राष्ट्रीय आवास बैंक
NATIONAL HOUSING BANK

**Requirement Proposal for undertaking Information Security & Cyber Security Audit for the Year 2023-24 & 2024-25 (July-June) of NHB, through Limited Tender for Empaneled IS & CS Auditors, published on the website of NHB on September 27, 2024.**

# The replies to the pre-bid queries received from the Empaneled IS & CS Auditors for the Pre-Bid Meeting held on October 04, 2024, are placed herewith.

**Pre-Bid Queries of Empanelled Bidders/Auditors and Bank's Response on**
**Requirement Proposal (RP) For undertaking Information Security & Cyber Security Audit**
**for the Years 2023-2024 (July-June) & 2024-2025 (July-June)**

## 1. M/s. AAA Technologies Ltd.

| Sr. No. | Particulars (RP reference ) | Query of Empanelled Bidders/Auditors | Response of the Bank to the Query |
|---|---|---|---|
| 1 | Page 5 1. PROJECT<br>Type of Audit<br>I. Information Security Audit & Cyber Security Audit<br>II. VAPT<br>III. Red Teaming Exercise of all Public Facing Applications<br>IV. Audit of vendors of IT & IS services | Following are the clarification required as per activity wise.<br>1.Location of audit required as per activity wise<br>2.Please mention is compliance / Revalidation audit will be the part of the scope of work | 1.The Services shall be performed at Delhi HO( data centre) , DR site at Mumbai or at such location required/ approved by NHB. Please also refer the RP for the same.<br>2. Yes, compliance / Revalidation audit is part of the scope. |
| 2 | Page 5 - Audit of vendors of IT & IS services | Total Number of Vendors to be audited and their locations or can the Vendor audit can be performed remotely | 03 vendors of IT Services (one mumbai & rest delhi ) & 01 vendor of IS Services at Delhi , |
| 3 | 3A. Wide Area Network (MPLS)<br>Presently NHB has MPLS connectivity between New Delhi, DR Site & Regional Offices (ROs) as under. MPLS services are in managed mode. | Whether we need to be visit the regional offices also as part of Audit . Please confirm | Visit of regional offices is not required. |
| 4 | Page 9 D. Evaluation of Web Facing Applications and Portals-<br>To carry Software Audit of Bank's internal applications for vulnerabilities and portals developed in-house as also newly implemented applications during Audit Period Details will be provided at the time of commencement of Audit/testing. | What would be scope coverage under 'Software Audit'. Whether we need to conduct the process audit or only the VAPT Audit | VAPT Audit is to be conducted. |
| 5 | Page 10 IV. Conducting Cyber Audit<br>Quarterly Phishing simulation exercise to be conducted by the Auditor in a scenario proposed by the Bank. | Total number of employees is required | Approx 250 employees. |
| 6 | Page 11 Information Security Audit & Cyber Security Audit | Total number of API's required and their methods required | Total no. of APIs at present is three . Methods will be shared to successful bidder. |
| | | Secure configuration review of, but not limited to, Bank's security solutions, OS, applications, servers, and network devices. : Do we have to conduct Review on all devices or on sample basis | Review to be conducted on all devices. |
| | | Total number of source code audit to be performed along with the line of code for each application | Total no. of source code audit- is for ten applications, line of code will be shared to successful bidder.. |
| | | Total Number of database | 52 database |
| | | Total Number of Web facing applications/portals : | Total Number of Web facing applications/portals at present is 13 . |
| | | Security Architecture(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.): How many architecture to be covered and their loaction | Security Architecture will be shared to successful bidder only. |
| | | Total Number of network and security devices for configuration review required | Total Number of network and security devices is approx 70 for configuration review. |
| | | Credential based application and servers' vulnerability scanning to be performed on annual basis by IS auditor: Confirm whether this activity should be done other than 4 Quarters VAPT | Credential based application and servers' vulnerability scanning to be performedonce once in every reporting cycle. |
| 7 | Page 12<br>5.2. Vulnerability Assessment, Analysis and Resolution | VAPT for developed/customized APIs: Total number of API to be covered | VAPT for developed/customized APIs is approx 3 . Total number of API to be covered will be shared with successful bidder. |
| | | Do we have to conduct credential scanning or Non- credential scanning | credential based scanning is to be conducted. |
| 8 | Page 14<br>5.4. Training Programs & Training Material for NHB officials | Total Number of network and security devices for VA | Total Number of network and security devices for VA is approx 70. |
| | | What would be frequency of the training | Training is to be conducted on a quarterly basis. |
| | | Total number of training to be conducted. | Four trainings in a year. |
| | | Number of participant in each session | Approx 250 participants |
| | | Can be training be conducted remotely. If not then what would be the location | Online training will be conducted |

