राष्ट्रीय आवास बैंक
NATIONAL HOUSING BANK

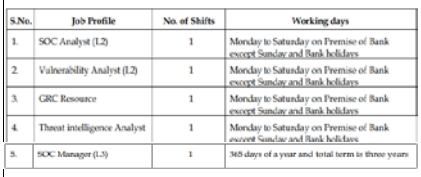
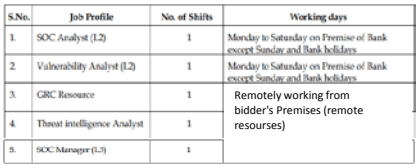
(संदर्भ: बोली संख्या: जीईएम/2024/बी/5312935 दिनांक: 22-08-2024)

कृपया अंग्रेजी देखें

Pre-Bid Queries from Prospective Bidder 1

S.No	Page No	Clause	Query	Response
		5. Scope of Work		
1	9	a. Install and commission adequate log collector at Bank sites (both DC & DR). Ensure that logs are being collected from all the in-scope devices. As appropriate suggest Bank and related stakeholders on required log-levels and support Bank in enabling the suggested log levels	Kindly confirm if the log collector needs to be installed only in DC & DR Site.	Bidder can propose to install log collector, but logs need be collected from Switches located in Regional offices and laptops and all other endpoints not connected with actiee directory as well.
2	9	d. Integrate the tickets with Bank's ticketing tool	Kindly provide inputs on bank's existing ticketing tool? Which OEM does the tool belong too?	Bank is using Manage engine as ticketing tool.
3	9	r. 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.	Does the bidder need to propose a separate tool for the phishing simulation exercises? Also can the general cyber security awareness be done online?	Awareness training can be conducted online/offline as mutually decided by the Bank. Bidder has to decide and present the methodology of conducting phishinhg excericse during the technical presentation
4	11	Additionally, log collectors and central log manager shall be deployed at Bank's Data Center and Data Recovery site.	Does the bank undertake to store to the logs locally at bank premise or can be stored in a online storage based in India like in public/private cloud in india region?	Please refer Clause 5 (SCOPE OF WORK) of the RFP.
5	14	5.3 SCOPE IN TERMS OF THE NUMBER OF SERVICES /DEVICES	Kindly provide inputs on the make & models of the devices to be integrated with the SOC Solution?	Servers(windows+linux), network devices, security solutions
6	84	7 BIDS (TECHNICAL & COMMERCIAL) AND BID EVALUATION METHODOLOGY a. Minimum Eligibility Criteria		
7	84	2. Bidder should have completed minimum 10 SOC implementation/operations service projects [from SOC establishment in India]- a) At least 2 projects of the above should be of value more than INR 50 lakh (exclusive of taxes). In case of ongoing projects, the value of completed services (up to a month prior to the release of this RFP) shall be considered	Is this appliclable for MSME? (as prior experince and turn over is exempt this clause should also be exempted)	Please refer ANNEXURE - V (MINIMUM ELIGIBILITY CRITERIA) of the RFP. As per Rule 170 of General Financial Rules (GFRs) 2017, MSME/ Start Up Bidders are exempted from submission of bid security i.e., EMD deposit. In view of same, exemption of bid security has been provided to MSMEs in the RFP. Further, requirement of prior turnover is waived for MSME/ Start-Up bidders in Minimum Eligibility Criteria. Criteria related to annual turnover of the bidder during last three years in Technical Eligibility Criteria is also relaxed for MSME bidders. All other terms & conditions of RFP shall remain same for MSME/ Startup bidders.
8	84	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	Is this applicalble for MSME? (again same reason as above)	Please refer ANNEXURE - V (MINIMUM ELIGIBILITY CRITERIA) of the RFP. As per Rule 170 of General Financial Rules (GFRs) 2017, MSME/ Start Up Bidders are exempted from submission of bid security i.e., EMD deposit. In view of same, exemption of bid security has been provided to MSMEs in the RFP. Further, requirement of prior turnover is waived for MSME/ Start-Up bidders in Minimum Eligibility Criteria. Criteria related to annual turnover of the bidder during last three years in Technical Eligibility Criteria is also relaxed for MSME bidders. All other terms & conditions of RFP shall remain same for MSME/ Startup bidders.
9	84	6. The bidder Company should have at-least 50 qualified Information Security / Cyber Security professionals (CISSP/DISA/CISA/CISM/ISO 27001 Lead Auditor/Lead Implementor certified) in their payroll.	Is this applicalble for MSME?	Please refer ANNEXURE - V (MINIMUM ELIGIBILITY CRITERIA) of the RFP.
10	29	5.6 DETAILED TECHNICAL REQUIREMENTS :	Some of the requirements/specifications mentioned in the technical requirments can be met only by deploying the solution On -prem while others could be met by deploying the tools remotely/on cloud as well For optimum and seemless intergation & performance the complete solution (all tools) should be deployed On-Prem (DC & DR) and operations can be managed as per tender specifications. Also major regulatory compliances require the financial bodies to store the raw logs for multiple years and if the service is terminated after 3 years or so, the service provider will hand over the raw logs but in absence of SIEM license by the bank, it will not be in a readable form. Perpetual licensing in name of Bank will allow the software to be retained and the raw logs can be mounted and shared to audit/ forensics if required even for years. All the Banks deploy using this model to comply for sharing the raw logs quickly in case of audit or forensics. This will not be possible with the pure service model in the absence of license ownership by the end customer. In case of vendor switch after 3 years, flexibility in retaining the license deployment. As a lot of custom rules, knowledge base will be created to accommodate the Bank's Security landscape, which will not be retained post the contract termination and the similar activity must be started from scratch.	Please be guided by the RFP terms and conditions.
11		On site Resources	At some place its mentioned 3 resources are required on-site and elsewhere its mentioned 4 reosurces and at another place 5 reosurces. Pls. clarify the exact on-site resources required.	We require 4 onsite resouces and 1 resource(Manager) working remotely from bidders location
12		Ticketing tool	Specs ask for SOC intergation with the existing tool while there are specifictaions also asking for a ticketing tool. Pls. clarify if a new ticketing tool needs to be provided as part of the project	Bank is using Manage engine
13		The solution should support integration with big data platforms	Pls. specify the Big Data platforms to be intergated	Bidder to provide best suitable option wrt to bank environement.
14		The solution should auto-failure to DR unit if the DC is down	Rephrase to add 1 click	Pls be guided by the terms and conditions of the RFP.
15		The solution should support restricting passed parameter to downstream/upstream task in the playbook.	pls. elobrate the requirement	The solution to be able to support paramater passing which are restricted to other downstream/upstream tasks in the playbook. Playbook refers to the manual/use cases.
16		The solution should support Active-Active high availability.	Include Active - Passive as well along with Active - Active HA	Please be guided by the RFP terms and conditions.
17		Solution should utilize data science techniques to identify kill chains for attacks such as lateral movements e.g. If a destination IP of one alert later becomes a source IP of another alert this suggests existence of a sequence.	Pls. change it to Data Science/AI ML	Please be guided by the RFP terms and conditions.
18		5.6.1 : The solution should allow for load balancing the network bandwidth	This is not applicable to SIEM. Also all the SIEM components support Active - Passive HA with no degradation in performance if any of the SIEM component goes down in HA cluster. Pls delete this clause	Please be guided by the RFP terms and conditions.
19	90	Technical evaluation 4- Annual Turnover	The scoring system is at disadvantage for MSME bidders as they can attain only 5 marks for turnover being less than 100Cr. This clause should be waived for MSME's or awarded 10 marks insetad of 5 marks	As per Rule 170 of General Financial Rules (GFRs) 2017, MSME/ Start Up Bidders are exempted from submission of bid security i.e., EMD deposit. In view of same, exemption of bid security has been provided to MSMEs in the RFP. Further, requirement of prior turnover is waived for MSME/ Start-Up bidders in Minimum Eligibility Criteria. Criteria related to annual turnover of the bidder during last three years in Technical Eligibility Criteria is also relaxed for MSME bidders. All other terms & conditions of RFP shall remain same for MSME/ Startup bidders.

Pre-Bid Queries from Prospective Bidder 2

Sr.No.	RFP Clause No.	Page No.	RFP Clause detail	Amendment Sought/Suggestion	Response
1	5.3	14,15	SCOPE IN TERMS OF THE NUMBER OF SERVICES /DEVICES	Kindly confirm if the number of devices mentioned in Section 5.3 of the RFP includes both DC and DR devices for SOC monitoring. If so, could you please provide the segregation of devices between DC and DR?	The count comprises of both DC and DR.
2	5.5	28	All 4 onsite resources shall be interviewed by the Bank and should be included in the project once Bank approves. Bank reserves the right of scanning / evaluating / interviewing the profiles selected for the project and requires commitment (at the time of bidding / evaluation phase) from the participant to provide profiles of 'Key' Resources who will be engaged in the project (e.g. Project Manager, Architect, SME etc.).	Amended Clause - All 2 onsite resources shall be interviewed by the Bank and should be included in the project once Bank approves. Bank reserves the right of scanning / evaluating / interviewing the profiles selected for the project and requires commitment (at the time of Project Kickoff) from the participant to provide profiles of 'Key' Resources who will be engaged in the project (e.g. Project Manager, Architect, SME etc.).	Please refer clause 5.5 of the RFP.
3	5.5	28, 29		 Note: SOC Analyst (L2) and Vulnerability Analyst (L2) will be provisioned onsite to Banks but GRC Resorce, Threat Intelligence Analyst and SOC Manager (L3) will be working remotely from Bidder's Premise.	Please refer clause 5.5 of the RFP.
4	7.ii.a.4	85	The bidder should own and have been managing well established Security Operations Centre (SOC) [as well as DR site] with its own threat intel platform.	Amended Clause - The bidder should own and have been managing well established Security Operations Centre (SOC) [as well as DR site] with the threat intel platform.	Please be guided by the RFP terms and conditions.
5	7.ii.a.6	85	The bidder Company should have at-least 50 qualified Information Security / Cyber Security professionals (CISSP/DISA/CISA/CISM/ISO 27001 Lead Auditor/Lead Implementor certified) in their payroll.	Amended Clause - The bidder Company should have at-least 25 qualified Information Security / Cyber Security professionals (CISSP/DISA/CISA/CEH/CISM/ISO 27001 Lead Auditor/Lead Implementor certified) in their payroll.	Please be guided by the RFP terms and conditions.
6	7.ii.a	86	For point 9 and 10, Auditor Certificate to be submitted by the Bidder	Kindly confirm if this clause pertains to points 8 and 9 in this section of the RFP, as point 10 is not mentioned.	Yes corrigendum has been added for this. For point 8 and 9, Auditor Certificate to be submitted by the Bidder
7	7.ii.a.8	85	Bidder's annual turnover should be more than INR 100 crores in each of the last three financial years (FY)	Bidder's annual turnover should be more than INR 50 crores in each of the last three financial years (FY)	Please be guided by the RFP terms and conditions.
8	7.ii.b.1	87	Experience of the bidder 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 services of value more than INR 50 Lakhs (Max Marks: 15) More than 2 and upto 5 such projects ---------- More than 5 and upto 10 such projects ---------- More than 10 such projects----------	Experience of the bidder 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 services of value more than INR 50 Lakhs (Max Marks: 15) More than 0 and upto 2 such projects - 5 Marks More than 2 and upto 4 such projects - 10 Marks More than 4 such projects - 15 Marks	Please be guided by the RFP terms and conditions.
9	7.ii.b.2	88	The number of professional staff in the area of Information Security/ Cyber Security as per the certifications mentioned in the RFP (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: 15) More than 50 but ≤ 100 ---------- More than 100 but ≤ 150 ---------- More than 150 ----------	The number of professional staff in the area of Information Security/ Cyber Security as per the certifications mentioned in the RFP (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: 15) More than 25 but ≤ 35 - 10 Marks More than 35 but ≤ 50 - 15 Marks	Please be guided by the RFP terms and conditions.
10	7.ii.b.4	90	Annual turnover of the bidder during last three years i.e. (Max Marks: 10) For NON MSME Bidders More than INR 100 crore but <= INR 500 crore---------- More than INR 500 crore but ≤ INR 1000 crore ---------- More than INR 1000 crore---------- For MSME Bidders Less than or equal to 100 crore ---------- More than INR 100 crore but ≤ INR 250 crore ---------- More than INR 250 crore----------	Annual turnover of the bidder during last three years i.e. (Max Marks: 10) For NON MSME Bidders More than INR 50 crore but <= INR 100 crore - 05 Marks More than INR 100 crore but ≤ INR 150 crore - 07 Marks More than INR 175 crore - 10 Marks	Please be guided by the RFP terms and conditions.
11	ANNEXURE - V (MINIMUM ELIGIBILITY CRITERIA)-Point No-9	105	Bidder should have positive net worth and should not be insolvent or should not have filed for bankruptcy	Bidder should have positive net worth in any of the 3 years in last 5 years.	Please be guided by the RFP terms and conditions.

