राष्ट्रीय
आवास बैंक
NATIONAL
HOUSING BANK

**GeM Bid Number:** *GEM/2026/B/7255685* **dated February 18, 2026 RFP Reference No.:** *NHB/Audit/RFP/03/2025-26* **Request for Proposal (RFP) for Undertaking Information & Cyber Security Audit of National Housing Bank.**

**The replies to the pre-bid queries received are placed herewith.**

ले. प. वि.
Audit Deptt.

**Reply to Pre-Bid Queries for Request for proposal (RFP) for Undertaking Information & Cyber Security Audit of National Housing Bank**

*(RFP Reference No.: - GEM/2026/B/7255685- NHB/Audit/RFP/03/2025-26 dated 18.02.2026)*

| S. no. | RFP Clause no | Activity/Existing clause Details | Bidder's Query/Suggestion/Remarks | NHB Response |
|---|---|---|---|---|
| 1. | Pg 22 of 125, Deliverables item 10 (Other Certifications & Reports); Commercial Bid Table 1/2 (Annexure VI). | "Other Certifications & Reports As per requirement specified by Bank." | Please clarify whether any additional certifications and reports requested during the contract will be included in the fixed Table 1 amount or will be treated as additional tasks billed at Table 2 man day rate (with prior approval). | **As per table I of Financial bid.** |
| 2. | Pg 21 of 125, Section 7 Project Schedule item 5 (Vendor(s) Audit of IT & IS services). | "Vendor(s) Audit of IT & IS services As per requirement specified by Bank. Reports to be submitted within 30 days from initiation of the audit." | Please provide an estimated number of vendors to be audited per year, indicate whether audits are onsite, offsite, or document based, and confirm expected notice period and access expectations for vendor coordination. | **Estimated number of vendors is ten which may increase during the period of contract. Visits may be required for certain vendors.** |
| 3. | Pg 15 of 125, Scope bullets under CS audit: annual review of CSOC use cases. | "Annual review of all use cases in CSOC is to be carried out by the auditor… recommendation along with full technical details of new cases…" | Please confirm the SIEM and SOAR tools in use, key onboarded log sources, and whether read only access to CSOC dashboards, use case rules, alert logic, and historical incidents will be provided for the annual use case review. | **The Bank is using Elastic SIEM and Fortinet SOAR.**<br><br>**Key Onboarded Log Sources: Major integrated sources include security, infrastructure, and application logs such as firewall, endpoint security, identity platforms, office 365, web/application servers, and other critical security telemetry already onboarded within the monitoring scope.**<br><br>**Read only access can't be provided. However, CSOC team** |

| | | | | |
|---|---|---|---|---|
| | | | | will be available for showing all use cases, alert logic, historical incidents, etc. |
| 4. | Pg 14 of 125, Conducting Cyber Audit: phishing simulation. | "Quarterly Phishing simulation exercise to be conducted by the Auditor in a scenario proposed by the Bank." | Please clarify expected target population per campaign (all users or specific groups), allowed lures and channels, whether credential capture simulation is permitted, required approvals, and the reporting metrics expected (click rate, submission rate, reporting rate, time to report, etc.). | **The phishing simulation is to be done for all officers of the bank through email. Credential capture simulation is permitted. Prior approval for conducting the phishing simulation should be taken.**<br><br>**Following report parameters are required -**<br>**1. List of users who submitted the data.**<br>**2. List of users who clicked the link.**<br>**3. List of Users who opened the email.**<br>**4. List of Users who submitted data more than once.**<br>**5. List of Users who clicked link more than once.**<br>**6. Default users – Users who submitted data in the previous simulation as well as in this simulation.**<br>**7. Moderate users – Users who clicked the link in the previous simulation as well as in this simulation.**<br>**8. User aware – Users who clicked or submitted in the previous simulation but not in this one.** |

