Pre-Bid Queries from Prospective Bidder 1

Sr No	Section	Clause	Query	NHB Reply
1	Minimum Eligiblity Criteria	Bidder should have completed minimum 10 SOC implementation/operations service projects [from SOC establishment in India] - c) Each of these projects should be of minimum annualized value INR 10 Lakh (exclusive of taxes). d) At least 2 projects of the above should be of annualized value more than INR 50 lakh (exclusive of taxes) each. In case of ongoing projects, the value of completed services (up to a month prior to the release of this RFP) shall be considered.	For wider partipication, request to amend clause as below: Bidder should have completed SOC implementation/operations service projects [from SOC establishment in India] - 1. One project of Security Operations Center of value greater than INR 7 Crores OR 2. Two projects of SOC of value greater than INR 5 Crores OR 3. Three projects of SOC of value greater than INR 3 Crores.	Please be guided by the RFP terms and conditions
2	Minimum Eligiblity Criteria	The bidder Company should have at-least 50 qualified Information Security / Cyber Security professionals (CISSP/DISA/CISA/CISM/CDAC/ CEH/ISO 27001 certified) in their payroll.	For wider partipication, request to amend clause as below: The bidder Company should have at-least 20 qualified Information Security / Cyber Security professionals (CISSP/DISA/CISA/CISM/CDAC/ CEH/ISO 27001 certified) in their payroll.	Please be guided by the RFP terms and conditions
3	Technical Eligibility Criteria	Experience the bidder has in carrying out Managed Cyber Security Operation Center (SOC) services or in implementation of SOC [from SOC establishment in India] - 1. Projects of SOC implementation / operations service of annualized value more than INR 10 Lakhs each (Max Marks 10) 15 or more such projects - 10 Marks More than 10 [and up to 14] such projects - 7 Marks 2. Projects of SOC implementation / operations service of annualized value more than INR 50 Lakhs each (Max Marks 10) More than 5 such projects - 10 Marks More than 2 and upto 5 such projects - 7 Marks	For wider partipication, request to amend clause as below: Experience the bidder has in carrying out Managed Cyber Security Operation Center (SOC) services or in implementation of SOC [from SOC establishment in India] - Projects of SOC implementation / operations service (Max Marks 10) One Order Value more than 7 Crores - 10 Marks Two Orders value more than 5 Crores - 7 Marks Three Orders value more than 3 Crores - 5 Marks	Please be guided by the RFP terms and conditions
4	Technical Eligibility Criteria	The number of professional staff in the area of Information Security/ Cyber Security (Bidder will provide a list of staff signed by authorized signatory on their letter head which will include Name, Qualification, designation, No of year of Experience, Certification, Date of Issue of Certificate and Date of Expiry of Certificate etc.) (Max Marks: 10) More than 150 - 10 Marks More than 100 but ≤ 150 - 7 Marks More than 50 but ≤ 100 - 5 Marks	For wider partipication, request to amend clause as below: The number of professional staff in the area of Information Security/ Cyber Security (Bidder will provide a list of staff self certified by authorized signatory on their letter head) (Max Marks: 10) More than 150 - 10 Marks More than 100 but ≤ 150 - 7 Marks More than 50 but ≤ 100 - 5 Marks	Please be guided by the RFP terms and conditions

5	Technical Eligibility Criteria	No. of SCBs/All India FIs/ Regulatory Bodies/BFSI Sector in India/ Large Corporates, where the bidder has provided SOC implementation /operations service [from SOC establishment in India] (Max Marks: 10) More than 10 - 10 Marks More than 7 but ≤ 10 - 7 Marks More than 5 but ≤ 7 - 5 Marks	For wider participation, request to amend clause as below: No. of SCBs/All India FIs/ Regulatory Bodies/BFSI Sector in India/ Large Corporates/PSU/Governement/Defence/Private and Public Limited, where the bidder has provided SOC implementation /operations service [from SOC establishment in India] (Max Marks: 10) More than 5 - 10 Marks More than 3 but ≤ 5 - 7 Marks	Please be guided by the RFP terms and conditions