Pre-Bid Queries from Prospective Bidder 3

Sl No.	Section and Clause reference	Page Number	RFP Text	Query	Response
1	Section - 7, Section 2, Subsection a and b	85 and 90	Bidder's annual turnover should be more than INR 100 crores in each of the last three financial years (FY)	As per the note: the requirement for prior turnover is waived for MSME/Start-Up bidders. However, the technical eligibility criteria includes a scoring system based on turnover, which may conflict with the earlier waiver.	As per Rule 170 of General Financial Rules (GFRs) 2017, MSME/ Start Up Bidders are exempted from submission of bid security i.e., EMD deposit. In view of same, exemption of bid security has been provided to MSMEs in the RFP. Further, requirement of prior turnover is waived for MSME/ Start-Up bidders in Minimum Eligibility Criteria. Criteria related to annual turnover of the bidder during last three years in Technical Eligibility Criteria is also relaxed for MSME bidders. All other terms & conditions of RFP shall remain same for MSME/ Startup bidders.
2	Section - 7, Section 2, Subsection a	85	2. Bidder should have completed minimum 10 SOC implementation/operations service projects [from SOC establishment in India]- a) At least 2 projects of the above should be of value more than INR 50 lakh (exclusive of taxes). In case of ongoing projects, the value of completed services (up to a month prior to the release of this RFP) shall be considered. 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	We request you to ammend as following: 2. Bidder/OEM should have completed minimum 10 SOC implementation/operations service projects [from SOC establishment in India]- a) At least 2 projects (Bidder / OEM) of the above should be of value more than INR 50 lakh (exclusive of taxes). In case of ongoing projects, the value of completed services (up to a month prior to the release of this RFP) shall be considered. 3.Bidder/OEM 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	Please be guided by the RFP terms and conditions.
3	Section 1, point 5	91	Rs.1,00,000/- (for non MSME bidders) Bid Security Declaration (MSME/Start Up Bidders). 'Bidder has to submit the "EMD/Bid Security Declaration" on their organization's letter head duly signed and stamped by their authorized signatory accepting that if they withdraw or modify their bids during period of validity of the bid, or if they are awarded the contract and they fail to sign the contract, or fail to submit a performance security before the deadline defined in the request for proposal (RFP) document, they may be Suspended/Blacklisted at Bank's discretion.	Estimated Project Value and past references seems misaligned, especially with the amount of EMD that has been requested. Kindly advise.	Project value is related to PBG.

Pre-Bid Queries from Prospective Bidder 4

Sr. No.	Page No.	Clause	Clarification Requested	Response
1	Page No. 9	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.	Requesting authorities to clarify on the EPS count? Shall we only consider 4000 EPS with 35% buffer or 7000 EPS?	EPS required is 4000, in case if peak is observed, scalability roadmap for 7000 EPS to be shared.
2	Page No. 9	Integrate the tickets with Bank's ticketing tool	Request you to please clarify on the Ticketing Tool	Ticketing tool-Manage engine
3	Page No. 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	Could you please clarify on the number of targeted users for phishing simulation and approx number of users that Bank will nominate for the training?	Targeted users for phishing simulation-300-400 employees
4	Page No. 11	Bidder has to provide OEM/SME training for all the tools/services namely but not limited to SIEM, SOAR, Vulnerability management tool, Threat intelligence feed, Threat intelligence platform etc.	Could you please clarify on the audience for this training ? Is it for the resources who will be managing SOC.	Phishing awarness training to be provided to all NHB employee. And specialised OEM/SME training would be sought for IT and IS resources.
5	Page No. 11	**Phase I- Implementation** Additionally, log collectors and central log manager shall be deployed at Bank's Data Center and Data Recovery site.	As per this clause shall we consider the data collection will only be from DC and DR.	Log collectors may be placed at DC and DR as envisaged by the the bidder. Logs need to be collected from DC And DR and other endpoints and network devices which are not connected to DC/DR located at different locations.
6	Page No. 13	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)	Could you please confirm about the data collection from Head Office (Delhi) and Regional Offices (ROs). Shall we provison collectors ? Or their data can be taken from DC, DR.	Logs collector may be placed at DC and DR and some endpoints which are not connected to DC/DR located at different locations.
7	Page no. 63	Continuous and regular monitoring of brand for any suspicious chatter, abuse of brand, phishing domains	Please confim about the number of domains, and domain names.	nhbonline.in nhbonline.info nhbonline.org nhbonline.net nhb.co.in nhb.ind.in nhb.net.in nhb.gen.in nhb.firm.in nhbonline.co.in nhbonline.ind.in nhbonline.net.in nhbonline.gen.in nhbonline.firm.in nationalhousingbankindia.com nhbonline.biz nhbonline.org.in nhb.org.in
8	Page no. 30	In addition to the advanced analytics capabilities like MDR, solution should have capabilities to define rules on event logs captured from various sources to detect suspicious activities	Please confirm MDR should be pat of SIEM or a separate requirement.	Please refer clause 5.6 of the RFP.
9	Page no. 29	Next Generation SIEM with security analytics capabilities shall be integrated with all devices in the Data Centre, DR site, systems, application and end-user devices. SIEM shall be integrated with application logs of target application for enFd-to-end security monitoring	Please provide the device details with OEM names and daily/weekly backup volume of each device.	Devices generally consists of servers(windows,linux),network devices(cisco switches/routers, cisco firepower,cisco ips), security solutions-(WAF, O365,NAC, FORCEPOINTS PROXY,EDR
10	Page no. 31	The proposed Solution must be able to identify patterns and must recommend actions based on the investigation output, using AI capabilities It must provide threat detection by running Sigma rules as a query against various security devices such as SIEM, EDR, and NDR. It is necessary for this platform to offer the repository of Sigma rules in the UI along with the option of converting any of the rules into a search query	Please confirm is bank using any EDR, NDR tool. If yes, please provide more details of the same.	Bank has integrated EDR solution with SIEM solution offered by Sophos .
11	Page no. 33	. The solution should support integration with big data platforms	please provide big data platform details	Bidder to provide best suitable option wrt to bank environement.
12	Page no. 35	The solution should be able to integrate with 3rd party backup solutions to maintain a backup of SIEM	please clarify is bank using any backup solution. If yes, please provide the details. or bidder have to propose the same.	Bank has a backup solution from DELL.
13	Page no. 35	Ability to set up a standardized incident management tool within IT department	Please clarify that Incident Management to be part of SIEM or a separate tool is required.	Part of the project
14	Page no.29	1. The solution should be an appliance or software with a clear physical or logical separation of the collection module, logging module and co-relation module	Please clarify if the bidder propose SaaS platform hosted on cloud. ?	PIs be guided by the terms and conditions of the RFP. All terms and conditions of the RFP to be satisfied, accordingly the bidder has to propose a solution.
15	Page no.29	4. The solution's licensing should be by the number of events per second and/or flow records per second, and the payout should be as per the events per second and/or flow records per second handled	The total license for the deployment is 7000 inluding events and flows, is our understanding correct ? Please also clarify on the online and offline event retention.	Please refer clause 5.6 of the RFP.
16	Page no.32	29. The solution should support log collection, flow collection and other standard method for integrating devices and applications. Logs obtained from Bank devices should be copied and stored in vendor SoC within 5 minutes from the actual log event at the integrated device	please clarify if flow collection is required for layer 4 or layer 7 or both. If both, please clarify the number of flows required? What type of port connectivity is required ex: 1 G / 10 G, copper / Fiber SFP and the type of SFPs in case of Fiber ports?	Yes, flow collection is required for both.
17	Page no.32	34. The solution should have high availability feature built in for automated switch over to secondary collector/integrator in the event of primary collector failing. No performance degradation is permissible even in case of failure	Can the bidder use load balancers in case High Availabiliity is not supported natively by the event collectors ? Load balancers also support N+1 redundancy.	High availabilityis desired, if a different configration is being proposed same should be brought out explicitly.
18	Page no.32	36. The bidder should support and integrate data (log and/or flow) collection from different OS and their versions but not limited to Windows, Linux, AIX, Solaris etc., networking devices, security devices and solutions, physical access control systems, etc., as required by Bank.	please clarify if flow collection is required for layer 4 or layer 7 or both. If both, please clarify the number of flows required? What type of port connectivity is required ex: 1 G / 10 G, copper / Fiber SFP and the type of SFPs in case of Fiber ports?	Yes flows required from both layer 7 and layer 4.
19	Page no.34	61. The solution should auto-failure to DR unit if the DC is down	Please clarify if the DR failover can be proposed on cloud.	PIs be guided by the terms and conditions of the RFP. All terms and conditions of the RFP to be satisfied, accordingly the bidder has to propose a solution.
20	Pg No 85	Bidder should have completed minimum 10 SOC implementation/operations service projects [from SOC establishment in India]- a) At least 2 projects of the above should be of value more than INR 50 lakh (exclusive of taxes). 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 you to amned this clause as below:** Bidder should have completed minimum **7** SOC implementation/operations service projects [from SOC establishment in India]- a) At least 1 projects of the above should be of value more than INR **10 Cr** (exclusive of taxes). In case of ongoing projects, the value of completed services (up to a month prior to the release of this RFP) shall be considered. **Given the critical nature of this project, we kindly request that you revise this clause as indicated.**	Please be guided by the RFP terms and conditions.

