked all of its branches and offices. The modes of connectivity to the branches/offices are a combination of VSAT, MPLS 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 and working under ADDM (Active Directory & Desktop Management). Besides this there are interfaces with applications and networks used by different institutions like MTNL, Customs, Reserve Bank of India etc.

The Bank has more than 13000 ATMs connected to the CBS through ATM Switch. Now customers can transfer funds to other bank accounts through ATM via IMPS facility. Other Alternate Delivery Channels of services like Internet Banking, POS, Mobile banking, UPI 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. 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/or through Dial-up connection.

Bank has implemented Enterprise Data Ware House 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 is also located at Delhi.

The Operating Systems used in different applications include different flavors of Unix like (Solaris, AIX, SCO etc.), various flavors of Windows, IBM AIX, HP Unix, Novell Netware, Tandem, DOS etc. Applications, which use messaging, include SWIFT, SFMS (RBI Infinet), Cash Management Services, Electronic Funds Transfer, Treasury and other RBI Projects etc. . 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 audit professionals.

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 27001:2013 compliant.

1.2. Purpose

Appointment of IS Auditor for audit of activities at Data Centers, Disaster Recovery Sites, HO Divisions and other offices/branches for 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, software, network, security etc.,
- Maintaining security, confidentiality, integrity and availability of data,
- Efficient utilization of resources-IT.
- Ensuring compliance of IT Security & Cyber Security Policies and procedures defined & reviewed by the Bank on time to time basis.
- Ensuring compliance of RBI Information Security Guidelines/ Alerts/Advisories/Cyber Security Framework/recommendation and other applicable external legal guidelines & regulations issued from time to time by RBI/Cert-In/NCIIPC/SEBI and other regulatory bodies etc.
- Provide recommendation and steps for compliance of the observations to mitigate the risk.

1.3. Project Scope

Detailed scope is at Annexure A. 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 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

Details of the tender will be available on www.pnbindia.in and www.etender.pnbnet.in.

1.	Date of commencement of availability of Bidding Documents for Sale	16-04-2021
----	--	------------



2.	Last date & time for submission of queries (by e-mail).	19-04-2021	
3.	Pre-Bid Meeting (if required same to be informed to interested bidders)	21-01-2021	
4.	Last date and time for receipt of Bidding Documents.	Last date and time for Hash submission	30.04.2021 upto 1400 Hrs
		Last date and time for online bid submission/Bid Re-Encryption	From 30.04.2021 1501 Hrs to 01.05.2021 1700 Hrs
		Time for submission of technical supporting document (Hard Copy)	Till 30.04.2021 1700 Hrs
5.	Date and Time of Technical Bid Opening.	01-05-2021 at 1100 Hrs	
6.	Cost of RFP	<p>Rs.10,000/- (Non refundable) plus 18% GST should be submitted online(NEFT) only in favor of Punjab National Bank before last date of bid submission in the following account:- IFSC Code : PUNB0492800 Bank & Branch : Punjab National Bank, Vill Jharsha Gurgaon Haryana 122001 Account No. 4928002200000069 Account Name:- Imprest AC ICD</p> <p>Proof of NEFT is to be submitted at the time of physical bid submission.</p> <p>*MSE bidder is exempted from payment of cost of RFP if bidder can furnish requisite proof subject to the satisfaction of Bank. This exemption is not applicable for traders, sole agents, distributors etc. Start-up bidder recognized by Department of Industrial Policy and Promotion (DIPP) is also exempted from payment of cost of RFP.</p>	



7.	Bid Security Amount	Bidder has to submit the “Bid Security Declaration” on their organization’s letter head duly signed and stamped by their authorized signatory accepting that if they withdraw or modify their bids during period of validity of the bid, or if they are awarded the contract and they fail to sign the contract, or fail to submit a performance guarantee before the deadline defined in the request for proposals (RFP) document, they will be Blacklisted.
8.	Place of opening of Bids	Punjab National Bank, IT Audit Cell, Inspection & Audit Division, Head Office 2 nd Floor, Plot-5, Sector-32, Gurugram, Haryana – 122001

Note:

- (i) Technical Bids will be opened online as well as in physical form but Commercial bid will be opened online only. Bidders may view the details through their terminal using their eTendering System [<https://etender.pnbnet.in>] registration login.
- (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) Bidders, who have not registered earlier with e-procurement site, would have to register with our e-procurement site.
- (iv) Scanned copies of Documents as per Annexure O of technical bid are to be submitted online through e-procurement site. However hard copies of the same are to be submitted in physical form also along with other supporting documents required for evaluation of technical bid.

Any query regarding the RFP may be sent to iadisaudit@pnb.co.in and vasudev@pnb.co.in addressed to The Chief Manager, Punjab National Bank, IT Audit Cell, Inspection & Audit Division, Head Office 2nd Floor, Plot-5, Sector-32, Gurugram, Haryana – 122001 before the Last date & time for submission of queries by e-mail.

1.6 Confidentiality

The RFP document 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. **Further, the auditors engaged in the auditing activities shall also be required to sign the non-disclosure agreement (NDA) before start of the audit.**



1.7 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.
- iv) It should be ensured that any data collected during the auditing work and report prepared thereof shall not be taken out of the bank premises by auditors/firms.

1.8 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, 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 or related to 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.

1.9 Disclaimer

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 download RFP from the Bank's web site www.pnbindia.in or www.etender.pnbnnet.in, The RFP completed in all respect with a bidding fee of Rs. 10,000/- (Rs. Ten Thousand only) plus GST shall be submitted on or before the last date.

MSE bidder is exempted from payment of cost of RFP if bidder can furnish requisite proof subject to the satisfaction of Bank. This exemption is not applicable for traders, sole agents, distributors etc. Start-up bidder recognized by Department of Industrial Policy and Promotion (DIPP) is also exempted from payment of cost of RFP.

Scanned copies of Documents as per Annexure O of technical bid are to be submitted online through e-procurement site. However hard copies of the same are to be submitted in physical form also along with other supporting documents required for technical bid.

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. In terms of guidelines issued by Government of India, Bank reserves the right for Sending the name of the firms having foreign tie-ups to the Ministry of Home Affairs (MHA), Government of India (GoI), for obtaining their No Objection Certificate (NOC) for shortlisting them for further process & such firms shall provide all required documents desired for obtaining the NOC from MHA (GoI).

Commercial Bid will be opened only for the short-listed Bidders who have qualified in the Technical Bid and NOC has been received by the Bank from MHA (GoI) for the firms having foreign tie-ups. The Commercial Bids will be opened on-line only.

Technical Bid and commercial Bid shall be signed using Digital Certificate by the Bidder so as to bind the bidder to the contract.

Bank reserves the right to opt for Reverse Auction. Reverse Auction may be adopted in case two or more bidders are technically eligible (Guidelines of Annexure G).

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 should be a registered legal entity in India and must be financially solvent.



- b) Should not be involved in Information Systems & Security Audit on regular basis (cyclic audits) of the Punjab National bank for last two financial years.
- c) Should not be a vendor/supplier for Software and Hardware components of the Bank or technical advisor/service provider of the bank.
- d) Should not be involved in implementing Security and network infrastructure of the Bank at Data Center, EDW, Treasury and DRS level.
- e) Should be an Indian Company /Firm /Limited Liability Partnership (LLP) Firm/ Organization /Independent subsidiary with an average annual turnover of Rs.3 (Three) Crores or more for the last three financial years and should be in net profits in last two financial years and should have registered office in India.
- f) Should have conducted minimum 2 Information Systems Security audits of any Scheduled Commercial Bank's Data Center connected with a minimum 500 offices, in last five years, out of which one audit should be in a public sector bank in India.

Conduct of Information Systems Security audit, as per point f, shall constitute (but not be 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 Systems and procedures as per Organization's IT Security Policy/ guidelines.
- g) Should have implemented BS 7799/ISO 27001:2013 security framework in any organization in India.
 - h) Should have at least 7 qualified professionals with CISA/CISSP and 1 with CHFI certification. The professionals must have IS Audit Experience of 2 or more years including at least one IS Audit for any organization defined at (f) above and should be on permanent roll of the organization.
 - i) 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.
 - j) Should be able to depute adequate no. of auditors, with industry standard certifications such as CISA/CEH/CISSP/CHFI/CISM/CGEIT/Sun Certified Security Administrator (SCSECA)/OCE(Oracle Certified Expert – Security Administrator)/CCSP/OSCP/Cisco CCIE-security to cover given scope with due



professional care & to provide deliverables as per clause 3 of "Detailed Scope" - Annexure A of RFP.

- k) Should be empanelled with Cert-In, Govt of India for Security Auditors with a valid certificate of empanelment as on date of submission of bids. De-empanelment by the Cert-In may lead to termination of the work contract.

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 Systems Auditor to conduct audit as per detailed scope as per Annexure A.

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 published on the bank's corporate website www.pnbindia.in or www.etender.pnbnet.in and will be binding on all the bidders. Further, bidders must provide name of the contact person, mailing address, telephone number, Email 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 deadlines for submission of bids.

2.5. Rights of PNB

PNB reserves the right to:-

- 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.
- Negotiate with Bidders.

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. Governing Law and Disputes

The Bid and the resulting Contract with the successful Bidders shall be governed in accordance with the Laws of India for the time being in force.

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 same shall be settled by Arbitration 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 or of the umpire, as the case may be, 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, and Commercial 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 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, i.e. before the pre-bid meeting date.

Both questions and responses (including an explanation of the query but without identifying the source of the inquiry) will be displayed on bank Website www.pnbindia.in or www.etender.pnbnet.in. 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, vasudev@pnb.co.in on or before the last date.

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 Bank 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.
- d) Bid security declaration furnished in accordance with ITB Section 3.2.8.
- e) An undertaking from the bidder (As per Annexure C) 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.
- f) Compliance statement as per annexure- H.

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. This will lead to cancellation of the bid and bidder will not be eligible to participate further in this bidding process.

- ii) Commercial Bid – Commercial Bid will comprise of Bid Form as per Annexure D submitted through online only.**

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.

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 Declaration**" on their organization's letter head duly signed and stamped by their authorized signatory accepting that if they withdraw or modify their bids during period of validity of the bid, or if they are awarded the contract and they fail to sign the contract, or fail to submit a performance guarantee before the deadline defined in the request for proposals (RFP) document, they will be Blacklisted.



- (ii) The “Bid Security Declaration” is required to protect the Bank against the risk of Bidder’s misconduct of any nature, which would result in Blacklisting of the Bidder by the Bank.
- (iii) The bidder may be blacklisted as per “Bid Security Declaration”, 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.

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). A Bidder may refuse the request without invoking its “Bid Security Declaration”. 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 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 (duly attested by notary public) 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.
- (ii) Any interlineations, erasures or overwriting shall be valid only if the person or persons signing the bid sign them.
- (iii) 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:

Certificate and other supporting document may be attached with the covering letter while submitting the 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.

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

Technical Bids will be submitted online as well as in physical form while commercial bid will be submitted online only.

Bidders should provide their 'Minimum Eligibility Criteria', 'Technical compliance' responses in only one original copy. The sealed envelope containing Technical responses shall then be sealed in one envelope marked "Technical Bid for appointment of IS Auditor for information system Audit and Security cum functional Audit of application software" 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.

All pages of the Bid including Brochures must be duly signed and stamped and 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 Dy. General Manager
IS Audit Department
Inspection and Audit Division
Punjab National Bank, Head Office
Plot No 5, Institutional Area
Sector 32, Gurgaon- 122001**

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

Bids received other than specified modes will be rejected.

Scanned copies of Documents as per Annexure O of technical bid are to be submitted online through e-procurement site. However hard copies of the same are to be submitted in physical form also along with other supporting documents required for evaluation of technical bid.

Commercial Bid – Commercial Bid will comprise of Bid Form as per Annexure D submitted online only.

Technical Bid and commercial Bid shall be signed using Digital Certificate by the Bidder so as to bind the bidder to the contract.

3.2.12. Deadline for Submission of Bids

Bids (Technical and Commercial) 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 Blacklisting of the bidder.. 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 Bid Security Declaration 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 by 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, Plot-5, Sector- 32, Gurugram, Haryana – 122001.