Pre-Bid Queries from Prospective Bidder 2

SI No.	Section Name & No	Page No.	Existing Clause	Clarifications sought	NHB Reply
1	5.6 DETAILED TECHNICAL REQUIREMENTS 5.6.1 SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)	27	The solution should have the capability to detect vulnerabilities including behavioural vulnerabilities such as excessive administrative logins, account sharing and unusual after- hours' activity by scanning Bank's databases and data warehouses.	The specification is mainly concerned with detecting and addressing anomalies and behavioural based vulnerability use cases which comes under UEBA. And the indepth scope of this is found in UEBA.Kindly requesting you to let us know if we are proposing UEBA here, if not kindly requesting to remove the clause.	The bidder has to be provide requested functionality as per terms & conditions of RFP.
2	2. NATIONAL HOUSING BANK	8&13	The head office of NHB is located in New Delhi and a regional office located at Mumbai. It has representative offices located at Hyderabad, Bengaluru, Kolkata and Ahmedabad. The Bank is envisaging a Managed Security Services model under which the prospective bidder shall provide 24x7monitoring from bidder's SOC. The scope would involve monitoring of core infrastructure & security components at Bank's Managed Data Centre (Delhi) & Disaster Recovery Centre (Mumbai), Head Office (Delhi) and Regional Offices (ROs).	Kindly Clarify whether our understanding about the data centers are correct.Main Data Center in Delhi and the Distaster Recovery Center in Mumbai. And there is a requirement to involve monitoring the core infrastructure and security components of the regional offices located at Hyderabad, Bengaluru, Kolkata and Ahmedabad.Kindly clarify whether there is a requirement of collecting the logs from those remote locations as well.	Yes. The bidder may access Bank's website related to details of regional offices.

Pre-Bid Queries from Prospective Bidder 3

S. No.	RFP Section	Pg No.	RFP Clause	Bidder Query	NHB Reply
1	5. SCOPE OF WORK	9	Independent assurance to be provided by the bidder for purging of logs after termination/ end of contract. Log storage with syslog server to be made available onsite at BANK's premises (both DC and DR), hardware and required tools to be provided by the bidder.	Kindly confirm our understanding is correct whereby the bidder will be responsible to provide the syslog servers at NHB's premises (Both DC and DR). Also confirm, if NHB's server team will be maintaining these servers (OS level activities) or the bidder is expected to perform this?	The bidder is responsible to provide and maintain syslog server and storage at NHB premises, both in DC and DR.
2	5. SCOPE OF WORK	10	Bidder will facilitate Bank to assess SOC functioning, including all physical facilities involved in service delivery, such as the SOC and areas where client data is stored / processed periodically. Monthly/periodic visit will be facilitated by the bidder to SOC premises where bank authorities can come, visit the SOC and meet with the resources hired for the project. The Staff hired can be called to bank premises in Delhi HO whenever required by Bank officials. All expenditure pertaining to this must be borne by the bidder.	Please confirm the frequency of the bidder resources visit to NHB premises at Delhi HO? Please also confirm, if the bidder is expected to borne the travel expenses of SOC resources or NHB staff travel expenses to bidder SOC?	The expenditure related to travel expenses of bidder's SOC resources to be borne by the bidder. Bidder will not bear the expenses of Bank's visit to SOC.
3	5. SCOPE OF WORK	10	Bank/ RBI/ Bank's nominated third-party auditors has rights to audit/surprise audit the service provider compliance with the agreement including rights of access to the provider's premises where relevant records and organization data is being held.	Please confirm the procedures and approximate frequency of audits that the Bank, RBI, or nominated third-party auditors might conduct?	At present, Bank's Information Security/ Cyber Security audit and VAPT are conducted on yearly basis and quarterly basis respectively, which are subject to change as per requirements of the Bank. Audits procedure and frequency of RBI audit are decided by the RBI.