| | | | | |
|---|---|---|---|---|
| 5. | Pg 14 of 125, Conducting Cyber Audit: phishing simulation responsibility. | "Quarterly Phishing simulation exercise to be conducted by the Auditor..." | Please confirm whether NHB will provide the phishing simulation platform and infrastructure (mailing domain, landing pages, tracking), or whether the auditor must provide it. If auditor provided, please confirm whether this is included in Table 1 pricing or treated as a separate reimbursable or Table 2 task. | **Phishing simulation platform and infrastructure is bidder's responsibility. The bank will not provide these. Pricing is included in Table 1 pricing.** |
| 6. | Pg 19 of 125, VAPT scope: pre deployment VAPT and application list updated. | "Selected Auditor will be responsible to conduct pre deployment VAPT of any application during the contract period... The list of applications under IS Audit/VAPT scope will be kept updated accordingly." | Please provide an estimated count of pre deployment VAPT requests during the contract and the expected notice period. Please also confirm the expected turnaround SLA for pre deployment VAPT reporting to meet release timelines. | **There is no definite count of pre-deployment audit of applications/enhancements.** |
| 7. | Pg 19 of 125, VAPT scope: verification of closure/compliance post report submission. | "Verification of the closure/compliance of VAPT observations post submission of the report..." | Please confirm the expected number of closure verification and retest cycles per quarter that are included, and the expected turnaround time from NHB teams for fix evidence and remediation sign off. Also clarify whether closure verification must be performed in production, staging, or both. | **Compliance verification and retesting is to be performed on ongoing basis.** |
| 8. | Pg 19 of 125, VAPT lifecycle; Pg 12 of 125, item on API/interface testing (Internal & External). | "VAPT of Bank's internal applications throughout their lifecycle..." and "Whether API/interface testing is conducted (Internal & External)" | Please confirm whether mobile applications are in scope if any exist for NHB services. Please also clarify whether API testing includes partner and third-party integrations (internal, external), and whether test environments and credentials will be provided for authenticated testing. | **No. of mobile application :- One**<br><br>**API testing includes partner and third-party integrations (internal, external). Test environments and credentials will be provided by NHB for authenticated testing.** |
| 9. | Pg 19 of 125, VAPT scope: list of applications kept updated. | "The list of applications under IS Audit/VAPT scope will be kept updated accordingly." | Please share the current list of in scope applications and portals (public facing and internal), and tag which are in scope for VAPT, pre deployment VAPT, software audit, source code review, and API testing. Also share | **Be guided as per RFP.** |

| | | | | |
|---|---|---|---|---|
| | | | environments (UAT, staging, production), URLs, and ownership for coordination. | |
| 10. | Pg 6 of 125, Scope: audit covers HO Delhi and RO Mumbai; RO list provided. Pg 21 of 125, Section 7 Project Schedule: deputing officials at HO Delhi and RO Mumbai; Pg 16 of 125 MPLS architecture notes. | Scope mentions coverage for head office at Delhi and Regional office at Mumbai and lists 17 Regional Offices connected to centralized DC. | Please clarify onsite expectations: whether onsite visits are required at all Regional Offices, or only at HO Delhi plus RO Mumbai (and DC/DR), with remaining RO coverage through remote evidence. Please also confirm expected frequency and duration of onsite presence. | **Be guided as per RFP.** |
| 11. | Pg 18 of 125, Security Architecture scope; Pg 14 and Pg 18, addressing gaps and fixing shortfalls. | "To undertake configuration of Security Architecture including Network and Applications..." and "Fixing/addressing shortfalls which can be addressed immediately." | Please confirm whether the selected auditor is expected to implement configuration changes and fixes, or only to recommend and validate fixes executed by NHB teams and OEM partners. If implementation support is required, please clarify whether it is included in Table 1 pricing or treated as additional tasks billed at Table 2 man day rate with prior approval and change control. | **Bidder has to provide proper recommendation with required rectification steps / command / configuration changes. Bidder to provide mitigation steps till the observation is complied.** |
| 12. | Pg 21 of 125, Section 7 Project Schedule: Red Teaming HY July 2025 to Dec 2025; Pg 30 of 125, Section 11.2 Payment terms: Red teaming report HY (July 2025 to Dec 2025). | Red teaming schedule includes "HY July 2025 to Dec 2025" and payment milestone also references the same period. | Since the RFP is being bid in Feb 2026, please clarify whether "HY July 2025 to Dec 2025" is a typographical error or whether NHB expects retrospective coverage. If retrospective, please confirm what evidence sources will be made available for that period and whether NHB will accept a fresh red team exercise post award along with a retrospective review report. | **Period in which red teaming exercise for HY July 2025 to Dec 2025 is to be conducted is :- April to June2026.** |
| 13. | Page 5 | Number of Devices for VA PT | Whether the VAPT of devices can be conducted remotely via secure VPN from the bidder's office, or is it mandatory to perform the activity onsite at the client's premises? | **VAPT exercise to be performed onsite at the client's premises.** |