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) The bidder's names, bid modifications or withdrawals and the presence or absence of requisite bid security declaration and such other details as the Bank at its discretion may consider appropriate will be announced at the time of bid opening.
- iii) Bids that are not opened and read out at bid opening shall not be considered for further evaluation, irrespective of the circumstances.
- iv) The Bank will prepare minutes of the bid opening.
- v) The technical bids would be evaluated by the Technical Committee. Bidders should be ready to give presentation, if required, 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.
- vi) 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 outrightly and may not subsequently be made responsive by the Bidder by correction of the non-conformity.
- vii) 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 was 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 online in the presence of representatives of short-listed Bidders. In case representatives of the short-listed bidders are not present, the commercial Bids shall be opened in their absence.
- 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 Declaration" may be invoked for blacklisting of the bidder by the Bank..

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 bidders 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 and all the evaluation criteria decided by the Bank.

3.4.2. Award Criteria

Bank will hold Reverse Auction in the event of two or more bidders being commercially eligible, post which the final price shall be arrived at (Procedure available on our e-procurement website).



Reverse Auction will be conducted for the items of Commercial Bid (as per Annexure D).

Base Price & Bid decrement value will be as per Bank's Discretion and will be communicated to all commercially eligible bidders before reverse auction.

Reverse auction will be conducted on Bank's E-Auction portal.

After Reverse Auction completion, Bidder having Lowest Weighted Yearly Cost (as per Annexure D) shall be treated as L1 bidder.

At any stage of the RFP, if Bank is left with only one eligible bidder, Bank reserves the right to award the contract to the said bidder.

Detailed guidelines Reverse Auction is provided in Annexure G.

3.4.3. Dead Line / Critical Dates

The bidder shall complete/perform 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 execution 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.

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 (Integrity pact, non-disclosure agreement, service level agreement, etc.) 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. Signing of the contract by the successful bidder will constitute formation of the contract.

3.4.7. Performance Guarantee

Within 15 days of the receipt of notification of award from the Bank, the successful Bidder shall furnish the Performance Guarantee from a scheduled commercial bank other than PNB, payable on demand for an amount equivalent to three percent (3%) 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 Bank Guarantee shall continue and hold good till the completion of the all the scheduled audits **(30 Months)** from the date of agreement, subject to the terms and conditions in the said Agreement.

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.

Failure of the successful bidder to comply with the requirement shall constitute sufficient grounds for the annulment of the award and blacklisting of the bidder, 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 settled by arbitration in accordance with the provisions of 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 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.



Further, Bank can terminate the Agreement at its sole discretion without assigning any reason, after giving the successful bidder a notice of 30 days

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.

The successful bidder shall be liable to indemnify PNB, at its own cost and expense, in respect of any losses sustained or suffered by any third party, on account of breach of any stipulation of this agreement by the successful bidder or any negligent or fraudulent act or omission by successful bidder in course of fulfilling its obligations under the RFP.

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 D giving therein total **bid price for one year. These prices will be applicable for minimum 2 years.** Bidder will have to perform the audit for 2nd year on the same price and terms and conditions if bank management intends & finds the services satisfactory.

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

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. On submission of First quarter report and presentation made. Also During first year audit report of One Time Review of Information Security Architecture of Data Centers at Delhi, Mumbai, Kolkata & Disaster Recovery Sites at New Delhi, Belapur, Mumbai along with Security Operation Centre and Network Operation Centre & onetime review of software (OS/DB/Application) licenses procured vis-à-vis installed in the Bank and providing recommendation of license management by the Bank.	25% of annual fee.
b. On submission of second quarter report, third EAPT report and presentation made.	25% of annual fee.
c. On submission of third quarter report and presentation made.	25% of annual fee.
d. On submission of fourth quarter report, sixth EAPT Report and presentation made.	25% of annual fee.
e. Payment for Security cum Functional Audit of Application Software.	On actual basis, quarterly.

4.9. Taxes and Duties

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

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 all 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 1 % 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.

In addition to the above, the Successful bidder will be liable to pay PNB, liquidated damages (LD) due to any deficiency in performance or all the obligations under the contract, 1% of Contract value per week maximum upto 10 % 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 (i.e. 5 Years +) 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.

4.17 Adherence to Standards & Right of Audit/Visit

The selected Bidder must adhere to laws of land and rules, regulations and guidelines prescribed by various regulatory, statutory and Government authorities.

The Bank and Regulatory bodies such as RBI reserves the right itself or through a Consultant to conduct audit/ongoing audit or visit the office locations of the selected Bidders. The cost of the audit/Consultant shall be borne by the Bank.

4.18 Extension of Contract Period

Bank at its own discretion may extend the contract period up-to four quarters on same rates, terms & conditions after expiry of the contract period of two years.

4.19 Variation

Any upward variation up to 10% in the number of offices covered under the scope of audit shall be covered under the contracted price and no additional cost shall be payable. Bank & Successful bidder may negotiate the additional prices for variation above 10% and maximum up to 25%.

4.20 Subcontracting

No Subcontracting of the work will be permissible.

4.21 Course of Audit

The Bank at its discretion, may attach it's IS audit team with the IS Audit Team of Selected bidder during the conduct of the Audits. The scope of work also includes extending training to our IS Audit Team, twice a year, and to share with them all the formats, Check lists, scoring sheets, scripts etc. that will be used during the process of audit.

4.22 SIGNING OF PRE CONTRACT INTEGRITY PACT



The bidder should submit Original Executed Integrity Pact along with the technical bid. The Integrity Pact must be executed on stamp paper of applicable value and must be signed by all the witnesses also. The Performa of Integrity Pact is as per (Annexure-N)



Annexure - A

1 SCOPE OF WORK

The role of the IS auditors is to see that the organization's assets are protected and suitable internal controls are in place to protect its information and information resources. IS audit is responsible for providing an organization with independent and objective views on the level of security that should be applied to the Information Systems. Computer Security on the other hand is responsible for implementing security in the computerized environment. The IS auditor will learn to co-exist with the Computer Security function and work together for the benefit of the whole organization ensuring that professional standards are always maintained.

The Scope of work mainly relates to conducting of Information System and Security Audit including Cyber Security Audit of different Information systems/applications/ Databases / Operating Systems / Security devices, appliances and Solutions / Network Equipment/ Information Technology (IT) Process like sharing information through web services, host to host etc. in use by the Bank, as listed below, including those systems used by other agencies for providing services in respect of activities which are outsourced.

Auditor is expected to carry out Information Security Audit activities including but not limited to the points mentioned in the scope of this RFP. Further the Auditor has to evaluate and comment on compliance by Bank as per RBI Circular on Cyber Security Framework, Information/Cyber Security Policy/ Procedures/Processes of the Bank, ISO 27001:2013 standards, other RBI guidelines and Industry best practices etc.

- The Guidelines & Advisories issued by RBI, Govt. of India, NPCI, UIDAI, Cert-In etc.
- Punjab National Bank Information System Audit Policy, IT Security Policies & Procedures and Cyber Security Policy.
- IT Act, 2000 as amended from time to time.

IS Audit of each of the systems shall broadly cover the following aspects:

1. Physical and Environmental controls
2. Logical access Controls
3. Operating System/database review including Vulnerability Assessment
4. Application Review
5. Business process Review
6. Vulnerability Assessment
7. Penetration Testing
8. Network and Security Review including VA and Penetration test
9. Backup procedure Review
10. Business Continuity/Disaster Recovery plans/practices
11. Review of Outsourced Activities (SOPs review)
12. Virus protection and Patch management.
13. Capacity utilization of servers and applications
14. Review of Basic minimum Configuration applicable for each system as per best practice i.e. Baseline Secure Configuration review.
15. Application Security Life Cycle (ASLC) review.
16. Database Configuration Audit.
17. Secure Code Practice Review.



18. IT General Controls Review.

19. General Process Controls Review.

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

a) **Office covered:**

- Data Centers at NewDelhi/Mumbai/Kolkata, NOC, SOC at New Delhi/Gurgaon/Kolkata/Mumbai.
- Disaster Recovery Sites at Mumbai/New Delhi
- Treasury Division, SWIFT Center at Mumbai/Gurgaon/Kolkata
- Digital Banking Division at New Delhi/Gurgaon/Kolkata
- Enterprise Data Warehouse & Zero Data Loss site at New Delhi/NCR/Mumbai/Kolkata/Gurugram.
- Bank's CTS Centers at Delhi, Chennai, Kolkata & Mumbai
- Bank's Contact Centers/ Call Centres at Gurgaon, Noida, Bhopal & Dehradun.
- Premises/activities of any third party/service providers (outsourced activities) to review compliance of services/T&C under service level agreements at New Delhi/NCR/Mumbai/Bengaluru/Chennai or any other bank's office/ Vendors location
- Other HO divisions/ Service Providers at New Delhi/ NCR/ Mumbai/Bangalore/Chennai/Gurgaon/Kolkata or any other bank's office at any place, where critical application/IT infrastructure is installed or may be installed in future.
- Locations of Service Providers to whom specific services are outsourced.
- Data Centers and Disaster Recovery Sites of RRBs of the Bank at New Delhi/Mumbai/Kolkata.

b) **Regular IS Audits.**

- Compliance testing, Vulnerability Assessment (Servers, Security & Network Devices and URLs), Penetration Testing, process audit, policy / procedure review, Device Level Audit etc, on quarterly basis including the compliance testing of previous test/audit report.
- Vulnerability Assessment (Servers(OS), Database systems, webserver, IOS of Security & Network Devices) including virtual instances/hypervisors etc, Penetration Testing of public facing applications/internal applications with URLs, process audit, policy / procedure review, Device Level Audit etc, on quarterly basis including the compliance testing of previous test/audit report .
- Conducting External Assessment of Equipments/ Applications/ Mobile Apps exposed to outside world (Including APIs) once every two months i.e. six times in a year including the compliance testing of previous test/audit report.
- Configuration Audit/Hardening review for Server/OS/Networking & Security Devices/Database/ firewall etc.
- Comment upon compliance to ISO 27001:2013 , PCIDSS etc standards (or later standard to which bank is certified/gets certified)



- Various Information Security audits and their compliance certificates which are required for the adherence to RBI/Cert-In/NPCI/UIDAI or any other regulatory body guidelines issued from time to time.
- Compliance audit of G Gopalakrishna Committee recommendation /Cyber security framework/ Comprehensive Cyber Security Framework for Regional Rural Banks (RRBs) or any other recommendations directed by RBI/NABARD.
- Defining Checklist for different applications/area of audit in Consultation with bank. Check list should be authorized by Bank before conduct of Audit, same will be changed as per the business/regulatory requirement during the course of audit.
- Evaluate the adequacy, gaps & implementation of operating processes, information security management system policies, internal control procedures / guidelines documents, Cyber Security Policy, Cyber Crisis Management Plan, Long Term/Short Term IT Plan of the Bank/
- Evaluate timely review & completeness of all IT Security related Policies and Guidelines with industry best practices & other regulatory as well as legal guidelines for various IT Infrastructure.
- 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. Review of Business Continuity Plan and its implementation across the Bank.
- If the formal procedures and Compensatory controls are not in place for any activity, evaluate the process applied, risk associated and give recommendations for improvement as per best practices.
- Providing 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.
- IS Auditor should assess the risk of occurrence of fraud as a part of IT risk assessment and audit process and provide recommendations for mitigating the same in the bank.
- IS Auditor will provide the report on root cause analysis (RCA)/ Forensic Audit of the security incidents, if required by the Bank.
- Review of Business continuity plan (BCP) of the critical systems and providing report based on BS 25999/ ISO 22301:2012.
- Review security of provisions made for enabling Work from Home for staff members.
- Provide assurance for new security initiatives being undertaken by the Bank.
- Checking the extant configuration / rules in eOBC, eUNI and PNB 1.0 and whether the required configuration / rules has been correctly addressed in PNB 2.0 set up.
- Comprehensive review of the BCP arrangement for all critical applications.
- Review of audit logs of CBS menus maintained by ITD along with the procedure of maintenance of logs.
- All the Vulnerability Scans, wherever feasible and desired by the Bank shall be Credential/ Authenticated scans.

c) Security cum Functional Audit

Security cum Functional Audit will be done before GO-Live for New in-house developed application/ After Major Changes in existing applications (both in-house and developed by external vendors).



- Bidders need to submit the quote for a Total of Approx 150 applications going live/ Major Changes per year (in-house/procured). Complete Scope is defined/provided in point no. 4.5 of Annexure A(Audit Scope).

The scope defined as above is illustrative but not exhaustive.

2 Schedule of Regular IS Audit:

The Information Systems & Security Audit will be done as per schedule as under:
Successful bidder will have to visit the respective location to conduct the Audits.
Individual Audit Report shall be issued for each of the following activities. The complete scope of these Audits is shared in this document.