| Sr. No. | Particulars (RP reference ) | Query of Empanelled Bidders/Auditors | Response of the Bank to the Query |
|---|---|---|---|
| 9 | Page 21 Point 30 - Performance Bank Guarantee (PBG) -The successful bidder will be required to provide PBG in the form of bank guarantee of value amounting to 10% of the total contract value from a scheduled commercial bank in the format as substantially prescribed in Annexure-VIII of the RP, | As per Office Memorandum by Ministry of Finance No. F.9/4/2020-PPD dated 12-11-2020, the Performance Security should be 3% of value of contract. Request you to consider the same | As per Manual for Procurement of Consultancy & Other Services (Updated June 2022) of Ministry of Finance Department of Expenditure, GOI :<br>"Performance Security (Rule 171 of GFR 2017): To ensure due performance of the contract, performance security [or Performance Bank Guarantee (PBG) or Security Deposit (SD)] is to be obtained from the successful bidder awarded the contract. Performance security should be for an amount of five (5) to ten (10) per cent of the value of the contract as specified in the bid documents [The value has been reduced to three (3) percent till 31.03.2023."<br>Hence, the successful bidder will be required to provide PBG in the form of Bank guarantee of value amounting to 10% of the total contract value as mentioned in the RP. |
| 10 | Page 41 Commercial Bid Format as per Annexure-II<br>(2) Compliance Statement Declaration in the format as prescribed in Annexure III<br>(3) ECS Mandate in the format as prescribed in Annexure IV<br>(4) Resolution Matrix in the format in Annexure V<br>(5) Certificate as per clause 41(b) in Annexure VI | Do we need to submit this Annexure on company letter head . Please confirm | Yes, the mentioned annexures have to be provided on the company's/firm's letter head duly stamped & signed by authorised signatory along with the bid |
| 11 | Page 48 Annexure VII<br>Letter of Competence Format | Do we need to submit this document along with the bid document or after once the bidder gets the work order<br>Please confirm the Value Rs 100 | Yes, Annexure VII has to be provided along with the bid on non-judicial stamp paper of Rs. 100 /-. |
| 12 | Page 52 Confidential Page 52 of 84<br>Annexure-IX<br>(To be executed on a non- judicial stamp paper)<br>Service Level Agreement | Do we need to submit this document along with the bid document or after once the bidder gets the work order<br>Please confirm the Value Rs 100 | Yes, the annexure to be submitted as part of the bid. |
| 13 | Page 66 Annexure X<br>CONFIDENTIALITY –CUM- NON DISCLOSURE AGREEMENT<br>(To be executed on a non- judicial stamp paper) | Do we need to submit this document along with the bid document or after once the bidder gets the work order<br>Please confirm the Value Rs 100 | Yes, the annexure to be submitted as part of the bid. |
| 14 | Page 70 Annexure XI<br>Pre-Contract Integrity Pact (To be executed on a non- judicial stamp paper) | Please confirm as we have already submitted the Pre-Contract Integrity Pact during our empanelment.<br>Do we need to submit this document along with the bid document or after once the bidder gets the work order .<br>Please confirm the Value Rs 100 | The annexure is required to be submitted by the successful bidder. |
| 15 | Page 81 Annexure-XIII<br>Declaration by the Bidder for Code of Integrity | Please confirm do we need to submit along with the bid on letter head | Yes, the mentioned annexure has to be provided on the company's/firm's letter head duly stamped & signed by authorised signatory along with the bid. |
| 16 | Page 82 Annexure-XIII<br>Declaration by the Bidder for Code of Integrity | Please confirm do we need to submit along with the bid on letter head | Yes, the mentioned annexure has to be provided on the company's/firm's letter head duly stamped & signed by authorised signatory along with the bid. |
| 17 | Annexures | We request if we could get the Annexures in word copy | Shall be provided as per request of the bidder. |