| | | | | |
|---|---|---|---|---|
| 14. | Page 15 | Black Box Security Audit of all public facing applications | Please confirm whether the VAPT of devices is required to be conducted strictly under a Black Box testing approach. | **VAPT to be conducted on credential-based scanning.** |
| 15. | Page 9 | Configuration Audit of Networking & Security Updates | With respect to device configuration audit, please confirm whether the review is to be conducted on a sample basis. If yes, kindly confirm whether the sample size will be up to 5% of the total devices. | **Complete inventory is required to be Audited.** |
| 16. | Page 12 | Security and Network Architecture review including hardening and check for DNSpionage activity | Kindly confirm how many Network Architecture Diagrams are available for review under the current scope. | **Be guided as per RFP.** |
| 17. | Page 9- point e.22- | Review of adequacy of Physical Security (Guards, Arms etc) | Need more clarification on checking the Adequacy of arms? | **Bidder to review the physical security of IT infrastructure as per industry standard.** |
| 18. | Page 9- point g.14 | Review of file permissions | File permissions shall be checked by installing a server analysis software or through the existing documentation as per IT policies. | **Both. Permission will be given on case-to-case basis.** |
| 19. | Page 11- point i.14- | Impact of Backend Updates | The impact is assessed at the time of updates and mentioned in change control. Kindly explain in detail about its scope. | **Gap analysis to be submitted by bidder.** |
| 20. | Page 12-point n.11- | Source code review report & logic testing report along with its closure status. | Do you have a developer environment or testing environment to test the logics of business application? | **Yes.** |
| 21. | Page 13-point n.37 | Data migration plan to be prepared and tested | Please give more clarity and context on data migration plan? | **This is for pre-deployment audit of application. Bidder to submit data migration gap analysis.** |
| 22. | | 6.5 Provide Ce6.5 Provide Certification/Compliance Report(s) for the IS Audit & CS Audit, VAPT, Red Teaming Exercise and for Audit of Vendors | Please confirm whether the deliverable from PwC will be shared with the regulator as required under this point. | **Yes.** |

| | | | | |
|---|---|---|---|---|
| | | of IT & IS services (Type – Documentation & Services) :- The bidder/selected auditor is to provide NHB a certification/compliance report each for IS Audit and for CS Audit (separately), for VAPT, Red Teaming Exercise and Audit of Vendors IT and IS services.rtification/Compliance Report(s) for the IS Audit & CS Audit, VAPT, Red Teaming Exercise and for Audit of Vendors of IT & IS services (Type – Documentation & Services) :- The bidder/selected auditor is to provide NHB a certification/compliance report each for IS Audit and for CS Audit (separately), for VAPT, Red Teaming Exercise and Audit of Vendors IT and IS services. | | |
| 23. | Red Team Scope related query | - | Is the assessment to perform external, internal, or both? | **External Assessment** |
| 24. | Red Team Scope related query | - | How many Active Directory domains are there and how many domains should be covered in the internal Red Team assessment? | **There is single AD domain.** |
| 25. | Red Team Scope related query | - | Is the Active Directory setup based in the cloud, on-premises, or a combination of both? | **Hybrid setup of AD.** |
| 26. | Red Team Scope related query | - | Is physical security testing part of the scope? If so, how many locations are included? | **Demonstrate the ability to gain unauthorized access into the bank's internal network.** |

| | | | | |
|---|---|---|---|---|
| | | | | Assess ability to move from initial foothold to privileged access.<br>Test ability to exfiltrate sensitive financial or business data.<br>Demonstrate the ability to pivot across critical segments.<br>Measure SOC effectiveness. |
| 27. | Red Team Scope related query | - | What are the primary objectives to be achieved in the Red Team assessment? | Based on NHB's existing infrastructure landscape and observations from previous assessments, phishing campaigns and social engineering exercises should be prioritized to assess and enhance the organization's resilience against these attack vectors. |
| 28. | Red Team Scope related query | - | Are there specific threats or scenarios that should be prioritized? | Based on NHB's existing infrastructure landscape and observations from previous assessments, phishing campaigns and social engineering exercises should be prioritized to assess and enhance the organization's resilience against these attack vectors. |
| 29. | Red Team Scope related query | - | In Red Team exercise, the team will focus more on the vulnerabilities which would give us an initial foothold in the network. In case we identify any high vulnerabilities during the scan, we will exploit them and leverage them for further attacks. However, the team will not | Yes. |

| | | | | |
|---|---|---|---|---|
| | | | utilize a thorough penetration testing approach for the remaining vulnerabilities as this is not a VAPT exercise. Could you please confirm if this approach aligns with your expectations? | |
| 30. | Red Team Scope related query | - | Is revalidation part of red team scope? | **Yes.** |
| 31. | Scope Of Work | | Please confirm whether Vulnerability Assessment and Penetration Testing (VAPT) activities will be conducted onsite or remotely. | **VAPT exercise to be performed onsite at the client's premises.** |
| 32. | Scope Of Work | | In the case of onsite execution, kindly clarify whether NHB will provision the infrastructure for the VAPT (attacking machine), with our team configuring the environment using your resources, or if AQM is expected to bring and manage the required infrastructure. This includes mobile devices (rooted/jailbroken and standard). | **NHB will provide desktops for VAPT.** |
| 33. | Scope Of Work | | In the event that identified vulnerabilities remain unresolved after the initial revalidation cycle, please specify the number of additional revalidation iterations included within the agreed scope. | **Compliance verification and retesting is to be performed on ongoing basis.** |
| 34. | Scope Of Work | | Please confirm whether a dedicated VAPT report is required specifically for APIs, including those involved in server-to-server communication that are not externally exposed. - If required, kindly provide an estimate of the total number of individual API endpoints to be assessed. | **API VAPT report may be incorporated in single report. At present 5 applications are using API which may increase during the contract period.** |
| 35. | Scope Of Work | | Please confirm the environment that will be provisioned for testing. As a best practice, VAPT should be conducted in a staging or UAT environment, not in production. | **VAPT of applications will be done on UAT environment.** |