S.NO	Activity	Periodicity
1	Process Review Audit Conducting Information Systems & Security Audit (Process Review Audit) as detailed for Data Centers at Bank's various locations (amalgamated entity) Disaster Recovery Sites at Bank's various locations (amalgamated entity) Treasury Division & SWIFT Centers, EDW & other Process Owner Divisions Technical Service Providers located at Delhi/NCR/Mumbai/Bangalore/Chennai Contact Centers/call Centres at Bank's various locations (amalgamated entity) CTS Grid at Delhi, Chennai, Kolkata & Mumbai	Quarterly
2	Other Process Audit as defined/provided in point no. 4.4 of Annexure A(Audit Scope)	As and When required by Bank
3.a	Device Level Audit (PDC, DR , NOC, SOC, HO, ZO & other administrative offices)	Quarterly
3.b	DLA of network devices at Branches and CO of Bank on sampling basis covering at most 5% devices.	Quarterly
4	Conducting Vulnerability Assessment (VA) and penetration test (PT).	Quarterly
5	Conducting external assessment of equipments/applications/Mobile Apps exposed to outside world [Both internal & External] once in two months i.e. six times in a year	Bi-monthly
6	Revalidation/Re-Checking of observations (VA & PT) which have been reported by different department/division as complied.	30 Days after submission of final report of VAPT
7	Revalidation/Re-Checking of observations (EA) which have been reported by different department/division as complied.	15 days after submission of final report of EAPT



8	RA Audit independently as well as per checklist specified by IDRBT Hyderabad	Bi-Annually
9.	Cyber Security Audit	Quarterly
10.	One Time Review of Information Security Architecture of Banks's Following locations:- 1. Data Centers 2. Disaster Recovery Sites 3. NOC 4. SOC 5. Zero Data Loss Sites	Only One time (at the beginning of the audit assignment)
11.	One time review of software (os/db/application) licenses procured vis-à-vis installed in the Bank Servers/Applications and providing recommendation of license management by the Bank.	Only One time (at the beginning of the audit assignment)
12.	Policy and Procedure Review	Yearly
13.	Comprehensive review of the BCP arrangement for all critical applications	Half-Yearly
14.	Review of audit logs of CBS menus maintained by ITD along with the procedure of maintenance of logs.	Half-Yearly

- In cases of exigencies, i.e. upon regulatory requirements or direction of top management, Bank at its discretion may direct the successful bidder for conduct of out of turn audit activities without any extra cost.
- All the process audits shall be conducted with direct involvement of CISA/CISSP professionals.

3 DELIVERABLES:

3.1 Time Lines

- Will provide schedule of audit, at least 7 working days prior to start of audit along with full credentials of Audit team (**consisting minimum 6 auditors with qualification & experience as defined in RFP**) who will be conducting the audit at PNB (onsite).
- Completion of quarterly Process Review Audit, Device Level Audit, VA & PT audit as mentioned above within 18 working days.
- Minutes of daily meeting will be prepared by next day where observations are based on discussion and will be signed by all participants.
- Giving draft report for discussions with owners within 3 working days after completion of audit.
- Discussion of the issues with Divisional Head/owner after 2 working days from date of submission of draft report(2 working days).



- f) Give final report within 3 working days after discussions with owners
(Total 28 working days) (18+3+2+3+2).

Activity	Duration*
Process Audit (Field Work)	18 Working Days
Vulnerability Assessment& Penetration Testing	
Device Level Audit	
External Assessment/ Security Cum Functional Audit of Application.	6 Working Days
Draft report preparation and submission	3 Working Days
Discussion on draft report	2 Working Days
Final report preparation and submission	3 Working Day
Follow-up audit	2 Working Days

The Security Cum Functional Audits have to be initiated within three days of allotment of audit and completed within 21 working days.

- g) Cyber Security Audit on quarterly basis and RA office to be audited on Bi-annual basis and same shall be executed as per directions of the Bank.
- h) One Time Review of Information Security Architecture, and Network Architecture of Data Centers, Disaster Recovery Sites, Zero Data Loss Sites, NOC, SOC Sites of all three Banks i.e. Punjab National Bank, erstwhile Oriental Bank of Commerce and erstwhile United Bank of India & one-time review of All software (os/db/application) licenses procured vis-à-vis installed in the Bank and providing recommendation of license management, shall be done during the first quarter of audit assignment after being awarded the work contract.
- i) One time Data Centre Sanitization and configuration review of Data Centres (PDC) and Disaster Recovery Sites (DRS).
- j) Where ever exception has to be taken/ compliances cannot be met by the Bank, the auditor shall provide compensatory controls to cover the risk and should also give step wise recommendation/methodology for implementing the controls.
- k) Any Zero Day Vulnerability should be reported to the Bank on same day without waiting for issuance of the audit reports irrespective of type of audit.
- l) Reasonable assurance for each of the areas in the scope of audit shall be provided explicitly in the audit reports.
- m) 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.
- n) Resources strength with experience as defined in 2.2(h) will be deployed keeping in view the scope of audit and time schedule.
- o) No inexperienced / less qualified resource should be deployed for audit. Details of auditor team will be provided to Bank before hand and will be deputed to assignment only after Bank's consent. The audit team as informed to the Bank should not be changed without consent of the Bank.



- p) Training to be provided to Bank's officials (around 20) on half yearly basis at NCR (National Capital Region) for a week.
- Training is to be given to internal IS Audit team on uses of Tools used for Audit purpose, preparation of the Reports based on the identified vulnerabilities (i.e identifying Risk Impact and Recommendation to mitigate the identified risks)
 - The IS Auditor should explain, to the bank's team all the processes, procedures involved in arriving at audit findings including interpretation of outputs generated by various audit tools.

3.2 REPORTS:

Report should be provided with snap shot / evidence/ documents details / CVE number from which observation made wherever is easily understood by Bank.

Reporting formats should at the minimum include

- a) Compliance status of previous quarter report will include observations with status as following –
Found complied/ found partially complied/ Found Non-complied/ Exception taken as a separate report.
- b) Audit report of current quarter with status Repeat/ Exception or New
- c) The IS Auditor shall provide different types of reports which would address all issues/observations regarding compliances.
- d) If repeated – (i) Since when on same server.
(ii) Since when on Similar asset.
- e) If exception– expiry date & authorized by whom.
- f) Vulnerability ID (Unique identification number (alpha numeric) for each vulnerability and the Identifier should be such that it is Unique for any previous Vulnerability process also.
- g) Vulnerability Identified (specific to equipments/ resources - indicating name and IP address of equipment, Application name where Vulnerability exists and office / department name and should not be generalized)
- h) Broad domain categorization of activity (Port/SQL injection/ Services/Physical access control/ Logical access control/ environment etc.)
- i) Risk category & Exploitable status as against – High, Medium, Low level observations.
- j) Servers/ Resources affected with IP address.
- k) Department (in office) to whom the Vulnerability 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/RBI against identified risk/observation.
- q) The reports shall be customised as per the requirements of the Bank.



- r) Additional mandatory or voluntary standards or regulations applicable to the banking industry as best practices should be reported under “Improvement /suggestions”
- s) Standards followed
- t) 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.
 - e. Analysis of vulnerabilities and issues of concern
- u) Personnel involved in the audit, including identification of any trainees.
- v) The various audit reports/ templates should be got integrated with the Bank’s ITGRC Application.
- w) All the reports should contain the URL, IP Address, Application and server name, host name etc in respect of the assets which are subjected to Audit.

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), which shall be capable of providing audit report, and 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/excel sheet. 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 Vulnerability wise
- c) Repeated
- d) Exceptions
- e) Broad domain activity wise
- f) Risk category & Exploitable status as against – High, Medium, Low level observations
- g) Servers/ Resources affected wise.
- h) Each server/ resources vulnerability history (activity wise) should be maintained so that trend analysis can be done at any point of time.
- i) Department wise Vulnerability reports.
- j) Report showing the major vulnerabilities for a given period of 3, 6 or 12 months for broad domain, server, resources, office, department wise etc.
- k) Report will be given in editable (Excel) and non-editable softcopy so that editable can be used in updating compliances by User Department
- l) Report will be given in signed hard copy also.
- m) Presentation on findings of audit will be given to Management by the Auditor within a week’s time of final report submission and should be accompanied by senior consultant for each quarterly audit.
- n) Any other adhoc report as per requirement by the Bank.



- o) Dashboards should be available in respect of the movement of posture of audits during given period based on various parameters.

3.4 RISK MOVEMENT

- a) Overall risk of each Office – High, Medium, Low
- b) Overall risk for Domain and department wise
- c) Risk movement as compared to previous audits – broad category wise.
- d) Will maintain history of all previous audit risks scores 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

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

- a) Bank's IT Policies (ISMS Policy, Cyber Security Framework, Cyber Crisis Management Plan, Business Continuity Policy, IT Procurement Policy and Outsourcing Policy), Risk Based Information Systems Audit Policy and other policies covering IS domain.
- b) External regulations i.e. IT Act 2000, IT (Amendment) Act 2008, RBI Information Security guidelines & recommendations, Banker's Evidence Act, Gopalakrishna Recommendation and any other legal and regulatory requirements by RBI/Cert-In and other regulatory bodies.
- c) Compliance to ISO 27001 standards (or later version) / PCIDSS etc 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 VULNERABILITY ASSESSMENT

Testing should not disrupt the Bank's 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 servers are placed. The same will also be carried out from a selected branch outlet for selected sample critical application/servers.

Appropriate updated commercial tools (e.g. Appscan, Nessus, Accunetix, burp suite, qualys and other duly tested tools/techniques) should be used for each phase of test for increasing the efficiency & effectiveness of audit. Auditor is to ensure that only licensed/proprietary audit tools are used for carrying out all the audit activities, uses of



freeware/shareware shall be avoided and auditor shall inform the details of audit tools in advance.

- a) Vulnerability assessment shall be carried out for all servers, applications, ATM Switch, network equipments, security equipments installed etc
- b) Configurations and Monitoring of logs of IPS/IDS, WAF/DAM, firewalls & other security devices and their response capabilities.
- c) Vulnerability assessment for reviewing the database security setting.
- d) Configuration Audit

Successful Bidder is expected to conduct the audit against the standard configuration document that bank has created, and also against the latest global standards and industry best practices

- 1) Server/OS Configuration Audit
- 2) Networking & Security Devices Configuration Audit
- 3) Database Configuration Audit/ Review

- e) Device Level 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:

- 1) Current network and security posture of the WAN, WiFi Devices.
- 2) Assessment of Network Devices for any security threats
- 3) Checking Configuration of Routers, switches, Firewall, Gateway, Proxy, Security Devices and WiFi Devices
- 4) Rule Review of firewall and other security devices (WAF, SIEM, PIM, ADDM etc)

Locations: Datacenters, DR Sites, NOC, SOC, Swift Centers, Depository, Trade Finance, CTS, Treasury, HO, ZO, CO and any other administrative office would be covered quarterly. Further a onetime DLA for Network and security devices will be conducted for all offices including all branches of the bank (Once in two year audit period).

- f) Secure Code Review
 - g) Configuration Review of Network and Security Devices as regards Baseline configuration/ Hardening Guidelines. Network Devices DLA for branch/ CO/ ZO etc be done on a sampling basis covering particular type/ Make of the device and the observations if any be replicated to all such devices. The DLA review for branches/CO/ ZO etc be done on quarterly basis, such that new devices added if any get covered.
 - h) Application Security Audit
 - i) Application programming Interface security Audit
- The scope defined as above is illustrative but not exhaustive.

4.2 EXTERNAL ASSESSMENT –

Testing should not disrupt the Bank's services. Test cases should not be selected that are destructive. The techniques and the tools used should have been thoroughly tested.

External Assessment - Test at the minimum should cover –



- a) To expose security gaps and demonstrate 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 Research and Verification Scanning
- h) Application Security Assessment/Mobile Security Assessment
- i) Firewall & Access Control List Mapping
- j) Attempt to guess passwords using password-cracking tools.
- k) Buffer Overflow
- l) Malicious Input Checks
- m) Vulnerabilities for defacement and unauthorized modification of corporate web sites.
- n) Search for back door traps in the programs.
- o) Attempt to overload the system using DDOS (Distributed Denial of Service) and DOS (Denial of Service) attacks as and when instructed by the Bank to do so.
- p) Check if commonly known holes/trap doors in the software, especially the browser and the email software exist.
- q) should cover following or LATEST "OWASP Top 10 Web Application Security Risks which are not limited to followings-

- 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

The scope defined as above is illustrative but not exhaustive.

