			Response to Pre-Bid Queries for RFP		
RFP Ref. No.		CPCM-09/2025-26 Date: 03-July-2025 GEM Bid No. GEM/2025/B/6412241			
RFP Name		RFP for selection of Service Provider for managing On-Site Security Operation Centre (SoC) for Stockholding			
Sr. No.	**Page No.**	**RFP Clause**	**Clause Description**	**Query**	**StockHolding Remarks**
1	11	Eligibility Criteria (For On-site Manpower Assignment)	Certified Ethical Hacker (CEH) or Certified in Cyber Security (CC) and /or Any SIEM / Firewall / ADC / EDRXDR OEM certified	Does any one of the mentioned certifications would help comply this condition?	As per RFP
2	26	Devices under Scope of Device Management	General Queries	Count of Crowdstrike modules/Services to be managed is not added under this point but is mentioned in detailed scope. Please specify which services from Crowdstrike have been availed and are under scope of this RFP.	Endpoint Protection, Data Protection, Falcon Overwatch are the High level offering from Crowdstrike. However further Details can be shared with the Selected bidder
3	42	Resource Management	General Queries	Is the count of 11 resources to be maintained on Saturday and Sunday as well	Refer RFP pg-42
4	53	Network and Security related Services - Security Monitoring	General Queries	This deliverable is more related to SOC monitoring. Please clarify the scope for this actionable	Apart from Monitoring, Solution and Device management also in scope
5	27	Security Testing: Activity	Network Penetration Testing	> Type of scan required: [Authenticated / Unauthenticated] > Do you require any customization in the Penetration Testing report? [Yes / No] If yes, specify the requirements: > Who will provide the scanning tool? [SHCIL / Eviden]" > Regulation Compliance (if any)	> Type of scan required: [Authenticated / Unauthenticated] **Both** > Do you require any customization in the Penetration Testing report? **Yes** > Who will provide the scanning tool? **Selected Bidder** > Regulation Compliance (if any) **Please refer the RFP**
6	27	Security Testing: Activity	Red Team Assessment (Internal + External)	> Phishing to be considered under red teaming or separately > Any specific scenario to be implemented, please specify	> Phishing will be considered within Red Team Assessment. Note: We would recommend you to look for a licensed tool which can be locally installed in Stockholding Environment to conduct this exercise. > Any specific scenario to be implemented, please specify Refer to RFP
7	27	Security Testing: Activity	Remote Exposure and Breach Assessment (External + Internal)	> Need more clarity on the requirement	Please refer the RFP
8	27	Security Testing: Activity	SOP Review	> Need more clarity on the requirement	The Solutions,Devices and Process under scope of Management need to be periodically reviewed
9	27	Security Testing: Activity	Configuration Audit (CA), Vulnerability Assessments (VA) & Penetration Testing (PT)	> VA Numbers are Internal OR external ? Is this activity to be considered separate activity ? > PT IPs are internal OR external ? Is this activity to be considered separate activity ? > Type of scan required: [Authenticated / Unauthenticated] >> Is false positive validation and removal required? [Yes / No] > Do you require any customization in the vulnerability assessment and PT reports? [Yes / No] If yes, specify the requirements: > Preferred vulnerability scanning tool: [Nessus / SAINT / Qualys / Other – Please specify] > Who will provide the scanning tool? [SHCIL/ Atos] > Regulation Compliance (if any)	> VA Numbers are Internal OR external ? Is this activity to be considered separate activity ? **VA numbers are both for Internal and External and has to be considered as Separate activity** > PT IPs are internal OR external ? Is this activity to be considered separate activity **PT IP's are both Internal and External and separate activity** > Type of scan required: [Authenticated / Unauthenticated] **Both** >> Is false positive validation and removal required? [Yes / No] **YES, Required** > Do you require any customization in the vulnerability assessment and PT reports? [Yes / No] **Yes, Required** If yes, specify the requirements: **Details will shared with the selected Bidder** > Preferred vulnerability scanning tool: [Nessus / SAINT / Qualys / Other – Please specify] **It should be licensed tool in adherence to CIS benchmark** > Who will provide the scanning tool? [SHCIL/ Atos] **Selected Bidder will provide the scanning Tool** > Regulation Compliance (if any) **Refer RFP**
10	27	Security Testing: Activity	AdHoc network security assessment	5 Ips Black /Grey Box - Is this Black + Grey Box testing ? > Is this only Scan requirement or full testing ?	Yes it is Black + Grey with full Testing
11	27	Security Testing: Activity	Vulnerability Assessment and External PT	> Is this all 60 Ips to be considered for with and without white listing ? = 60*2? For each activity VA and PT ?	Yes

12	27	Security Testing: Activity	Adhoc Revalidation post any planned / unplanned audits findings implementation	> kindly clarify the 10 Units definition	These are adhoc scans required in case of any Audit/Compliance exigency, i.e, minimum one IP, maximum 10 IP.