21	Pg No 85	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	**We request you to amned this clause as below:** 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. **Out of 5 POs, 1 PO should be of value more than INR 10 cr** *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 **Given the critical nature of this project, we kindly request that you revise this clause as indicated.**	Please be guided by the RFP terms and conditions.
22	Pg No 85	The bidder Company should have at-least 50 qualified Information Security / Cyber Security professionals (CISSP/DISA/CISA/CISM/ISO 27001 Lead Auditor/Lead Implementor certified) in their payroll.	**We request you to amend this clause as below:** The bidder Company should have at-least 10 qualified Information Security / Cyber Security professionals (CISSP/DISA/CISA/CISM/CEH/ISO 27001 Lead Auditor/Lead Implementor certified) in their payroll. Additionally, The Bidder must have at least 50 (forty) full time technical support professionals on its permanent roll in India who have relevant skill, competency/certification in Security solutions (Any OEM certified professional). **Certificate from HR/Authorized Signatory should be submitted at the time of bid submission.**	Please be guided by the RFP terms and conditions.
23	Pg No 87	Experience of the bidder 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 services of value more than INR 50 Lakhs (Max Marks: 15) More than 2 and upto 5 such projects More than 5 and upto 10 such projects More than 10 such projects	**We request you to amend this clause as below:** Experience of the bidder 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 services of value more than INR 50 Lakhs (Max Marks: 15) More than 2 and upto 4 such projects More than 4 and upto 6 such projects ≥ 7 such projects	Please be guided by the RFP terms and conditions.
24	Pg No 88	The number of professional staff in the area of Information Security/ Cyber Security as per the certifications mentioned in the RFP (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: 15) More than 50 but ≤ 100 More than 100 but ≤ 150 More than 150	**We request you to amend this clause as below:** The number of professional staff in the area of Information Security/ Cyber Security professional/any security OEM certified professional (Bidder will provide a undertaking signed by authorized signatory on their letter head along with the valid certificates) (Max Marks: 15) More than 50 but ≤ 100 More than 100 but ≤ 150 More than 150	Please be guided by the RFP terms and conditions.
25	Pg No 89	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 5 but ≤ 7 More than 7 but ≤ 10 More than 10	We request you to amend this clause as below: 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 2 but ≤ 4 More than 4 but ≤ 6 More than 7	Please be guided by the RFP terms and conditions.
26	Pg No 91	Bidder having a SoC and DR SOC functional in India for: (Max Marks 10) 2 years More than 2 years	We request you to amend this clause as below: Bidder having a SoC : (Max Marks 10)	Please be guided by the RFP terms and conditions.
27	Pg No 91	The bidder's SOC infrastructure must be ISO certified or must provide SOC -2 audit report. (Bidder must provide a copy of valid ISO Certification for the SOC facility or extract of most recent SOC-2 report) (Max Marks 10)	as per under stand here required Company ISO Certificate and OEM Tools SOC -2 audit report , so kindly clarify	Yes, bidder to provide copy of ISO certficate. Else SOC2 Audit report.

Pre-Bid Queries from Prospective Bidder 5

Sr. No.	Section	Page No	RFP Clause	Bidder Query	NHB Response
1	5. SCOPE OF WORK	9	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.	Is bidder also expected to provide NBAD solutions to monitor flow? If yes, what is the sizing in terms of Flows Per Minute (FPM) across each locations?	Bidder to provide SIEM solution with EPS required 4000, in case if peak is observed,scalability roadmap to support 7000 eps to be provided.
2	5. SCOPE OF WORK	9	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.	Please specify the requirements for commercials feeds on TIP.	1) Integrating top rated real time threat intelligence feeds with SIEM , Cross refernce with interanal data. 2) Provide IOC's wrt to latest malware, zero day exploits. 3) Perform proactive threat hunting for the bank.
3	5. SCOPE OF WORK	9	a. Install and commission adequate log collector at Bank sites (both DC & DR). Ensure that logs are being collected from all the in-scope devices. As appropriate suggest Bank and related stakeholders on required log-levels and support Bank in enabling the suggested log levels	Is bidder expected to provide hardware infra at Bank site for Log collection ? Or NHB will provide the necessary Infra/ VM ?	All harware/sftware has to be provided by bidder.
4	5. SCOPE OF WORK	9	d. Integrate the tickets with Bank's ticketing tool	What is your ITSM tool? Is it on-prem or on cloud ? Please provide the version number ?	ITSM Tool-Manage engine
5	5. SCOPE OF WORK	9	i. 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.	We understand the log can be stored at MSSP cloud or OEM cloud of proposed solution. Please clarify if there is any requirement of log storage within NHB environment.	Please be guided by the RFP terms and conditions.
6	5. SCOPE OF WORK	10	l. The bidder has to provide the bank with read/write access to the SIEM platform.	In a MSSP setup read / write access is not provided to clients to ensure data integrity and confidentiality of other clients. Request you to remove this clause from RFP.	Please be guided by the RFP terms and conditions.
7	5. SCOPE OF WORK	10	n. 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.	1- Please confirm the frequency of the bidder resources visit to NHB premises at Delhi HO? 2- Please also confirm, if the bidder is expected to borne the travel expenses of SOC resources or NHB staff travel expenses to bidder SOC?	1) Onsite resource availability:- a) Monday-Saturday. b) Banking hours, 10am-6pm 2) NHB wil not borne any resource travel expenses
8	5. SCOPE OF WORK	10	p. 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. We request addition of below three clauses for audit purpose: -Any third-party engaged by the client to audit EY will not be a competitor; -The audit shall be restricted to only the physical files in relation to the engagement letter and client and any third-party engaged by client will accept confidentiality obligations with EY in relation to such audit; -No access to EY's systems or hands on or intrusive testing will be permitted	Please be guided by the RFP terms and conditions.
9	5. SCOPE OF WORK	10	w. Bidder shall store all the logs for minimum 1 year – of which 181 days will be stored on-line. 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.	Online logs can be shared within one day. Logs after 181 days / offline logs will be shared on best effort basis depending upon the amount of data required. Please share your concurrence.	Bidder to be able to provide complete data for any requested time frame by the Bank even if stored online or archived.
10	5. SCOPE OF WORK	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	300- 400 users
11	5. SCOPE OF WORK	11	y. Bidder has to provide OEM/SME training for all the tools/services namely but not limited to SIEM SOAR, Vulnerability management tool, Threat intelligence feed, Threat intelligence platform etc.	Please specify the frequency and mode of training required by NHB. Please provide the count of people to whom training needs to be delivered.	Training medium online/offline can be mutually decided by bank/bidder. General awareness training to the complete bank staff. Specialised training to IT/IS staff
12	5.1 DEPLOYMENT MODELS & SERVICE DELIVERY METHODOLOGY	13	Brand monitoring and protection service	Please provide name of your 2 domains for this service.	nhbonline.in nhbonline.info nhbonline.org nhbonline.net nhb.co.in nhb.ind.in nhb.net.in nhb.gen.in nhb.firm.in nhbonline.co.in nhbonline.ind.in nhbonline.net.in nhbonline.gen.in nhbonline.firm.in nationalhousingbankindia.com nhbonline.biz nhbonline.org.in nhb.org.in

13	5.2 SCHEDULE OF REQUIREMENTS	13	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). The solutions, products and technology sought in the RFP are for security of Bank infrastructure and assets against all kinds of cyber threats.	Please provide total number of locations of NHB. DC - Delhi DR- Mumbai Head Office - Delhi NDR ? Number of Regional Offices ? What is the connectivity / bandwidth between HO, RO & NDR with NHB DC & DR. Please confirm of Log collectors are required at only NHB DC & DR location. Logs from other location will be sent to log collectors deployed at NHB DC & DR.	RO-15 existing. Planning 2 more ; HO and RO connectivity is through mpls; Log collector to be placed in DC and DR location. Logs to be collected from Switches in ROs and other endpoints not connected through DC.
14	5.4 SCOPE OF CORE SERVICES	15	• Deep Packet inspection	What is your requirement for Deep Packet Inspection ? Please provide the details and sizing.	to ensure network security, data management,traffic optimization
15	5.4 SCOPE OF CORE SERVICES	17	Ticketing and Reporting Solution Incident ticket will be opened in bidder's Ticketing System for any security breach or virus outbreak	Does it mean, Bidders ITSM will integrate with NHB ITSM bi-directional where all incident creation and assigning will happen on bidders ITSM and will get automatically assigned to resolver groups of NHB into their current ITSM. Please confirm if our understanding is correct.	yes
16	5.4 SCOPE OF CORE SERVICES	17	Ticketing and Reporting Solution Incident ticket will be opened in bidder's Ticketing System for any security breach or virus outbreak	If not the above then, please provide number of resolver groups to be enabled in bidders ITSM to be used as centralized ITSM for Incident Management Lifecycle.	
17	5.4 SCOPE OF CORE SERVICES	18	SOC Security • The solution should support all standard built applications without any additional cost. Solution should support agent-less architecture	All SIEM comes with light-weight agents which needs to be installed on server for log collection. Request you to remove agent-less requirement from RFP.	Bidder to ensure all servers,network devices, security solutions are integreated with SIEM
18	5.5 PROJECT TEAM STRUCTURE	23	Vulnerability Analyst Onsite resource • Performing red teaming and phishing exercises	Please provide the frequency and scope of red team and phishing exercise required by NHB.	a. 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. As mentioned in the above clause ATLEAST quartertly phishing and Vulnerability excercise needs to be conducted.
19	5.5 PROJECT TEAM STRUCTURE	28	Manpower Support working days schedule: SOC Manager (L3) 1 365 days of a year and total term is three years	Request to you change the clause as below for SOC Manager: Monday to Saturday on Premise of Bank except Sunday and Bank holidays	Please be guided by the RFP terms and conditions.
20	5.6.12 OTHER GENERAL REQUIREMENTS	30	The solution should have the capability to detect vulnerabilities including behavioral 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 provide number of users in your environment for UBA sizing?	300-400 users
21	5.6.12 OTHER GENERAL REQUIREMENTS	58	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 Last mile connectivity shall be the responsibility of the vendor/ SOC-provider and Bank at their respective ends.	We propose to use IPSEC VPN over existing Internet connectivity of NHB.	Please be guided by the RFP terms and conditions.
22	5.16 SERVICE LEVELS (SLs)	67	5.16.1 STIPULATED TIME SCHEDULE Phase 1 4 . T + 30 days	Transition and Implementation of services will require a minimum of 12 weeks. Request you to change this clause to T+90 days	Please be guided by the RFP terms and conditions.
23	5.16 SERVICE LEVELS (SLs)	68	5.16.1 STIPULATED TIME SCHEDULE Phase 2 3 . T + 30 days	SOC operations can be live after completion of Implementation. Request you to change this clause to T+90 days	Please be guided by the RFP terms and conditions.
24	5.16.2 SERVICE LEVELS& THRESHOLDS	72	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.	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	Please be guided by the RFP terms and conditions.