4.3 PENETRATION TESTING (INTERNAL/EXTERNAL)

The objective of the Penetration Testing is to evaluate the security of Organization' s IT infrastructure by safely trying to exploit vulnerabilities of network and applications as well as controls & processes around the networks & applications. Penetration Testing **should include both external testing (outside the network trying to come in) and internal testing (from inside the network).** This may be achieved by conducting both reconnaissance and a comprehensive penetration test. The Penetration Tests should cover but not limited to OWASP Top 10 attacks.

Scope of work for Penetration Testing:



a. Test for threats:-

Man-in-Middle Attack, Brute force Attack, Buffer Overflow, Cross-Site Scripting, SQL Injection, Remote code execution, Directory Traversal etc.

c. Tests for Vulnerabilities that can be exploited:-

Insecure services such as SNMP, Missing patches and versions, default passwords, vulnerabilities based on version of device/server, SQL, XSS and other web application related vulnerabilities, weak encryption, port Scan, SSL Certificate and Ciphers, SMTP related vulnerabilities such as open mail relay, strong authentication scheme, DoS vulnerabilities, sample and default applications/pages, DNS related vulnerabilities such as DNS cache poisoning, information disclosure such as internal IP disclosure, potential backdoors, older vulnerable version etc.

The scope defined as above is illustrative but not exhaustive.

- During the course of Penetration Testing, the personnel of the Audit Firm will exercise due diligence so that the functioning of critical applications of the Bank is not affected adversely causing disruption to business.
- The Penetration Testing should use the industry standard penetration test methodologies (like ISSAF, OSSTMM, ISECOM etc.)
- Penetration testing report should include proof of concept in the form of a screenshot or log, which substantiates the finding and can be useful aid towards remediation.
- In case of any new application launched by the bank during the contract period, IS audit (Vulnerability Assessment, Penetration Testing, and APPSEC etc) is to be conducted on UAT as and when required within Bank's prescribed timeframe without any additional cost to the Bank.
- External Penetration Testing should include all the Public facing Assets (Approx 350 Public IPs/ URLs) of the Bank

4.4 Process Review Audit:

Assess whether the data processing that takes place in systems and IT occurs in a controlled environment, supporting data CIA triad (Confidentiality, Integrity, and Availability). Review of all associated Policy and Procedures against standard Global; Best Practices/RBI norms

Scope includes detailed assessment of the following:-

- Audit of controls over operations including communication network, data preparation and entry, production, file library, documentation and program library, Help Desk and technical support, capacity planning and performance, Monitoring of outsourced operations etc.
- SDLC - Application Security Framework to be followed for customizations done to the Software.
- Verify adherence to Legal & Statutory Requirements.
- Segregations of Roles/Responsibilities.
- Review of documentation for formal naming standards, design process of job roles, activity, groups, profiles, assignment, approval & periodic review of users,



assignment & use of Super user access.

- Review of coverage of UAT test cases.
- Restart/Recovery/Backup & Restoration procedures
- Controls implemented in the system for :Input/Output and Processing Functionality
- Logical Access Controls - Review all types of Application Level Access Controls including proper controls for access logs and audit trails for ensuring Sufficiency & Security of Creation, Maintenance and Backup of the same. Only authorized users should be able to edit, input or update data in the applications or carry out activities as per their role and/or functional requirements
- Accuracy of event logging, adequacy of Audit trails.
- Interface controls - Application interfaces with other applications and security in their data communication.
- Authorization controls such as Maker Checker & Exceptions etc.
- Data integrity & File Continuity Controls
- Assess controls for user maintenance, password policies are being followed and as per bank's IT& IS security policy.
- Assess controls for segregation of duties and accesses of production staff and development staff with access control over development, test and production regions.
- Review of all types of Parameter maintenance and controls implemented.
- Change management procedures.
- Capacity Management Assessment. (hardware and software).
- Ownership of generic IDs if any, is clearly established and accountability can be fixed in case of lapses/misuse if any.
- To check whether generic user IDs can be replaced with individual user IDs.
- Identify gaps in the application security parameter setup in line with the bank's Security policies and leading best practices
- Audit of management controls including systems configuration/ parameterization & Systems development.
- Security configuration of desktops used by department users to ensure Active directory services are properly implemented (on sampling basis a max of 10%).
- Identification of Potential Data Leakage sources and its mitigation.
- To carryout of sample audit of branches for ensuring various branch level/user level controls are in place. Sample audit of branches to be decided by Bank which will cover various geographical area, types of connectivity being used .The scope is not limited to followings
 - a) Verification of Branch inventory and its asset list
 - b) LAN connectivity usage of Internet as per the Bank policy
 - c) Anti Virus signature update/distribution of desired patches on the endpoints
 - d) Implementation status of Network access control
 - e) User integration status of active directory
 - f) SWIFT related controls such as VLAN segregation in line with SWIFT guidelines.

The assessment points mentioned above is illustrative but not exhaustive and should be done in consonance with standards like ISO 27001, PCIDSS, legal & regulatory



requirements, Bank's current IT, IS & Cyber Security Policies and global best practices.

4.4.1 INTERNET BANKING, MOBILE BANKING, MOBILE APPS, MOBILE APPLICATION SYSTEM AND OTHER ALTERNATE DELIVERY CHANNELS

- a) Detailed review of the Internet Banking, Mobile Banking and other ADC (alternate Delivery Channels) like Mobile Apps (both iOS and Android), IMPS, UPI, Wallet, eAadhaar etc. for application security vulnerabilities against industry global standards such as OWASP, PCIDSS etc and assessment of security architecture vis-à-vis the RBI and other regulatory guidelines.
- b) Bank's internet, mobile banking, Mobile Apps & other ADCs product line, transaction flow.
- c) Those adequate internal controls are in place to minimize errors, discourage fraud.
- d) Security Assessment of Interfaces (i.e. API etc) with other organizations for utility payments & other purposes etc.
- e) Security Assessment of Interfaces (i.e. API etc) with other applications.
- f) Review Process of creation/management of internet & mobile banking IDs / 3D security management / 2nd factor authentication / IBS Shield etc as additional security features.
- g) PINS/Password management
- h) Authentication controls
- i) Applications Security & Control Review
- j) Review to ensure strong access control measures & Confidentiality in the transmission, processing or storing of customer data.
- k) Process of Creation/Activation/Resetting/Delivery of M-PINS in Mobile Banking.
- l) Review of Reconciliation process and suggestions if required.
- m) Check adequacy & adherence to operational / accounting/ reconciliation/statutory guidelines issued by RBI & other regulatory bodies w.r.t mobile banking, Internet Banking and other ADC (alternate Delivery Channels) like Mobile Apps, IMPS, UPI, Wallet etc.
- n) Perform automated and manual tests like HTML source code Analysis, SQL injection, Session Hijacking, LDAP Injection, Authentication Bypass etc.
- o) Perform analysis/Verification of audit logs / Audit trails of transactions, Exception List, Incident management report etc.
- p) In respect of Branch audits (device level audits), the auditor should do the Audit of sample number of branches and provide a template for automated capture of information related to the audit from various other branches. The parameters to review based on actuals received and corrective action should be recommended.

5.4.2 OPERATING SYSTEM (OS)

- a) Set up and maintenance of operative system parameters.
- b) All the Security features available in the OS are enabled/taken advantage of as far as possible.
- c) Vulnerabilities in OS are being taken care of. Compensatory controls for known vulnerabilities are in place.
- d) Security configuration of devices with respect to OEM latest released relevant patches and software versions.



- e) Changes in system software are controlled in line with the organization's change management procedures. Proper record is maintained and authenticated regarding installation, its up-gradation, re-installation and maintenance.
- f) Use of sensitive system software utilities is in controlled manner and it is monitored and logged.
- g) Root and sensitive passwords are used in controlled manner. Their use is logged and monitored.
- h) Performance, scalability, availability and check for unnecessary services.
- i) Patches and new versions are updated as and when released by OEM/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
- j) Review of availability and performance requirement of applications (including web based) i.e. availability of IT components/applications, response time of application, restore time for problems etc.
- k) Review of Generic User.
- l) Logging and Auditing

4.4.3 SOFTWARE

- a) Release of software is governed by formal procedures ensuring sign-off through testing, IT Balance Score Card & Service Validation handover etc.
- b) Review of change control activities, including SRS/Testing etc. are appropriately taken by the change control committee.
- c) All requests for change are assessed in a structured way for all possible impacts on the operational system and its functionality are reviewed.
- d) Impact analysis of changes made.
- e) Check for the latest supported version of the security patches for the application versions used in the Bank and the observations should be in respect of the same.
- f) Associated documents and procedures are updated accordingly.
- g) 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.
- h) Access log is monitored.
- i) Multilevel/Duplicate / Generic access ID in the system.
- j) Audit trail / Audit log generation and management.
- k) Communicating users with new features during version upgradation.
- l) Regular updation of job cards with new version releases.
- m) Secure Code Review
- n) Code obfuscation
- o) If outsourced, escrow arrangement with application owner.
- p) Media of the Applications should be present in the Software Library.
- q) Data Dictionary updation
- r) Escrow assurance
- s) Static analysis of code
- t) Application Security Framework standards are adhered.
- u) Business logic flaws, if any.



4.4.5 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) Database configuration Audit/review.
- f) 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, authenticity and availability are taken as per IT Security Policy.
- g) Logical access controls which ensure the access to data is restricted to authorized users
- h) Confidentiality and privacy requirements are met.
- i) Authorization, authentication and access control are in place
- j) Segregation of duties is ensured for accessing data.
- k) Purging policy-procedures of Data Files.
- l) 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.
- m) Protection of Sensitive Information during Transmission and Transport.
- n) Rotation of duties.
- o) Review of controls procedures for sensitive DB passwords.
- p) 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.
- p) Audit of Application Databases/ Review.

4.4.6 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 (t-1) basis.
- (c) Monitoring procedures effectiveness for branch level client's updations.
- (d) Antivirus rules/policy review as per Global st practices /RBI Guidelines.
- (e) Assurance on release of patches by various osd vis-a-vis implementation status on desktops/pcs/servers/systems and submit a gap analysis report.
- (f) Ensuring Organization units are created as per the business requirement and users are authenticated through active directory system.
- (g) BCP on ad system, back up and its resilience.

4.4.7 OUTSOURCING

- 1. Compliance of Bank's Outsourcing Policy.
- 2. Compliance of Bank's Acceptable Usage of IT Policy. -,



3. Review of Coverage of confidentiality clause and clear assignment of liability for loss resulting from information security lapse in the vendor contract.
4. Review of financial and operational condition of service provider with emphasis to performance standards, confidentiality and security, business continuity preparedness.
5. Review of SLA and NDA with vendors.
6. Review of access provided to third party contractors working onsite.
7. Responsibility and liability of vendors as defined according to Information Security policy and procedures of the Bank.
8. Service Level Agreements (SLAs): Audit of SLA management for all kinds of services like Data Centre, DR site, ATM Switch, Internet Banking, Physical Security, Facility Management, etc.
9. Monitoring of vendors activities as per SLAs.
10. Review of formal agreements which takes care of all the risks associated with outsourcing.
11. Compliance with RBI guidelines as per circular no. DBOD.NO.BP. 40/ 21.04.158/ 2006-07 dated 3rd November, 2006 and circular no DBS.CO.PPD.BC. 5 /11.01.005/2008-09 dated 22nd April, 2009.
12. If vendor uses their own systems to access Bank's data, either working from Bank's premises or from their (vendor organization) remote locations, following points needs to be audited:

- Outsourced Vendor Audit

- Services provided by vendor to Bank.
- Customer, employee, & company data and information the vendor has access to.
- Usage of Bank's data/information by vendor.
- Data/information processing & storage by vendor.
- Process to transfer data to and from the vendor.
- Process to destroy data and information shared with vendors.
- Information security policy of the vendor organization.
- User registration and de-registration process of vendor organization.
- User access review process of vendor organization.
- Vendor's procedures for provisioning, monitoring, and management of privileged user accounts.
- Controls to restrict access to vendor organization's internal network.
- Employee background verification process of vendor organization.
- Periodic Information security awareness training conducted by vendor for their employees.
- BCP/DR review
- Process for returning assets upon exit of employee from the vendor organization.
- Detection, prevention and recovery controls of the vendor organization to protect against malicious or unauthorized code and software.
- Network security controls of the vendor organization to protect itself from threats.
- Patch management process of vendor organization.