| | | | | |
|---|---|---|---|---|
| 36. | Scope Of Work | | Please specify the number of applications along with the approximate lines of code to be covered under Source Code Review. | **As of now, the total number of applications(public/non-public facing) are 26. There may be an increase of 05 applications. Further details will be shared with the selected bidder.** |
| 37. | Scope Of Work | | Kindly confirm whether any SCR tool is currently integrated within your SDLC process. | **No.** |
| 38. | Scope Of Work | | Please clarify whether open-source tools are permitted for VAPT and SCR activities. | **No.** |
| 39. | Scope Of Work | | In the case of licensed tools, please confirm who will be responsible for procuring the licenses. Our team can utilize existing licenses for Burp Suite Professional and Nessus Professional. | **Be guided as per RFP.** |
| 40. | Scope Of Work | | Please confirm whether physical red teaming is required or only logical is part of the scope. | **Both required.** |
| 41. | Scope Of Work | | Please clarify whether third-party integrations (payment gateways, Chatbots , etc.) fall within the assessment scope, or will be excluded. | **Yes.** |
| 42. | Scope Of Work | | Please clarify whether VPN or secure remote access will be required for offsite testers. | **No.** |
| 43. | Scope Of Work | | Please confirm the total number of employees, onsite support staff, and vendors expected to participate in the IT and cybersecurity awareness training. | **As on date, the number of expected participants is around 500. However, the number may change if any recruitment takes place.** |
| 44. | Scope Of Work | | Kindly specify whether specialized training sessions for the IT/security team will be separate from general awareness sessions or integrated into the same program. | **These will be separate sessions.** |

| | | | | |
|---|---|---|---|---|
| 45. | Scope Of Work | | Kindly clarify whether training delivery is expected in both online and offline modes, or if mode selection will be decided by AQM. | **Generally, trainings are conducted virtually.** |
| 46. | Scope Of Work | | Please provide a comprehensive inventory of all IT infrastructure components to be covered under the assessment scope, including servers (application, database, web, file), network devices (routers, switches, firewalls, IDS/IPS, load balancers), endpoints (desktops, laptops, thin clients), mobile devices (corporate-issued, BYOD, rooted/jailbroken if applicable), cloud resources (VMs, containers, SaaS/PaaS/IaaS services), and peripheral systems (storage, backup appliances, printers, IoT devices). Kindly share the digital inventory count for each category, specify whether third-party managed systems are included, and clarify how virtualized environments (VMware, Hyper-V, cloud instances) should be represented in the inventory (as separate assets or grouped under host systems). | **Details will be provided to successful bidder.** |
| 47. | Scope Of Work | | Kindly provide total number of Network devices, Servers (along with OS), Database (along with Versions) | **Tentative network devices are 70. Bank has SQL Server, Oracle and IBM Db2. etc, Same be increased during contract period.** |
| 48. | Scope Of Work | | Total number of applications (Intranet and Internate facing) | **For list of applications, please be guided by RFP. However, same can be increased during the period of contract.** |
| 49. | Deliverables | | Total number of Daksh Users | **16** |
| 50. | Deliverables | | Total number of change management for audit period | **Change requests/management may vary for the audit period.** |

| | | | | |
|---|---|---|---|---|
| 51. | 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 defenses and check the mitigating controls already in place by simulating the objectives and actions of an attacker. | Please clarify the following queries:<br>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?<br><br>2. Also confirm the domains that would be part of SOW. | **Auditor is expected to conduct both External and Internal Assessment. Detailed scope shall be shared to successful bidder.** |
| 52. | 6.9 | 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:<br>1. What is the average size of forensic images that are required to be taken ?<br>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?<br>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? | **This is a need based. Details shall be shared to successful bidder on need basis.** |
| 53. | 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:<br>1. How many Regional Offices are included in the scope of the Security Architecture Design? | **Please refer NHB website for the list of Regional Offices .** |
| 54. | 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:<br>1. On how many approx. components configuration review needs to be performed. | **Configuration review to be done on all IT infrastructure e.g. servers, endpoints, network devices, security solutions etc.** |
| 55. | 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:<br>1. How many APIs are currently in production and included in the scope of vulnerability assessment? | **At present 5 applications are using API which may be increased during the contract period.** |