25	5.16.2 SERVICE LEVELS& THRESHOLDS	73	Maximum penalty in a month will be capped to 25% of monthly SOC operations charges except service uptime. Bidder shall not be responsible for SL impact where the delay is not attributable to the bidder. All such cases have to be adequately evidenced.	This is a MSSP service and 25% is too high. Request you to change the capping to 5% monthly.	Please be guided by the RFP terms and conditions.
26	5.16.3 PERIOD OF CONTRACT	74	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.	Please change this point as some of regulatory requirement may need technology procurement and that would lead to additional cost. Any change incurring material cost shall have to be paid separately by NHB	Please be guided by the RFP terms and conditions.
27	7 BIDS (TECHNICAL & COMMERCIAL) AND BID EVALUATION METHODOLOGY	85	6. The bidder Company should have at-least 50 qualified Information Security / Cyber Security professionals (CISSP/DISA/CISA/CISM/ISO 27001 Lead Auditor/Lead Implementor certified) in their payroll.	For wider participation, 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.
28	8 COMMERCIAL TERMS AND CONDITIONS	94	100% payment of CAPEX (implementation cost of Phase I) in Arrear shall be made after successful implementation and sign-off by the Bank.	Please change it to 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.
29	9 GENERAL TERMS AND CONDITIONS	97	23. Liquidated Damages 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. It is clarified that the liquidated damages shall be over and above the penalty, if any, imposed under the contract.	Please revise liquidated damages recovery from 10% to 2.5%	Please be guided by the RFP terms and conditions.
30	ANNEXURE - XVI (SERVICE LEVEL AGREEMENT)	136	(iii) 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.
31	ANNEXURE - XVI (SERVICE LEVEL AGREEMENT)	138	3.20 Audit 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.	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.
32	5.1 DEPLOYMENT MODELS & SERVICE DELIVERY METHODOLOGY	11	In any case bank shall not procure any license (for SIEM, end to end vulnerability management or any other tool) or any software/ hardware required for setup and operationalizing the SOC.	Please confirm whether the license needs to be procured under the name of Bidder or the Bank?	Bank shall not procure any license all hardware and software needs to be procured by the bidder for the bank.
33	5.4 SCOPE OF CORE SERVICES	19	Vulnerability Management service - The bidder to ensure Vulnerability Assessment and Penetration Testing for all systems/sub systems/network devices shall be performed quarterly.	Could you please provide the number of servers and network devices to be covered. Additionally, does this include configuration review of servers, operating systems, databases, network devices, as well as application and API security testing. If yes please provide the number of servers, operating systems, databases, network devices, applications, APIs to be consider in scope	number of assets are mentioned in the RFP. YES it includes all.
34	5.5 PROJECT TEAM STRUCTURE	21	Carry out Network security assessment	Could you please provide more details on what is expected from this activity	strengthen network security
35	5.5 PROJECT TEAM STRUCTURE	23	Performing red teaming and phishing exercises	Could you please provide the frequency of res team and phishing exercises.	can be decided mutually by Bank and bidder
36	5.5 PROJECT TEAM STRUCTURE	23	Ensure compliances to advisories and alerts received from regulatory agencies such as RBI, CERT-In, NCIIPC and IDRBT etc.	Could you please provide more details on what is expected from this activity	IOC blocking, taking requisite action as desired.
37	5.5 PROJECT TEAM STRUCTURE	21	Performing vulnerability assessment & Penetration testing of Bank's IT infrastructure, that includes, but not limited to devices vulnerability scans, network vulnerability scans, web vulnerability scans, application vulnerability scans and database vulnerability scans etc.	Could you please provide the number of servers and network devices to be covered. Additionally, does this include configuration review of servers, operating systems, databases, network devices, as well as application and API security testing. If yes please provide the number of servers, operating systems, databases, network devices, applications, APIs to be consider in scope	All asset details mentioned in RFP, Please refer section 5.3

38	5.5 PROJECT TEAM STRUCTURE	21	Carry out Firewall policy review	Could you please clarify whether the scope of work includes reviewing the firewall policy only, or if it also encompasses reviewing existing configurations and rules. If both are required, could you provide the approximate number of firewalls and rules to be considered, as well as the expected frequency of these review.	The complete review needs to be undertaken for 5 firewalls
39	5.5 PROJECT TEAM STRUCTURE	22	Ensure testing based on scoped and tailored CIS benchmarks.	Could you please clarify if configuration reviews are included in the scope. If yes, what will be the frequency of these reviews.	Yes, can be decided mutually by bank and bidder.
40	5.6.11 Vulnerability Management	51	The proposed vulnerability management service should cover all the requirements stated in this RFP Bank is looking for a single service for both traditional vulnerability management as well as Dynamic Application Security Testing.	Could you please clarify the expectations for the dynamic application security testing. Additionally, could you provide an approximate number of applications that will be included in the scope	approximately 16 number of applications.
41	5.6.11 Vulnerability Management	52	Proposed Vulnerability Management service must provide report templates, including following examples but not limit to, - CVE Analysis Report - Credential Scan Failures - Critical and Exploitable Vulnerabilities Report - Elevated Privilege Failures - Exploit Frameworks - Explotable by Malware - Malicious Code Preventation Report - Outstanding Remediation Tracking - Prioritize Assets - Unsupported OS Report - Vulnerabilities by Common Ports - Vulnerability Detail Report - Vulnerability Management - Web Services - Windows Unsupported and Unauthorized Software - Wireless Configuration Report	Are there specific formats or customization requirements for these reports? Will they need to be generated regularly, and if so, what is the expected frequency for each type of report. Additionally, how should these reports be integrated into existing security dashboards or management systems, and are there any particular tools or platforms with which they need to be compatible	Yes,customized reports can be decided mutually by bank and bidder.
42	5.6.11 Vulnerability Management	53	Proposed service must capable to determine asset exposure score automatically using AI based techniques. The asset exposure should be automatically calculated based on asset criticality and vulnerabilities active on the system.	How should the asset exposure scoring integrate with existing asset management and vulnerability assessment systems. Are there any specific examples or use cases available for how these scores will be utilized.	Use cases need to be built as decided by the Bank
43	5.6.11 Vulnerability Management	53	Proposed Vulnerability Management service provides passive scanning to detect vulnerability by monitoring the network package	Could you please provide more details on what is expected from this activity	The activity is expected to make NHBs IT infrastructure resillient towards cyber attacks
44	5.6.11 Vulnerability Management	54	Proposed Vulnerability Management service provides Malware detection policy. It can check the running processes/files MD5 against the virus definition database from over 25 anti-virus service vendors	Could you please provide more details on what is expected from this activity	The activity is expected to make NHBs IT infrastructure resillient towards cyber attacks

Pre-Bid queries from Prospective Bidder 6

REFERENCE OF TENDER DOCUMENT						
S. No.	**SEC. No.**	**Page No.**	**Clause No.**	**Subject**	**BIDDER'S QUERY**	**Response**
1	ANNEXURE - V (MINIMUM ELIGIBILITY CRITERIA)	85	2	Bidder should have completed minimum 10 SOC implementation/operations service projects [from SOC establishment in India]- a) 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 you to kindly confirm the experience of establishment/ Operation and maintenance of On-Premise Security Operation Center will also be considered. Kindly clarify.	Yes, Please be guided by the RFP terms and conditions.
2	ANNEXURE - V (MINIMUM ELIGIBILITY CRITERIA)	85	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	We request you to kindly confirm the experience of establishment/ Operation and maintenance of On-Premise Security Operation Center will also be considered. Kindly clarify.	Please refer ANNEXURE-V of the RFP.
3	ANNEXURE - V (MINIMUM ELIGIBILITY CRITERIA)	85	5	The bidder Company should have at-least 50 qualified Information Security / Cyber Security professionals (CISSP/DISA/CISA/CISM/ISO 27001 Lead Auditor/Lead Implementor certified) in their payroll.	We request you to kindly amend this clause as: The bidder Company should have at-least 50 qualified Information Security / Cyber Security professionals (CISSP/DISA/CISA/CISM/ISO 27001 Lead Auditor/Lead Implementor certified/ CEH) in their payroll.	Please be guided by the RFP terms and conditions.
4	ANNEXURE - V (MINIMUM ELIGIBILITY CRITERIA)	86	Note	For point 9 and 10, Auditor Certificate to be submitted by the Bidder	Kindly clarify against which criteria bidder has to submit the Auditor Certificate, since there is no point no. 10 and Point No.9 is related to positive networth, insolvency and bankruptcy.	For point 8 and point 9
5	6 INSTRUCTIONS TO BIDDERS	75	Earnest Money Deposit (EMD)	For Non-MSME Bidders a) All the Bids must be accompanied by a refundable interest free security deposit of Rs.1,00,000/- (Rs. One Lakh only), by way of an e-payment in favour of National Housing Bank. Account details are mentioned below. The proof of payment shall be submitted in the "Technical Proposal". Registered MSEs (Micro and Small Enterprises) shall be exempted from payment of EMD subject to submission of valid registration certificate.	We would like to apprise you that as per the GEM GTC, bidder having turnover more than INR 500 Crore in any of the last 03 FY are exempted from furninishing EMD on GeM portal. Kindly confirm if this exemption is applicable for this bid or not.	Please be guided by the RFP terms and conditions.
6	Technical Eligibility Criteria	87	1	Experience of the bidder 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 services of value more than INR 50 Lakhs (Max Marks: 15) More than 2 and upto 5 such projects ---------- More than 5 and upto 10 such projects ---------- More than 10 such projects--	We request you to kindly confirm the experience of establishment/ Operation and maintenance of On-Premise Security Operation Center will also be considered.	Please refer Clause 7 of the RFP.
7	Technical Eligibility Criteria	89	3	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 5 but ≤ 7 ---------- More than 7 but ≤ 10 ---------- More than 10---------- *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	We request you to kindly amend this clause as: No. of SCBs/All India FIs/ Regulatory Bodies/BFSI Sector in India/ Large Corporates/ Government Organization/PSU, where the bidder has provided SOC implementation /operations service [from SOC establishment in India] (Max Marks: 10) More than 5 but ≤ 7 ---------- More than 7 but ≤ 10 ---------- More than 10---------- *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	Please be guided by the RFP terms and conditions.
8	Technical Eligibility Criteria	90	4	Annual turnover of the bidder during last three years i.e. (Max Marks: 10) For NON MSME Bidders More than INR 100 crore but <= INR 500 crore----- More than INR 500 crore but ≤ INR 1000 crore ----- More than INR 1000 crore---------- For MSME Bidders Less than or equal to 100 crore ---------- More than INR 100 crore but ≤ INR 250 crore ---------- More than INR 250 crore---------- ----------	In the eligibility criteria you have asked a turnover of INR 100 Crore, however in the technical eligibility criteria maximum marks will be awarded on turnover of INR 1000. Also the turnover asked here is average tunrover of last 3 FY or turnover in each of the last 3 FY. Kindly confirm. We request you to kindly amend this clause as: Annual turnover of the bidder during last three years i.e. (Max Marks: 10) For NON MSME Bidders More than INR 100 crore but <= INR 200 crore----- More than INR 200 crore but ≤ INR 400 crore ----- More than INR 400 crore---------	Please be guided by the RFP terms and conditions.
9	Vulnerability Management	51	5.6.11	The proposed vulnerability management service should cover all the requirements stated in this RFP Bank is looking for a single service for both traditional vulnerability management as well as Dynamic Application Security Testing.	What are the total number of assets to be considered for vulnerability management? Pls share the breakup of assets along with the quantity.	The details aof assets along with breakdown are mentioned in the RFP.

