Pre-Bid Queries /Request from Empanelled Bidders and Bank's Response
Requirement Proposal (RP) For Undertaking Information Security & Cyber Security Audit
for the Year 2022-2023 (July-June) dated 10-08-2023

A. M/s Pricewaterhouse Coopers (PwC)

Queries pertaining to IS & Cyber Security Audit			
S.No.	**Particulars**	**Query / Request of Empanelled Bidder**	**Response of the Bank to the Query / Request**
Project Scope of Work - Phase -1 - Evaluation			
1	Cyber Security Set-up.	Please give us a clarity in difference between of Information security and cyber security risk assessment. Also, expectation around the same.	Information security and cyber security risk assessment are standard terms related to information and cyber security. The scope of the same is mentioned in the RP.
2	Conduct Red Teams exercise on half-yearly basis to identify the vulnerabilities and the business risk, assess the efficacy of the defences and check the mitigating controls already in place by simulating the objectives and actions of an attacker.	Do we have to perform red team exercise as a part of audit engagement?	Yes, to conduct Red Teams exercise on half-yearly basis. Please refer the RP and specifically Point 1 B of the RP (Page 4)
3	As per the standard and latest industry practices and guidelines as indicated in the RFP.	Please share your expectation on conducting cyber audit. Any specific framework to be followed or Just the industry best practices	The scope of audit is defined in RP.
4	SAP related Queries	What is the current version of SAP	Shall be shared with the Successful Bidder
5		Number of inscope company codes/ entities	
6		Let us know the business processes to consider for the review	
7		Can you share the IT/ System landscape diagram	
8		Do we have a RCM for list of configuration controls, business process controls, WRICEFs	
9		Kindly share the existing user access, roles & SOD details	
10		What is the application wise user count	
11		List the SAP modules to be considered for review	
12		Share the list of custom-built processes to be considered for review.	

4. Project Deliverables - 4.4 - Provide Certification/Compliance Report for the ISA & CSA			
13	The bidder/selected empanelled auditor is to provide NHB a certification/compliance report each for ISA and for CSA (separately) and for VAPT	We presume that the report/certificate shared after the audit engagement are solely used for internal teams to mitigate the identified gaps and not to be extended to any regulatory body	Please refer the RP and specifically Page No. 50 and 51 of the SLA in the RP.
User Training			
14	1. User Training Imparting IT & cyber security awareness training for Bank's employees and onsite staff handling Bank's IT infrastructure in form of lecture, seminar/webinar, interactions, and presentations on quarterly basis. The training material will 7 also be shared with the Bank. The training shall be carried out at Delhi in 2/3 sessions at various operational levels, in a single /two days.	Bidder is expected to develop training and awareness material, evaluation, provide training as part of this engagement. As this is an Audit engagement. Please confirm	Please refer the RP and specifically Page Nos. 06, 07 and 10 of RP
Performance Bank Guarantee (PBG)			
15	Performance Bank Guarantee (PBG) will be shared post confirmation of the project.		Please refer the RP and specifically clause 11.1 - Payment Terms of RP (Page No. 15)

Queries pertaining to VAPT.

S.No.	Query / Request of Empanelled Bidder	Response of the Bank to the Query / Request
Architecture Review		
1	Please share the number of locations to be covered as part of network architecture review.	DC (HO -Delhi) &DR(Mumbai)
2	Please share the details of cloud environment in place?	No cloud environment as on date.
3	Please share the number of accounts/subscriptions in cloud environments to be covered as part of architecture review.	Not Applicable
Network VAPT		
4	Please share the number of external IP addresses in scope of network VAPT assessment.	No of network devices = 35 No. of servers (physical and virtual) = 136 As on date the number of external applications are 11, internal applications are 4 and public facing applications are 4 but this may increase in the next year
5	Please share the number of internal IP addresses in scope of network VAPT assessment.	
Configuration Review		

6	Please provide the number of network devices / security solutions in scope of configuration review.	No of network devices = 35 No. of servers=136 (physical and virtual)
7	Please provide the details of cloud services (CSP specific) along with number of instances to be covered as part of scope.	Not Applicable
Application Security Assessment		
8	Provide the number of internal web applications to be covered as part of application security assessment (DAST).	04
9	Provide the number of mobile applications (android/iOS) to be covered as part of application security assessment (DAST). *Note: Please count android and iOS as different apps.*	01
API Security Assessment		
10	Provide the number of REST APIs (number of requests) to be covered as part of API security assessment.	Approximately 11 (Details to be shared with successful bidder)
11	Provide the number of SOAP APIs (number of requests) to be covered as part of API security assessment.	There are no SOAP APIs.
Revalidation		
12	Please confirm do we have to perform revalidation of all the findings comes out in the report	Yes revalidation of all the findings which comes out in the IS &Cyber Security report and VAPT report.

