Reply to Pre-Bid Queries for Requirement proposal (RP) for Undertaking Information Security & Cyber security Audit of National Housing Bank

(RFP Reference No.: - GEM/2025/B/6767020 - NHB/Audit/RFP/02/2025-26 dated October 08, 2025)

S. no.	RFP Clause no	Activity/Existing clause Details	Bidder's Query/Suggestion/Remarks	NHB Response
1	3.11 Limitation of Liability	The IS & CS auditor's aggregate liability, in connection with the obligations undertaken as a part of this Project, whether arising under this Project regardless of the form or nature of the action giving rise to such liability (whether in contract, tort or otherwise), other than the circumstances mentioned in the sub-clause (ii) below, shall be limited to ……… times of the total contract value.	Provide clarification on the exact cap on the liability of the IS and CS auditor	**One time of the total contract value.**
2	NA	NA	We note that the scope of work under the RFP indicates services such as recommending / framing / suggesting changes / modifications of security policy, evaluation of policy documents. We understand that these services will not be performed from a legal perspective and will only be performed from a technical/ commercial perspective. We propose inclusion of the following clause: "Notwithstanding anything to the contrary, kindly note that we do not provide any legal services directly or indirectly since we are not permitted to provide the same. Our scope is limited to technical/commercial aspect, and our services will not include provision of any legal services or legal advice. No work performed by our employees shall be construed as legal service/legal advice."	**The bidders shall be providing the unconditional acceptance of the RFP terms & conditions.**

3	3.20 Audit	The IS & CS auditor shall allow and grant NHB, its authorized personnel, its auditors (internal and external) and/or the Reserve Bank of India/ other regulatory & statutory authorities, and their authorized personnel, unrestricted right to inspect and/ or audit its books and accounts, to provide copies of any audit or review reports and findings made on the IS & CS auditor, directly related to the Services. In case any of the Services are further outsourced/ assigned/ subcontracted to other IS & CS auditors in terms of the RP, it will be the responsibility of the IS & CS auditor to ensure that the authorities /officials as mentioned above are allowed access to all the related places, for inspection and/ or audit.	We propose inclusion of the following clause: “Any audit shall be subject to the following: (i) the audit shall be restricted to the engagement and shall be conducted with prior reasonable notice (ii) NHB or its authorized representatives shall execute a Non-Disclosure Agreement before such audit which shall govern the conduct of the audit and any results thereof; (iii) the auditors or the representatives of the NHB for the audit shall not be the IS & CS auditor's competitors; (iv) the audit shall not be conducted more than once in a calendar year and twice in entirety; and (v) any findings during the audit, shall be shared with the IS & CS auditor and be discussed and agreed mutually between the NHB and the IS & CS auditor for its closure.”	**The bidders shall be providing the unconditional acceptance of the RFP terms & conditions.**
4	3.16 non-compete	The IS & CS auditor will neither approach nor make any proposal for work for any employee of NHB directly or indirectly during the validity of this Agreement and for one year from the date of termination of this Agreement.	Please clarify if passive hiring is permitted—for instance, when an employee applies through public recruitment channels without any direct solicitation	**The bidders shall be providing the unconditional acceptance of the RFP terms & conditions.**
5	Evaluation of the extant design of Security Architecture	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.	Please clarify the following queries: 1. Can you provide details about the scope for the Red Teaming Exercises? Whether it would be External or Internal. Are there any specific scenarios that need to be covered?	**The Red teaming exercise will include social engineering and physical access attempts. Auditor is expected to conduct the External Assessment.**