10	Vulnerability Management	51	5.6.11	The proposed vulnerability management service should cover all the requirements stated in this RFP Bank is looking for a single service for both traditional vulnerability management as well as Dynamic Application Security Testing.	what are the total number of web applications considered for DAST testing? Pls share the breakup of internal and external applications	total 16 applications
11	Vulnerability Management	51	5.6.11	The proposed vulnerability management service should cover all the requirements stated in this RFP Bank is looking for a single service for both traditional vulnerability management as well as Dynamic Application Security Testing.	Is penetration testing also in scope? If yes what are the total number of assets/applications considered for Penetration Testing.	yes, the details of assets are mentioned in the RFP.
12	5. Scope of work	10	r	The end-users shall also be educated by the bidder regarding general cyber security awareness concepts through sessions/ computer-based trainings on quarterly basis.	The vendor wants to know if NHB currently uses a security awareness and training platform. If so, can the vendor utilize this platform to conduct the training and awareness sessions? Also mention the tolls name.	No platform is being used by NHB presently
13	5. Scope of work	10	r	The end-users shall also be educated by the bidder regarding general cyber security awareness concepts through sessions/ computer-based trainings on quarterly basis.	If there is no existing solution or platform, can the vendor recommend a SaaS-based security and awareness training program?	Bidder to recommend solution as per banks environment. No Hardware software will be procured by the Bank, the vendor will have to provide the requisite hardware and software.
14	5. Scope of work	10	r	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 provide the number of target audience for the training and awareness program	Approx 300-400
15	5. Scope of work	10	k.	The bidder should be able to isolate and clearly identify the bank's customer information, documents, records, and assets to protect the confidentiality of the information.	Do you have an existing classification Labeling tool such as: Microsoft MIP/AIP?	No
16	5. Scope of work	10	k.	The bidder should be able to isolate and clearly identify the bank's customer information, documents, records, and assets to protect the confidentiality of the information.	Do you have a requirement for a Labeling/Data Classification solution?	No
17	5. Scope of work	10	k.	The bidder should be able to isolate and clearly identify the bank's customer information, documents, records, and assets to protect the confidentiality of the information.	Do you have any existing documented policies, standards, or frameworks done for Data Classification?	Yes
18	5. Scope of work	10	k.	The bidder should be able to isolate and clearly identify the bank's customer information, documents, records, and assets to protect the confidentiality of the information.	Do you use any classification solution (Labelling software) at the moment?	No
19	5. Scope of work	10	k.	The bidder should be able to isolate and clearly identify the bank's customer information, documents, records, and assets to protect the confidentiality of the information.	Do they have a classification framework document that states what labels you wish to implement and the encryption method for each label?	Yes
20	5. Scope of work	10	k.	The bidder should be able to isolate and clearly identify the bank's customer information, documents, records, and assets to protect the confidentiality of the information.	Do you have a requirement to classify the old data (historical data) and the new data as well? Or just the new data?	Yes
21	5. Scope of work	10	k.	The bidder should be able to isolate and clearly identify the bank's customer information, documents, records, and assets to protect the confidentiality of the information.	Are you looking to use an auto-labeling client site where it automatically labels files based on conditions like credit card numbers when a user is creating or modifying a file that has not got a label?	No
22	5. Scope of work	10	k.	The bidder should be able to isolate and clearly identify the bank's customer information, documents, records, and assets to protect the confidentiality of the information.	Please highlight Use cases for Data Classification.	Use cases will be built as mutually decided by the Bank and bidder
23	5. Scope of work	46	5.6.7 TICKETING TOOL	Specification of Ticketing tool	Please let us know do we have any existing ITSM in production.	Manage engine is being used currently.
24	5. Scope of work	46	5.6.7 TICKETING TOOL	Specification of Ticketing tool	Please let us know for how many technicains and group of deparments are looking for ITSM tool.	IT team and IS team.
25	5. Scope of work	46	5.6.7 TICKETING TOOL	Specification of Ticketing tool	Please let us know for on-prem ITSM solution do we need supply hardware also along with ITSM software or just ITSM software along with implemenation service of it.	No Hardware software will be procured by the Bank, the vendore will have to provide the requisite hardware and software.
26	5. Scope of work	46	5.6.7 TICKETING TOOL	Specification of Ticketing tool	Please let us know, how many license of ITSM instance are expecting based on current department in the production unit.	Bidder has to propose taking into account NHB requirements
27	5. Scope of work	46	5.6.7 TICKETING TOOL	Specification of Ticketing tool	Please let us know, are we looking for any custom action for automation in ITSM	Please refer clause 5.6.7 of the RFP.
28	5. Scope of work	46	5.6.7 TICKETING TOOL	Specification of Ticketing tool	Please let us know, do we need to include problem management,change management and service request module along with Incident management in ITSM	Please refer clause 5.6.7 of the RFP.
29	5. SCOPE OF WORK	9	a	a. Install and commission adequate log collector at Bank sites (both DC & DR). Ensure that logs are being collected from all the in-scope devices. As appropriate suggest Bank and related stakeholders on required log-levels and support Bank in enabling the suggested log levels	Please confirm if our understanding is right ? Will NHB provide the Virtual Environment (Compute resource: cpu, ram, and hdd) for log collector in DC and DR. If Yes, bidder will propose the required sizing with NHB with the CSOC solution proposal.	No Hardware software will be procured by the Bank, the vendore will have to provide the requisite hardware and software.

30	5. SCOPE OF WORK	9	b	b. Integrate and monitor all logs through a SIEM. Create correlation rules and customize existing rules and use cases for proper security monitoring and incident reporting. Bidder should use proven threat feeds to proactively identify threats in Bank's environment	Request for Clarification : What is current Servers Nos. (windows/linux both virtual and physical) are at present in NHB's DC and DR location?	Details of assets are mentioned in RFP
31	a.Minimum Eligibility Criteria			Addition of New Clause : "Suggestion for Bidder Pre-Qualification"	Request for Modification : We request the tendering committee to add the below mention clause, this will help NHB to get participation from well known qualifies bidder in Manage SOC services. - ISO 27001:2013 (or later), - ISO 20000-1:2011 (or later) - SOC 2 Type 2 certified - CMMI Lev-V And shall have to furnish copies of the same.	Please be guided bythe terms and conditions of RFP.
32	a.Minimum Eligibility Criteria			Addition of New Clause : "Suggestion for OEM Pre-Qualification" Proposed CSOC SIEM Solution	Request for Modification : The Bidder Manage SOC SIEM solution must be in existence for more than 08 years. relevant document to prove the same must be during bid submission. Also, the Proposed SIEM solution/services must have been deployed in 3 scheduled commercial Banks for the last 5 years in India. **Justification:** *The entire SOC Services is based on the SIEM Solution. The SIEM Tool is at the CORE and its used for security and risk management to support the needs of attack detection, investigation, response, and compliance.* *By asking for this "SIEM solution must be in existence for more than 8 years" NHB is not only ensuring the MSOC services with a proven platform, but Bank will also get a trusted solution vendor those who have relevant experience for using the top-notch SIEM Tool that will be highly beneficial to them in the long run for better cyebr security threat management.*	Please be guided bythe terms and conditions of RFP.
33	5. SCOPE OF WORK	9	d	d. Integrate the tickets with Bank's ticketing tool	Request for Clarification : what is the current itsm/ticketing tool, at present deployed in NHB.	Manage engine
34	5. SCOPE OF WORK	9	i	i. 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.	Request for Clarification : Its will be helpful to know the Bank's requirement, can we propose SIEM Log collectors that can handle the log retention as mentioned below, or plz suggest - Three months - Online ? - Six Months - Offline ?	Please refer Clause 5 of the RFP.
35	5. SCOPE OF WORK	9	k.	k. The bidder should be able to isolate and clearly identify the bank's customer information, documents, records, and assets to protect the confidentiality of the information.	Request for Clarification : Dose NHB has deployed Data Loss Prevention(DLP) tool and (if yes), dose they want bidder to also provide the NHB's DLP solution management under Manage Services services ?	Yes, DLP managed services are not envisaged but DLP needs to be integrated with SIEM, for which the complete responsibility lies with Bidder.
36	5. SCOPE OF WORK	10	l, m, n	l. The bidder has to provide the bank with read/write access to the SIEM platform m. Bank will have complete oversight and ownership over the rule definition, customization and related data/ logs, meta-data and analytics related to SOC services. n. 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.	Request for Modification : Under Manage SOC Services this is not a desirable option to provide access to SIEM, as this is a shared platform service hence bidder cannot extend the full access to external parties. Although what we understand from these clauses, here NHB's explicitly is looking for "read/write access to the SIEM platform, access SOC functions and" Then we suggest NHB must ask the bidder to deploy the solution in NBH's SOC environment (cloud/on-premise) where the bidder will provide resources to manage NHB-owned SOC. Also please confirm whether, NHB's is looking for dedicated Named SOC resources for its Manage SOC requirements ? Please confirm the requirement.	Please be guided bythe terms and conditions of RFP.
37	5. SCOPE OF WORK	10	o	o. The data & information related to SOC services to be held within Indian jurisdiction only and data sovereignty to be maintained at all times	Request for Clarification : Can the bidder Propose Manage SOC services compliant with "Meity Empanelled Cloud Service Providers"	Please refer Clause 5 of the RFP.
38	5. SCOPE OF WORK	10	p	p. Bank/ RBI/ Bank's nominated third-party auditors has rights to audit/surprise audit the service providercompliance with the agreement including rights of access to the provider's premises where relevant records and organization data is being held.	Request for Clarification : As this is a Manage SOC offering, we already have proper compliance and information security standards with recognised accredited bodies (ISO, CMMI, SOC). Also under the Manage SOC, where the Events processor and collecot all the Logs and Data resides with Bank only. Also if the Bank is looking to Manage SOC with a dedicated hosting facility then the bank do periodic visits in the hosting providers audits.	Please refer Clause 5 of the RFP.

39	5. SCOPE OF WORK	10	r	r. 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.	Request for Clarification : What is the total no. of users, is the bank looking for a specific tool to access NHB's user's "cyber-awareness". With addition to normal CBT (Compute Bases Trainning) to make it more effective NHB can also ask for "Email phishing" simulation. that will be more specific and give a complete 360 view of user awareness by capturing thier acction in the event of actual email phishing attacks. Kinldy confirm the volumetrics and updated the commercial template with BoQ for this solution.	Awarness training to be provided to all Bank employee(Approx 300-400 users) , can be conducted in online/offline mode muutually decided by the bank and bidder.
40	5. SCOPE OF WORK	10	s	s. Bidder can suggest more technologies as relevant for security of Bank. The bidder responsibility is to integrate and run the SOC operations for three (3) years as per the service level agreement defined in this RFP. The bidder is supposed to bring in all kinds of hardware, software, storage required to realize Bank vision and purpose as outlined above.	Request for Clarification : Under Mange SOC services is focused on monitong of security events by the SOC resources/analysts. All integration will only be in Manage SOC scope. Not the deployment and configuration and Administraino of the any security tools.	All integration, deployment and mnagement of SOC and security solutions will be responsibility of the bidder
41	5. SCOPE OF WORK	10	w	w. Bidder shall store all the logs for minimum 1 year – of which 181 days will be stored on-line. 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.	Request for Clarification : Please confirm the bifurcation for On-line and Off-line : NHB Online will be 181 days and Offline will be 184 days is offline total 1 years ? And for Offline data Archival storage will be provided by NHB's existing backup solution ?	Please be guided bythe terms and conditions of RFP. No Hardware/software shall be procured/provided by the Bank
42	5. SCOPE OF WORK	10	y	y. Bidder has to provide OEM/SME training for all the tools/services namely but not limited to SIEM, SOAR, Vulnerability management tool, Threat intelligence feed, Threat intelligence platform etc.	Request for Clarification : Under Manage SOC Services this is not a desirable option to provide training for the proposed SIEM, SOAR and TI solutions as the entire solution and management ownership is with Bidder SOC team only. What is the best we can provide under ManageSOC is SOC dashboard-level training for the Bank team. to understand the day-to-day operation status and understanding of threat landscap of NHB's	Please refer Clause 5 of the RFP.
43						
44						
45						