4	5. SCOPE OF WORK	10	Bidder shall store all the logs (including raw logs) for minimum 180 days. Bidder should be able to provide the stored logs to Bank, if need be, within a day’s notice and without any cost to Bank. Bank may ask logs for any time duration of the storage or applying any filter.	Please confirm if NHB expects this 180 days logs to be entirely available online or is it a combination of online and offline logs? Also please confirm, if NHB will be providing storage for offline backups or the vendor to take care of this?	Raw logs for minimum 180 days should be stored in syslog servers. SIEM logs can be stored online or offline mode. However, Bidder should be able to provide the stored logs to Bank, if need be, within a day’s notice and without any cost to Bank. All the costs pertaining to log storage including hardware, software, storage etc. to be borne by the bidder.
5	5.1 DEPLOYMENT MODELS & SERVICE DELIVERY METHODOLOGY	11	Perpetual licenses of vulnerability management tool mutually decided by bank and bidder must be provided by bidder.	Please confirm whether the perpetual license needs to be procured under the name of Bidder or the Bank?	The license can be perpetual or non-perpetual and not need to be procured on Bank's name.
6	5.1 DEPLOYMENT MODELS & SERVICE DELIVERY METHODOLOGY	12	Digital Forensics and root cause evaluation	As per the RFP document page no. 12, bidder is responsible for development and implementation of processes mentioned. Please confirm if digital forensics and root cause is in scope?	Yes
7	5.4 SCOPE OF CORE SERVICES	17	Bidder has to integrate with bank’s ticketing solution	Please confirm the current ticketing tool available at NHB.	Manage Engine Service Desk
8	5.5 PROJECT TEAM STRUCTURE	20	Vulnerability Analyst -Carry out Network security assessment	Please provide some additional insights for the network security assessment activities.	As per industry practice
9	5.5 PROJECT TEAM STRUCTURE	22	Performing red teaming and phishing exercises	Please confirm the activities to be performed under Red teaming and Phishing. Also please confirm, what will be the frequency at which each of these exercises will be carried out.	As per industry practice. At present, red teaming and phishing exercise needs to be carried on quarterly basis, which is subject to change as per Bank's requirements.
10	5.5 PROJECT TEAM STRUCTURE	24	Bidder’s resources deployment should ensure a 24*7 operational SOC. No additional resources shall be added to the project without the bank’s explicit approval.	Please confirm if NHB requires dedicated set of offsite resources for 24*7 SOC operations.	Bidder’s resources deployment should ensure a 24*7 operational SOC, as per terms and conditions of RFP.
11	5.6.3 THREAT INTELLIGENCE & ANALYTICS	33	Threat Intelligence should provide data feeds and API's for automated consumption by the SIEM Tool and ingestion in Bank’s security devices such as network firewalls, WAF, EDR, content filtering solution etc.	Request you to share some additional insights on the requirement to integrate TI feeds to NHB security devices.	Please be guided by the RFP terms and conditions

12	5.6.10 OTHER GENERAL REQUIREMENTS	43	The bidder to conduct trainings at least on monthly basis. through SMEs for Bank staff and SOC team in topics (but not limited to) related to SIEM, threat hunting, security baselines, VAPT, GRC, SOAR, Threat intelligence, cyber awareness best practices. Training calendar for the quarter to be prepared by the bidder within 7 days of start of the quarter and to be approved by the Bank	Please confirm if NHB expects this training to be held onsite or remotely. Also, confirm the role and the team of the bank employees expected to be trained in these sessions.	As decided by the bank.
13	5.16.1 STIPULATED TIME SCHEDULE	51	Project Timelines - Phase I and Phase II	Please confirm, if the bidder can propose the activity timelines and the finalization of timelines can be mutually agreed.	Please be guided by the RFP terms and conditions
14	5.16.2 SERVICE LEVELS& THRESHOLDS	53	5.16.2 SERVICE LEVELS& THRESHOLDS	Please confirm, if the bidder can propose the SLA and penalties and the finalization of timelines can be mutually agreed.	Please be guided by the RFP terms and conditions

Pre-Bid Queries from Prospective Bidder 4

SI. No	Query	NHB Reply
1	3 Weeks extension to submission date from existing of 27.02.2024	Please be guided by the RFP terms and conditions
2	We also request couple of more days to put up additional queries	Please be guided by the RFP terms and conditions
3	There is no minimum criteria on choice of SIEM solution. We recommend to add gartner leader and challangers quadrant restriction.	Please be guided by the RFP terms and conditions