6	Annexure-II	For any additional task assigned including forensic investigation of a cyber security incident as per the requirement of the Bank beyond the scope of work.	Please clarify the following queries: 1. What is the average size of forensic images that are required to be taken? 2. 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? 2. Will SIEM access will be given as part of log analysis, or we have to conduct log analysis offline as part of digital forensics piece?	**Forensic audit is a separate assignment. Forensic Audit shall be assigned to auditor, if required, by the Bank. Details shall be shared accordingly.**
7	6.1 Information Security Audit & Cyber Security Audit (Type - Services)	The Security Architecture Design includes the Head Office, and the Regional Offices combined i.e., including the interconnection between the two offices and the interfaces used by various applications on the NHB network.	Please clarify the following queries: 1. How many Regional Offices are included in the scope of the Security Architecture Design?	**Presently Bank has 17 Regional offices.**
8	6.1 Information Security Audit & Cyber Security Audit (Type - Services)	To undertake configuration of Security Architecture including Network and Applications of NHB to address the same.	Please clarify the following queries: 1. On how many approx. components configuration review needs to be performed.	**Network device approx. 70, Servers approx. 190, Active directory, EDR, WAF, Proxy, NAC, Database, SAN, Backup solution**
9	6.1 Information Security Audit & Cyber Security Audit (Type - Services)	Review of all Application Programming Interfaces (APIs) in the production for vulnerabilities.	Please clarify the following queries: 1. How many APIs are currently in production and included in the scope of vulnerability assessment?	**At present four applications have API.**
10	6.1 Information Security Audit & Cyber Security Audit (Type - Services)	Coverage of secure configuration review of, but not limited to, Bank's security solutions, OS, applications, servers, and network devices.	Please clarify the following queries: one. Please confirm the number and types of security solutions, OS platforms, applications, servers, and network devices in scope.	**Network device approx. 70 (switch, firewall, NAC, VPN devices), Servers approx. 190 (Ubuntu, RHEL, Windows), Active directory, EDR, WAF, Proxy, NAC, Database, SAN, Backup solution, thirty applications, Desktops-300 (may be increased during audit period).**
11	6.1 Information Security Audit & Cyber Security Audit (Type - Services)	To undertake Source code audit of Bank's public facing applications. Source code review for in-house developed applications to be performed.	Please clarify the following queries: 1. Number of applications for which source code audit will be performed. 2. The lines of code in each application.	**At present, the number of applications is eleven, for which source code audit will be performed.**

12	6.1 Information Security Audit & Cyber Security Audit (Type - Services)	Configuration review to be performed for firewalls, WAF, and proxy. Firewall, WAF, Proxy, Antivirus, DLP and NAC rule/policy review to be performed.	Please clarify the following queries: 1. The number of firewalls, WAFs, proxies, antivirus, DLP, and NAC solutions in scope.	**Firewall-6, WAF solution, NAC-2, VPN-2, Proxy solution-1, EDR-1, DLP (inbuilt with EDR & Office 365)**
13	6.1 Information Security Audit & Cyber Security Audit (Type - Services)	Credential based application and servers' vulnerability scanning to be performed on annual basis by IS auditor.	Please clarify the following queries: 1. Please confirm the number of applications and servers in scope for credential-based scanning. 2. It will be performed only once (annually) or twice a year? What is the frequency?	**All applications the applications and servers mentioned in scope of RFP shall be subject to credential-based scanning. The frequency for scanning is as per frequency of IS & CS audit mentioned in the RFP.**
14	6.2 Vulnerability Assessment, Analysis and Resolution	VAPT of Bank's internal applications throughout their lifecycle (pre implementation, post implementation, after major changes).	Please clarify the following queries: 1. 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.	**At present, Bank is having 07 nos of Internal applications.**
15	6.2 Vulnerability Assessment, Analysis and Resolution	Bidder / selected empanelled 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.	Please clarify the following queries: 1. How many such applications are generally developed?	**Development cannot be predicted, however for estimation purpose, it may be approx. ten.**
16	6.2 Vulnerability Assessment, Analysis and Resolution	The list of applications under IS Audit/VAPT scope will be kept updated accordingly.	Please clarify the following queries: 1. As per the RFP, there are 25 applications as of now, above which new applications can be added. Hope our understanding is correct.	**Yes, application may be increased.**
17	6.2 Vulnerability Assessment, Analysis and Resolution	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 clarify the following queries: 1. Please confirm whether we have to perform external PT. If yes, then kindly confirm the No. of Public Ips. 2. Confirm if any other activity needs to be included in this.	**External PT to be performed. Presently the nos of public IPs are 140.**
18	6.4 Training Programs & Training Material for NHB officials	The bidder/ selected empanelled auditor will develop courseware, impart training, and provide training material for the NHB officials, NHB Administrators and other related users.	Please clarify the following queries: 1. Please confirm how many times the training material needs to be provided, as well as the frequency of the training sessions.	**The IT & cyber security awareness training for Bank's employees, on-site support staff/vendors handling Bank's IT infrastructure, (including specialised security training for IT team) in form of lecture, seminar/webinar, interactions, and**