Pre-Bid Queries from Prospective Bidder 7

SNO	Section	Page no	Clause no	clause refernce	Request for amendment	Response
1	7 Bids (Technical & Commercial) and Bid Evaluation Methodology	85	Minimum Eligibility Criteria	Bidder should have completed minimum 10 SOC implementation/operations service projects [from SOC establishment in India]- a) At least 2 projects of the above should be of value more than INR 50 lakh (exclusive of taxes). In case of ongoing projects, the value of completed services (up to a month prior to the release of this RFP) shall be considered.	Bidder should have completed minimum 5 SOC implementation/operations service projects [from SOC establishment in India]- a) At least 2 projects of the above should be of value more than INR 50 lakh (exclusive of taxes). 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	7 Bids (Technical & Commercial) and Bid Evaluation Methodology	85	Minimum Eligibility Criteria	The bidder Company should have at-least 50 qualified Information Security / Cyber Security professionals (CISSP/DISA/CISA/CISM/ISO 27001 Lead Auditor/Lead Implementor certified) in their payroll.	The bidder Company should have at-least 10 qualified Information Security / Cyber Security professionals (CISSP/DISA/CISA/CISM/ISO 27001 Lead Auditor/Lead Implementor certified) in their payroll.	Please be guided by the RFP terms and conditions.
3	7Bids (Technical & Commercial) and Bid Evaluation Methodology	87	technical Eligibility Criteria	Experience of the bidder 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 services of value more than INR 50 Lakhs (Max Marks: 15) More than 2 and upto 5 such projects ----- ----------5 More than 5 and upto 10 such projects --- ----------10 More than 10 such projects---------- ----------15	Experience of the bidder 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 services of value more than INR 50 Lakhs (Max Marks: 15) More than 1 and upto 2 such projects ------- ---------5 More than 2 and upto 5 such projects ------- ---------10 More than 5x such projects---------- ----------15	Please be guided by the RFP terms and conditions.
4	7Bids (Technical & Commercial) and Bid Evaluation Methodology	87	Minimum Eligibility Criteria	The number of professional staU in the area of Information Security/ Cyber Security as per the certifications mentioned in the RFP (Bidder will provide a list of staU 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: 15) More than 50 but ≤ 100 ----------5 More than 100 but ≤ 150 ---------- 10 More	The number of professional staU in the area of Information Security/ Cyber Security/IT Professional as per the certifications mentioned in the RFP (Bidder will provide a list of staU 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: 15) More than 50 but ≤ 100 ----------5 More than 100 but ≤ 150 ----------10 More than ---------- 15	Please be guided by the RFP terms and conditions.
	7Bids (Technical & Commercial) and Bid Evaluation Methodology	87	Minimum 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 5 but ≤ 7 ---------- --------5 More than 7 but ≤ 10 ---------- ----------10 More than 10---------- ----------15 *A Large Corporate is an organization with more than INR 100 crores as the annual	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 1 but ≤ 2 ---------- -----5 More than 3 but ≤ 5 ---------- ----10 More than 5---------- ----------15 *A Large Corporate is an organization with more than INR 100 crores as the annual	Please be guided by the RFP terms and conditions.

Pre-Bid Queries from Prospective Bidder 8

Sr. No	RFP Page No	RFP Section Details	Existing Clause	Clarification/Query of Bidder	Response
1	8	2. NATIONAL HOUSING BANK Point b.	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.	Please let us know the type of connectivity that exists between each of the HO, Regional office &Branch office locations. (For e.g. IPSEC VPN, MPLS, P2P Link etc.)	MPLS
2	9	5. SCOPE OF WORK Points a. s.	Install and commission adequate log collector at Bank sites (both DC &DR). The bidder is supposed to bring in all kinds of hardware, software, storage required to realize Bank vision and purpose as outlined above	We request provisioning &hardware management of infra for the log collector and other SOC components at Bank sites to be taken care by the client while the software/application will be supported by the bidder. Please advise if otherwise.	Bank will procure/provide any hardware or software. All requirements will have to borne by the bidder
3	9 17	5. SCOPE OF WORK Point d. 5.4 SCOPE OF CORE SERVICES 5 Ticketing and Reporting Solution	Integrate the tickets with Bank's ticketing tool Bidder has to integrate with bank's ticketing solution	Please let us know if bidder can make use of it's own ITSM tool in place of integrating with Bank's ticketing tool. In case if integration with Bank's ticketing tool is mandatory, please provide ticketing tool OEM &product name and suggest whether the integration needs to be unidirectional or bi-directional with respect to bidder's tool/solution.	Manage engine is the ticketing tool
4	10 18	5. SCOPE OF WORK Point l. 5.4 SCOPE OF CORE SERVICES 9. Security Content Service	The bidder has to provide the bank with read/write access to the SIEM platform. Bank staff is to be provided read/write access of the platform	We suggest providing read-only access to SIEM platform for the Bank since providing read-write access to client in addition to the service provider often results in dual ownership issues and challenges from an operations/administration perspective. Hoping this is acceptable.	Please be guided by the RFP terms and conditions.
5	10	5. SCOPE OF WORK Point n.	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.	Since the SOC services will be delivered by a shared team catering to multiple customers, meeting up with the SOC service delivery manager can be arranged in place of individual resources. Hoping this is acceptable.	Please be guided by the RFP terms and conditions.
6	10	5. SCOPE OF WORK Point w.	Bidder shall store all the logs for minimum 1 year – of which 181 days will be stored on-line.	Please let us know the exact desired offline retention period or shall we assume it to be as 184 days removing 181 days out of the 365 days (1 Year) period.	1 year logs to be stored, 181 days data to be stored on line. Bank at any point can ask for logs and bidder shall provide data
7	11	5. SCOPE OF WORK Point y.	Bidder has to provide OEM/SME training for all the tools/services namely but not limited to SIEM, SOAR, Vulnerability management tool, Threat intelligence feed, Threat intelligence platform etc	It is being assumed that the trainings will be carried out virtually/remotely via online medium. Please share across the no. of participants per training session as well as the frequency &no. of trainings to be conducted.	SOC training to be held only for IT/IS team as decided by bank whether to conduct online or offline. Bank will notify in prior to conduct training
8	11	5.1 DEPLOYMENT MODELS & SERVICE DELIVERY METHODOLOGY	Onsite service shall include deployment of three (03 no.) resource for coordinating incident management, vulnerability management and GRC responsibilities at Bank's preferable premise at Delhi during business hours (10 am- 6 pm; Monday to Saturday)	Please suggest if additional count of resources can be factored in for onsite deployment or need to limit to the given resource quantity only.	4 resources to work onsite and soc manager L3 to work remotely from bidders premise
9	11	5.1 DEPLOYMENT MODELS & SERVICE DELIVERY METHODOLOGY Phase I - Implementation	Additionally, log collectors and central log manager shall be deployed at Bank's Data Center and Data Recovery site.	It is being understood that the central log manager as well as logs processing components will be deployed within bidder's DC &DR sites with only log collectors at Bank sites. Please advise if there is any gap in this undertanding.	Log collector to be placed at DC/DR site, additionally logs from end points not connected to DC also need to be collected.
10	11	5.1 DEPLOYMENT MODELS & SERVICE DELIVERY METHODOLOGY Notes 2	Bidder SoC should also have a DR facility (both people and technology DR)	Request you to consider DR facility with only people DR for SOC services in place of both people &technology DR.	Please be guided by the RFP terms and conditions.
11	12	5.1 DEPLOYMENT MODELS & SERVICE DELIVERY METHODOLOGY Notes 4.	Any interfaces/custom connectors/parsers/data pipelines etc. required for integration be developed by the bidder for successful implementation of the SOC at no extra cost to the bank.	Custom connectors/parsers/plugins for devices/tools/solutions in future not supported out of the box by the SIEM solution will involve necessary commercials (OTC) accordingly. Hoping this is acceptable.	all present and future integrations and plugins are the responsibility of the bidder. All costs will have to be borne by the bidder. NHB will not bear any additional costs for any integration/plugin/parser creation or any other such activity required for the project.
12	13	5.2 SCHEDULE OF REQUIREMENTS	The complete responsibility of Integration with existing/new IT devices, security devices lies with the bidder which includes building parser, connection etc.	Since the bidder does not manage the devices/tools/solutions in place at the bank, it is suggested that the responsibility of integration should rest with client's respective infra teams or applicable vendors, while the bidder can provide necessary assistance in the form of SOP's etc. for SIEM integration.	all present and future integrations and plugins are the responsibility of the bidder. All costs will have to be borne by the bidder. NHB will not bear any additional costs for any integration/plugin/parser creation or any other such activity required for the project.
13	14	5.2 SCHEDULE OF REQUIREMENTS	Bank is looking for a Security Service Player which shall provide a "second layer of eyes approach" on the existing internal Security Controls &Monitoring services	Please let us know whether existing internal security controls &monitoring services are handled inhouse or outsourced to a partner/vendor.	outsourced
14	14	5.3 SCOPE IN TERMS OF THE NUMBER OF SERVICES / DEVICES	 S. No. / Item Description / Total No. of units (approx.)* 1 / No. of Windows Server / 100 2 / No. of Endpoints / 300	Please suggest whether integration of endpoints into SIEM is mandatory or can be disregarded as ingestion of logs from servers &system security solutions is already considered.	Mandatory
15	15	5.4 SCOPE OF SERVICES Point 1 SIEM Solution	Requirements - Deep Packet Inspection	Please suggest if Deep Packet Inspection is mandatory or can be considered as optional as it would involve significant infra &commercials.	Required
16	15	5.4 SCOPE OF SERVICES Point 2 Security Orchestration, Automation and Response (SOAR)	Bank staff is to be provided read/write access of the platform	Since the SOAR solution is deployed as part of a shared multitenant platform, access to the same will not be feasible. However necessary data can be derived from SOAR solution and can be shared across with the client. Hoping this is acceptable.	Please be guided by the RFP terms and conditions.
17	17	5.4 SCOPE OF SERVICES 4 Logging Capability and Storage	The logs should be stored and transmitted in encrypted format	We suggest relaxing the requirement of log storage in encrypted format.	Please be guided by the RFP terms and conditions.
18	18	5.4 SCOPE OF CORE SERVICES 5 Ticketing and Reporting Solution	Bank staff is to be provided read/write access of the platform	Since the ticketing solution is deployed as part of a shared multitenant platform, we can provide read access to the same in place of read/write accesss. Hoping this is acceptable.	Please be guided by the RFP terms and conditions.
19	18	5.4 SCOPE OF CORE SERVICES 10. Threat Hunting	The bidder should ensure proactive threat hunting on continuous basis.	In place of threat hunting on a continous basis we propose considering threat hunting frequency on a weekly/fortnightly/monthly basis.	Please be guided by the RFP terms and conditions.
20	20	5.4 SCOPE OF CORE SERVICES 11 Vulnerability Management service	Bank staff is to be provided read/write access of the platform	Being part of a shared setup, access to platform for the bank staff will not be feasible. Hoping this is acceptable.	Please be guided by the RFP terms and conditions.
21	20	5.4 SCOPE OF CORE SERVICES 11 Vulnerability Management service	The bidder has to perform Vulnerability assessment & Penetration testing, Firewall review of Bank's IT infrastructure, that includes, but not limited to devices vulnerability scans, network vulnerability scans, web vulnerability scans, application vulnerability scans and database vulnerability	While it is understood that VAPT exercises need to be carried out on a quarterly basis, please let us know the frequency of firewall review for effort estimation &commercial purposes.	Atleast quarterly
22	20 21	5.5 PROJECT TEAM STRUCTURE Point 1. SOC Analyst (L2 level) Onsite resource Point 2. Vulnerability Analyst Onsite resource	Certifications - CISM,CEH or OSCP or CISA or LPT,CCNP	Please advise if any 1 amongst the mentioned certifications would suffice or specific combinations are required. It is suggested to consider candidates with certifications other than the ones listed as well.	Combiation as mentioned
23	20	5.5 PROJECT TEAM STRUCTURE Point 1.	Job Description Implementation and management of security gateways, VPNs Manage security devices Risk analysis for change management for security devices Qualification &Skills	Would suggest to relax the on-site L2 resource requirements of possessing security gateways, VPNs product administration experience as well as having experience in managing security devices, carrying out risk analysis for security devices, vulnerability assessments and penetration testing since such skillsets are usually not present within SIEM tool/solution/technology resources.	Please be guided by the RFP terms and conditions.
24	21	5.5 PROJECT TEAM STRUCTURE Point 2. Vulnerability Analyst Onsite resource	Job Description Carry out Network security assessment Performing red teaming and phishing exercises	Please let us know the frequency of network security assessment, red teaming & phishing exercises for effort estimation &commercial purposes.	Atleast Quarterly or as decided by the bank.
25	23	5.5 PROJECT TEAM STRUCTURE Point 3. GRC Resource Onsite resource	CISA/ CISM/ CISSP/ ISO 27001 LI/ LA and Certified Privacy Professional ISO 27701 certification desirable	Please advise if any 1 amongst the mentioned certifications would suffice or specific combinations are required. It is suggested to consider candidates with certifications other than the ones listed as well.	Combination
26	28	5.5 PROJECT TEAM STRUCTURE Point b)	All 4 onsite resources shall be interviewed by the Bank and should be included in the project once Bank approves.	It is suggested to relax the requirement of interviews by the Bank as timelines for onboarding of resources could be impacted due to the same.	Please be guided by the RFP terms and conditions.