- Usage of any End of Life (EoL) unsupported operating systems (including but not limited to WinXP, Win 2000, Win 2003, SQL Server).
- Incident management process of vendor organization.

4.4.9 BUSINESS CONTINUITY

- Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) and their adequacy and effectiveness w.r.t BCP/DR framework.
- Comprehensive review of the BCP arrangement for all critical applications.
- Perform one to one mapping of DR and DC equipments (servers, network, security devices) with respect to configuration, OS version, patch updates.
- Report deviations (if any) in (b) above and risk associated with it.
- Specify events which could restrict successful shifting to DRS in case of any disruptions at main site.
- Restoration of backup at DRS
- Review of BIA process (RTO/RPO).
- Time delay in transmission and restoration of daily data at DRS.
- Backup storage – system and data
- Offsite storage and movement of backups.
- Data Backup – periodic media verification for its readability.
- Successful bidder shall depute an audit team at DC and DRS during drill and oversee actual execution.(every quarter)
- Comment on success of Drill exercises.
- Evaluate timely review of BCP guidelines.
- DR Plan Review.
- Check adherence to operational/statutory guidelines issued by RBI & other regulatory bodies w.r.t BCP.
- Compliance with Bank's Disaster Recovery Plan aspects
- Log shipping management
- BCP manual, including Business Impact Analysis, Risk Assessment and DR process.
- Implementation of policies
- Back-up procedures and recovery mechanism using back-ups.
- Storage of Back-up (Remote site, DRS etc.)
- Redundancy – Equipment, Network, Site etc.
- DRS installation and Drills - Management statement on targeted resumption capability (in terms of time required & extent of loss of data)
- Evidence of achieving the set targets during the DRS drills in event of various disaster scenarios.
- Debrief / review of any actual event when the DR/BCP was invoked during the year

4.4.9 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 and review.



- c) Checking for unauthorized software
- d) Software storage controls
- e) License management

4.4.10 HELP DESK

- a) Help desk facility which provides first-line support and advice
- b) Escalation matrix and its assessment
- c) Prioritization of reported problems.
- d) Timely resolution of reported problems
- e) That problems and incidents are resolved, and the cause investigated to prevent any recurrence
- f) Incident handling
- g) Trend analysis and reporting
- h) Development of knowledge base
- i) Root cause analysis
- j) Problem tracking and escalation with proper documentation
- k) Audit trails of problems and solutions

4.4.12 STORAGE MANAGEMENT

Review of all associated Policies and Procedures related to storage management including purging of data against standard Global; Best Practices/RBI norms.

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

4.4.13 MEDIA STORAGE:

- a) Check for assignment of responsibilities for media (magnetic tape, cartridge, disks and diskettes) library management backup
- 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.
- e) Review of all associated Policies and Procedures related to storage management including purging of data against standard Global; Best Practices/RBI norms.



4.4.14 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.
- c) Protections of records from loss, destruction and falsification in accordance to statutory, regulatory, contractual and business requirements.

4.4.15 CTS (Cheque Truncation System)

- a) Detailed review of the CTS architecture vis-à-vis the RBI guidelines.
- b) Review on internal controls in place to minimize error & frauds.
- c) Interface with CBS & other applications.
- d) Authentication Controls.
- e) Review of the work flow.
- f) Vulnerability/Threat Assessment.

4.4.16 MAIL MESSAGING SYSTEM AUDIT

The Mail messaging audit shall cover following aspects:-

- a) Overall Mail Messaging System Managements including DLP solution
- b) Architecture & design review of mail messaging system.
- c) Performance of Mail Messaging Servers.
- d) Configuration Audit for all servers, Network devices (Router, Firewall, Switches) used in Mail Messaging system.
- e) Impact analysis of mail servers.
- f) Assessment of capacity management.
- g) Review of passwords policy and inactive users

4.4.17 Security Operations Centre

- a) Detailed Review of SOC infrastructure/implementation/ architecture vis-à-vis the RBI guidelines and global standards.
- b) Review of SOC processes.
- c) Review SLA Management process for SOC
- d) Review the configuration parameters of all SOC security devices and provide relevant recommendation, if required.
- e) Review of adequacy of staff
- f) Review of reporting responsibility and periodicity of report
- g) Review of information sharing by bank's DC/DR team without source service provider team.
- h) Review of work authorization system between outsource service provider and bank's team
- i) Access Control, Customer Data Privacy & Confidentiality



- j) Review of logs of different security devices and its compliances.
- k) Verification of necessary logs from all the critical systems such as webserver /database system/OS/Firewalls/Router/NTP/ATM switch
- l) Ensuring extraction of sample audit logs from the systems as per the retention policy of the Bank/regulatory guidelines.
- m) Real-time view of audit logs to ensure real-time monitoring of incidences.

4.4.18 ATM Switch Application, interfaces, process review

- a) ATM Switches System security review including VAPT. , Audit of ATMs/CDMs/BNAs on sample basis
- 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 (Including API),.
- e) Business Continuity Plan including BIA
- f) Maintenance of manual records.
- g) Process review audit of ATM center management at Bank's identified location (Presently DBD-HO at Delhi & other locations mentioned above) 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.
- h) Review of prognosis.
- i) Assessment of banks interfaces (Including API), with ATM switches
- j) Status of required certification as per international as well as regulatory stipulations.
- k) Audit of network and application architecture.
- l) Audit of transaction storage and transmission controls.
- m) Audit of transactions monitoring process, queue management, load balancing.
- n) Physical security of infrastructure.
- o) Secure configuration review of ATM switch infrastructure - servers, databases, etc.
- p) Review of HSM (Hardware Security Model) management process.
- q) Sensitive data storage and transmission (controls for card holder data protection).
- r) User management review, Vendor management.
- s) Patch management process review.
- t) Encryption and transmission of data across networks.
- u) BCP & DR framework along with backup process.
- v) Secure development and coding process.
- w) Transaction monitoring and fraud risk monitoring process.
- x) Helpdesk review.
- y) Any other controls as per PCI DSS standard.
- z) ATM switch application interface with CBS, NPCI, VISA, Mobile Banking, IB, MCT etc.
- aa) Review of transmission of information between CBS and ATM switch setup.
- bb) Change Management Process.
- cc) TMK, ZMK, CVK etc along with implemented encryption.



- dd) Ensuring encryption used in transactions/communication/pin generation at the appropriate level in line with industry best practices.

4.4.19 MANAGING FACILITIES

- a) Physical surrounding which protects the IT equipment and people against man-made and natural hazards.
- b) Installation of suitable environmental & physical controls and Surveillance System which are regularly reviewed for their proper functioning.
- c) Closed circuit television system (CCTV) area for monitoring entry/exit points and strategic locations within the server room.
- a) Environmental threat protection
- b) Access to facilities.
- c) Personnel health and safety.
- d) Preventive maintenance policies.
- e) Uninterrupted Power Supply – its placement, maintenance, capacity etc.
- f) Electrical fittings
- g) Data Center Infrastructure- Network cabling, raceways, server/communication racks, rack power distribution unit.
- h) Fire Protection
- i) Insurance
- j) Inspection and escalation policies
- k) Check for various Audit compliance (Fire drills, Electric audit etc)

4.4.20 MANAGING OPERATIONS and CORE BANKING SOLUTION (CBS)

- a) IT support functions are performed regularly and in an orderly fashion.
- b) Operational procedure for Data Center, Zero Data Loss Site and DRS.
- c) Reviews of Admin (OS/DB etc) user activity log.
 - (i) No. of Admins
 - (ii) Activity Logging, authentication and monitoring.
- d) Review of parameter maintenance process and controls implemented therein.(To be checked on Sample basis)
- e) User management
- f) Day begins and Day end process in CBS.
- g) Reviews of console log activity during system shutdown and hardware/software re initialization.
- h) Review of operator log to identify variances between schedules and actual activity.
- i) Monitoring of system performance and resource usage to optimize computer resource utilization.
- j) Personnel scheduling - Shift hand-over process
- k) Coordination with change, availability and business continuity management
- l) Preventive maintenance.
- m) Automated operations documentation.
- n) Interface controls over other applications interfaced with Finacle i.e. ATM, Online Bills/Tax payments, Internet Banking, RTGS, SFMS, and Credit Card etc.
- o) Cryptographic Controls.
- p) Use of Internet in Data Center & DRS.
- q) Data Masking



- r) Review of control mechanism ie(Maker-Cheker, Segregation of Duties, rotation of duties)

4.4.21 HARDWARE

- a. Hardware acquisition, installation, usage and disposal procedures. Disposal Procedure Review as per global best practices /RBI Norms.
- 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.
- g. Adequacy of storage and scalability.

4.4.22 NETWORKING & SECURITY EQUIPMENTS:

- Selection of Router, Firewall, Proxy, Intrusion Prevention System, Switch, Modems and other Network and Security equipments 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, VPN 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.
- Firewall rule based review.
- Integration of various extranets with Bank's network
- Current network & security posture of the WAN architecture & WiFi environment
- IP Addressing schemes and their allocations
- Physical & Logical Separation of the Networks
- WiFi, WAN, Network & Security Products & technologies deployed – Their adequacy.



- IP Sec implementation.
- Network bottlenecks & performance issues.
- SLAs with third parties & monitoring of key performance indicators by bank.
- Scalability & Robustness of Network.
- Availability and quality of system documentation.

4.4.23 NETWORK MANAGEMENT

- a. Overall Network management.
- b. Complete review of Network design and architecture – provides scalability, redundancy etc.
- 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, MPLS 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.
- f. Whether logs connected with Network Incident management received from Security Operation Center are being analyzed effectively and action taken (if required).
- g. Review of IPV6 implementation in the Bank.
- h. Ensuring snmpv3 is implemented, encryptions with highest standard are used .

4.4.24 Cyber Security Audit:

The detailed scope of the same are depicted below:

- a. Detailed review of the Cyber security architecture vis-à-vis the RBI guidelines.
- b. Test should measure a device's ability to protect a host by sending strikes and verifying that the device successfully blocks the attacks.
- c. To ensure the always-on user experience in the midst of complexity and exploding traffic volume.
- d. Review RTO & RPO of critical business applications in line with Bank's Policy (BIA).
- e. Review of rules in SIEM/ DAM/ PIM/ AD/ AV and all other SOC devices
- f. To generate real-world legitimate traffic, distributed denial of service (DDoS), exploits, malware, and fizzling at the same time and from the same port combined with full control of the load capacity.
- g. To measure and harden the performance, security and stability of Application Delivery Controllers (ADC), anti-DDoS applications, next-generation firewalls, next generation IPS devices, SMTP Filter (Mail Gateway) and other deployed equipment with up to the available real world throughput by injecting of real-world application, attack, and malformed traffic. The attack scenario may be designed for each of the deployed security component like several of DDoS related traffic to be injected for Anti DDoS system. The various types of malformed emails such as spoofing emails, emails



- containing malicious attachment to be generated to measure the preparedness of the deployed systems.
- h. Ensure all the devices hosted in DC/DR/ **branch systems (user pc/network equipment)** are sync with NTP server.
 - i. To review the parameter setting of above deployed equipments and ensure appropriate controls are in place.
 - j. Perform the License review of under scope equipments/systems. Perform annual analysis on deployed IOS/ Firmware version vis-a-vis latest stable version released by OSD/OEM. IS Auditor has to analyze applicability of new version w.r.t Bank's environment.
 - k. Ensuring latest version of TLS 1.3 with modern cipher is being used at public facing application as part of perimeter controls.
 - l. Assurance on deployment of cloud security on systems hosted in clouds.

