



निरीक्षण एवं लेखा परीक्षा प्रभाग, प्रधान कार्यालय
प्लॉट संख्या ५, सेक्टर ३२, गुरुग्राम – १२२००१
INSPECTION & AUDIT DIVISION, HEAD OFFICE
PLOT NO.5, SECTOR-32, GURUGRAM, HARYANA-122001

Response to Pre Bid Queries: RFP for Appointment of external IS Auditor for Conducting Source Code Review of Applications (Web / Mobile)

Sl. No.	RFP Page No.	RFP Clause Name and No.	RFP Clause	Bidder's Query / Suggestion / Remarks	Bank's Response
1	8	3.1-Scope	The bidder will use automated licensed tools	We request to change the clause to commercial and licensed automated tools	Please refer corrigendum 1 (Sl. No. 1)
2	8	3.1-Scope	For vendor managed application(s) / portal(s) the audit is to be conducted either at vendor location or offsite as per the discretion of the Bank	Please specify the number of vendor apps at each location as specified in RFP	More than 90 % of the applications are in house
3	9	3.2- Timelines	The activity is to be completed in 4 tranches of 50 apps/ 15 days each	Does it also include re-validation of applications as patching process from Bank/ Vendor might take time and will impact timeline.	The timeline specified (60 Days) is for scanning and sharing first audit report. Revalidation has to be done as and when the compliance is submitted.
4	29	40.17 - Variation	Any upward variation up to 15 % in the number of audits covered under the scope of audit shall be covered under the contracted price and no additional cost shall be payable.	Does it imply that scope may exceed by around 15% and additional scope shall be paid at contracted price or does it needs to be accommodated in existing quote shared	Number of applications to be audited may exceed by 15% and additional scope shall be paid at contracted price per audit.
5	29	40.19 - Course of Audit	The scope of work also includes extending training to our IS Audit Team, twice a year, and to share	The total project duration is expected to be 60 days. Please share training schedule planned to	The timeline specified (60 Days) is for scanning and sharing first audit report.



निरीक्षण एवं लेखा परीक्षा प्रभाग, प्रधान कार्यालय

प्लॉट संख्या ५, सेक्टर ३२, गुरुग्राम – १२२००१

INSPECTION & AUDIT DIVISION, HEAD OFFICE

PLOT NO.5, SECTOR-32, GURUGRAM, HARYANA-122001

			with them all the formats, check lists, scoring sheets, scripts etc. that will be used during the process of audit.	be conducted twice in a year. Will it impact payment terms as source code review might get completed early	
6	31	Point 3 - Eligibility Criteria	Should have been empanelled / engaged by at least one Scheduled Commercial Bank, in last five financial years for conducting IS Audit.	Please clarify, is it atleast one order in last five years OR atleast one five years old order. Request to change clause to: Should have been empanelled / engaged by at least one Scheduled Commercial Bank or financial Institute, in last Three financial years for conducting IS Audit, if five years old order is required to be shared	Please be guided by RFP
7	8	3.1- Scope of work	For vendor managed application(s) / portal(s) the audit is to be conducted either at vendor location or offsite as per the discretion of the Bank.	Please share how many applications are to be audited at vendor's location?	More than 90 % of the applications are in house
8	9	3.2- Scope of work	The entire activity is to be concluded within 60 days from the date of issuance of Purchase Order.	Please suggest if timeline of 60 days is for initial audit or for revalidation audits also?	The timeline specified is for scanning and sharing first audit report.
9	11	6.- MINIMUM ELIGIBILITY CRITERIA	Should be registered as a company in India as per Company Act 1956 & 2013 / Partnership firm registered under LLP Act, 2008,	The partnership firms are registered under The Partnership Act, 1932 and LLP are registered under LLP Act 2008. Hence request to reword	Please refer corrigendum 1 (Sl. No. 2)



निरीक्षण एवं लेखा परीक्षा प्रभाग, प्रधान कार्यालय

प्लॉट संख्या ५, सेक्टर ३२, गुरुग्राम – १२२००१

INSPECTION & AUDIT DIVISION, HEAD OFFICE

PLOT NO.5, SECTOR-32, GURUGRAM, HARYANA-122001

			operating in the field of IS Audit for at least 3 years as on the date of RFP	the clause as follows: Should be registered as a company in India as per Company Act 1956 & 2013 / Partnership firm registered under Partnership Act, 1932/ LLP registered under LLP Act, 2008, operating in the field of IS Audit for at least 3 years as on the date of RFP	
10	9	3. SCOPE OF WORK / DELIVERABLES	The activity is to be completed in 4 tranches. Details of milestones to be achieved is as under	What are the details of the applications to be audited such as: - Web based or mobile based or thick client - Number of lines of code in the in-scope applications - Technologies of used at Front End & Back End of the applications - Platform where the code is hosted	- Mostly Web based and Mobile based but not limited to these only - Total lines of code is approximately between 6000000 - 7000000 - Mostly Dot Net / Java / php but not limited to these only. - Mostly Oracle WebLogic / IIS / Apache Tomcat / IBM WebSphere but not limited to these only
11	49	Annexure - M PERFORMA	Annexure - M PERFORMA FOR INTEGRITY PACT	Is the integrity pact to be submitted by successful bidder or by all the bidders?	Integrity pact is to be submitted by all bidders and it should be