27	28	5.5 PROJECT TEAM STRUCTURE Point d)	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. The Bank reserves the right to have discussions with the selected resources on work done.	Since the SOC services of the bidder are supported by a shared platform team catering to multiple customers, sharing across names &profiles of the resources would not be feasible. Also subsequently providing an undertaking &discussions with the resources as mentioned would not be possible. Instead, bank can carry out necessary discussions with the SOC/Program Manager as he/she would be their single point of contact. Hoping this is acceptable.	Please be guided by the RFP terms and conditions.
28	28	5.5 PROJECT TEAM STRUCTURE Point e)	Up to 15 days of leaves per year shall be acceptable without any commercial impact to the SOC provider.	Request you to relax this clause or consider leave approval on a case by case basis & mutual discussion between the bidder &the Bank.	Please be guided by the RFP terms and conditions.
29	31	5.6 DETAILED TECHNICAL REQUIREMENTS 5.6.1 SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) Points 18. 19. 20. 25.	The platform must improve threat visibility and investigation depth, speed and consistency with AI based automated analysis of EDR, NDR and SIEM telemetry sources The Platform must support AI based Investigation notes/outcome to be chronologically captured and presented The Platform must support export of AI based Investigation notes/outcome in pdf or csv format. The proposed Solution must be able to identify patterns and must recommend actions based on the investigation output,	Request you to consider machine learning (ML) in place of AI for each of the stated points.	Please be guided by the RFP terms and conditions.
30	31	5.6 DETAILED TECHNICAL REQUIREMENTS 5.6.1 SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) Point 26	The platform must have the ability to create custom hunting rules or hypotheses using Universal Threat Hunting Language like Kestrel or should have the capability to support queries through natural language prompts.	Request you to relax the mentioned clause/requirement as the said feature might not be present within the solution of each of the applicable OEMs.	Please be guided by the RFP terms and conditions.
31	32 33	5.6 DETAILED TECHNICAL REQUIREMENTS 5.6.1 SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) Points 31. 37.	The solution should have connectors or similar integrators to support the devices/applications, wherever required the bidder should develop customized connectors/integrators at no extra cost. The proposed solution should have connectors to support listed devices/ applications, wherever required the bidder should develop customized connectors.	In case of any device/tool/solution integration over &above the provided inventory as part of Section 5.3 or in future, there could be a need to develop custom parsers and/or connectors and would involve additional commercials accordingly. Hoping this would be acceptable.	all present and future integrations and plugins are the responsibility of the bidder. All costs will have to be borne by the bidder. NHB will not bear any additional costs for any integration/plugin/parser creation or any other such activity required for the project.
32	34	5.6 DETAILED TECHNICAL REQUIREMENTS 5.6.1 SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) Points 61. 62	The solution should auto-failure to DR unit if the DC is down The solution should auto replicate all the rules, logs, data, etc., to DR site for continuing the operations without any loss in data	Please suggest if the solution design considering SIEM for DR in place of DR for SIEM will be acceptable. This implies that DC infra devices will forward logs to DC SIEM setup & DR infra devices to DR SIEM setup with no data sync or replication between DC &DR.	Please be guided by the RFP terms and conditions.
33	40	5.6 DETAILED TECHNICAL REQUIREMENTS 5.6.4 THREAT INTELLIGENCE & ANALYTICS Point 2	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 relax the requirement of ingestion of threat intelligence data into Bank's security devices.	Please be guided by the RFP terms and conditions.
34	43	5.6 DETAILED TECHNICAL REQUIREMENTS 5.6.4 THREAT INTELLIGENCE & ANALYTICS Point 35	The bank needs to be provided with read/write access to Threat intelligence portal/dashboard.	Provisioning read/write access to Bank will not be feasible &instead read-only access can be provided. Hoping this is acceptable.	Please be guided by the RFP terms and conditions.
35	43	5.6 DETAILED TECHNICAL REQUIREMENTS 5.6.4 THREAT INTELLIGENCE & ANALYTICS Point 39	Dynamic Malware Sandboxing should be available	Request you to relax this clause or requirement since the capability might not be present within the solution of each of the applicable OEMs.	Please be guided by the RFP terms and conditions.
36	46	5.6 DETAILED TECHNICAL REQUIREMENTS 5.6.7 TICKETING TOOL Point 1	The tool should be a software base solution which can be installed and configured on different OS like Linux, Ubuntu, Windows, etc.	Since ticketing tool/solution can involve a hardened/customized OS and deployed as a physical/software appliance, request you to relax the given requirement.	Please be guided by the RFP terms and conditions.
37	46	5.6 DETAILED TECHNICAL REQUIREMENTS 5.6.7 TICKETING TOOL Point 4	The solution should be able to integrate with Active directory for user authentication	Request you to relax this requirement since local tool/solution based authentication can be in place for the ticketing tool/solution.	Please be guided by the RFP terms and conditions.
38	50	5.6 DETAILED TECHNICAL REQUIREMENTS 5.6.10 REPORTING TOOL Points 1. 2.	The proposed solution should be a software-based solution which can be host on premise in Bank datacenter The solution should be easily installed and configurable on different OS platform like Linux, Ubuntu, Windows, etc.	Since reporting tool/solution can involve a hardened/customized OS and deployed as a physical/software appliance within bidder's data centre or on cloud, request you to relax the given requirements.	Please be guided by the RFP terms and conditions.
39	50	5.6 DETAILED TECHNICAL REQUIREMENTS 5.6.10 REPORTING TOOL Point 7	The solution should integrate with Active directory for user authentication	Request you to relax this requirement since local tool/solution based authentication can be in place for the reporting solution.	Please be guided by the RFP terms and conditions.
40	50	5.6 DETAILED TECHNICAL REQUIREMENTS 5.6.10 REPORTING TOOL Point 13	The solution should support different views relevant for different stake holders including top management, operations team, CISO Office	Request you to consider the visibility of common dashboard consisting of multiple widgets based on log source data as well as SIEM ticket/alerts data in place of this requirement.	Please refer Clause 5.6 of the RFP.
41	51	5.6 DETAILED TECHNICAL REQUIREMENTS 5.6.10 REPORTING TOOL Point 20	The proposed solution should support Key Performance Indicators (KPIs) reporting into a unified dashboard specifically tailored for the NHB SOC which offer a streamlined and holistic view of essential metrics and data points.	Request you to consider the visibility of common dashboard consisting of multiple widgets based on log source data as well as SIEM ticket/alerts data in place of this requirement.	Please refer Clause 5.6 of the RFP.
42	58	5.6 DETAILED TECHNICAL REQUIREMENTS 5.6.12 OTHER GENERAL REQUIREMENTS Point 1	During the course of the contract, in case the Bank changes the location of its Data Centre (DC) or Disaster Recovery (DR) site, the vendor/ CSOC provider shall ensure connectivity to the new site from its own DC and DR sites with the costs borne by vendor.	Request you to relax this clause/requirement.	Please be guided by the RFP terms and conditions.
43	59	5.6 DETAILED TECHNICAL REQUIREMENTS 5.6.12 OTHER GENERAL REQUIREMENTS Point 9	The proposed solution should have capabilities to store the event data in its original format in the central log storage	Request you to consider storage of event data in SIEM native format in place of the original format within central log storage.	Please be guided by the RFP terms and conditions.
44	60	5.7 HIGH LEVEL DELIVERABLES Security Event Monitoring and Response	Log Monitoring; Server Monitoring; Security and Network Device monitoring Deliverables Real-time alerts for priority tickets on email and SMS	Request you to consider real-time alerts for priority tickets on email or SMS.	Please be guided by the RFP terms and conditions.

