HO: Inspection and Audit Division
Plot No. 5, Institutional Area, Sector-32, Gurugram-122001
Email: iadisaudit@pnb.co.in

Consolidated Response to Pre Bid Queries of RFP For Appointment of IS Auditor For Information System Audit And Security Cum Functional Audit Of Application Softwares

S.No	Page Number	Clause Number	Clause	Queries	Bank's Remarks
1	11	2.2. Minimum Eligibility Criteria for Bidder(s)	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.	We believe this should be allowed for existing auditors also as they have good understanding of existing applications and infrastructure at bank that will help improve quality of work	The vendor should not have been appointed as full time auditor for conducting Information Systems & Security Audit of the Punjab National bank for the last two financial years.
			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.	Since the scope of the RFP is more towards applications and infrastructure audits, we request you to permit companies with experience in auditing banks with VAPT/ App sec/ IS for scheduled bank's with more than 500 branches	Please be guided by the RFP
			h) Should have at least 7 qualified professionals with CISA/CISSP and 1 with CHFI certification	We request you to allow consultants with certifications with OSCP/ CISM/ CEH which are more relevant and technical certificates considering the VAPT/ AppSec and Functional audits required to be conducted for this work	Please be guided by the RFP

2	80	Annexure 1 - Technical Compliance Sheet	I) Should have local representing offices at Delhi & NCR location, 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.	If bidder doesn't have office in any one location can it be managed based on need. Can the Chennai and Kolkata locations be managed from Bangalore office	Please be guided by the RFP
3	23	3.4. Award of Contract	After Reverse Auction completion, Bidder having Lowest Weighted Yearly Cost (as per Annexure D) shall be treated as L1 bidder.	Taking into consideration the criticality of this bid, we request PNB for conducting techno-commercial evaluation rather than L1 evaluation where technical parameters can be given 80% weightage and commercial parameters to be given 20%	Please be guided by the RFP
4	33	Annexure - A (1.a)	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	Please provide the count of Third party/ service provided under scope	There are approximately 100 service providers of the Bank, located at various locations. The number is dynamic and the bidders should consider the size of the Bank, on-going amalgamation and future growth in the next two years about number of service providers while making their estimates. Details shall be shared with the successful bidder.

5	33	Annexure - A (1.a)	Other HO divisions/ Service Providers at New Delhi/ NCR/ Mumbai/Banglore/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.	Please provide the count of HO divisions to be covered under scope	There are 36 HO divisions of the Bank, located at various locations. The number is dynamic and subject to change as per Bank's discretion and the bidders should take the size of the Bank, on-going amalgamation and future growth in the next two years into consideration while making their estimates. The details shall be shared with the successful bidder.
6	33	Annexure - A (1.a)	Other HO divisions/ Service Providers at New Delhi/ NCR/ Mumbai/Banglore/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.	Please provide the details and count of "any other bank‘s office at any place, where critical application/IT infrastructure is installed or may be installed in future"	The requirement is dynamic and dependent on Bank's future requirements. Please be guided by the RFP.
7	33	Annexure - A (1.a)	Locations of Service Providers to whom specific services are outsourced.	Please provide the location details and count of service providers	It will be shared with successful bidder.
8	33	Annexure - A (1.a)	Data Centers and Disaster Recovery Sites of RRBs of the Bank at New Delhi/Mumbai/Kolkata.	Please provide the count of DC & DR sited for each location	There are 9 RRBs of the Bank with DCs and DRs at New Delhi, Mumbai and Kolkata. The details shall be shared with successful bidder.
9	33	Annexure - A (1.b)	**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**	Please define the requirement with Compliance testing	Please be guided by the RFP.

			testing of previous test/audit report.		
10	33	Annexure - A (1.b)	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.	Please provide count of in scope Servers, Security & Network Devices and URLs	It will be shared with successful bidder.
11	33	Annexure - A (1.b)	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.	Please provide the count of IPs to be covered as part of Penetration Testing	The count is dynamic and the bidders should take the size of the Bank, on-going amalgamation and future growth in the next two years into consideration while making their estimates. The details shall be shared with successful bidder.
12	33	Annexure - A (1.b)	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.	Please share the count of in-scope process, policies and procedures	It will be shared with successful bidder.

13	33	Annexure - A (1.b)	**Vulnerability Assessment (Servers(OS), Database systems, webservers, 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 .	Please provide the count of in scope devices including Servers(OS), Database systems, webservers, IOS of Security & Network Devices) including virtual instances/hypervisors etc	The detailed break-up of assets for various activities under scope shall be shared with successful bidder.
14	33	Annexure - A (1.b)	Vulnerability Assessment (Servers(OS), Database systems, webservers, 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 .	Please share the count of public facing & internal applications	The detailed break-up under scope shall be shared with successful bidder.
15	33	Annexure - A (1.b)	Vulnerability Assessment (Servers(OS), Database systems, webservers, 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	Please share the expectation with Device Level Audit	Please be guided by the RFP.

			quarterly basis including the compliance testing of previous test/audit report .		
16	33	Annexure - A (1.b)	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.	Please share the count of in scope Equipment/ Applications/ Mobile Apps exposed to outside world (Including APIs)	The detailed break-up under scope shall be shared with successful bidder.
17	33	Annexure - A (1.b)	Configuration Audit/Hardening review for Server/OS/Networking & Security Devices/Database/ firewall etc.	Please share the count of in scope Server/OS/Networking & Security Devices/Database/ firewall etc.	The detailed break-up under scope shall be shared with successful bidder.
18	33	Annexure - A (1.b)	Comment upon compliance to ISO 27001:2013 , PCIDSS etc standards (or later standard to which bank is certified/gets certified)	Please share the list of applicable compliance	The regulatory requirements will have to be fulfilled by the successful bidder w.r.t compliances.
19	34	Annexure - A (1.b)	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.	Please provide details of applicable compliances	The regulatory requirements will have to be fulfilled by the successful bidder w.r.t compliances.
20	34	Annexure - A (1.b)	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.	Please provide details of all the applicable compliance audit	The regulatory requirements will have to be fulfilled by the successful bidder w.r.t compliances.

21	34	Annexure - A (1.b)	IS Auditor will provide the report on root cause analysis (RCA)/ Forensic Audit of the security incidents, if required by the Bank.	Please elaborate on the expectation, is it required that bidder will perform the RCA on an incident?	Please be guided by the RFP.
22	34	Annexure - A (1.b)	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.	Please share details around eOBC, eUNI, PNB 1.0 & PNB 2.0	It will be shared with successful bidder.
23	34	Annexure - A (1.b)	Comprehensive review of the BCP arrangement for all critical applications.	Please share the count of in-scope applications	It will be shared with successful bidder.

All prospective bidders are advised to be guided accordingly.