| | | | | |
|---|---|---|---|---|
| 56. | 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:<br>1. Please confirm the number and types of security solutions, OS platforms, applications, servers, and network devices in scope. | **Be guided as per RFP.** |
| 57. | 6.1 Information Security Audit & Cyber Security Audit (Type - Services) | To undertake Source code audit of Bank's public facing applications.<br>Source code review for in-house developed applications to be performed. | Please clarify the following queries:<br>1. Number of applications for which source code audit will be performed.<br>2. The lines of code in each application. | **Please refer RFP. Lines of code will be shared with successful bidder.** |
| 58. | 6.1 Information Security Audit & Cyber Security Audit (Type - Services) | Configuration review to be performed for firewalls, WAF, and proxy.<br>Firewall, WAF, Proxy, Antivirus, DLP and NAC rule/policy review to be performed. | Please clarify the following queries:<br>1.The number of firewalls, WAFs, proxies, antivirus, DLP, and NAC solutions in scope. | **4 pair of Firewall in HA mode. Security solutions are at DC & DR site both.** |
| 59. | 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:<br>1. Please confirm the number of applications and servers in scope for credential-based scanning.<br>2. It will be performed only once (annually) or twice a year? What is the frequency? | **Audit of all applications and servers will be conducted as credential-based scanning.** |
| 60. | 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:<br>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. | **Internal applications are 8. However, same may be increased during period of contract.** |
| 61. | 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 | Please clarify the following queries:<br>1. How many such applications are generally developed? | **As of now, the total number of applications (public/non-public facing) are 26. There may be an increase of 05 applications.** |

| | | | | |
|---|---|---|---|---|
| | | with the bank and as per requirement of Bank. | | |
| 62. | 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:<br>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.** |
| 63. | 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:<br>1. Please confirm whether we have to perform external PT. If yes, then kindly confirm the No. of Public Ips.<br>2. Confirm if any other activity needs to be included in this. | **ISP 1 - 32 DC**<br>**ISP 2 - 32 DC**<br>**ISP 1 - 32 DR**<br>**ISP 2 - 32 DR** |
| 64. | 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:<br>1. Please confirm how many times the training material needs to be provided, as well as the frequency of the training sessions. | **Frequency of Awareness Training is quarterly and Training material is to be provide atleast annually.** |
| 65. | 6.5 Audit of vendors of IT & IS services | Audit of vendors of IT & IS services | Please clarify the following queries:<br>1. What is the number of vendors for which the audit needs to be performed, and what will be the frequency of it. | **10 vendors to be audited annually.** |
| 66. | 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 | 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 specify the total no. of auditors required to be deployed at HO/ another Regional offices of NHB during the contract period | **Be guided as per RFP.** |

| | | | | |
|---|---|---|---|---|
| 67. | Compliance Assessment with IS 17802 (Part I & II) standards published by Bureau of Indian Standards (BIS) | Compliance Assessment with IS 17802 (Part I & II) standards published by Bureau of Indian Standards (BIS) | Does the work requires vendors to be Empanelled Web Accessibility Auditors with Department of Empowerment of Persons with Disabilities, Ministry of Social Justice & Empowerment, Govt. of India ? | **Be guided as per RFP.** |
| 68. | xii. 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. | xii. 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. | Kindly elaborate | **The Bank will share IS-RMF parameters with the selected bidder. The work pertains to compliance checking against some defined parameters.** |
| 69. | Annexure 2-16 | Annexure 2-16 | Many Annexure documents mentioned from Page No. 79-124 needs to be submitted on Non-judicial Stamp Paper so kindly specify the Value of Stamp paper | **Rs. 100 non-judicial stamp paper.** |
| 70. | Clause-5/Phase-I(Evaluation)/iv(Evaluation of compliance and assessment under Digital Personal Data Protection (DPDP) Act) | With the DPDP act now in effect, it is essential to evaluate the current data handling process, consent mechanism, data processing workflows, and security controls to ensure alignment with statutory obligations. The IS auditor will be required to conduct a detailed compliance review, identify gaps, and recommend corrective actions to strengthen our data protection posture. | Kindly confirm the total number of business processes handling Personal Data that are expected to be covered under the DPDP assessment. | **Less than 10 business processes handle personal information. The detailed information will be shared with the selected bidder.** |
| 71. | Clause-5/Phase-I(Evaluation)/iv(Evaluation of compliance and | With the DPDP act now in effect, it is essential to evaluate the current data handling process, | Please confirm the total number of departments and branches / Regional Offices | **For detail, please refer NHB website.** |

| | | | | |
|---|---|---|---|---|
| | assessment under Digital Personal Data Protection (DPDP) Act) | consent mechanism, data processing workflows, and security controls to ensure alignment with statutory obligations. The IS auditor will be required to conduct a detailed compliance review, identify gaps, and recommend corrective actions to strengthen our data protection posture. | that are required to be included in the DPDP compliance review | |
| 72. | Clause-5/Phase-I(Evaluation)/iv(Evaluation of compliance and assessment under Digital Personal Data Protection (DPDP) Act) | With the DPDP act now in effect, it is essential to evaluate the current data handling process, consent mechanism, data processing workflows, and security controls to ensure alignment with statutory obligations. The IS auditor will be required to conduct a detailed compliance review, identify gaps, and recommend corrective actions to strengthen our data protection posture. | Please provide the approximate number of existing policies, procedures, standards, and SOPs forming part of the organization's Data Protection and Privacy framework | **There is no specific policy for data protection and Bank's IS Policy and Cyber Security framework covers data privacy and data protection.**<br><br>**The detailed information will be shared with the selected bidder.** |
| 73. | Clause-5/Phase-I(Evaluation)/iv(Evaluation of compliance and assessment under Digital Personal Data Protection (DPDP) Act) | With the DPDP act now in effect, it is essential to evaluate the current data handling process, consent mechanism, data processing workflows, and security controls to ensure alignment with statutory obligations. The IS auditor will be required to conduct a detailed compliance review, identify gaps, and recommend corrective | Please confirm whether the DPDP assessment is expected to cover all departments at the Head Office and Regional Offices | **Yes.** |