				presentations are to be conducted by the auditor on quarterly basis.
19	Audit of vendors of IT & IS services	Audit of vendors of IT & IS services	Please clarify the following queries: 1. What is the number of vendors for which the audit needs to be performed, and what will be the frequency of it.	**At Present following nos of vendors are subject to vendor audit.** **8 - vendor for IT outsource services.** **1 - vendor for CISO services**
20	Phase 1 -I	> Network and the devices in use, Firewall Rule Base Review. > Operating Systems – Setup, Configuration, Tuning, License Audit, etc. > Database, Systems and Applications (Web facing and non-Web facing) – Setup, configuration, Tuning, Database Audit, etc.	Kindly confirm number of network devices, applications (web facing and non-web facing), database to be reviewed	**Network device approx. 70 (switch, firewall, NAC, VPN devices), Servers approx. 190 (Ubuntu, RHEL, Windows), Active directory, EDR, WAF, Proxy, NAC, Database, SAN, Backup solution, thirty applications, Desktops-300 (may be increased during audit period).**
21	Phase 1 -I	> Pre-Audit / Verification of KRI returns within the timelines prescribed by the Bank. > Pre-Audit / Verification of Public facing applications and databases within prescribe timelines. > Pre-Audit / Verification of Cyber Security Incident Summery. > Pre-Audit / Verification of any other returns, required to submit to Reserve Bank of India (RBI).	Successful bidder will review the returns but is not required to provide attestation. Please confirm our understanding.	**The Auditor has to review and validate the return.**
22	Phase 1 -I	Cybersecurity set-up	Please specify areas and controls to be covered in "cybersecurity set-up"	**The auditor will need to review all areas of existing cyber security setup.**

23	Phase 1 -I	Pre-Audit / Verification of any other returns, required to submit to Reserve Bank of India (RBI).	Please specify number of returns required to be reviewed	**The number of returns cannot be specified as this is RBI's requirement**
24	Phase 1 -I	Evaluation of the extant security architecture, change recommendations /new designs/layouts, and documentation of the security architecture so as to conform to the RBI Guidelines, International Standards, and Industry wide accepted best practices.	Kindly specify which RBI guidelines, international standards are to be considered.	**Please refer the master circulars/directions/guidelines issued by RBI on IT systems, infrastructure etc on time to time. Further the auditor needs to ensure that compliances are as per Cert in/ other regulatory directions.**
25	Phase 1 -I	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.	Successful bidder will not be responsible for implementing controls for the vulnerabilities identified. Please confirm our understanding.	**The auditor shall be providing the recommendations and support. Based on the recommendations, Bank shall fix the vulnerabilities.**
26	Phase 1 -I	Evaluation of the current Operational Procedure and Security Policy for processes that have been computerized. Recommending and framing operation procedure and security policy for these processes.	Kindly confirm number of policies/procedures to be reviewed and also to be designed.	**The bank will provide the copy of all the internal policies and SOP pertaining to the project. Further the auditor needs to ensure that compliances are as per RBI/Cert in/ other regulatory directions.**
27	Phase 1 -I	Evaluation of web application configuration and testing reporting of gaps/vulnerabilities/improvements (if any). Suggesting solutions/mitigating strategies to tackle the same.	Kindly confirm number of web applications to be covered	**At present, approx. thirty number of web applications to be covered.**

28	Phase 1 -I	To carry Software Audit of Bank's internal applications and portals (including the applications and portals developed during the audit period).	Kindly confirm number of applications and portals to be covered	**At present, approx. thirty number of web applications to be covered.**
29	General	NA	Please confirm the location(s) from which the project has to be carried out.	**The base location from which the audit is to be conducted is Head office of NHB at Delhi. Sample based onsite audit is acceptable only for regional offices.**
30	6	The Auditors shall carry out audit activities and furnish audit reports for various functions separately. In addition to the reports, the Auditors shall also provide Compliance Certificates.	Kindly confirm areas for which compliance certificate is required.	**Please refer the deliverables section of the RFP.**
31	Format for Commercial Bid (to be submitted along with a covering letter)	Format for Commercial Bid (to be submitted along with a covering letter)	Commercial bid annexure is not required to be uploaded on GEM portal and bid amount needs to be submitted on GEM. Please confirm our understanding	**The commercial bid annexure is required to be submitted along with the other documents as mentioned in RFP on GeM Portal.**
32	Annexure VIII	Format of Bank Guarantee	Bank guarantee is to be submitted by successful bidder only. Please confirm our understanding	**Bank guarantee is to be submitted by successful bidder only.**
33	Annexure X	Confidentiality cum NDA	Confidentiality cum NDA is to be submitted by successful bidder only. Please confirm our understanding	**Confidentiality cum NDA is to be submitted by successful bidder only.**
34	General	NA	We kindly request to please extend bid submission date from 29th October 2025 to 07th November 2025	**The last date of submission of financial bid is 29.10.2025.**