45	60	5.7 HIGH LEVEL DELIVERABLES Security Event Monitoring and Response Log Monitoring; Server Monitoring; Security and Network Device monitoring	Deliverables High Criticality Security alert (Priority 1): Resolution: 1 hour Medium Criticality Security alert (Priority 2): Resolution: 6 hours Low Criticality Security alert (Priority 3): Resolution: 24 hours Logs of specified retention period as asked by Bank: within 24 hours New use case creation as suggested by Bank: within 3 working days New device integration as suggested by Bank: within 5 working days.	Since resolution of an incident can have dependencies on multiple aspects like bank's existing partners/vendors, OEM, internal teams etc., request you to relax the resolution timelines for the SOC bidder in context of the RFP. Also, please consider timelines for use-case creation, device integration &furnishing of logs to the bank based on mutual discussion &agreement with the bidder in place of the given values.	Please be guided by the RFP terms and conditions.
46	63	5.7 HIGH LEVEL DELIVERABLES Brand Monitoring and Protection Service	Regular monitoring and immediate (within 3 hours of alert generation) reporting of any Critical/ High Threat	Request you to relax the requirement of 3 Hours of alert generation or consider based on mutual discussion between bidder &the bank.	Please be guided by the Clause 5.7 of the RFP.
47	64	5.8 RESPONSIBILITIES BETWEEN BIDDER & BANK FOR AGREED ACTIVITIES.	Setup VPN tunnel Setup Smart connector server / VM &access to Bidder's team Configuration required to be performed in Log Source	Request you to consider primary responsibility of the Bank for the mentioned activities since the devices/hardware infra for the same would not be managed by the SOC bidder in context of the RFP.	Please be guided by the RFP terms and conditions.
48	67	5.16 SERVICE LEVELS (SLs) 5.16.1 STIPULATED TIME SCHEDULE	List of technical and staffing requirements to be shared with the Bank --> T+10 days	Request you to consider T+15 days for the same in place of given T+10 days	Please be guided by the RFP terms and conditions.
49	67 68	5.16 SERVICE LEVELS (SLs) 5.16.1 STIPULATED TIME SCHEDULE	Deploying SOC resources for integration and deployment of SOC as per the shared profiles --> T+15 days	Request you to consider T+20 days for the same in place of given T+15 days	Please be guided by the RFP terms and conditions.
50	67 68	5.16 SERVICE LEVELS (SLs) 5.16.1 STIPULATED TIME SCHEDULE	Delivery, configuration and deployment of all of Managed Security Services as defined in RFP document --> T+30 days	Request you to consider T+90 days for the same in place of given T+30 days	Please be guided by the RFP terms and conditions.
51	68	5.16 SERVICE LEVELS (SLs) 5.16.1 STIPULATED TIME SCHEDULE	List of staffing requirements to be shared with the Bank --> T+10 days	Request you to consider T+15 days for the same in place of given T+10 days	Please be guided by the RFP terms and conditions.
52	68	5.16 SERVICE LEVELS (SLs) 5.16.1 STIPULATED TIME SCHEDULE	Deploying SOC resources for 24*7 SOC operations --> T+20 days	Request you to consider T+60 days for the same in place of given T+20 days	Please be guided by the RFP terms and conditions.
53	68	5.16 SERVICE LEVELS (SLs) 5.16.1 STIPULATED TIME SCHEDULE	Commissioning of all of Managed Security Services as defined in RFP document --> T+30 days	Request you to consider T+60 days for the same in place of given T+30 days	Please be guided by the RFP terms and conditions.
54	69	5.16 SERVICE LEVELS (SLs) 5.16.2 SERVICE LEVELS& THRESHOLDS Monitoring &Incident Alerting	High Criticality Security Alerts (Priority 1) to be resolved within 1 hour Medium Criticality Security Alerts (Priority 2) to be resolved within 6 hours Low Criticality Security Alerts (Priority 3) to be resolved within 24 hours	Since resolution of an incident can have dependencies on multiple aspects like bank's existing partners/vendors, OEM, internal teams etc., request you to relax the resolution timelines for the SOC bidder in context of the RFP.	Please be guided by the RFP terms and conditions.
55	70	5.16 SERVICE LEVELS (SLs) 5.16.2 SERVICE LEVELS& THRESHOLDS 2. Incident Investigation Reports and Closure	Sending out detailed investigation report post alert notification. Action plan/ mitigation steps should be alerted to designated bank personnel as per the below SL: - High Criticality incident within 1 hour of the event identification. - High priority incident within 6 hours of the event identification. - Medium priority incident within 24 hours of the event identification	Please clarify whether the given SLA's are only for action plan/mitigation steps or even for detailed investigation report post alert notification.	Please refer clause 5.16 of the RFP.
56	71	5.16 SERVICE LEVELS (SLs) 5.16.2 SERVICE LEVELS& THRESHOLDS 4. SOC Use Case Implementation	All new use cases approved/requested by Bank shall be implemented within one working day of approval	Request you to relax the given SLA or consider based on mutual discussion between bidder &the bank.	Please be guided by the RFP terms and conditions.
57	71	5.16 SERVICE LEVELS (SLs) 5.16.2 SERVICE LEVELS& THRESHOLDS 5. Security and Privacy breach including Data Theft / Loss/ Corruption/Moving	The report shall be submitted within 5 working days to Bank.	Request you to consider 7 working days in place of the mentioned 5 days.	Please be guided by the RFP terms and conditions.
58	72	5.16 SERVICE LEVELS (SLs) 5.16.2 SERVICE LEVELS& THRESHOLDS 7. Reports and Dashboard	1. Daily Reports: By 10:00 AM everyday 2. Weekly Reports: By 10:00 AM, Monday 3. Monthly Reports: 5th working day of each month	Request you to consider the following Daily Reports by --> 1 PM, Everyday Weekly Reports --> 4 PM, Monday Monthly Reports --> 18th of each month	Please be guided by the RFP terms and conditions.
59	-	-	Generic Query	Please suggest whether any custom business/financial applications need to be integrated into SIEM and if yes please provide following details for each of the applications. i) Front-End &Backend technology in use (For e.g., Apache, IIS, MSSQL DB, MySQL DB etc.) ii) Deployment Type (For e.g. On-prem/SaaS) iii) Supported Integration Method (For e.g., Rsyslog, Connector/Plugin, API etc.) iv) Underlying Operating System (For e.g., RHEL, CentOS, Windows etc.) v)Log Format (For e.g., CEF, LEEF, JSON etc.)	yes all bank applications, need to be integrated with SIEM
60	-	-	Generic Query	For the purpose of UBA functionality within SIEM, please provide the total number of your organization users who have accounts either in AD/VPN/Proxy &so on?	All bank staff and additional endpoints not covered under DC
61	-	-	Generic Query	Request you to share across the details &breakup of the infra at the HO as well as at Regional &each of the branch offices seperately for SIEM integration in terms of Device/Tool/Solution/Application Make &Model/Solution Name, Setup type (Physical/Virtual), HA mode (Active-Standby, Active-Active), Deployment Type (On-prem/SaaS), Operating system info with version no. along with it's quantity/count.	Details of assets are availabal ein RFP.
			SLA		Please be guided by the RFP terms and conditions.
62	69	Annexure XVI - SLA	Monitoring & Incident Alerting All Critical, High Medium and low priority events should be logged as incident tickets and responded 1. Log Analysis Services 2. 24x7 monitoring of all in-scope devices. 3. Categorization of Incidents into High, Medium and Low priority shall be carried out in consultation with the selected bidder during the contract period. 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 resolveSL compliance measured/month Penalty 97.5% and above N.A. 95% to 97.49% 1% of monthly paymentd within 24 hours 92.5% to 94.99% 3% of monthly payment 90% to 92.49% 5% of monthly payment <90% 25 % of monthly payment	Overall SLA penalties should be capped @ 5 % of the applicable fees for Monthly Payment	Please be guided by the RFP terms and conditions.

63	70	Annexure XVI - SLA	Incident Response. Sending out detailed investigation report post alert notification. Action plan/ mitigation steps should be alerted to designated bank personnel as per the below SL: High Criticality incident within 1 hour of the event identification. High priority incident within 6 hours of the event identification. Medium priority incident within 24 hours of the event identification	Request to increase the response time frame for Criticality incident from 1 Hours to 2 hour and Overall SLA penalties should be capped @ 5 % of the applicable fees for Monthly Payment	Please be guided by the RFP terms and conditions.
64	72	Annexure XVI - SLA	Service uptime Compliance to be measured on monthly service uptime basis	Overall SLA penalties should be capped @ 5 % of the applicable fees for that Moth	Please be guided by the RFP terms and conditions.
		Payment Terms			
65	94	3. Payment Terms	Payment Schedule100% payment of OPEX in Arrear shall be made after completion of every Month.	Request to change the payment term to Monthly in advance	Please be guided by the RFP terms and conditions.
		Termination			
66	54	Annexure XVI - SLA - Cl. 2.8	Termination-NHB may by not less than fifteen (15) calendar days written notice of termination to the Consultant, (except in the event listed in paragraph (g) below, for which there shall be a written notice of not less than sixty (60) days) such notice to be given after the occurrence of any of the events specified in paragraphs (a) to (f) of this Clause-2.8.l, terminate this Contract:	Termination for convenience is subject to 90 days' notice and payment of applicable termination fees.	Please refer ANNEXURE - XVI (SERVICE LEVEL AGREEMENT) of the RFP.
		The liquidated damages			
67	97	23. Liquidated Damages	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. It is clarified that the liquidated damages shall be over and above the penalty, if any, imposed under the contract.	**Request to kindly revise this as below:** Request to change -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 5% of the contract value for non-performance/delayed performance as and by way of liquidated damages. It is clarified that the liquidated damages shall be over and above the penalty, if any, imposed under the contract.	Please be guided by the RFP terms and conditions.
	Annexure XVI - SLA	Service Level Agreement		Kindly note that the terms of the SLA are subject to mutual negotiations and agreement prior to execution. However, Consultant is sharing few major concerns below.	Please refer ANNEXURE - XVI (SERVICE LEVEL AGREEMENT) of the RFP.
	Annexure XVI - SLA - Cl. 3.10	General Indemnity		Kindly revise as: The Consultant shall, at its own cost and expenses, defend and indemnify NHB against all claims arising out of the infringement of third party Intellectual Property Rights, including patent, trademark, copyright, trade secret or industrial design rights, arising from use of the Products or any part thereof in India or outside India.	Please be guided by the RFP terms and conditions.
	Annexure XVI - SLA - Cl. 3.11	Limitation of Liability		Liability shall be capped at annual contract value and only exceptions are indemnity for third party IP infringement	Please refer ANNEXURE - XVI (SERVICE LEVEL AGREEMENT) of the RFP.
	Annexure XVI - SLA - Cl. 2.8	Termination for convenience		Termination for convenience is subject to 90 days' notice and payment of applicable termination fees.	Please refer ANNEXURE - XVI (SERVICE LEVEL AGREEMENT) of the RFP.

Pre-Bid Queries from Prospective Bidder 9

SR.NO	Page No. of RfP	Section No. of RFP	Clause as per RFP	Clarification sought by Bidder	
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 ANNEXURE - V (MINIMUM ELIGIBILITY CRITERIA) of the RFP.
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 ANNEXURE - V (MINIMUM ELIGIBILITY CRITERIA) of the RFP.

Pre-Bid queries from Prospective Bidder 10

Tender Page No	Sr No	Section	Clause	Query	Response
87	1	Technical Eligibility Criteria- Experience Criteria	Experience of the bidder 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 services of value more than INR 50 Lakhs (Max Marks: 15)	For wider participation, request to amend clause as below , Requesting to please relax SOC implementation of Value More than 10 Lacs. More than 10 such project worth Value Rs 10 Lacs will get full 15 marks. Here to please give Rs 10 Lacs order value instead of Rs 50 Lacs order value.	Please be guided by the Clause 7 of the RFP.
90	4	Technical Eligibility Criteria- Annual turnover of the bidder during last three years for MSME Bidder	Annual turnover of the bidder during last three years for MSME Bidder More than INR 250 crore- 10 marks	Since floated tender encouraging MSME/Start Up for maximum participation , so requesting to you please give the full 10 marks to these Start-Up/MSME companies those not having 250 Cr turn over for fair participation.	Please be guided by the Clause 7 of the RFP.