| | | | | |
|---|---|---|---|---|
| | | actions to strengthen our data protection posture. | | |
| 74. | Clause-5/ Phase-II(Communication)/i( User Training) | Imparting 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 on quarterly basis. The training material will 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 in online/offline mode. The auditor shall provide Information Security-related training to all stakeholders, as and when required by the Bank. This may include, but is not limited to, secure coding practices, application security guidelines, and awareness on common security vulnerabilities and controls. | What is the total number of participants expected to be covered under the quarterly cyber security awareness program across all locations? | **As on date, the number of expected participants is around 500. However, the number may change if any recruitment takes place.** |
| 75. | Clause-5/ Phase-II(Communication)/i( User Training) | Imparting 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, | Considering the presence of multiple Regional Offices, please confirm whether awareness sessions should be conducted centrally (e.g., Delhi) with virtual participation from Regional Offices, or if separate in-person sessions at other locations are required | **The cyber security awareness sessions are generally conducted virtually.** |

| | | | | |
|---|---|---|---|---|
| | | seminar/webinar, interactions, and presentations on quarterly basis. The training material will 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 in online/offline mode. The auditor shall provide Information Security-related training to all stakeholders, as and when required by the Bank. This may include, but is not limited to, secure coding practices, application security guidelines, and awareness on common security vulnerabilities and controls. | | |
| 76. | Clause-5/ Phase-II(Communication)/i( User Training) | Imparting 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 on quarterly basis. The training material will 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 in online/offline mode. The auditor shall provide | Is there a defined batch size limit per session that should be considered while planning the training schedule? | **The training sessions are generally conducted in two batches on the same day. Batches are divided based on designation.** |

| | | | | |
|---|---|---|---|---|
| 78. | Clause-5/ Phase-II(Communication)/i( User Training) | Imparting 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 on quarterly basis. The training material will 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 in online/offline mode. The auditor shall provide Information Security-related training to all stakeholders, as and when required by the Bank. This may include, but is not limited to, secure coding practices, application security guidelines, and awareness on common security vulnerabilities and controls. | Kindly confirm whether the Bank will provide the venue and necessary infrastructure (AV setup, projector, seating arrangements, etc.) for the training sessions in Delhi, or is the auditor expected to arrange the same? | **The cyber security awareness sessions are generally conducted virtually. If conducted physically, the bank will take care of the arrangement.** |
| 79. | Clause-5/ Phase-II(Communication)/i( User Training) | Imparting 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 on quarterly | Kindly confirm whether the auditor is expected to issue participation/completion certificates to attendees as part of the cyber security awareness and specialized IT training sessions. | **No, it is not required.** |

| | | | | |
|---|---|---|---|---|
| | | Information Security-related training to all stakeholders, as and when required by the Bank. This may include, but is not limited to, secure coding practices, application security guidelines, and awareness on common security vulnerabilities and controls. | | |
| 77. | Clause-5/ Phase-II(Communication)/i( User Training) | Imparting 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 on quarterly basis. The training material will 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 in online/offline mode. The auditor shall provide Information Security-related training to all stakeholders, as and when required by the Bank. This may include, but is not limited to, secure coding practices, application security guidelines, and awareness on common security vulnerabilities and controls. | Please confirm the expectations for specialized IT security training sessions | **Please be guided by the RFP terms and conditions.** |

| | | | | |
|---|---|---|---|---|
| | | basis. The training material will 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 in online/offline mode. The auditor shall provide Information Security-related training to all stakeholders, as and when required by the Bank. This may include, but is not limited to, secure coding practices, application security guidelines, and awareness on common security vulnerabilities and controls. | | |
| 80. | Clause-5/ Phase-II(Communication)/i( User Training) | Imparting 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 on quarterly basis. The training material will 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 in online/offline mode. The auditor shall provide Information Security-related training to all stakeholders, as | The RFP requires the auditor to "Conduct Red Teams exercise on half-yearly basis". Could the Bank please clarify the exact scope and boundaries of this exercise? Specifically, does it include physical security bypass (facility intrusion) and social engineering (Vishing, Smishing), or is it strictly limited to Digital/Network Red Teaming? | **Red team exercise is a well-defined mechanism. It's part ethical hacking/penetration to find the gaps in the system.** |