13	27	Security Testing: Activity	Report Analysis (VA PT Audits (Initial and Confirmatory)	> kindly clarify the expectation.	**Clarification:** -Identifying vulnerabilities using CVE and CWE etc. -Assessing risk in line with the Stockholding ISMS Policies and regulatory Guidelines (SEBI,RBI, etc) -Prioritizing remediation -Verifying remediation -Providing recommendations in line with Stockholding's Network and Security Infrastructure -Creating a report as per Stockholding's requirement -Follow-up for Closure with Relevant Stake holders
14	27	Security Testing: Activity	BAS (Breach and Attack Simulation)	>Kindly clarify the expectations. >scenarios expected	Please check SEBICSRF guidelines
15	27	Security Testing: Activity	CART(Continuous Automated Red Teaming)	>Kindly clarify the expectations. >scenarios expected	Please check SEBICSRF guidelines
16		Consulting Services	SNA Report	1. Please give an overview of the different network and security components, and other IT assets (such as OS, servers, DBs, Gateways, Domain Controllers, , in your network that is required to be reviewed as part of SNA? 2. Would you also require us to review any specific application or product? 3. Please provide a list of locations in scope, including cloud environment (if any) 4. Are you looking to do this assessment against a specific compliance requirement / standard/ framework / regulation? 5. Are you okay with remote reporting? The assessment and the results shall be presented onsite.	1. Please find the scope of assets and products and Location under RFP pg-26 2. Please find the scope of assets and products and Location under RFP pg-26 3. Please find the scope of assets and products and Location under RFP pg-26 4. Please refer RFP 5. No
17		Consulting Services	Risk Assessment Report	1. Will the risk assessment activity be limited only to the network devices? 2. We assume that your existing Risk Assesment methodology and template can be utilized, and there are no changes - please confirm. 3. Please confirm that the Risk Assessment must look after compliance of what standard, framework, regulation apart from ISMS, if applicable. 4. We assume that you will have one centralized repository of all network devices, and one core team participating in the risk assessment - please confirm. 5. Are you also looking for advisory support (tracking) to mitigate the risk? 6. Are you okay with remote reporting? The assessment and the results shall be presented onsite.	1. Please refer RFP 2. The methodology will be inline with Stockholding and Regulatory requirements. Any changes has to be adopted by the selected Bidder 3. Please refer RFP 4. Centralized repositary available, Core Team available for risk assessment 5. Please refer RFP 6. No
18	28	Consulting Services	15 Policies & Procedures to be reviewed & 5 new Policies Development	1. Please confirm the standard, framework, regulation against which these documents must be reviewed, updated and created. RFP has references of ISMS and "industry best practices". 2. We assume that each document-related findings reported from different audits / assessment shall be provided prior to working on the documents. 3. Can we work on the documentation remotely, and discuss the updated / new documents onsite?	1. These Policies and Documents should be inline with Stcokholding's ISMS Policies and Regulatory Guidelines. 2. Stockholding will share the relevant information for the purpose of Document creation. In case, if there is no Document available the same has to created and provided to Stockholding as per requirement 3. The Documentation and Discussion has to be done Onsite
19	28	Consulting Services	Advisory support	1. Would you be able to give us a bifurcation of onsite and remote support expectation? 2. Can we share a daily or block rate with you, as having a defined effort for "Advisory Support" may not be feasible.	1. The advisory support as and when needed has to be conducted onsite 2. No separate rate card and should be included as per Commercial Bid Format