	Pre-Bid Queries from Prospective Bidder 5

S.N	**Page No. of RfP**	**Section No. of RFP**	**Clause as per RFP**	**Clarification sought by Bidder**	**NHB Reply**
1	68	a. Minimum Eligibility Criteria	2. Bidder should have completed minimum 10 SOC implementation/operations service projects [from SOC establishment in India]- a) Each of these projects should be of minimum annualized value INR 10 Lakh (exclusive of taxes). b) At least 2 projects of the above should be of annualized value more than INR 50 lakh (exclusive of taxes) each. In case of ongoing projects, the value of completed services (up to a month prior to the release of this RFP) shall be considered	We request NHB to consider our request and modify the clause as beloew: "Bidder should have completed **minimum 5** SOC implementation/operations service projects [from SOC establishment in India]- a) These projects should have an average annualized value INR 3 Lakh (exclusive of taxes). b) At least **1 project** of the above should be of annualized value more than INR 50 lakh (exclusive of taxes) each. In case of ongoing projects, the value of completed services (up to a month prior to the release of this RFP) shall be considered	Please be guided by the RFP terms and conditions
2	68	a. Minimum Eligibility Criteria	3. Bidder should have successfully provided minimum 5 SOC implementation /operations service [from SOC establishment in India] to SCBs/All India FIs/ Regulatory Bodies/BFSI organizations/ Large Corporates* in India. *A Large Corporate is an organization with more than INR 100 crores as the annual turnover for at least each of last three financial years (2022-23, 2021-22, 2020-21)	We request NHB to consider our request and modify the clause as: Bidder should have successfully provided minimum 5 SOC implementation /operations service [from SOC establishment in India] to SCBs/All India FIs/ Regulatory Bodies/BFSI organizations/ Large Corporates* in India. *A Large Corporate is an organization with more than **INR 30 crores** as the annual turnover for at least each of last three financial years (2022-23, 2021-22, 2020-21)	Please be guided by the RFP terms and conditions

Pre-Bid Queries from Prospective Bidder 6

S.No.	Section	Heading	Point	Clarifications	NHB Reply
1	Section 6	Minimum Eligibility Criteria, Point 6	The Bidder must be empaneled with CERT-In as Information Security Audit Organization.	Cert-In Empanelment enables organization to conduct information security audits and certifications. As an Organizations operating a Security Operations Center (SOC) need specific certifications to ensure effective cybersecurity practices like SOC2 and ISO 27001	Please be guided by the RFP terms and conditions
2	Section 6	Minimum Eligibility Criteria, Point 7	The bidder Company should have at-least 50 qualified Information Security / Cyber Security professionals (CISSP/DISA/CISA/CISM/CDAC/ CEH/ISO 27001 certified) in their payroll.	While we understand the importance of experience, we believe strict adherence may limit qualified bidders. Our team has extensive expertise in SOC implementation. Granting this relaxation would allow for broader participation and ensure fair competition.	Please be guided by the RFP terms and conditions
3	Section 6	Minimum Eligibility Criteria, Point 2	Bidder should have completed minimum 10 SOC implementation/operations service projects [from SOC establishment in India]	While we understand the importance of experience, we believe strict adherence may limit qualified bidders. Our team has extensive expertise in SOC implementation. Granting this relaxation would allow for broader participation and ensure fair competition.	Please be guided by the RFP terms and conditions
4	Section 5.5	PROJECT TEAM STRUCTURE	GRC Expert Onsite resource	We suggest that the GRC (Governance, Risk, and Compliance) expert should be directly employed by the bank rather than being an employee of the service provider. The experience mentioned in the Request for Proposal (RFP) appears to be less compared to the job description (JD), indicating the necessity for a more experienced candidate who can directly contribute to the bank's requirements	Please be guided by the RFP terms and conditions
5	Section 5.5	PROJECT TEAM STRUCTURE	Program Manager (L3 Support)	Since resolution falls within the scope of the Managed Security Service Provider (MSSP), deploying it at the client's premises seems redundant. Therefore, I recommend seeking relaxation on this requirement. Instead, we could consider deploying additional L1/L2 support onsite to better address the client's needs.	only '3' resources have been mentioned as Onsite resources where as L3 resource ("Project Manager") is not mentioned as an onsite resource. Please be guided by the RFP terms and conditions.