निरीक्षण एवं लेखा परीक्षा प्रभाग, प्रधान कार्यालय
प्लॉट संख्या ५, सेक्टर ३२, गुरुग्राम – १२२००१
INSPECTION & AUDIT DIVISION, HEAD OFFICE
PLOT NO.5, SECTOR-32, GURUGRAM, HARYANA-122001

		FOR INTEGRITY PACT		If it is to be submitted by all the bidders, the document should be on company letterhead or should be on STAMP PAPER	executed on non-judicial stamp of Rs. 100 and submitted in original.
12	55	Annexure - N REFERENCE DATA SHEET	Annexure - N REFERENCE DATA SHEET	Details of whom to be mentioned here? What is expected from bidders in this annexure?	Details of organization / Contact person(s) where previous IS Audit assignments have been completed
13	8	3. Scope	To conduct the Source Code Review for approximately 200 applications (Web / Mobile).	We request PNB to clarify the Type (Android, iOS, etc.) of mobile and Web applications with count along with No of Lines of Code for each application.	- Web based (Mostly Dot Net / Java / php but not limited to these only) and Mobile based (Android /iOS but not limited to this only) - Total lines of code is approximately between 6000000 - 7000000
14	8	3. Scope	The Source code review of applications are to be carried out simultaneously.	We request PNB to make it flexible as it depends on the total tool/license installed.	Please be guided by RFP
15	8	3. Scope	The Auditor has to conduct Source Code Review of in – House applications onsite and licensed tools will have to be installed in Bank's environment for the same.	We request PNB to have the minimum specification of workstations/servers as below, per license: CPU: i5 and above. Generation: 10 and above. RAM: 16 GB and above.	Requisite workstations will be provided by the Bank to the successful bidder.



निरीक्षण एवं लेखा परीक्षा प्रभाग, प्रधान कार्यालय
प्लॉट संख्या ५, सेक्टर ३२, गुरुग्राम – १२२००१
INSPECTION & AUDIT DIVISION, HEAD OFFICE
PLOT NO.5, SECTOR-32, GURUGRAM, HARYANA-122001

				Unhindered power backup and high bandwidth internet (for updating of tool/OS, downloading documents /code/plugin, etc.)	
16	8	3. Scope	For vendor managed application(s) / portal(s) the audit is to be conducted either at vendor location or offsite as per the discretion of the Bank.	We request PNB to specify the numbers of such vendors and locations. As it is directly proportional to the number of licenses and travel expenses of auditors; to do so will impact the cost of the Bid.	More than 90 % of the applications are in house.
17	8	3. Scope	All the Audit Findings / Exception reports shall be supported by adequate audit evidence and same shall be documented and included in the audit report to be submitted to the Bank.	We request PNB to provide more clarity on "exception".	The exceptions granted against any finding as per extant guidelines of the Bank should be incorporated in the final audit report.
18	8	3. Scope	The auditor has to conduct the revalidation of observations till the time all gaps are plugged in.	We request PNB to specify the timelines for revalidation and the maximum number of revalidations.	Please be guided by RFP
19	9	3.2 Timelines	The activity is to be completed in 4 tranches. Details of milestones to be achieved is as under:	We request PNB to specify the timelines for revalidation and a maximum number of revalidations.	Please be guided by RFP
20	9	3.3 Reports	a) The IS Auditor shall provide different types of reports which would address all issues /	We request PNB to define the different types of reports, and is it for one application? If yes, What different types of reports bank want,	Different types of reports means report in different format such as .pdf, .csv, .xlsx, .xls etc. / reports as per different vulnerability



निरीक्षण एवं लेखा परीक्षा प्रभाग, प्रधान कार्यालय
प्लॉट संख्या ५, सेक्टर ३२, गुरुग्राम – १२२००१
INSPECTION & AUDIT DIVISION, HEAD OFFICE
PLOT NO.5, SECTOR-32, GURUGRAM, HARYANA-122001

			observations regarding compliances.	and what are the parameters for the reports?	standards such as OWASP TOP 10, SANS 25, CWE Top 25 etc. / reports as per different compliance standards such as PCI-DSS, CIS etc. but not limited to these only.
21	9	3.3 Reports	b) 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.	Do we have to follow any specific standard?	Please be guided by RFP
22	9	3.3 Reports	c) 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)	Request the bank to kindly clarify whether the VAPT of the server/equipment has to be performed over which these application will be hosted?	Only Source Code review of the applications is to be Conducted.
23	9	3.3 Reports	d) Broad domain categorization of activity (Port/SQL injection/ Services/Physical access control/ Logical access control/ environment etc.)	Source code review of the application only identifies vulnerabilities in the application's source code. Please suggest what PNB is looking for with respect to Port/Services/Physical access	As applicable for Source Code review