B. M/s KPMG

Sr. No.	Document Name	Page No.	Clause Name	Particular Clause	Query / Request of Empanelled Bidder	Response of the Bank to the Query / Request
1	Quotation for undertaking Information Security & Cyber Security Audit for the Year 2022-23 (July-June)	General Queries	-	-	We request NHB to extend the bid submission for one week, As we have to take internal approvals, compliance, legal, documents submission, etc.	The timeline for submission of commercial bids/quotations is being extended by three working days (from 25-08-2023 (Friday) before 6:00 p.m. to **30-08-2023 (Wednesday) before 6:00 p.m.**).
2	Quotation for undertaking Information Security & Cyber Security Audit for the Year 2022-23 (July-June)		-	-	We request NHB to clarify Do we have to submit a non-refundable RFP Cost of Rs. Five Thousand (Rs. 5,000/-)	Please refer the RP, wherein there is no mention about RFP cost.

3	Quotation for undertaking Information Security & Cyber Security Audit for the Year 2022-23 (July-June)/Requirement Proposal.	4	Evaluation of security needs of the current IT infrastructure of NHB	Pre-Audit / Verification of Cyber Security Incident Summary within prescribed timelines and any other such returns, required to be submitted to Reserve Bank of India (RBI), within prescribed timelines.	We understand that we may perform cyber security incident verification for those occurred during our audit period. Please let us know if our understanding is correct.	Yes.
4	Quotation for undertaking Information Security & Cyber Security Audit for the Year 2022-23 (July-June) /Requirement Proposal.	8	Information Security Audit & Cyber Security Audit (Type - Services)	To undertake Source code audit of Bank's public facing applications	We request NHB to clarify the number of applications for which source code audit will be performed. We also request NHB to clarify the lines of code in each application.	Public facing applications= 04 (ARRS-65589, RRP-14295, GRIDS-316901, HFR-67319) (As on date)
5	Quotation for undertaking Information Security & Cyber Security Audit for the Year 2022-23 (July-June) /Requirement Proposal.	9	Vulnerability Assessment, Analysis and Resolution (Type – Documentation & Service)	VAPT of Bank's internal applications throughout their lifecycle (pre-implementation, post implementation, after major changes).	We request NHB to clarify the count of internal applications and also request and the approximate count of VAPT to be conducted in pre implementation, post implementation and after major changes.	As on date the number of external applications are 11, internal applications are 4 and public facing applications are 4 but this may increase in the next year
6	Quotation for undertaking Information Security & Cyber Security Audit for the Year 2022-23 (July-June) /Requirement Proposal.	9	Vulnerability Assessment, Analysis and Resolution (Type – Documentation & Service)	Bidder /Auditor will be responsible to conduct pre deployment VAPT of any application during the contract period, in coordination with the bank and as per requirement of Bank. The list of application under IS Audit/VAPT scope will be kept updated accordingly.	We request NHB to clarify that count of applications to be tested before deployment.	As per the requirement of the Bank.

7	Quotation for undertaking Information Security & Cyber Security Audit for the Year 2022-23 (July-June) /Requirement Proposal.	36	Annexure II	Forensic Investigation of a cyber security incident	We request NHB to confirm what all locations are covered as part of RFP? We request NHB to confirm Does these include any remote locations as well ? We request NHB to confirm What is the average size of forensic images that are required to be taken ? We request NHB to confirm Who will bear the cost of Hard disks used for imaging, since this will be based on the size of image and number of devices that may be part of the incident?	Forensics investigation will be as per the need and requirement of the Bank. The hard disks required for imaging will be provided by the Bank.
8	Quotation for undertaking Information Security & Cyber Security Audit for the Year 2022-23 (July-June) /Requirement Proposal.	36	Annexure II	Forensic Investigation of a cyber security incident	We request NHB to confirm if KPMG team will be given SIEM access as part of log analysis or we have to conduct log analysis offline as part of digital forensics piece? We also request NHB to confirm if KPMG team will be given SIEM access as part of log analysis or we have to conduct log analysis offline as part of digital forensics piece?	SIEM access will be provided to the forensic investigator as per the need and requirement of the Bank.

9	Quotation for undertaking Information Security & Cyber Security Audit for the Year 2022-23 (July-June) /Requirement Proposal.	36	Annexure II	Forensic Investigation of a cyber security incident	We request NHB to confirm What all solutions are in place at NHB to conduct or enable the forensics investigator to perform end to end forensics -- for example EDR, SIEM, ELR (enterprise log repository) and is the coverage adequate (all endpoints/ network devices are integrated with security/ monitoring solutions)?	Bank will enable the forensic investigator to perform forensics as per extant tools and controls available at the time of incident.
10	Quotation for undertaking Information Security & Cyber Security Audit for the Year 2022-23 (July-June) /Requirement Proposal.	47	OBLIGATIONS OF THE IS AUDITOR- 3.3 (Service Level Agreement)	Conflict of Interest	We request to curtail the "Conflict of Interest" to the Engagement team only and members/ Affiliates to be termed as members/ Affiliates in India	It may be noted that the obligation mentioned in these clauses is on the IS Auditor, who is a Company/ Partnership Firm selected for carrying out IS Audit. Therefore, it cannot be limited to the team members only. Further, the expression "Affiliates" generally means with respect to any Person, any Person directly or indirectly Controlling, controlled by or under common Control with, that Person and these obligations are intended to apply equally on their Affiliates as well. Therefore, the modification suggested is not acceptable.
11	Quotation for undertaking Information Security & Cyber Security Audit for the Year 2022-23 (July-June) /Requirement Proposal.	47	OBLIGATIONS OF THE IS AUDITOR- 3.6 (Service Level Agreement)	Prohibition of Conflicting Activities	We propose NHB to curtail the "Conflict of Interest" to the Engagement team only and members/ Affiliates to be termed as members/ Affiliates in India	
12	Quotation for undertaking Information Security & Cyber Security Audit for the Year 2022-23 (July-June) /Requirement Proposal.	65	Commitments of Bidders- 3.4 (Pre-Contract Integrity Pact)	Commitments of Bidders	We propose NHB to curtail the "Conflict of Interest" to the Engagement team only and members/ Affiliates to be termed as members/ Affiliates in India	