Pre-Bid Queries from Prospective Bidder 7

Sr no.	RFP Section	Page no.	Points / Clause	Queries	Suggestion	NHB Response
1	General		Bid End Date/Time		Extension of bid submission date by 30 Days	Please be guided by the RFP terms and conditions
2	3	8	To train and upskill Bank's team on security operations and governance skills	Please share no. of participants and frequency for conducting training		As decided by the bank.
3	3	8	To train and upskill Bank's team on security operations and governance skills	Please share training content expected for security operations and governance		As decided by the bank.
4	5	9	This section provides the scope of work for this RFP. Selected bidder will be responsible for integrating, operating and 24*7 monitoring Bank's SOC, equipped with set of tools such as, Security Information and Event Management (SIEM), SOAR, Threat Intelligence Platforms (TIP), and all other tools that are required to comply to the scope and service levels at bidder's site. SIEM solution offered should support sustained 4000 EPS (Events per Second) and/or equivalent Flow records per second with 35% buffer capacity. Bidder to also provide a scalability roadmap to 7000 EPS and/or equivalent flow records per second.	Bidder proposal to NHB should be in total 5400 EPS considering 35% buffer. Please confirm.		Bidder to provide the proposal for 4000 EPS, keeping in mind a buffer of 35%. Additionally a road map to be provided for increasing EPS count to 7000 EPS.
5	5	9	This section provides the scope of work for this RFP. Selected bidder will be responsible for integrating, operating and 24*7 monitoring Bank's SOC, equipped with set of tools such as, Security Information and Event Management (SIEM), SOAR, Threat Intelligence Platforms (TIP), and all other tools that are required to comply to the scope and service levels at bidder's site. SIEM solution offered should support sustained 4000 EPS (Events per Second) and/or equivalent Flow records per second with 35% buffer capacity. Bidder to also provide a scalability roadmap to 7000 EPS and/or equivalent flow records per second.	Please share estimated flows per minute (FPM)	For SIEM sizing EPS and FPM calculations are done separately	Bidder to provide the proposal for 4000 EPS, keeping in mind a buffer of 35%. Additionally a road map to be provided for increasing EPS count to 7000 EPS.
6	5	9	This section provides the scope of work for this RFP. Selected bidder will be responsible for integrating, operating and 24*7 monitoring Bank's SOC, equipped with set of tools such as, Security Information and Event Management (SIEM), SOAR, Threat Intelligence Platforms (TIP), and all other tools that are required to comply to the scope and service levels at bidder's site. SIEM solution offered should support sustained 4000 EPS (Events per Second) and/or equivalent Flow records per second with 35% buffer capacity. Bidder to also provide a scalability roadmap to 7000 EPS and/or equivalent flow records per second.	Bidder can propose hardware sizing for log storage and collection for 7000 EPS. Please confirm OR Bidder can propose hardware sizing for log storage and collection for 5400 EPS and share hardware specs requirement for 7000 EPS		Log storage should be able to cater for minimum 180 days, as mentioned in RFP.
7	5	9	This section provides the scope of work for this RFP. Selected bidder will be responsible for integrating, operating and 24*7 monitoring Bank's SOC, equipped with set of tools such as, Security Information and Event Management (SIEM), SOAR, Threat Intelligence Platforms (TIP), and all other tools that are required to comply to the scope and service levels at bidder's site. SIEM solution offered should support sustained 4000 EPS (Events per Second) and/or equivalent Flow records per second with 35% buffer capacity. Bidder to also provide a scalability roadmap to 7000 EPS and/or equivalent flow records per second.	Please share integration requirement with SOAR platform for automation and enrichment		Integration would depend on the use cases agreed for automation by the bank.