निरीक्षण एवं लेखा परीक्षा प्रभाग, प्रधान कार्यालय
प्लॉट संख्या ५, सेक्टर ३२, गुरुग्राम – १२२००१
INSPECTION & AUDIT DIVISION, HEAD OFFICE
PLOT NO.5, SECTOR-32, GURUGRAM, HARYANA-122001

				control/Logical access control/environment?	
24	9	3.3 Reports	f) Servers / Resources affected with IP address.	Will the bank provide the mapping of the IP addresses and approved application names?	The requisite details will be provided to the successful bidder wherever required.
25	9	3.3 Reports	Department (in office) to whom the Vulnerability relates.	Mapping of departments with respect to applications is required.	The details of applications along with the departments / divisions will be provided to the successful bidder.
26	9	3.3 Reports	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.	We request PNB for "removal step-wise" we required details about the applications like type of application, host OS, type web server, database's host OS, type of database, middleware, type of APIs, authentication mechanism, expected number of protocols to be cover; will all these details shared during the audit ?	The requisite details will be provided to the successful bidder wherever required.
27	9	3.3 Reports	Provision for updating owner's compliance comments.	We can update the owner's compliance comments in every revalidation/final report. w.r.t owner should share the comments in specific timeline.	Please be guided by RFP
28	9	3.3 Reports	k) Explicit reference to key policy and procedure documents of	We require policy and procedure documents of the Bank/RBI against	The requisite details will be provided to the successful bidder wherever required.



निरीक्षण एवं लेखा परीक्षा प्रभाग, प्रधान कार्यालय

प्लॉट संख्या ५, सेक्टर ३२, गुरुग्राम – १२२००१

INSPECTION & AUDIT DIVISION, HEAD OFFICE

PLOT NO.5, SECTOR-32, GURUGRAM, HARYANA-122001

			the Bank / RBI against identified risk/observation.	which we can refer the observations. Also what if the shared documents do not contain the reference point / control?	If the shared documents do not contain the reference point / control, the same shall be finalized by the Bank after discussion with the successful bidder.
29	9	3.3 Reports	l) The reports shall be customised as per the requirements of the Bank.	We can do the same however, we might require the necessary data from the Bank. Subject to availability of data.	The requisite details will be provided to the successful bidder wherever required.
30	9	3.3 Reports	m) Additional mandatory or voluntary standards or regulations applicable to the banking industry as best practices should be reported under "Improvement / suggestions"	If the severity of observation is high or critical will it still be considered or reported as an Improvement /suggestion?	Bank shall finalize the same after discussion with the successful bidder.
31	9	3.3 Reports	n) Standards followed	We request PNB to specify the "Standards followed".	The report should contain the vulnerability reporting / compliance standards / any other standard followed by the auditor.
32	9	3.3 Reports	q) 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.	We request PNB to kindly confirm if these details will be provided by the bank?	The requisite details will be provided to the successful bidder wherever required.



निरीक्षण एवं लेखा परीक्षा प्रभाग, प्रधान कार्यालय

प्लॉट संख्या ५, सेक्टर ३२, गुरुग्राम – १२२००१

INSPECTION & AUDIT DIVISION, HEAD OFFICE

PLOT NO.5, SECTOR-32, GURUGRAM, HARYANA-122001

33	10	4. LOCATION / METHODOLOGY OF AUDIT(S)	<p>The Auditor has to conduct Source Code Review of in – House applications onsite (Bank's Location) and licensed tools will have to be installed in Bank's environment for the same. For vendor managed application(s) / portal(s) the audit is to be conducted either at vendor location or offsite as per the discretion of the Bank.</p> <p>The successful bidder may be required to visit on-site (Bank's offices) / vendor site (i.e. Bangalore / Hyderabad/ Mumbai / Chandigarh / Mysore / Chennai/ Pune / Ahmedabad / Kolkata) for conducting the audit.</p>	Request the bank to kindly clarify whether we need to visit these location for source code Review of the application.	Please be guided by RFP
34	27	40.9. Delays in the Performance	<p>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:</p> <p>i. Claiming Liquidated Damages</p>	<p>We propose an appropriate cap on LD and also propose the following: "Bidder shall not be liable for Liquidated Damages in this clause if the default/delay is not solely attributable to the bidder"</p>	Please be guided by RFP (Clause 40.10)



निरीक्षण एवं लेखा परीक्षा प्रभाग, प्रधान कार्यालय
प्लॉट संख्या ५, सेक्टर ३२, गुरुग्राम – १२२००१
INSPECTION & AUDIT DIVISION, HEAD OFFICE
PLOT NO.5, SECTOR-32, GURUGRAM, HARYANA-122001

			ii. Termination of the agreement fully or partly and claim liquidated damages. iii. Imposing penalty.		
35				Request the bank to kindly confirm if this is a multi-year engagement. If yes, then for how many years?	Please be guided by RFP
36				As per our understanding, implementation of any technology solution, applying patches is out of scope. Kindly confirm.	Please be guided by RFP
37				Request the bank to kindly confirm if this engagement will be run on project based model or loan staff model. If loan staff model how many resources will be required?	Please be guided by RFP
38				Please specify total number of pre-audit in year.	Please be guided by RFP