4.4.25 REGISTRATION AUTHORITY

- a) Audit of all RA functions
- b) Compliance to the requirements of Chief Certifying Authority (CCA)/ IT act 2000 & 2008, Rules and Regulations.
- c) Compliance of RA functions as per CA (Certified Authority) checklist.
- d) Reconciliation of digital signatures issued/ revoked by RA with CA
- e) Digital Certificates details/record maintenance as per CA requirements.
- f) Issuing certificate to CCA for compliance as per CA checklist.
- g) SSL / TLS Certificates/ self generated certificate deployment policy and thorough Assessment of Internal Certificate Issuing Server

4.4.26 SWIFT CENTER REVIEW

- Data Center controls related to SWIFT systems (DC and DR)
- Access controls, Authentication framework
- Application Registration Controls
- IT Architecture Audit - related to SWIFT Transaction processing
- Incident and Change Management
- Audit for OS Security baselines and Application Security Controls
- Review of Firewall rules and Network security/ Management controls of all other interfacing systems including CBS
- Network Security controls of SWIFT infrastructure
- Disaster Recovery and Business Continuity Process
- Compliance in line with Bank's RTO and RPO
- Version Control and Change Management Process
- Scalability and Availability
- IT Operations for SWIFT related Applications
- Log monitoring process pertaining to SWIFT Infrastructure, assurance on log manipulation, Ensure logs cannot be manipulated /deleted by third party including administrator of the system.
- Application Security Review of SWIFT Infrastructure
- Arrangements for source code review
- Review of Risk Assessment and suggest mitigation measures for the identified service
- VAPT of OS, Database and Network devices



- Review of SWIFT architecture including VPNs hosting SWIFT Alliance access, Payment validation (AML and suspicious transactions) engine.
- Perform malware analysis of memory of important systems
- Control assessment at the key entry points for malware
- Review of malware Incident Management and Response
- Active scanning of the target hosts to identify any malware infections
- SWIFT certificate / SSL review
- Encryption of data in static / transmit mode
- Review of outsourcing arrangement (SLA) vis-a-vis industry standards
- Review of Firewall internal/ external rules w.r.t. SWIFT
- Antivirus scanning on servers and user PCs
- Review of security controls / Management controls of all other interfacing systems including CBS
- Arrangements for Anti-phishing/ takedown of rogue applications
- Review of Standard Operating Procedures
- Review of Middleware between systems
- Review of Fraud Risk Management System related to SWIFT activities/ functions
- IT General controls review
- Creation, approval of SWIFT transaction process in Core Banking
- Control at pre-transmission stage (i.e. before sending payment messages to Bank with which Nostro Account is maintained)
- Controls post transmission of payment messages
- Review of Nostro Reconciliation Process
- Review of operations carried out by Trade Finance Team
- Review of various SWIFT related activities/ functions carried out by domestic branches
- To comply with SWIFT Customer Security Program - Guidance given by SWIFT covering 16 mandatory and 11 advisory controls of SWIFT customer security controls framework
- Compliance audit post ATR submitted by the Bank on remediation of the identified gaps.
- Application security assessment based on standards like OWASP Top 10, etc.
- Functionality review of SWIFT systems
- Validation of financial parameters, etc.
- Assessment of gaps in implementation of policies
- Compliance to the legal/regulatory guidelines.
- Controls and implementation of advisory/circular issued by RBI/SWIFT system to strengthen the SWIFT infrastructure.

4.4.27 Migration Audit

- a) Review of Data Migration strategy/methodology followed by the Bank. Review of data mapping performed by the Bank.
- b) Review of Data Migration tools/scripts configured/developed by Bank.
- c) Review of data validation performed by the Bank.
- d) Review of logs of data migration activity and the identified errors in accuracy, integrity, conformity and completeness of data reconciled and uploaded into Target System and whether they have been rectified by Bank.



- e) Review of appropriate data integrity checks like batch totals, check digit totals, number of records & other value parameters.

4.4.28 Privacy and Data Protection

Privacy and Data Protection Audit shall cover following aspects:--

- a) Controls established for data conversion process
- b) Information classification based on criticality and sensitivity to business Operations
- c) Fraud prevention and Security standards
- d) Isolation and confidentiality in maintaining the records of Bank's customer
- e) Information, documents, records by banks
- f) Procedures for identification of owners
- g) Procedures of erasing, shredding of documents and media containing sensitive information after the period of usage.
- h) Media control within the premises.
- i) Aadhaar authentication infrastructure

4.4.29 Review of IT Management Tools and IT Processes

The review of IT Management tools and Processes should cover but not limited to following aspects:--

- a) S D L C and Change Management
- b) Incident Management
- c) Network Management
- d) Backup & Media Management
- e) Help Desk
- f) Escrow assurance
- g) Vendor & SLA Management
- h) Asset Management
- i) Enterprise Management System
- j) IT Governance
- k) Cyber Security Management Plan
- l) Anti-Virus Management
- m) Implementation of Active Directory & Desktop Management (ADDM)
- n) Implementation of INFORMATION RIGHTS MANAGEMENT (IRM)
- o) Review of DC-DR Replication
- p) Patch management system
- q) DMS
- r) SSL Certificates deployment and thorough Assessment of Internal Certificate Issuing Server

4.4.30 WIDE AREA NETWORK AUDIT/ DEVICE LEVEL 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:

- 1) Checking Configuration of Routers, switches, Proxy, Gateways, WiFi Devices etc
- 2) Current network & security posture of the WAN architecture & WiFi environment
- 3) IP Addressing schemes and their allocations
- 4) Physical & Logical Separation of the Networks
- 5) WiFi, WAN, Network & Security Products & technologies deployed – Their adequacy.
- 6) IP Sec implementation.
- 7) Network bottlenecks & performance issues.
- 8) Study of Inter-operability of CO/ZO LANs with Corporate WAN.
- 9) Availability of the Network and capacity management review.
- 10) SLAs with third parties & monitoring of key performance indicators by bank.
- 11) Scalability & Robustness of Network.
- 12) Entire administration of the Network Management tools & EMS.
- 13) Availability and quality of system documentation.
- 14) Integration of various extranet with Bank's network.
- 15) Firewall rule review.

4.4.31 DATA GOVERNANCE:

1. Review of existing Data Classification
2. Perform data risk Assessment to access security looping from where data can get leaked.

4.4.32 Policy, Process and Procedure Review:

- Information Security Policy
- Cyber Security Policy
- Data Privacy Policy
- Integrated Risk Management Policy
- Fraud Risk Management Policy
- Operational Risk Management Policy
- Cyber Crisis Management Plan
- IT Policy
- Business Continuity Plan & Disaster Recovery Policy
- Information/Cyber Security Processes, Procedures & Guidelines.
- IT Processes, Procedures & Guidelines
- Review of Information Security/Cyber Security vis-à-vis RBI Circular on Cyber Security Framework
- Review of preparedness of the Bank vis-à-vis RBI Circular on Cyber Security Framework in Banks.
- Vetting of Self-assessment of gaps vis-à-vis Baseline Security & Resilience Requirements.
- Review of IT infrastructure from the point of view of Information/Cyber Security
- Review of the Current Security Architecture and Security Technology of the organization.



- Review Vulnerability Assessment [VA] and Penetration Testing [PT] for Servers and Network/Security devices, Application Security Testing [Web and Mobile App Sec] being done for the bank.
- Incident Management review in which IS auditor should review whether Incidents are managed, monitored and reported as per the RBI guidelines or other regulators like Cert-in, NCIIPC etc.
- Review Secure Configuration Documents adopting best practices for Servers OS, Web application, Database, Security Devices, Network Devices, Desktops, Laptops, Mobile devices etc.
- Review of Network Security including various wireless technologies, Security Design, Access Control, etc.
- Review of the existing network topology/ Network Security Architecture and deployment of the security controls within the organization like Firewalls, IDS/IPS, DDoS, network segmentation, NBAD, WAF, Mail Gateway, Patch Management, Active Directory (AD), AV, SIEM, PIM, DAM, Anti APT etc.
- Review of access rules (ACLs) of network & security devices.

4.4.33 REGULATORY/COMPLIANCE AUDIT:

The following are the regulatory/compliance audits as required by RBI/NPCI/UIDAI/SEBI and other regulatory bodies. The complete scope and requirements for said audits will be as per their respective regulatory body guidelines/circulars as applicable on the date of audit.

Further, the compliance certificate has to be submitted by the auditor for these audits.

1. Pre Paid Instruments Audit(PPI) as required by RBI
2. Aadhar Based operations and system of bank(Compliance with UIDAI requirements)
3. System and application Audit of UPI Services as required by NPCI.
4. PCIDSS Audit of credit card
5. Annual IS Audit of Depository Services
6. Any Other Regulatory /Compliance Audit as required to be complied by the bank.

4.4.34 IT General Controls Review:

The IS Auditors shall assess the data processing that takes place in systems and IT occurs in a controlled environment, supporting data integrity and security and the need of complying with local laws and their requirements relating to information security.

The scope of work for IT General Controls Review:

- Change Management Review
- User Access management
- Backup Management
- Incident Response Management
- Observing DR Drill Activities
- Integration of system servers, devices with PIM



- Others (Audit logging and review mechanism, Patch Management, Antivirus Management etc.

4.4.35 Access Control and Change Management:

- Review of access control process for Bank's employee/SI/Vendor/Contractor to any BANK assets including DC/DR/NLDC and other locations as per Information Security Policy of BANK, RBI/other regulatory guidelines & industry best practice.
- Review of Change management process for IT assets including applications, H/w, Network & security solutions etc.

4.4.36 Audit Findings and Reports:

Risk analysis along with Risk Matrix with scoring model should be submitted as part of audit findings. Deliverables under the IS Audit – the Service Provider will deliver detailed reports as below:

The following reports are an indicative that should be covered for the area-wise auditing-

- IS Audit (Technical & Process) Report of all the areas covering the objectives, efficiency and effectiveness
- Presentation to the Top Management of the findings of the Reports
- Risk Analysis Report
- Recommendations for Risk Mitigation

4.4.37 IT Support & IT Asset Management:

- Utilization monitoring – including report of prior year utilization
- Capacity planning – including projection of business volumes
- IT (S/W, H/W & N/W) Assets, Licenses & maintenance contracts
- Insurance
- Disposal – Equipment, Media, etc.

4.5 SECURITY CUM FUNCTIONAL AUDIT OF NEW APPLICATIONS

Security cum Functional Audit will be done before GO-Live for New in-house developed application/ After Major Changes in existing applications (both in-house and developed by external vendors). Scope of Security cum Functional Audit include:-

- Functionality implemented vis-à-vis the Bank's requirements.
- Input, processing and output controls across various schemes across the bank.
- Coverage and adequacy of UAT test cases.
- IS Audits i.e. Vulnerability Assessment, Penetration Testing, External Assessment, Configuration Audit, Data Migration Audit, Application security Audit etc.
- Controls for performing/changing parameter setup of functionality across applications.
- Through-put validation
- Automated batch processing, scheduled tasks, critical calculations etc
- IT General Control Review
- In case of web based application, the validation against top 10 OWASP vulnerabilities.



- Regular updation of job cards with new version releases.
- Checks against network attacks
- Code Review, wherever possible
- Code obfuscation
- Application Security & Controls Review
- Database Security & Integrity Review
- Review of Interface Controls with other applications (both Internal and External)
- Review of Network & Communication Controls with relation to the application package
- Test of robustness of the system by running a specific number of transactions on it
- Evaluation of Efficiency & Effectiveness of the package vis-à-vis business processes and requirements. Whether the objectives of the application are likely to be fulfilled by implementation.
- Assessment of the risk component in the package
- Compliance testing of the changes in software made for mitigation of the discrepancies pointed out in the audit report
- Availability of necessary audit logs and its accuracy and effectiveness.
- Integration with Delivery Channels including data and transaction integrity for the same.
- Suggestions for mitigating the risks.
- If outsourced, escrow arrangement with application vendors.
- Regulatory compliance (Any compliance with regards to regulatory guidelines).

4.6 Forensic Audit/ Forensic Analysis/Investigations: Bank may assign Forensic Analysis/Investigations as per the requirement, same to be conducted as by adhering following minimum guidelines:

- a. The bidder should have well established procedure for conducting Forensic Analysis/Investigation and the same shall be provided to Bank.
- b. The original evidence should be acquired in a manner that protects and preserves the integrity of the evidence and examination of the evidences should be done in the copy of the original evidences.
- c. Persons conducting an examination of digital evidence should have suitably trained and should have sufficient experiences.
- d. Activity relating to the seizure, examination, storage, or transfer of digital evidence should be documented, preserved, and available for review.
- e. The process or lifecycle of doing forensics should be followed as per the Industry best practice and regulatory guidelines.
- f. The bidder shall provide their findings with recommendations in report format as per the incidence investigation process.
- g. Bidder should arrange to deployment of forensic team within 1 hours of reported incidences.

The above scope is illustrative and subject to change as per the requirement of the Bank and may vary on case to case basis.

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 Network 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.
- h) Incorporation of Secure Code practices across Bank's applications.

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.



Annexure – B

Performance Guarantee Form

Date:

To,
The Dy. General Manager
IS Audit Department
Inspection and Audit Division
Punjab National Bank, Head Office
Plot No 5, Institutional Area
Sector 32, Gurgaon- 122001

Dear Sir,

PERFORMANCE BANK GUARANTEE – RFP FOR APPOINTMENT OF IS AUDITOR FOR IS AUDIT AND SECURITY CUM FUNCTIONAL AUDIT OF APPLICATION SOFTWARES.