8	5	9	Ensure proper archival, purging and retention of logs for future analysis as per Bank's requirement. Independent assurance to be provided by the bidder for purging of logs after termination/ end of contract. Log storage with syslog server to be made available onsite at BANK's premises (both DC and DR), hardware and required tools to be provided by the bidder	1. Pl clarify the log retention timelines for both online and offline log retntion. 2. Pl. provide the relevant details such specific address of DC and DR and technical details including fiber connections or copper cabling etc for hosting of syslog server.		Raw logs for minimum 180 days should be stored in syslog servers. SIEM logs can be stored online or offline mode. However, Bidder should be able to provide the stored logs to Bank, if need be, within a day's notice and without any cost to Bank. DC is in New delhi and DR is in Mumbai, specific details will be shared post selection of successful bidder.
9	5	10	The bidder will conduct phishing simulation exercises (at least on quarterly basis) to check the awareness levels of Bank's users against phishing threats. The end-users shall also be educated by the bidder regarding general cyber security awareness concepts through sessions/ computer-based trainings on quarterly basis.	Please share total no. of users for anti phishing campaign		It will be for the complete bank staff based in Head Office and regional offices. At present, approx. count is 350.
10	5.1	11	Syslog server with Log Storage shall be installed at Bank site (both DC & DR) and other components such as SIEM/ Rules & correlation engine, advanced detection, triggering & response platforms are at bidder's SOC as per regulatory guidelines.	Bidder has to propose separate syslog solution to bank for DC & DR. Please confirm		Yes
11	5.1	11	Perpetual licenses of vulnerability management tool mutually decided by bank and bidder must be provided by bidder.	Please share total no. of IPs to be considered for licensing. Further, licenses are usually subscription based. Kindly confirm Please share frequency for vulnerability scanning		The license can be perpetual or non-perpetual and not need to be procured on Bank's name. At present, Bank's Information Security/ Cyber Security audit and VAPT are conducted on yearly basis and quarterly basis respectively, which are subject to change as per requirements of the Bank. Bank's IT Infrastructure has been mentioned in the RFP.
12	5.1	11	Overall scope to ensure full coverage of 24*7*365 log monitoring aspects of various security solutions, devices, software, applications like firewalls, network intrusion prevention systems, WAF, DAM, PIM, DLP, Anti-DDOS, Anti-APT, Honeypot, etc. and critical network security devices at the Data Centers, Data Recovery Request for Proposal (RFP) : Setting up Security Operations Centre (soc), SIEM and Security Tools Implementation Confidential Page 12 of 128 (DR) Site (near DR and far DR), branches and other locations identified by National Housing Bank.	Pl. share the complete asset inventory with specific oem / model names for integration validation. Please share total no. of locations bidder need to consider for proposing log collectors		Asset inventory has been shared in RFP. Specific details would be shared post selection of bidder.Log collector to be installed in DC and DR
13	5.1	12	Digital Forensics and root cause evaluation	On demand Digital forensic services can be proposed by bidder. Please confirm		Digital forensics and RCA as directed by the bank need to be carried out by the bidder.
14	5.4	16	Alternatively, bidder & OEMs could leverage Bank's existing ITSM tool for ticketing and incident management etc.	Please share OEM name for integration feasibility check		Manage Engine Service Desk
15	5.4	16	To provision a dedicated incident dashboard, which shall provide a systematic view of the various tickets along with their criticalities.	Bidder shall leverage NHB's ITSM tool for dashboarding and reporting. Please confirm.		Please be guided by the RFP terms and conditions.
16	5.4	17	Incident ticket will be opened in bidder's Ticketing System for any security breach or virus outbreak	Bidder can directly raise ticket in NHB ITSM solution. Please confirm.		Please be guided by the RFP terms and conditions.

17	5.5	25	Up to 15 days of leaves per year shall be acceptable without any commercial impact to the SOC provider.	Bidder request to change this point as manpower in bidders payroll is eligible for bidders leave policy		Please be guided by the RFP terms and conditions.
18		29	The solution should have the capability to detect vulnerabilities including behavioural vulnerabilities such as excessive administrative logins, account sharing and unusual after- hours' activity by scanning Bank's databases and data warehouses. The solution should identify issues such as missing patches, weak passwords, unauthorized changes and misconfigured privileges. Further, comprehensive reports should be provided along with suggestions to address all vulnerabilities	Bidder request to modify this compliance point as suggested	The solution should have the capability to integrate with vulnerability tool including behavioural vulnerabilities such as excessive administrative logins, account sharing and unusual after-hours' activity by scanning Bank's databases and data warehouses. The solution should identify issues such as missing patches, weak passwords, unauthorized changes and misconfigured privileges. Further, comprehensive reports should be provided along with suggestions to address all vulnerabilities	Please be guided by the RFP terms and conditions.
19	5.6.1	31	The solution should support integration with big data platforms	Bidder request to clarify requirement for integration with big data platform	It should be other way round, big data platform should support integration of SIEM solution	Data migration to a big data platform if required in future should be supported by the Bidder. Please be guided by the RFP terms and conditions.
20	5.6.1	31	The Solution should have the capability of integrating threat intel from public sources and government as directed by the bank	Please share protocol for threat intel integration, majority of solution support STIX/ TAXII		Specific details would be shared post selection of bidder.
21	5.6.1	31	The solution should be able to integrate with incident management and ticketing tools	Pl. confirm if Bank's incident management and ticketing tool supports open API or email to ticket creation portal		Yes
22	5.6.2	34	The solution should offer the ease of creating custom playbooks which needs to be flexible and multi-conditional. The solution should also allow developing playbook without the need of coding. This will be tailored to NHB's specific security procedures.	Creation of playbook depends upon the IR process and it may require need of coding. Request you to modify the point.		Please be guided by the RFP terms and conditions.
23	5.6.1	41	Following types of connectivity (dedicated leased line) shall be established by the vendor/ SOC-provider 1. Vendor Data Centre (DC) to NHB DC 2. Vendor DC to NHB Disaster Recovery (DR) site 3. Vendor DR to NHB DC 4. Vendor DR to NHB DR	Bidder can create Ipsec tunnel instead of configuring dedicated leaseline		Bidder has to provide dedicated leased lines. Please be guided by the RFP terms and conditions.
24	5.7	44	Real-time alerts for priority tickets on email and SMS	Bank can provide SMS gateway for integration. Please confirm		Bidder is expected to provide. Please be guided by the RFP terms and conditions.
25	5.16.1	51	STIPULATED TIME SCHEDULE	Please share detailed signoff and acceptance criteria for both Phases	Bidder recommends overall 90 days stipulated time for phase 1 specifically for activity 4 and phase 2 specifically for activity 3	Please be guided by the RFP terms and conditions.
26	5.16.1	51	STIPULATED TIME SCHEDULE	Bidder and NHB can mutually agree to separate project timelines. Please confirm.		Please be guided by the RFP terms and conditions.
27	5.16.1	51	STIPULATED TIME SCHEDULE- Phase 1	Bidder needs to supply, install and configure collector, VM, syslog server etc. in phase 1. Please confirm		Please be guided by the RFP terms and conditions.
28	5.16.1	51	STIPULATED TIME SCHEDULE- Phase 2 Commissioning of all of Managed Security Services as defined in RFP document	Please define commissioning of services		Services should be up and running, as per the satisfaction of Bank.
29	5.16.2	53	Monitoring & Incident Alerting 1.High Criticality Security Alerts (Priority 1) to be reported within 30 minutes and resolved within 1 hour 2. Medium Criticality Security Alerts (Priority 2) to be responded within 3 hours and resolved within 6 hours 3. Low Criticality Security Alerts (Priority 3) to be responded within 8 hours and resolved within 24 hour	Bidder request to change resolving SLA, resolver team will be from bank IT and network team. Please confirm	Bidder providing standard managed security service which pertains to standard incident notification SLA	The bidder has to report the alert within stipulated timelines.