20		Consulting Services	Remote Exposure and Breach Assessment	1. Number of teams participating in the assessment? (Please include the count of teams / sub-divisions) 2. Please give an overview of the kind of assets and technologies involved in remote setup. 3. You'd like us to review your existing BCP / DR plan from remote access perspective only, right? OR is your expectation to do a complete BCP / DR review, including BIA? 4. Please elaborate your expectation of a DLP process review?	1. There would be 3 Teams (2 to 3 members per team) participating in the assessment 2. Please refer RFP. Further details will be shared with the selected Bidder 3. Yes, Further detaisl will be shared with selected Bidder 4. Key Focus Areas (Policy Review, Technical Controls, Compliance Requirements, Identify Deficiencies, Prioritize Improvements, Data Discovery and Classification, Regular Testing, Policy Updates, Technology Upgrades, Stakeholder Communication, Policy Enforcement, Incident Response, User Awareness and Training, Integration with Security Architecture)
21	NA	General Queries	General Queries	Existing Solutions: What are the currently deployed SIEM, SOAR, PAM, and PIM solutions ?	Details will be shared with selected Bidder
22	NA	General Queries	General Queries	Integrations: Are there any existing integrations with other tools or platforms that the bidder should be aware of?	Yes, there are Integrations with SIEM, MDR, PAM etc.
23	NA	General Queries	General Queries	Backup Solution: What is the currently deployed backup solution in the environment?	Details will be shared with selected Bidder
24	NA	General Queries	General Queries	Log Management Responsibility: Will the selected service provider be responsible for the log management process, or is this handled internally?	The Seleted bidder will be responsible for end to end Log Management
25	9	Eligibility Criteria	The bidder should be a company registered under Indian Companies Act, 1956 or a Partnership Firm registered under Indian Partnership Act, 1932 with experience of managing SOC services for the period of 7 years.	We request to also allow participation of LLPs and revise the clause as follows: Revised Clause: The bidder should be a registered company in India under the Companies Act 1956 / 2013 or an LLP registered under the LLP Act 2008 / Partnership Act 1932, with experience of managing SOC services for the period of 7 years.	No Change
26	9	Eligibility Criteria	The bidder should have an average annual turnover of at least Rs. 14 Crores per annum for last 03 (three) financial years (2021-22, 2022-23 and 2023-24). It should be of individual company and not of Group of Companies	Request you to change the criteria for minimum Rs. 200 Crores per annum turnover	No Change
27	9	Eligibility Criteria	The Bidder should have Positive Net worth minimum Rs. 3.5 crores for each of the last 03 (three) audited financial years	Request you to change the criteria for minimum Rs. 400 Crores positive net worth.	No Change
28	9	Eligibility Criteria	The bidder should have executed or managed from customer premise with at least 1 project from BFSI segment, during any of the last 05 (five) years with any one of the following: • 01 (one) SOC contract with network-security device management from customer premises having value not less than Rs. 5.6 Crores for any Corporate entity in India	Request you to modify the criteria for minimum (5) SOC contracts to shortlist the technically advanced bidders who has managed multiple similar engagements.	No Change
29	9	Eligibility Criteria	The bidder Company should have at-least 15 valid qualified Information Security / Cyber Security professionals (CISA or CISM or CISSP or CEH or ISO/IEC 27001:2022 certified lead auditors) in their payroll.	Request you to change the criteria for minimum 50+ resources.	No Change
30	17	Commercial Bid Evaluation	Cumulative score of 60 marks in the Technical evaluation	Request you to increase the scoring for technical evaluation to 70 marks	No Change
31	17	Commercial Bid Evaluation	L1 bidder will be selected based on the lowest quote submitted	We understand this is QCBS bid, can you please explain your selection method.	It is Least Cost Selection (LCS) bid and not QCBS bid
32	19	Understanding of Scope	End point Security (On-premise and/or Cloud based	What is the number of endpoints ?	3000 End points

33	20	Understanding of Scope	Web Application Firewall (On-premise and/or Cloud based WAF)	Please provide a list of WAF with make and model number under RFP scope.	Please refer to page no. 26 for the list of Hardware and Software Components deployed at Stockholding
34	22	Understanding of Scope	Active Directory Management (Standalone as well as on Private cloud deployment)	What is you AD deployment architecture ? How authentication is handled on-prem and on-cloud ?	Please refer to page no. 26 for the list of Hardware and Software Components deployed at Stockholding