35	5	Further, the Bank has its Regional Offices at Ahmedabad, Bengaluru, Bhopal, Bhubaneshwar, Chandigarh, Chennai, Delhi, Guwahati, Hyderabad, Jaipur, Lucknow, Kolkata, Mumbai, Patna, Raipur, Ranchi, and Thiruvananthapuram. which are connected to the centralized Data Centre located at Head Office. IS & CS Audit will cover the access control mechanism implemented for these offices also.	1. Kindly confirm if access management is done centrally and 2. Whether travel to regional offices is required?	**The Access management is done centrally. Travel to regional offices is need basis.**
36	Phase I - I - C	IS & CS Auditor must interact with all Head of the Departments (HODs) in the Bank to obtain their views/feedback towards Information Security & Cyber Security measures taken by the Bank and evaluate the gaps (if any) based on their feedback.	NHB will appoint a SPOC to facilitate coordination between auditors, HODs and other NHB stakeholders during the audit. Please confirm our understanding	**NHB will appoint a SPOC to facilitate coordination between auditors, HODs and other NHB stakeholders during the audit. However, auditor needs to interact with all Head of the Departments (HODs) in the Bank to obtain their views/feedback towards Information Security & Cyber Security measures taken by the Bank and evaluate the gaps**
37	Phase II-II	On completion of the compliance review, the IS & CS auditor has to provide IS Audit & CS Audit compliance document/reports to that effect.	Please confirm the timeline for initiating the compliance review after submission of draft audit report.	**Please refer the Project schedule section of the RFP.**

38	10.25	The successful bidder(s) will sign a Service Level Agreement (SLA), the Confidentiality cum Non-Disclosure Agreement (NDA) and Pre-Contract Integrity Pact as per Annexure IX, X & Annexure XI with NHB within 30 days of award of the service order or within such extended period as may be decided by the Bank.	Service Level Agreement (SLA), the Confidentiality cum Non-Disclosure Agreement (NDA) and Pre-Contract Integrity Pact as per Annexure IX, X & Annexure XI are not required at the time of submission of bid. It will be required to be submitted by successful bidder. Please confirm our understanding	**Pre-Contract Integrity Pact shall be submitted by the bidder with all the other required documents as mentioned in the RFP.**
39	Section 5 – Scope of Work	IS & CS Audit to cover HO, DR Site, and 17 Regional Offices	Please confirm whether physical visit is required for all Regional Offices or sample-based onsite audit is acceptable with remote validation for others. What is the base location from which the audit is to be conducted?	**The base location from which the audit is to be conducted is Head office of NHB at Delhi. Sample based onsite audit is acceptable only for regional offices.**
40	Section 5(a) – IT Infrastructure	Coverage includes Head Office, DR Site, Regional Offices	Request approximate count and types of network/security devices (firewalls, routers, switches, servers, endpoints) for estimation of audit effort.	**Network device approx. 70 (switch, firewall, NAC, VPN devices), Servers approx. 190 (Ubuntu, RHEL, Windows), Active directory, EDR, WAF, Proxy, NAC, Database, SAN, Backup solution, thirty applications, Desktops-300 (may be increased during audit period).**
41	Section 5(a) – Cyber Security Framework	Includes CSOC and Cyber Security Preparedness Indicators	Kindly confirm if the CSOC setup (SIEM, EDR, SOC operations) will be included in detailed configuration review and monitoring log verification.	**Please refer Annexure I of RFP**
42	Section 5 – Red Teaming Exercise	Half-yearly red teaming on public-facing applications	Please clarify whether red teaming includes social engineering, and physical access attempts or limited to network/web exploitation. Are we expected to conduct both Internal as well External Assessment?	**Red teaming will include social engineering and physical access attempts. Auditor is expected to conduct both External Assessment.**