30	5.16.2	53	Incident Investigation Reports and Closure	Please clarify closure point in this SLA point		SOC provider to assist Bank in closure of incident.
31	5.16.2	55	For each breach/ data theft/data corruption/ Data mining issue/ privacy breach, penalty will be levied as per following criteria. Any security incident detected 1% of the entire monthly billing per month. This penalty is applicable per incident. These penalties will not be part of overall SLA penalties cap per quarter. In case of serious breach of security wherein the data is stolen, mined, privacy breached or corrupted, Bank reserves the right to terminate the contract.	Bidder request to delete this SLA point	MSSP bidder is responsible for detection of threats by integrating existing security technologies and controls, any breach SLA is not covered in MSS model	The clause will be applicable in case of Security and Privacy breach including Data Theft / Loss/ Corruption/Mining pertaining to Bank's data and operations.
32	5.16.2	55	Review of security baselines configuration and configuration review of all IT infrastructure and cyber security components on a quarterly basis	Please share total IT asset details such as make , model , count etc.		Details as mentioned in the RFP, specific details will be shared with successful bidder.
33	5.16.3	57	This RFP is not exhaustive in describing the functions, activities, responsibilities, and services for which the consultants will be responsible. The Bidder, by participation in this tender, implicitly confirm that if any functions, activities, responsibilities or services not specifically described in this RFP are necessary or appropriate for the proper performance and required for compliance of Statutory or Regulatory compliance and they will be deemed to be implied by and included within the scope of services under this RFP at no extra cost and Bidder's response to the same extent and in the same manner as if specifically described in this RFP and Bidder's response.	The costing is based on the existing regulatory landscape any change incurring material cost shall have to be paid separately by NHB	Please change this point as some of regulatory requirement may need technology procurement and that would lead to additional cost	Please be guided by the RFP terms and conditions.
34	7b	71	For all project experience requirement, bidders must provide a copy of Contract/ Purchase Order, along with a certificate of successful work completion from the client specifying the scope of services, value of contract and period of contract. In case of on-going projects, bidders shall provide phase completion certificate from the client specifying the scope of services delivered, value of services delivered and duration of phase.		Request to change it to either Purchase Order/Copy of Contract or Completion Certificate for proofs of project experience.	The bidder may either provide PO/ contract copy or completion certificate, as mentioned in RFP.
35	8	73	100% payment of CAPEX (implementation cost of Phase I) in Arrear shall be made after successful implementation and sign-off by the Bank.	Bidder recommends revised payment structure for CAPEX	90% of CAPEX payment to be done on hardware delivery and 10% on completion of Capex activities	Please be guided by the RFP terms and conditions.
36	9.23	77	If the consultant fails to complete the due performance of the contract in accordance with the specifications and conditions agreed during the final contract negotiations, NHB reserves the right to recover damages maximum of 10% of the contract value for non-performance/delayed performance as and by way of liquidated damages.		Buyer to revise liquidated damages recovery from 10% to 2.5%	Please be guided by the RFP terms and conditions.
37	3.11	115	The Consultant'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.		Liability is recommended to be restricted to the contract value	Please be guided by the RFP terms and conditions.
38	3.11	115	Under no circumstances, NHB shall be liable to the Consultant for direct, indirect, incidental, consequential, special or exemplary damages arising from termination of this Agreement, even if he has been advised of the possibility of such damages		Requesting to change this point, as this is not as per natural laws of justice	Please be guided by the RFP terms and conditions.