## 2. M/s. Ernst & Young LLP

| S. No | Query of Empanelled Bidders/Auditors | Response of the Bank to the Query |
|---|---|---|
| 1 | How many Severs/End Points/Application (Web, Mobile, API..etc) is being covered for VAPT | For details on Servers/End Points & Application, refer the RP. One mobile application shall be covered in the VAPT. |
| 2 | Bidder has to perform Revalidation as well for the devices as per VAPT Scope | Yes, compliance / Revalidation audit is part of the scope. |
| 3 | Are the vulnerability scans performed with authentication (using credentials) or without authentication | credential based scanning is to be conducted. |
| 4 | Is there any ticketing tool in place like service now /JIRA etc ? | Manage Engine |
| 5 | What are the size of applications (High, Medium, Low). No. of pages will help to classify | Will be shared with successful bidder only. |
| 6 | Is it the responsibility of the bidder to acquire the necessary tools for vulnerability scanning, or will the bank provide these tools? | RP may be referred for the same. |
| 7 | How many of the locations will be included for VAPT assessment | RP may be referred for the same. |
| 8 | Please clarify solution license needs to be procured on the name of bidder or by NHB | Solution license needs to be procured on the name of bidder |
| 9 | Our understanding is that Client (NHB) will be responsible for handling the implementation of patching and remediation. Bidder will not implement patching on client systems. Hope our understanding is correct? | Yes, NHB will be responsible for handling the implementation of patching and remediation. |
| 10 | What are the SLA's defined for closure of vulnerabilities | 7 days for High risk, 15 days for Medium risk & 25 days for low risk. |
| 11 | How many public application for RED Team exercise | 13 public applications at present for RED Team exercise |
| 12 | How many locations to be covered for ISA, CSA, VAPT and Red Team exercise | DC at Delhi & DR at Mumbai |
| 13 | During CSA and ISA Audit hope all relevant documents related to Firewall Conguration files, Architecture review will be provided by NHB. Hope this understanding is Correct ? | Network diagram, Firewall configuration will only be provided by NHB |
| 14 | Is there any tool for NHB asset inventory ? | Yes, Manage engine |
| 15 | How many Training Programs to be conducted by service provider | Four trainings in a year. |
| 16 | Please confirm the standards/laws against which the ISA has to be conducted. Please provide the names of the laws, standards and guidelines | RP may be referred for the same. |
| 17 | Please confirm the standards/laws against which the CSA has to be conducted. Please provide the names of the laws, standards and guidelines | RP may be referred for the same. |