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 10% of the Contract Price of Rs..... (in words and figures), as per the said 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. 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.
- IV. 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.
- V. 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.
- VI. 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.
- VII. 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.
- VIII. 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).
- IX. 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.
- X. 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.
- XI. 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.



- XII. 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 toand
- 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 (c) 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.....2020.....

Yours faithfully,

For and on behalf of theBank,

(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

Technical BID FORM

Date:

To,
The Dy. General Manager
IS Audit Department
Inspection and Audit Division
Punjab National Bank, Head Office
Plot No 5, Institutional Area
Sector 32, Gurgaon- 122001

REG: RFP FOR APPOINTMENT OF IS AUDITOR FOR IS AUDIT AND SECURITY CUM FUNCTIONAL AUDIT OF APPLICATION SOFTWARES

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 Declaration" in the required format 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 25% 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 2020

(Signature and the capacity of the person duly authorized to sign Bid for and on behalf of)



Annexure – D

Commercial BID FORM

Date:

To,
The Dy. General Manager
IS Audit Department
Inspection and Audit Division
Punjab National Bank, Head Office
Plot No 5, Institutional Area
Sector 32, Gurgaon- 122001

Dear Sir,

REG: RFP FOR APPOINTMENT OF IS AUDITOR FOR IS AUDIT AND SECURITY CUM FUNCTIONAL AUDIT OF APPLICATION SOFTWARES

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

S No	Particulars	Yearly Cost, Amount including all expenses excluding GST (A)	Weightage(B)	Weighted Yearly Cost (A*B/100) (C)
1	Regular IS Audits (Defined in clause 2)	XX	70	XX
2	SECURITY CUM FUNCTIONAL AUDIT OF New in-house developed application/ After Major Changes in existing applications (both in-house and developed by external vendors) (150 Applications per year)	xx	30	xx
3	Total Weighted Yearly Cost Rs (1+2) (in figures)			xx
	Total Weighted Yearly Cost Rs (1+2) (in words)			XX



We hereby understand and declare that the commercial evaluation will be done on the basis of Total Weighted Yearly Cost, while

- Payment for assignment under S.No 1 will be on the basis of payment terms given in section 4.8 of the RFP.
- Payment for assignments under S.No 2 will be on rate contract basis for the actual work done, i.e. actual number of functional audits conducted.

We understand that these yearly prices will be applicable for minimum 2 years (extensible by 4 quarters at the discretion of the Bank). 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, 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 Declaration" in the required format are furnished with this bid form.

We further undertake, if our bid is accepted, to conduct Information System Audit in accordance with the said bidding document.

If our bid is accepted, we will obtain the guarantee of a bank in the form prescribed by you for a sum equivalent to 25% 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.

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.

Dated this day of 2020

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



Annexure –E

Undertaking- 1

To,

Date

The Dy. General Manager
IS Audit Department
Inspection and Audit Division
Punjab National Bank, Head Office
Plot No 5, Institutional Area
Sector 32, Gurgaon- 122001

Dear Sir,

REG: RFP FOR APPOINTMENT OF IS AUDITOR FOR IS AUDIT AND SECURITY CUM FUNCTIONAL AUDIT OF APPLICATION SOFTWARES

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.

Dated at _____ this _____ day of _____ 2020

(Signature and the capacity of the person duly authorized to sign Bid for and on behalf of)



**Annexure –F
Undertaking -2**

Date:

To,
The Dy. General Manager
IS Audit Department
Inspection and Audit Division
Punjab National Bank, Head Office
Plot No 5, Institutional Area
Sector 32, Gurgaon- 122001

Dear Sir,

**REG: RFP FOR APPOINTMENT OF IS AUDITOR FOR IS AUDIT AND SECURITY CUM
FUNCTIONAL AUDIT OF APPLICATION SOFTWARES**

- 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 6) 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 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 nationalized Bank/ RBI/IBA or any other Government agency. No legal action is pending against us for any cause in any legal jurisdiction.
- h) We are not vendor for Software and Hardware components of the Punjab National Bank at Data Center, EDW, and Treasury & DRS level.



- i) We are not involved in implementing Security and network infrastructure of the Bank at Data Center, EDW, and Treasury & DRS level.
- j) We were not involved in involved in Information Systems & Security Audit on regular basis (cyclic audits) of the Punjab National bank for last two financial years.
- k) We undertake that adequate number of representatives, as desired by the Bank, shall be provided at Delhi & NCR location, Mumbai, Kolkata, Chennai/Bengaluru within three months of award of contract. Representative at any other desired location shall also be provided within three months of receipt of such requirement.

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

- 1)
- 2)
- 3)

(Signature and the capacity of the person duly authorized to sign Bid for and on behalf of)



Annexure - G

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 – H

COMPLIANCE STATEMENT

DECLARATION

We hereby undertake and agree to abide by all the terms & conditions and Scope of audit stipulated by the Bank in the RFP including all annexure, addendum and corrigendum.

Signature and Seal of Bidder

Date:-



Annexure - I

Technical Compliance Sheet

S.No.	Criteria	Details
a	Bidder should be a registered legal entity in India and must be financially solvent.	<p>Successful bidder's Firm/Company Name:</p> <p>Registered Head office:</p> <p>Offices at other locations:</p> <p>1</p> <p>2</p> <p>Brief Profile:</p> <p>Year of commencement of Business</p> <p>Website:</p> <p>Authorized person:</p> <p>Designation:</p> <p>Phone No:</p> <p>Email Address:</p> <p>Attach Copies of certificates of Registration, Incorporation and commencement of business, etc., as the case may be.</p>
b	Should not be involved in Information Systems & Security Audit on regular basis (cyclic audits) of the Punjab National bank for last two financial years.	Signed Undertaking in annexure F
c	Should not be a vendor for Software and Hardware components of the Punjab National Bank or technical advisor/service provider of the Bank.	<p>Provides following hardware and software to the Bank:</p> <p>Signed Undertaking in annexure F</p>
d	Should not be involved in implementing Security and network infrastructure of the Bank at Data Center, EDW, Treasury & and DRS level.	<p>Provides following services and support to the Bank:</p> <p>Signed Undertaking in annexure F</p>
e	Should be an Indian Company /Firm /Limited Liability Partnership (LLP) Firm/Organization /Independent subsidiary with an average annual turnover of Rs.3 (Three)	<p>Turnover and profit during last 3 years: (In Indian Rupee)</p> <p>2017-18 2018-19 2019-20</p> <p>Turnover</p>



	Crores or more for the last three financial years and should be in net profits in last two financial years and should have registered office in India.	Net Profit Attach copy of audited balance sheets of above periods.																
f	Should have conducted minimum 2 Information Systems Security audits of any Scheduled Commercial Bank's Data Center connected with a minimum 500 offices, in last five years, out of which one audit should be in a public sector bank in India.	Conducted following IS Audits in last three years: Organizations Fill details in Annexure J																
g	Should have implemented BS 7799/ ISO 27001 security framework in any organization.	Implemented BS7799/ ISO 27001 security framework in last three years: Organization Fill details in Annexure K																
h	Should have at least 5 qualified professionals with CISA/CISSP certification and IS Audit Experience of 2 or more years including at least one IS Audit for any organization defined at 2.2 (f) above and should be on permanent roll of the organization.	No. of Professionals on the permanent roll of the bidding company with certifications <table><tr><td>1. CISA</td><td></td></tr><tr><td>2. CISSP</td><td></td></tr><tr><td>3. CEH</td><td></td></tr><tr><td>4. OSCP</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. CHFI</td><td></td></tr><tr><td>8. Others(Specify)</td><td></td></tr></table> Fill details in Annexure L	1. CISA		2. CISSP		3. CEH		4. OSCP		5. SCSECA/OCE		6. CCIE-Security		7. CHFI		8. Others(Specify)	
1. CISA																		
2. CISSP																		
3. CEH																		
4. OSCP																		
5. SCSECA/OCE																		
6. CCIE-Security																		
7. CHFI																		
8. Others(Specify)																		
i	Should not have been blacklisted by any nationalized Bank/ RBI/IBA or any other Government agency.	Signed Undertaking in annexure F																



j	Should be able to provide deliverables as per clause 3 of Annexure A-A1 of RFP.	<p>a) Time Lines – should be able to deploy adequate number of auditors to complete the audit process within stipulated time.</p> <p>Give details in Annexure M</p> <p>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). 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).</p> <p>c) Reporting formats - should provide reports as per clause 3.2 of scope of audit.</p> <p>d) Name of Tool used:</p> <p>Successful bidder shall also be capable of providing audit report through some tool 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. Bidder will also specify the tool name along with no. of licenses it will deploy in the Bank to fulfill the tasks as per given scope and timelines.</p> <p>e) Provide Risk Movement for various activities.</p> <p>(Undertaking in Annexure F)</p>
k	Should be empanelled with Cert-In, Govt of India for Security Auditors with a valid certificate of empanelment as on date of submission of bids.	Documentary evidence for empanelment with Cert-In.
l	Should have a local representing offices at Delhi & NCR location,	Undertaking from Bidder



	Mumbai, Kolkata, Chennai/Bengaluru, and in case of non-availability of local office the bidder shall undertake to set-up the same within 30 days of award of the work-order and shall communicate the address of the office to the bank.	
--	--	--

Place:

Date:

Seal & Signature of Bidder



ANNEXURE J

IS Audit Assignments:

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

Place:

Date:

Seal & Signature of Bidder



ANNEXURE K

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 L

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 (in years)	
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, cyber security 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 minimum 6 qualified professionals as per para 2.2(h) and 2.2(j) are to be furnished on a separate sheet including their Credential in the specialized qualification and their previous employment record.

Attach Copy of Certificates for proof of qualification & Certification copy of qualified professionals as per para 2.2(h) and 2.2 (j) of RFP.

Place:

Date:

Seal & Signature of Bidder



ANNEXURE M

Number of auditors (approx) [having minimum experience as defined under 2.2(h) & Annexure I (h)] to be deployed for audit.

S.NO	Activities	Number of team members who will be deployed for Conducting Audit, Draft Discussion & Report Compilation
	A	B
1	Compliance to System and Procedure [Quarterly]	1. CISA
2	VAPT- Vulnerability Assessment & Penetration Testing from intranet [Quarterly]	2. CCIE Security
		3. SCSECA/OCE
		4. OSCP
3	WAN Audit [Quarterly]	5. CEH
		6. CISSP
		7. Other (Please specify)
4.	EAPT- External attack and penetration test from internet [six in a year]	1. CEH/CISSP/CCI E/CISA
		2. OSCP
		3. Others(Specify)
5.	SECURITY CUM FUNCTIONAL AUDIT OF New in-house developed application/ After Major Changes in existing applications (both in-house and developed by external vendors) (150 Applications per year)	1. CISA
		2. CCIE Security
		3. SCSECA/OCE
		4. OSCP
		5. CEH
		6. CISSP
		7. Other (Please specify)

Details of audit team members to be also provided.

Place:

Date:

Seal & Signature of Bidder



ANNEXURE-N

PERFORMA FOR INTEGRITY PACT

To,
The Dy. General Manager
IS Audit Department
Inspection and Audit Division
Punjab National Bank, Head Office
Plot No 5, Institutional Area
Sector 32, Gurgaon- 122001

Subject: Submission of Tender for the work.....

Dear Sir,

I/We acknowledge that Punjab National Bank is committed to follow the principle of transparency equity and competitiveness as enumerated in the Integrity Agreement enclosed with the tender/bid document.

I/We agree that the Notice Inviting Tender (NIT) is an invitation to offer made on the condition that I/We will sign the enclosed integrity Agreement, which is an integral part of tender documents, failing which I/We will stand disqualified from the tendering process. I/We acknowledge that THE MAKING OF THE BID SHALL BE REGARDED AS AN UNCONDITIONAL AND ABSOLUTE ACCEPTANCE of this condition of the NIT.

I/We confirm acceptance and compliance with the Integrity Agreement in letter and spirit and further agree that execution of the said Integrity Agreement shall be separate and distinct from the main contract, which will come into existence when tender/bid is finally accepted by Punjab National Bank. I/We acknowledge and accept the duration of the Integrity Agreement, which shall be in the line with Article 6 of the enclosed Integrity Agreement.

I/We acknowledge that in the event of my/our failure to sign and accept the Integrity Agreement, while submitting the tender/bid, Punjab National Bank shall have unqualified, absolute and unfettered right to disqualify the tenderer/bidder and reject the tender/bid in accordance with terms and conditions of the tender/bid.