39	3.2	117	The Consultant 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 Consultant, directly related to the Services. In case any of the Services are further outsourced/ assigned/ subcontracted to other consultants in terms of the RFP, it will be the responsibility of the Consultant to ensure that the authorities /officials as mentioned above are allowed access to all the related places, for inspection and/ or audit.	Requesting to delete this clause	MSSP is shared platform service, audit of premises is not permitted as we are bound to data confidentiality for shared pool of clients	Please be guided by the RFP terms and conditions.

Pre-Bid Queries from Prospective Bidder 8

Ser.	Query	NHB Response
1	. Bidder's average annual turnover should be more than INR 100 crores in each of the last three financial years (FY) i.e.2020-21, 2021-22, 2022-23. We are MSME & Start Up registered Company, our products are 100% Make in India, our products are also meeting the quality & technical specification of your Tender. So, we are seeking the relaxation for Startups Medium Enterprise under the Office Memo Dated 20th Sept'2016, GOI Guidelines. Requesting to please allow & exempt us for Turn Over Criteria.	As mentioned in the RFP, For MSME/ Start-Up bidders, condition of prior turnover is waived.
2	Since tender Scope of works are wide, so for proper estimation & exact technical documentations we need additional time. Requesting you to please extend the tender deadline for at least 10 working days.	Please be guided by the RFP terms and conditions

Pre-Bid Queries from Prospective Bidder 9

Ser.	**Query**	**NHB Response**
1	· The SIEM solution should allow lightning fast hot search of data for a minimum of 365 days and also allow the searchable storage to be expandable.	Please be guided by the RFP terms and conditions
2	· The solution’s security data lake should be capable of scaling into an enterprise wide data lake to maintain the centralization of data.	
3	· The solution provides a single platform for log management, SIEM, UEBA, incident management and SOAR.	
4	· The platform should have content management to manage siem content such as use cases, parser, lookup, tpi etc, The vendor should have threat research team that publishes new content on regular basis	

Pre-Bid Queries from Prospective Bidder 10

S.No	Page No	Para No.	Description	Query details	NHB Reply
1	11	5.1 DEPLOYMENT MODELS & SERVICE DELIVERY METHODOLOGY	Perpetual licenses of vulnerability management tool mutually decided by bank and bidder must be provided by bidder.	Can we provide licenses through a subscription model for Vulnerability Management	The license can be perpetual or non-perpetual and not need to be procured on Bank's name.
		Point 2			
2	36	5.6.6 TICKETING TOOL	as per compliance solution be software based	We have ticketing tool which have capabiltity to integrate with another paltform which have API Capability.	Refer Corrigendum and terms of RFP
			hosted on premise in Bank datacenter	but as per compliance it should be hosted on premises .	
				Shall we proposed this ticking tool solution .	
3	25	5.5 PROJECT TEAM STRUCTURE	Successful bidder/ SOC provider will have to submit names and profiles of the resources working the project on a quarterly basis and match the criteria in the RFP. SOC provider will also be required to submit an undertaking on a quarterly basis, that no one, other than profiles shared with the Bank, are deployed on the project.	For Remote Support engineer , required dedicated or shared model basis .Please clarify.	Onsite resources are dedicated. For other resources, the bidder to cater RFP terms and conditions.
		d) Quality of Staff-			