43	Section 5(b) – Phased Audit Approach	Phase I – Evaluation, Phase II – Communication, Phase III – Review & Certification	Clarify if each phase will be separately scheduled with acceptance sign-off or all phases run continuously within a single audit cycle.	**The project milestones are mentioned in the deliverables & project Schedule section of the RFP.**
44	Section 5(d) – Web Facing Applications	25+ applications listed (SAP, CRAMIS, PMAY-CLSS, GRIDS, UIDF, etc.)	Please confirm which of these applications are external-facing and which are internal; also, whether test URLs or UAT instances will be provided.	**Will be shared with successful bidder**
45	Section 5(d) – Source Code Review	Source code audit of public-facing applications	Confirm the number of applications for which source code will be shared, the language/stack (Java, .NET, PHP, etc.), and whether access will be local or remote.	**Approx 13. At present all applications are on dot(.) Net**
46	Section 5(d) – API Security Review	Review of APIs in production environment	Kindly provide indicative count of APIs and whether Postman collections / API documentation will be shared for testing.	**At present four applications have API.**
47	Section 5(d) – Audit of Mobile Applications	All applications and portals implemented in the Bank	Clarify if any Android or iOS mobile apps are in scope; if yes, please confirm APK/IPA access and test environment details.	**1 app for android & iOS both**
48	Section 5 – Evaluation of IT Infrastructure	DC (Delhi) and DR Site (Navi Mumbai)	Please confirm if both sites are managed by in-house NHB teams or outsourced to a data-centre service provider, and whether vendor coordination will be facilitated.	**Both sites are managed by inhouse NHB team in coordination with outsourced service provider.**
49	Section 5 – Cyber Security Evaluation	Conduct Red Team exercise on half-yearly basis	Confirm whether the Red Team engagement will be executed on production or isolated replicated environment.	**Red Team engagement will be executed Replicated environment.**
50	Section 5 – Risk Assessment	Review of KRI returns and RBI submissions	Please clarify the list of KRIs to be validated and the reporting cycle to RBI (monthly/quarterly).	**KRIs are as per RBI return and the frequency is quarterly.**
51	Section 5(c) – Evaluation of System Implementation	SAP, CRAMIS, PMAY-CLSS, GRIDS, UIDF, etc.	Confirm if SAP system audit includes both functional access control and BASIS configuration review.	**Yes. SAP system audit includes both functional access control and BASIS configuration review.**

52	Section 5(c) – Department Interaction	IS & CS auditor must interact with all HODs	Request approximate number of departments / stakeholders to plan interview sessions.	**Bank has 22 Departments at HO and seventeen regional offices. The major interaction of IS& CS auditor is with ITD, CISO & Audit dept.**
53	Section 5 – Outsourced Services	Audit of vendors of IT & IS services	Kindly provide number of vendors in scope (for example: AMC, SOC, cloud, DR, or network vendors).	**At Present following nos of vendors are subject to vendor audit. 8 - vendor for IT outsource services. 1 - vendor for CISO services**
54	Section 6 – Deliverables	List of deliverables (IS Audit, CS Audit, VAPT, Red Team, Vendor Audit, Training)	Clarify whether each deliverable needs a separate certification letter or consolidated report submission.	**Each deliverable requires separate certification/report.**
55	Section 6.1 – IS & CS Audit	Firewall, WAF, Proxy, DLP, NAC policy review	Kindly confirm whether auditors will be given read-only administrative access or observation-based review with screenshots/logs.	**The auditors will be given read-only admin access.**
56	Section 6.1 – Configuration Review	Antivirus, AD, Patch, User Access Management	Confirm if tools like Nessus/Qualys, Microsoft Baseline Analyzer, or internal scripts can be used for verification.	**Auditor may use both tools.**
57	Section 6.2 – VAPT	Quarterly VAPT and post-remediation verification	Confirm if re-testing will be considered part of quarterly deliverables or treated as separate effort.	**Retesting is part of quarterly VAPT exercise. Further for other takes as mentioned in RFP, the retesting shall be done as per scope.**
58	Section 6.2 – VAPT	Credential-based scanning of servers	Please confirm whether credentialed scans are required for Windows, Linux, and DB servers; and whether local admin credentials will be shared.	**Yes**
59	Section 6.2 – Patch Review	Quarterly patch and security update review	Confirm whether patch review covers only OS and applications or also includes firmware/network devices.	**Patch review includes firmware/network devices also**
60	Section 6.2 – Email Security Testing	Check DKIM, SPF, DMARC controls	Confirm if email spoofing tests can be performed with NHB approval.	**Yes.**