| Sr. No. | Particulars (RP reference ) | Query of Empanelled Bidders/Auditors | Response of the Bank to the Query |
|---|---|---|---|
| 18 | Please confirm the number of entities and locations to be included as part of the ISA and CSA | | The Services shall be performed at Delhi HO( data centre) , DR site at Mumbai or at such location required/ approved by NHB.<br>Please also refer the RP for the same. |
| 19 | Please list the Business functions in scope for ISA and CSA | | IT & network infrastructure. |
| 20 | Will separate work papers for each of the controls be required to be submitted for ISA and CSA? | | Yes, separate report for each of the controls are required to be submitted for ISA and CSA. |
| 21 | Please provide the sampling methodology to be followed for testing for ISA and CSA | | all devices to be covered for testing for ISA and CSA. |
| 22 | Do you maintain a central repository of documents for all entities/locations or is the documentation maintained separately for each entity/location for ISA and CSA? | | Yes, a central repository of documents for all entities/locations is maintained separately for each entity/location for ISA and CSA |
| 23 | Are recommendations required to be provided for each gap identified for ISA and CSA? | | Yes, recommendations are required to be provided for each gap identified for ISA and CSA as part of the IS & CS report |
| 24 | Does the audit certificate need to be submitted on EY letterhead for ISA and CSA? | | Yes, audit certificates/reports are to be submitted on letterhead for ISA and CSA |
| 25 | Please confirm if we need to consider remediation and/or revalidation review as a part of the scope for ISA and CSA | | Yes, compliance / Revalidation audit is part of the scope. |
| 26 | Are there any additional activities that need to be considered in scope for ISA and CSA | | Please refer RP for the same. |
| 27 | Please provide the indicative start date for ISA and CSA | | The indicative/expected start date of the project is November 01, 2024 as mentioned in the RP. |
| 28 | Please provide the duration expected for ISA and CSA | | Please refer the contract period clause mentioned in RP |
| 29 | Please confirm if there is a particular deadline for submission of the IS and CS Audit certificate (if required) | | Please refer the clause no. 02 (iii) of the RP. |
| 30 | Please confirm if the engagement delivery mode- remote/in office/hybrid | | The audit is to be conducted in the NHB's office/premises . |
| 31 | Is audit assessment, remediation and post implementation review expected for ISA and CSA? | | Compliance / Revalidation audit is part of the scope. Further, for assessment, remediation related querries, please refer the RP. |
| | **3. M/s. SecurEyes Techno Services Pvt. Ltd** | | |
| **S. No.** | **Particulars (RP reference )** | **Query of Empanelled Bidders/Auditors** | **Response of the Bank to the Query** |
| 1 | Audit of Infrastructure | Do we have to do audit of all infra or we can do audit on sampling basis | All infrastructure is to be audited. |
| 2 | Count of Application | Please provide Application count and size of application | Approx. 17 applications at present. Application size will be shared to succesful bidder |
| 3 | Training Expectation | Please elaborate number of trainings and count of trainee. | Four trainings in a year. |
| 4 | Phase - II would be 2-3 weeks | It will also depend on the fetching time of Bank IT team. | No further clarification/response is required on the query as discussed during the meeting. |
| 5 | Penalty will be charged @ 2% of the total contract value per week on delay in submission of audit report & audit compliance report in phase – I, II and III respectively | Penalty is subject to reasons of delay from the vendor side. | No further clarification/response is required on the query as discussed during the meeting. |
| | **4. M/s AKS Information Technology Services Private Limited** | | |
| **S. No** | **Query of Empanelled Bidders/Auditors** | | **Response of the Bank to the Query** |
| 1 | Web Application Name & URL | | Approx. 17 applications at present. Application name & URL will be shared to succesful bidder |
| 2 | Developer Contact Details | | Details will be shared with the successful bidder. |
| 3 | Application will be host on (State Data Center, NIC, Private server, Amazon Server) | | All applications are hosted on Bank's data center except for one. |
| 4 | Application Server with Version (i.e. IIS 5.+B7:B210.Apache, Tomcat, etc. ) | | Details will be shared with the successful bidder. |
| 5 | Front-end Tool [Server side Scripts] (i.e. ASP, Asp.NET, JSP, PHP, etc.) | | Details will be shared with the successful bidder. |
| 6 | Back-end Database (MS-SQL Server, PostgreSQL, Oracle, etc. ) | | 3MS-SQL Server, Oracle |
| 7 | Operating System Details<br>(E.g. Windows, Linux, AIX, Solaris, etc.) | | Two types of OS - Linux |
| 8 | Whether the application contains any content management module(CMS) (If yes then which?) | | Yes ( one application i.e NHB website) |
| 9 | Authorization No. of roles & types of privileges for the different roles | | Details will be shared with the successful bidder. |
| 10 | Total No. ( Approximate) of Input Forms | | Details will be shared with the successful bidder. |
| 11 | Total No. of input fields | | Details will be shared with the successful bidder. |
| 12 | No. of login modules | | Approx. 250 |
| 13 | Is there any paymeny gateway ? | | Yes |
| 14 | Whether audit to be conducted remotely? Yes or NO | | The audit is to be conducted in the NHB's office/premises . |
| 15 | Whether application/website was audited earlier. If yes, then mention the year also. | | Yes |
| 16 | Is application behind any WAF (Web application Firewall)? | | Yes |
| 17 | Number of Web Services, if any | | Details will be shared with the successful bidder. |
| 18 | Number of methods in all web services | | Details will be shared with the successful bidder. |
| 19 | Number of Input Fields in methods of web services | | Details will be shared with the successful bidder. |
| 20 | **Query on Scoping Sheet for Web Services/API Security Testing**-Web Application Name & URL | | 03 Applications using API and rest of the details will be shared with the successful bidder. |
| 21 | Developer Contact Details | | Details will be shared with the successful bidder. |
| 22 | Which type of testing required? (Grey Box, White Box, Black Box) | | Grey Box & Black box |
| 23 | Name of API | | Details will be shared with the successful bidder. |