35	42	Resource Management	Minimum 11 resources [as per below table] for DC and DR Site should be available on site fulfilling all the shifts	Can bidder propose a hybrid model which will have a on-site resource for Governance / PMO and rest to be provided remotely. This will be a cost effective approach.	Refer RFP pg-42. This is completely onsite based engagement and remote/hybrid is not allowed.
36	3	EMD	General Queries	We wish to highlight that we have annual turnover of more than ₹ 500 Crore, in all of the past three completed. financial years. We are exempt from submitting the bid security as per the General Terms & Condition on GeM 4.0 (Version 1.23) dated 5th March 2025 (Clause 4.xiii.(m).v).shows we are exempt from submitting the EMD for this RFP. Request you to please confirm the same that we can submit our bid without submitting the EMD	Exemption of EMD as per GeM circular is accepted.
37	61	Service Level Agreement (SLA) and Penalty	Total Monthly Penalty = Sum of All Penalties (excluding penalty on resource management), Capped at 10% of Monthly contract value	Modify as: Total Monthly Penalty = Sum of All Penalties (excluding penalty on resource management), Capped at 5% of Monthly contract value	No Change
38	72	Performance Bank Guarantee (PBG)	Successful Bidder shall, at own expense, deposit with the StockHolding, within Fifteen (15) days on issuance of PO	Modify as: Successful Bidder shall, at own expense, deposit with the StockHolding, within Fifteen (30) days on issuance of PO	No Change
39	74	Termination Clause	StockHolding reserves right to terminate the contract by giving 90 days prior written notice in advance against any of the following conditions – a) If penalty amount (excluding penalty on resource management) is equal to or more than 10% of monthly contract value for consecutively 3 times in a particular year; b) If penalty amount on Resource Management is equal to or more than 10% of monthly contract value for consecutively 3 times in a particular year; c) If at any point of time, the services of bidders are found to be non-satisfactory;	Propose to add below new-sub clause in the existing clause:- Termination by the Bidder for Breach: In the event StockHolding materially breaches this definitive Agreement or any statement of work, which breach is not cured within thirty (30) days after written notice specifying the breach is given to the StockHolding, the bidder may terminate this defenitive Agreement or any portion thereof or the applicable statement of work by giving written notice to the StockHolding.	No Change
40	76	Right to Audit and Due-Diligence	Right to Audit and Due-Diligence The records of the Service Provider/Bidder with respect to any matters / issues covered under the scope of this RFP shall be made available to StockHolding / its auditors at any time during normal business hours, as often as StockHolding requires, to audit, examine, and make excerpts or transcripts. The cost of such audit will be borne by the StockHolding. Access to books and records/Audit and Inspection would include access to all books, records and information relevant to the outsourced activity available with the Service Provider/bidder. For technology outsourcing, requisite audit trails and logs for administrative activities should be retained and accessible to the StockHolding based on approved request. The Service Provider/bidder shall be subject to risk management and security and privacy policies that meet the industry standards	Propose changes in the existing clause as below:- Right to Audit and Due-Diligence:- The records of the Service Provider/Bidder with respect to any matters/issues covered under the scope of this RFP shall be made available to StockHolding / its auditors at any time during normal business hours, as often as StockHolding requires, to audit, examine, and make excerpts or transcripts, provided that StockHolding shall give the Service Provider/Bidder at least seven (7) days' prior written notice of such audit. The cost of such audit will be borne by the StockHolding. Access to books and records / Audit and Inspection would include access to all books, records and information relevant to the outsourced activity available with the Service Provider/Bidder. For technology outsourcing, requisite audit trails and logs for administrative activities should be retained and accessible to the StockHolding based on approved request.	No Change