| | | | | |
|---|---|---|---|---|
| | | and when required by the Bank. This may include, but is not limited to, secure coding practices, application security guidelines, and awareness on common security vulnerabilities and controls. | | |
| 81. | 5. Scope of Work, Phase-I Evaluation, point (d) | 5. Scope of Work, Phase-I Evaluation, point (d) | The RFP lists 24 web-facing applications/portals but mentions that "Some more applications may be added during the course of Audit." For accurate commercial sizing, could the Bank specify a cap or maximum number of applications that will be in scope for the quarterly VAPT? | **As of now, the total number of applications (public/non-public facing) are 26. There may be an increase of 05 applications.** |
| 82. | 6. Deliverables, Section 6.2 (Vulnerability Assessment, Analysis and Resolution) | 6. Deliverables, Section 6.2 (Vulnerability Assessment, Analysis and Resolution) | The clause mandates the auditor to "conduct pre deployment VAPT of any application during the contract period, in coordination with the bank". Since this can be highly variable, is there a limit to the number of ad-hoc pre-deployment VAPTs required per year, or will these be billed separately out of the defined man-day rate? | **Pre-deployment audit of any enhancement/enablement pertaining to current applications (with likely increase in number by 5) is to be carried out by the auditor.** |
| 83. | 5. Scope of Work, Phase-I Evaluation, point (iii) Conducting Cyber Audit | 5. Scope of Work, Phase-I Evaluation, point (iii) Conducting Cyber Audit | The RFP mentions a "Quarterly Phishing simulation exercise to be conducted by the Auditor". Could the Bank provide the approximate number of internal users/employee email IDs that will be targeted during these quarterly phishing simulation campaigns? | **As on date, the number of expected participants is around 500. However, the number may change if any recruitment takes place.** |
| 84. | 5. Scope of Work, Phase-I Evaluation, point (iii) Conducting Cyber Audit | 5. Scope of Work, Phase-I Evaluation, point (iii) Conducting Cyber Audit | The schedule outlines quarterly VAPT exercises and half-yearly Red Teaming exercises. During the quarters where both exercises coincide, will the Bank allow the Red Teaming and VAPT assessments to be | **No.** |

| | | | | |
|---|---|---|---|---|
| | | | conducted as a combined engagement, or must they be executed as entirely separate modules with dedicated resources? | |
| 85. | 5. Scope of Work, Phase-I Evaluation, point (iii) Conducting Cyber Audit | 5. Scope of Work, Phase-I Evaluation, point (iii) Conducting Cyber Audit | The RFP mentions "VAPT for developed/customized APIs." Could the Bank provide an approximate count of the internal and external APIs that are currently in production and will fall under the VAPT scope? | **At present 5 applications are using API which may be increased during the contract period.** |
| 86. | 5- Scope of work | 5- Scope of work | Can access controls for regional offices be tested remotely? | **Yes.** |
| 87. | 5- Scope of work | 5- Scope of work | For firewall review and OS configuration, will there be any guidelines provided by the Bank? | **No.** |
| 88. | 5- Scope of work | 5- Scope of work | Will the Bank provide a checklist for the Data Center IT Infrastructure Audit? If not what standard will be followed? | **Bank will provide complete details of all IT infrastructure.** |
| 89. | 5- Scope of work | 5- Scope of work | Review of Antivirus- Will it be done on a sampling basis? | **No.** |
| 90. | 5- Scope of work | 5- Scope of work | For network facility and equipment management firewall rule review, will it be done on a sampling basis? | **No.** |
| 91. | 5- Scope of work | 5- Scope of work | Pre-Implementation IS Audit of Applications/ Systems - How many application will be covered ? | **Be guided as per RFP.** |
| 92. | 5- Scope of work | 5- Scope of work | Coordination for STQC certification: What documents will be prepared? Is it a advisory role? | **Documents required for obtaining STQC certification.** |
| 93. | 6.4 | 6.4 | How many training sessions will be conducted, and what will be the mode of the training? | **Frequency of Training is quarterly.** |
| 94. | 7 – Project Schedule | 7 – Project Schedule | Other certifications and reports – what are the certifications and reports? Please clarify. | **Be guided as per RFP.** |
| 95. | 7 – Project Schedule | 7 – Project Schedule | What is the expected date of issuance of work order / start of assignment? | **Be guided as per RFP.** |