| **Sr. No.** | **Particulars (RP reference )** | **Query of Empanelled Bidders/Auditors** | **Response of the Bank to the Query** |
|---|---|---|---|
| **24** | API(s) Development technology/Framework | | Details will be shared with the successful bidder. |
| **25** | API(s) developed are SOAP or Rest based | | Details will be shared with the successful bidder. |
| **26** | Number of Endpoints hitting by API | | Details will be shared with the successful bidder. |
| **27** | No. of API(s) per Endpoint | | Details will be shared with the successful bidder. |
| **28** | No. of Methods/Function calls per API | | Details will be shared with the successful bidder. |
| **29** | Average number of input or parameters per Method/Function | | Details will be shared with the successful bidder. |
| **30** | Any Work flow required to access method/Function call within different API(s) | | Details will be shared with the successful bidder. |
| **31** | **Query on Mobile Application Security Testing-** Mobile Application Name | | 01 mobile application |
| **32** | Development platform Details | | Android, IOS |
| **33** | Application Server with Version (i.e. IIS 5.0.Apache, Tomcat, etc. ) | | Details will be shared with the successful bidder. |
| **34** | Front-end Tool [Server side Scripts] (i.e. ASP, Asp.NET, JSP, PHP, etc.) | | Details will be shared with the successful bidder. |
| **35** | Back-end Database (MS-SQL Server, PostgreSQL, Oracle, etc. ) | | Details will be shared with the successful bidder. |
| **36** | Authorization No. of roles & types of privileges for the different roles | | Details will be shared with the successful bidder. |
| **37** | Whether the application contains any content management module(CMS) (If yes then which?) | | Details will be shared with the successful bidder. |
| **38** | Total No. ( Approximate) of Input Screens | | Details will be shared with the successful bidder. |
| **39** | Number of Web Services, if any | | Details will be shared with the successful bidder. |
| **40** | Number of methods in all web services | | Details will be shared with the successful bidder. |
| **41** | Whether audit can be remotely? Yes or NO | | The audit is to be conducted in the NHB's office/premises . |
| **42** | **Query on Cyber Security Audit**-Total No. of Nodes | | RP may be referred for the same. |
| **43** | No. of Servers with details (Windows, Linux, Sun Solaris etc) | | RP may be referred for the same. |
| **44** | No. of Desktops/Laptops | | RP may be referred for the same. |
| **45** | No. of Routers | | Seven |
| **46** | No. of Switches (L3, L2 with details) | | Fifty five |
| **47** | No. and make of firewalls/ UTM devices | | Eight firewalls. |
| **48** | No. of IDS/IPS | | inbuilt functionality of firewall |
| **49** | No. of Wireless Access points | | Zero |
| **50** | Is VLAN configured? | | Yes |
| **51** | For External Penetration Testing: No. of Public IPs | | Thirteen |
| **52** | Do you have any security policies & procedures? | | Yes |
| | **Services (Options)** | | |
| **53** | **Query on Web Application/Website/Web Services Security Testing**-Application Name | | Approx. 17 applications at present. Application name will be shared to succesful bidder |
| **54** | Developer Contact Details | | Details will be shared with the successful bidder. |
| **55** | Application Server with Version (i.e. IIS 5.+B7:B210.Apache, Tomcat, etc. ) | | Details will be shared with the successful bidder. |
| **56** | Front-end Tool [Server side Scripts] (i.e. ASP, Asp.NET, JSP, PHP, etc.) | | Details will be shared with the successful bidder. |
| **57** | Back-end Database (MS-SQL Server, PostgreSQL, Oracle, etc. ) | | Details will be shared with the successful bidder. |
| **58** | Authorization No. of roles & types of privileges for the different roles | | Details will be shared with the successful bidder. |
| **59** | Total No. ( Approximate) of Input Forms | | Details will be shared with the successful bidder. |
| **60** | No. of Lines of Code | | Details will be shared with the successful bidder. |