13	Quotation for undertaking Information Security & Cyber Security Audit for the Year 2022-23 (July-June) /Requirement Proposal.	65	Commitments of Bidders- 3.4 (a) (Pre-Contract Integrity Pact)	The Bidder shall avoid any conflict of interest while discharging contractual obligations and bring, beforehand, any possible instance of conflict of interest to the knowledge of NHB, while rendering any advice or service.	We want to clarify to NHB team that we cannot disclose any potential conflicts. Any conflict related declaration can be given as on the current date only'	This Clause is part of the Pre-Contract Integrity Pact. The obligation on the Bidder under this clause is continuing in nature and may not be limited to "current date". At any point of time during the period of Contract it comes to the knowledge of the Bidder that there may arise possible instance of conflict of interest in discharging its duty under this Contract, the same is to be reported to NHB. Moreover, no changes can be acceptable to the Pre-Contract Integrity Pact as it is the format given by the CVC.
14	Quotation for undertaking Information Security & Cyber Security Audit for the Year 2022-23 (July-June) /Requirement Proposal.	48,49	Limitation of Liability - 3.11 (Service Level Agreement)	Limitation of Liability	We propose NHB to limit the liability arising under this contract It shall be limited to one times of the total contract value. We also propose to NHB that "We shall not be liable for any indirect or consequential losses".	Clause 3.9 of the Service Level Agreement, spell out the circumstances in which the liability of the IS Auditor will arise whereas Clause 3.11 specifies the quantum of liability. The liability arising under this contract shall be limited to one times of the total contract value, except in case of claim arising out of infringement of Intellectual Property Rights which will be based on actual loss suffered by NHB.
15	Quotation for undertaking Information Security & Cyber Security Audit for the Year 2022-23 (July-June)	4	PHASE – I EVALUATION	Evaluation of the extant design of Security Architecture	We request NHB to clarify the red team scenarios and the frequency for the red team exercise.	To conduct Red Teams exercise on half-yearly basis. Please refer the RP and specifically Point 1 B of the RP (Page 4)

C. M/s AKS IT Services Pvt. Ltd.

Sr. No	Requirement Proposal Section	Page No	Content of the RP	Query / Request of Empanelled Bidder	Response of the Bank to the Query / Request
1	4 Project Deliverables 4.2. Vulnerability Assessment, Analysis and Resolution	9	VAPT of Bank's internal applications throughout their lifecycle (pre-implementation, post implementation, after major changes). Bidder /Auditor will be responsible to conduct pre deployment VAPT of any application during the contract period, in coordination with the bank and as per requirement of Bank. The list of application under IS Audit/VAPT scope will be kept updated accordingly.	Please let us know the frequency of VAPT of bank's internal application and tentative no. of bank's application in our SoW.	04 times in a year External applications= 11 Internal applications = 4 *"As on date the number of external applications is 11, internal applications -4 and public facing applications – 4 but this may increase in the next year"*
2	4 Project Deliverables 4.1. Information Security Audit & Cyber Security Audit	8	To undertake Source code audit of Bank's public facing applications.	Please let us know the frequency of source code review and no. of bank's public facing application in our SoW with approx. no. of lines of code.	Once in a year. As on date the number of public facing applications are 4 but this may increase in the next year (ARRS-65589, RRP-14295, GRIDS-316901, HFR-67319) (As on date)
3	4 Project Deliverables 4.2. Vulnerability Assessment, Analysis and Resolution	9	The penetration testing exercise should be carried out like offensive security certified professionals so that the robustness of IT security infrastructure of the Bank can be assessed	Please confirm whether we have to perform external PT. If yes, then kindly confirm the No. of Public Ips.	Yes, Number of public Ips to be audited as on date are 11, but this may increase in the next year

Please be informed that the timeline for submission of commercial bids/quotations has been extended by three working days (from 25-08-2023 (Friday) before 6:00 p.m. to **30-08-2023 (Wednesday) before 6:00 p.m.**).

The quotations must be received by the Bank at the address specified in the Requirement Proposal, by **30-08-2023 (Wednesday), before 6:00 p.m.**

The quotations must be received by the Bank at the address specified, not later than the last date of submission of quotation /Commercial Bid as indicated above. **Any Bid received by NHB after due deadline for submission of Bids prescribed by NHB will be rejected and returned unopened.**