| | | | | |
|---|---|---|---|---|
| 96. | 7 – Project Schedule | 7 – Project Schedule | Will audits for periods starting Jan-2026 be done retrospectively if LOA is issued later? | **Be guided as per RFP.** |
| 97. | 8 – Duration of Contract | 8 – Duration of Contract | What is the tentative overall contract duration (in months) from date of work order? | **Be guided as per RFP.** |
| 98. | 9 – Penalty | 9 – Penalty | Is the 10% penalty cap applicable per phase or on the total contract value overall? | **Be guided as per RFP.** |
| 99. | 9 – Penalty | 9 – Penalty | Will delays attributable to NHB (access, approvals, data) be excluded while calculating penalty? | **Be guided as per RFP.** |
| 100. | 6.8 – IS 17802 (Part I & II) | 6.8 – IS 17802 (Part I & II) | Is IS 17802 compliance assessment to be performed once or on a recurring basis during the contract? | **It will be part of IS audit review.** |
| 101. | 6.9 – STQC Certification | 6.9 – STQC Certification | For which application(s)/system(s) is STQC certification envisaged? | **Currently, STQC certification is envisaged for Bank's website/app, Grievance portal, Recruitment portal. The scope may increase on need basis during the period of contract/as per directions of Ministry.** |
| 102. | 6.9 – STQC Certification | 6.9 – STQC Certification | Will STQC and other third-party certification fees be borne by NHB separately from the contract value? | **The fee will not be borne by auditor.** |
| 103. | 6.4 – Training Material | 6.4 – Training Material | Should training content be provided only in soft copy, or also in printed copies? | **soft copy** |
| 104. | 6 – Deliverables; 7 – Project Schedule | 6 – Deliverables; 7 – Project Schedule | How many onsite man-days are expected at HO Delhi and at DR site Mumbai respectively? | **Be guided as per RFP.** |
| 105. | General Terms & Conditions, pt. 8 – Onsite FTE | General Terms & Conditions, pt. 8 – Onsite FTE | What is the minimum number of full-time onsite professionals required at HO? | **Be guided as per RFP.** |
| 106. | General Terms & Conditions, pt. 8 – Onsite FTE | General Terms & Conditions, pt. 8 – Onsite FTE | Are onsite resources required to be exclusively deployed for NHB (no sharing with other projects)? | **Be guided as per RFP.** |

| | | | | |
|---|---|---|---|---|
| 107. | 10.8, 10.12; Annexure V & VI – Masked / Unmasked Commercial | 10.8, 10.12; Annexure V & VI – Masked / Unmasked Commercial | Should Annexure VI be submitted both as masked (with Technical Bid) and unmasked (with Commercial Bid)? | **Be guided as per RFP.** |
| 108. | Annexure V – Technical Bid Covering Letter | Annexure V – Technical Bid Covering Letter | In masked commercial bid, should only rates be masked or total values also be removed/blanked out? | **Be guided as per RFP.** |
| 109. | 10.10 – EMD | 10.10 – EMD | Is EMD acceptable only via e-payment (NEFT/RTGS), or are BG/DD formats also permitted? | **EMD acceptable only via e-payment (NEFT/RTGS).** |
| 110. | 10.11 – Submission of Bids; 10.12 – Signing of Bids | 10.11 – Submission of Bids; 10.12 – Signing of Bids | Are scanned PDFs with authorized signatory's DSC sufficient, or are any physical originals required at bid stage? | **No physical/original required as of now. Bank may ask original/additional documents during technical evaluation.** |
| 111. | 10.5 – Integrity Pact (Stamp Paper) | 10.5 – Integrity Pact (Stamp Paper) | Can a scanned Integrity Pact on ₹100 stamp paper be uploaded on GeM with original submitted post-award? | **Pre integrity pact is required to be uploaded along with technical bid.** |
| 112. | 11.1 – Price | 11.1 – Price | Please confirm that the quoted price must be all-inclusive, including GST and all out-of-pocket expenses. | **Price is inclusive of all taxes, GST, all out-of-pocket expenses, other charges etc.** |
| 113. | 11.2 – Payment Terms | 11.2 – Payment Terms | What is the standard payment timeline (number of days) from invoice and acceptance of deliverables? | **Be guided as per RFP.** |
| 114. | 10.21 – Liquidated Damages; 9 – Penalty | 10.21 – Liquidated Damages; 9 – Penalty | Can both penalty (Clause 9) and liquidated damages (Clause 10.21) be applied for the same delay? | **Be guided as per RFP.** |
| 115. | 10.19(i) – Outsourcing; 10.23 – Assignment; SLA 3.12 – Sub-contract | 10.19(i) – Outsourcing; 10.23 – Assignment; SLA 3.12 – Sub-contract | Can specialist CERT-In empanelled partners/OEMs be engaged for specific activities with prior NHB approval? | **Be guided as per RFP.** |
| 116. | Annexure VI – Commercial Bid; Table 2 (Man-day Rates) | Annexure VI – Commercial Bid; Table 2 (Man-day Rates) | Is there any minimum number of man-days per additional assignment (forensics/migration) that NHB will commit? | **Be guided as per RFP.** |

राष्ट्रीय आवास बैंक, नई दिल्ली NATIONAL HOUSING BANK DELHI
ले. प. वि.
Audit Deptt.

****