Yours faithfully

(Duly authorized signatory of the Bidder)

To be signed by the bidder and same signatory competent / authorized to sign the relevant contract on behalf of Punjab National Bank.

INTEGRITY AGREEMENT

This Integrity Agreement is made at on thisday of2020.

BETWEEN



Punjab National Bank is a Bank constituted under The Banking Companies (Acquisition & Transfer of Under-takings) Act 1970, having its Head Office at Sector 10, Dwarka, New Delhi-110075 and inter-alia a Branch Office/ Circle Office at _____ (Hereinafter referred as the Principal/Owner', which expression shall unless repugnant to the meaning or context hereof include its successors and assigns)

AND..... (Name and Address of the Individual/firm/Company) Through..... Details of duly authorized signatory) (Hereinafter referred to as the "Bidder/Contractor" and which expression shall unless repugnant to the meaning or context here of include its successors and permitted assigns)

Preamble

WHEREAS the Principal / Owner has floated the Tender for (.....Name of Work.....) (hereinafter referred to as "Tender/Bid") and intends to award, under laid down organizational procedure, contract for hereinafter referred to as the "Contract".

AND WHEREAS the Principal/Owner values full compliance with all relevant laws of the land, rules, regulations, economic use of resources and of fairness/transparency in its relation with its Bidder(s) and Contractor(s). AND WHEREAS to meet the purpose aforesaid both the parties have agreed to enter into this Integrity Agreement (hereinafter referred to as "Integrity Pact" or "Pact"), the terms and conditions of which shall also be read as integral part and parcel of the Tender/Bid documents and Contract between the parties.

NOW, THEREFORE, in consideration of mutual covenants contained in this Pact, the parties hereby agree as follows and this Pact witnesses as under:

Article 1: Commitment of the Principal/Owner

1) The Principal/Owner commits itself to take all measures necessary to prevent corruption and to observe the following principles:

(a) No employee of the Principal/Owner, personally or through any of his/her family members, will in connection with the Tender, or the execution of the Contract, demand, take a promise for or accept, for self or third person, any material or immaterial benefit which the person is not legally entitled to.

(b) The Principal/Owner will, during the Tender process, treat all Bidder(s) with equity and reason. The Principal/Owner will, in particular, before and during the Tender process, provide to all Bidder(s) the same information and will not provide to any Bidder(s) confidential / additional information through which the Bidder(s) could obtain an advantage in relation to the Tender process or the Contract execution.

(c) The Principal/Owner shall Endeavour to exclude from the Tender process any person, whose conduct in the past has been of biased nature.



2) If any information comes to the notice of the Principal/owner on the conduct of any of its employees which is a criminal offence under the Indian Penal code (IPC)/Prevention of Corruption Act, 1988 (PC Act) or is in violation of the principles herein mentioned or if there be a substantive suspicion in this regard, the Principal/Owner will inform the Asstt. General Manager Vigilance Officer and in addition can also initiate disciplinary actions as per its internal laid down policies and procedures.

Article 2: Commitment of the Bidder(s)/Contractor(s)

1) It is required that each Bidder/Contractor (including their respective officers, employees and agents) adhere to the highest ethical standards, and forthwith report the Principal/Owner about all suspected fraudulent act or corruption or Coercion or Collusion of any person connected with the tender process which it has knowledge or becomes aware any time, during the tendering process and throughout the negotiation or award of a contract.

2) The Bidder/Contractor commits himself/itself to take all measures necessary to prevent corruption. He/it commits himself/itself to observe the following principles during his/its participation in the Tender process and during execution of the Contract:

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

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

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

3. The Bidder/Contractor of foreign origin shall disclose the names and addresses of agents/representatives in India, if any. Similarly Bidder/Contractor of Indian Nationality shall disclose names and addresses of foreign agents/representatives, if any. Either the Indian agent on behalf of the foreign principal or the foreign principal directly could bid in a tender but not both. Further, in cases where an agent participate in a tender on behalf of one manufacturer, he shall not be allowed to quote on behalf of another manufacturer along with the first manufacturer in a subsequent/parallel tender for the same item.

4. The Bidder/Contractor will, when presenting his/its bid, disclose any and all payments he/it has made, is committed to or intends to make to agents, brokers or any other intermediaries in connection with the award of the Contract.

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



6. The Bidder/Contractor will not, directly or through any other person or firm indulge in fraudulent practice means a willful misrepresentation or omission of facts or submission of fake/forged documents in order to induce public official to act in reliance thereof, with the purpose of obtaining unjust advantage by or causing damage to justified interest of others and/or to influence the procurement process to the detriment to the interests of Principal/Owner.

7. The Bidder/Contractor will not, directly or through any other person or firm use Coercive Practices against principal/owner and/or other bidder(s)/contractor(s). Coercive practices mean the act of obtaining something, compelling an action or influencing a decision through intimidation, threat or the use of force directly or indirectly, where potential or actual injury may befall upon a person, his/ her reputation or property to influence their participation in the tendering process.

Article 3: Consequences of Breach

Without prejudice to any rights that may be available to the Principal/Owner under law or the Contract or its established policies and laid down procedures, the Principal/Owner shall have the following rights in case of breach of this Integrity Pact by the Bidder(s)/Contractor(s) and the Bidder/ Contractor accepts and undertakes to respect and uphold the Principal/Owner's absolute right:

1) If the Bidder/Contractor, either before award or during execution of Contract has committed a transgression through a violation of Article 2 above or in any other form, such as to put his reliability or credibility in question, the Principal/Owner at its discretion, is entitled to disqualify the Bidder/Contractor from the Tender process or terminate/determine the Contract, if already executed or exclude the Bidder/Contractor from future contract award processes after giving 14 days' notice to the contractor. The imposition and duration of the exclusion will be determined by the severity of transgression and determined by the Principal/Owner. Such exclusion may be forever or for a limited period as decided by the Principal/Owner.

2) Forfeiture of EMD/Performance Guarantee/Security Deposit: If the Principal/Owner has disqualified the Bidder(s) from the Tender process prior to the award of the Contract or terminated/determined the Contract or has accrued the right to terminate/determine the Contract according to Article 3(1), the Principal/Owner apart from exercising any legal rights that may have accrued to the Principal/Owner, may in its considered opinion forfeit the entire amount of Earnest Money Deposit, Performance Guarantee and Security Deposit of the Bidder/Contractor.

3) Criminal Liability: If any act/omission or conduct of a Bidder or contractor conduct of a Bidder or Contractor, or of an employee or a representative or an associate of a Bidder or Contractor which constitutes corruption within the meaning of IPC/PC Act brought to the notice of the Principal/Owner, or if the Principal/ Owner has substantive suspicion in this regard, the Principal/Owner shall be at liberty to inform the same to law enforcing agencies for further investigation.

Article 4: Previous Transgression



- (i) The Bidder declares that no previous transgressions occurred in the last 5 years with any other Company in any country confirming to the anticorruption approach or with Central Government or State Government or any other Central/State Public Sector Enterprises in India that could justify his exclusion from the Tender process.
- (ii) If the Bidder makes incorrect statement on this subject, he can be disqualified from the Tender process or the contract, if already awarded, can be terminated for such reason. Principal/owner will be entitled to exclude the contractor from future tender/contract award processes for a period not exceeding three years.
- (iii) Without prejudice to any other legal rights or remedies available to the principal under the relevant clauses of the tender document.

Article 5: Equal Treatment of all Bidders/Contractors/Subcontractors

- 1) The Bidder(s)/Contractor(s) undertake(s) to demand from all subcontractors a commitment in conformity with this Integrity Pact. The Bidder/Contractor shall be responsible for any violation(s) of the principles laid down in this agreement/Pact by any of its Subcontractors/ sub-vendors.
- 2) The Principal/Owner will enter into Pacts on identical terms as this one with all Bidders and Contractors.
- 3) The Principal/Owner will disqualify Bidders, who do not submit, the duly signed

Pact between the Principal/Owner and the bidder, along with the Tender or violate its provisions at any stage of the Tender process, from the Tender process.

Article 6- Duration of the Pact

This Pact begins when both the parties have legally signed it. It expires for the Contractor/ Vendor 12 months after the completion of work under the contract or till the continuation of defect liability period, till the Contract has been awarded. If any claim is made/lodged during the time,

the same shall be binding and continue to be valid despite the lapse of this Pacts as specified above, unless it is discharged/ determined by the Competent Authority, Punjab National Bank.

Article 7-Independent External Monitor (IEM)

1. The Principal/Owner has appointed competent and credible Independent External Monitor(s) (IEM) Sh. Raj Kumar Singh, IRS (Retd) (Mob no.9818696406, 8141488880) (mrraising@gmail.com, mrraising@yahoo.com) for this Pact in consultation with the Central Vigilance Commission. The task of the Monitor is to review independently and objectively, whether and to what extent the parties comply with the obligations under this Pact.

2. The IEM is not subject to instructions by the representatives of the parties and performs his functions neutrally and independently. He reports to MD& CEO, Punjab National Bank.



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

4. In case of tenders having estimated value exceeding Rs 60 lakhs, the Principal/Owner will provide to the IEM sufficient information about all the meetings among the parties related to the Project and shall keep the IEM apprised of all the developments in the Tender Process.

5. As soon as the IEM notices, or believes to notice, a violation of this Pact, he will so inform the Management of the Principal/Owner and request the Management to discontinue or take corrective action, or to take other relevant action. The IEM can in this regard submit non-binding recommendations. However, beyond this, the IEM has no right to demand from the parties that they act in a specific manner, and/or refrain from action or tolerate action.

6) The IEM shall submit a written report to the MD & CEO, of the Principal/Owner within 6 to 8 weeks from the date of reference or intimation to him by the Principal/Owner and, should the occasion arise, submit proposals for correcting problematic situations.

7) The word "IEM" would include both singular and plural.

8) IEMs will not use or pass on any information or document provided to it regarding plans, technical proposals and business details for the purpose of competition or personal gains etc.

Article 8- Other Provisions

1. This Pact is subject to Indian Law, place of performance and jurisdiction is place where office of the Principal/Owner, who has floated the Tender, is located.

2. Changes and supplements need to be made in writing.

3. If the Contractor is a partnership or a consortium, this Pact must be signed by all the partners or consortium members. In case of a Company, the Pact must be signed by a representative duly authorized by board resolution.

4. Should one or several provisions of this Pact turn out to be invalid; the remainder of this Pact remains valid. In this case, the parties will strive to come to an agreement to their original intentions.

5. It is agreed term and condition that any dispute or difference arising between the parties with regard to the terms of this Integrity Agreement / Pact, any action taken by the Owner/Principal in accordance with this Integrity Agreement/ Pact or interpretation thereof shall not be subject to arbitration.

Article 9- LEGAL AND PRIOR RIGHTS

All rights and remedies of the parties hereto shall be in addition to all the other legal rights and remedies belonging to such parties under the Contract and/or law and the same shall be deemed to be cumulative and not alternative to such legal rights and remedies aforesaid. For the sake of brevity, both the Parties agree that this Integrity Pact will have precedence over the Tender/Contact documents with regard any of the provisions covered under this Integrity Pact. IN WITNESS WHEREOF the parties have signed and executed this Integrity Pact at the place and date first above mentioned in the presence of following witnesses:



..... (For and on behalf of Principal/Owner)

..... (For and on behalf of Bidder/Contractor)

WITNESSES:

1. (Signature, name and address)

2. (Signature, name and address)

Place:

Dated:



ANNEXURE O

Check list for the Documents to be submitted

Document	Particular	YES/NO	Page No	
			From	To
Company Details	Brief Profile			
Audited Balance Sheets	Copy of balance sheets for 2017-2018, 2018-19 and 2019-20			
Authorization Letter of signatory	Power of Attorney for authorized signatory, duly attested by notary public/Board Resolution.			
Reference Data Sheet	List of Minimum two references (Section 3.2.10)			
Bid Security Declaration	As per Section 3.2.8			
Annexure C	Technical BID Form			
Annexure E	Undertaking 1			
Annexure F	Undertaking 2			
Annexure H	Compliance Statement			
Annexure I	Technical Compliance Sheet			
Annexure J	IS Audit assignments			
Annexure K	BS7799/ ISO 27001 security framework implementation			
Annexure L	Professional details with copy of certificates.			
Annexure M	Number of auditors (approx) to be deployed for audit			
Annexure N	Integrity Pact			

Commercial bid (On-Line)

Sl. No.	Documents
1.	Commercial bid as per Annexure-D (only on-line submission required)