61	Section 6.2 – API Testing	VAPT for developed/customized APIs	Request confirmation on number of APIs and expected authentication methods (JWT, OAuth, Basic Auth, etc.).	**At present four applications have API.**
62	Section 6.3 – Reporting	IS/CS Audit Report: Detailed Findings, Compliance, Knowledge Transfer	Clarify whether Bank requires separate executive summary for senior management and technical report for IT team.	**Please refer the deliverables section of the RFP.**
63	Section 6.4 – Training Programs	Quarterly employee awareness training	Kindly specify expected audience count, language preference (English/Hindi), and if NHB expects on-site session recordings or LMS upload.	**Training will be in bilingual and will be conducted online.**
64	Section 7 – Project Schedule	Audit report submission timelines (15 Jan 2026 & 30 July 2026)	Clarify whether separate timelines apply for VAPT, Red Team, and Vendor Audit deliverables or follow same date.	**Yes. For timelines, please refer the project Schedule section of the RFP.**
65	Section 7 – Quarterly Deliverables	VAPT reports to be submitted within 45 days from last day of quarter	Please confirm if NHB expects report submission even if remediation is ongoing or after closure verification.	**The maximum Timelines permitted for VAPT is 45 days from the last date of the quarter under audit.**
66	Section 6 – Vulnerability Exploitation	Penetration testing scope	Please confirm if controlled exploitation is allowed to validate identified vulnerabilities.	**It may be allowed, while ensuring uninterrupted operation of production services.**
67	Section 6 – Tools & Automation	Auditor shall use industry-accepted tools	Confirm if use of open-source tools (e.g., Nmap, Nikto, SQLMap) alongside licensed tools is permitted.	**Yes**
68	Section 6 – Re-Testing	Validation after remediation	Please confirm the number of re-testing cycles included per quarter (one or multiple).	**Validation is required on all the compliances submitted by the bank.**
69	Section 5 - Scope of Work (I – Risk Assessment & Identification of Security Needs)	Pre-Audit / Verification of any other returns, required to submit to Reserve Bank of India (RBI	What are the specific returns being mentioned here? Does it include compliance reports submitted in DAKSH portal?	**Yes**

70	Section 5 - Scope of Work (I – Risk Assessment & Identification of Security Needs)		Please clarify whether the Bank expects a formal risk assessment methodology to be followed (e.g., ISO 27001) for review of IS - RMF	**Yes**
71	Section 6 - Deliverables Review of IS-RMF and Risk Registers	Review of Information Security – Risk Management Framework (IS-RMF) document and creation of Information Security Risk Registers based on the IS-RMF of the Bank.	Please clarify if the deliverable should include creation of a new Risk Register template or only populate the Bank's existing IS-RMF register based on audit findings.	**Creation of a new Risk Register template based on IS-RMF of the Bank is required.**
72	Section 5 - Scope of Work (I. Risk assessment and identification of security needs, sub-section c. Evaluation of the System implementation in the Bank)		Please clarify which specific regulations, guidelines, or security standards the current Operational Procedures and Security Policies are to be evaluated against.	**The bank will provide the copy of all the internal policies and SOP pertaining to the project. Further the auditor needs to ensure that compliances are as per RBI/Cert in/ other regulatory directions.**
73	Scope of Work (II. Detailing the Security Gaps)	Audit of all Outsourced activities and services	Kindly confirm if the vendor audit will require evaluation against RBI IT Outsourcing Guidelines (2023) and whether vendor self-certifications / third-party SOC 2 reports can be accepted as evidence.	**Yes**
74	Section 6 - Deliverable, Sub-section 6.3 IS Audit & CS Audit Report (Type - Documentation)		Kindly confirm the expected scope and content of the Knowledge Transfer report. Should it primarily document the awareness sessions conducted along with participant feedback?	**The report shall be based on the detailed interaction done during the entire project implementation.**

75	Section 6 - Deliverable, Sub-section 6.3 IS Audit & CS Audit Report (Type - Documentation)		What are the specific RBI Guidelines to be audited against for the IS and CS Audit?	**Please refer the master circulars/directions/guidelines issued by RBI on IT systems, infrastructure etc. on time to time.**
76	Section 6. Deliverables Sub-section 6.2 Vulnerability Assessment, Analysis and Resolution (Type – Documentation & Service)	Fixing/addressing shortfalls which can be addressed immediately.	Are we expected to fix the vulnerabilities as well or only provide recommendations and support?	**The auditor shall be providing the recommendations and support. Based on the recommendations, Bank shall fix the vulnerabilities.**

****