41	97	ANNEXURE – 9 – Format of Non-Disclosure Agreement	Confidentiality Obligations: The Receiving Party shall, at all times maintain confidentiality and prevent disclosure of Confidential Information of Disclosing party with at least the same degree of care as it uses to protect its own confidential information but in no event with less than reasonable care. The Receiving Party shall keep the Confidential Information and Confidential Materials and any copies thereof secure and in such a way so as to prevent unauthorized access by any third party. The Receiving Party agrees not to disclose, transmit, reproduce or make available any such Confidential Information to any third parties and shall restrict disclosure of Confidential Information only to a limited group of Recipient's directors, concerned officers, employees, attorneys or professional advisors who need to have access to the Confidential Information for the purposes of maintaining and supporting the services and each of whom shall be informed by Receiving Party of the confidential nature of Confidential Information and agree to observe the same terms and conditions set forth herein as if specifically named a Party hereto. The Receiving Party shall not, unless otherwise agreed herein, use any such Confidential Information and Confidential Materials for its own benefit or the benefit of others or do anything prejudicial to the interests of the Disclosing Party or its customers or their projects	Propose the changes in the existing clause as below:- Confidentiality Obligation:- The Receiving Party shall, at all times, maintain confidentiality and prevent disclosure of Confidential Information of the Disclosing Party with at least the same degree of care as it uses to protect its own confidential information, but in no event with less than reasonable care. The Receiving Party shall keep the Confidential Information and Confidential Materials and any copies thereof secure and in such a way so as to prevent unauthorized access by any third party. The Receiving Party agrees not to disclose, transmit, reproduce, or make available any such Confidential Information to any third parties and shall restrict disclosure of Confidential Information only to a limited group of the Recipient's directors, concerned officers, employees, attorneys, or professional advisors who need to have access to the Confidential Information for the purposes of maintaining and supporting the services, and each of whom shall be informed by the Receiving Party of the confidential nature of the Confidential Information and agree to observe the same terms and conditions set forth herein as if specifically named a Party hereto. The confidentiality obligations of the Receiving Party shall remain in effect during the term of the Agreement and for a period of three (3) years following its expiration or termination. The Receiving Party shall not, unless otherwise agreed herein, use any such Confidential Information and Confidential Materials for its own benefit or the benefit of others, or do anything prejudicial to the interests of the Disclosing Party or its customers or their projects. The Receiving Party shall not use the Confidential Information in any way to create a derivative work out of it or reverse engineer or use for any commercial purpose or for any purpose detrimental to the Disclosing Party. The Receiving Party shall not make copies of Confidential Information unless the same are reasonably necessary. The Receiving Party shall immediately notify the Disclosing Party in the event of any unauthorized use or	No Change
42	73	Right to alter RFP	Right to alter RFP a. StockHolding reserves the right to alter the RFP terms and conditions at any time before submission of the bids. b. StockHolding reserves the right to modify, amend, alter and/or cancel the entire RFP at any stage without assigning any reason whatsoever. We further understand and accept that StockHolding's decision in this regard will be final and binding on all bidders.	Propose to add changes in th existing clause as below:- Right to alter RFP a. StockHolding reserves the right to alter the RFP terms and conditions at any time before submission of the bids. b. StockHolding reserves the right to modify, amend, alter and/or cancel the entire RFP at any stage without assigning any reason whatsoever. We further understand and accept that StockHolding's decision in this regard will be final and binding on all bidders. c.Provided that in the event of any such alteration, amendment, or cancellation, the Bidder shall be given reasonable notice in writing, and if required, adequate time to revise or withdraw its bid without any liability or penalty. The Bidder shall not be held responsible for any costs incurred due to such changes made solely at the discretion of StockHolding.	No Change
43	NA	Suggestion to add new clause	Suggestion to add new clause	During the Term of this definitive Agreement and for a period of one year thereafter, neither Party shall (either directly or indirectly through a third party) solicit to employ, cause to be solicited for the purpose of employment to any employee/s (including the employees who have been exposed or introduced to other Party during initial discussion between Parties or engaged to provide/perform the services under any definitive agreement entered between Parties) of the other Party or aid any third person to do so, without the specific written consent of the other Party. The said restriction shall also apply to each Party's affiliates, agents, vendors, contractors, and any third parties with whom such Party has a relationship (collectively, "Representatives"). Parties agree that Representatives are equally restricted from poaching or soliciting or inducing any employees of other Party to leave their employment or engagement with such other Party.	No Change
44	26	Device Management	SIEM LEC / Logger Server	Please confirm the OEM and version of the SIEM platform currently in use	Details can be shared with the Selected bidder
45	26	Device Management	SIEM LEC / Logger Server	Please confirm the OEM and version of the MDR platform currently in use.	Details can be shared with the Selected bidder
46	26	Device Management	SIEM LEC / Logger Server	Can you provide the split of on-prem vs cloud-based security tools	Details can be shared with the Selected bidder
47	NA	General Queries	General Queries	Please share the ticket volumetric details last 6 month for reference	Details can be shared with the Selected bidder

48	55	Transition Management	StockHolding recognizes that the transition process and its effectiveness has a significant impact on the success of ongoing services. Transition involves one-time activities required to transfer responsibility for the services, including processes, SOP (Standard Operating Procedure), assets, facilities, technology and other knowledge to the MSSP. StockHolding has considered a transition period of 3 months from existing MSSP to new MSSP for smooth transfer of the SOC services handover process.	As per the RFP, the transition period is 90 days. We request clarification if the deployment of engineers can extend up to 100 days considering onboarding, background checks, and relocation timelines.	No Change
49	9	Eligibility Criteria	General Queries	Requesting to please allow bidding as Consortium so then the RFP qualification criteria may be met jointly as Consortium partners; this will enhance the competitiveness of the bid	Consortium is not allowed for this tender.
50	18	Understanding of Scope	General Queries	Requesting for explicit clarity on which tools, HW and SW must be procured, supplied and deployed by the bidder [VERSUS] which tools, HW and SW shall be re-used from SHCIL repository.	Please refer to page no. 26 for the list of Hardware and Software Components deployed at Stockholding
51	NA	General Queries	General Queries	The RFP deals only with services, activities and manpower. No HW or SW or licensing or Capex. Kindly confirm.	The RFP deals only with services, activities and manpower. However if the selected bidder is bringing any solution then the Software, License, Implementation & Support cost will be part of this RFP
52	16	Technical Evaluation Criteria	3) Projects of SOC implementation and/or managing SOC (onsite/from customer premises) to BFSI Sector in India during last 05 (five) years in India	Request to modify as: Atleast 05 Projects of SOC implementation and/or managing SOC (onsite/from customer premises) in India during last 07 (five) years in India	No Change
53	16	Technical Evaluation Criteria	5) Bidder having CERT-In Empanelled as on RFP Date	Requesting to either remove this clause or allow bidding through Consortium partners	No Change
54	14	Bid preparation and Submission Details	General Queries	As the scope is vast and extensive, the bid preparation must thoroughly take into account the upcoming SHCII technical answers to the pre-bid queries together with the associated corrigendum; therefore, kindly requesting to consider bid submission timeline somewhere near first or second week of Aug-2025.	No Change
55	NA	General Queries	General Queries	The MSSP will be using CrowdStrike Managed Detection & Response service and will NOT bring in it's own EDR / SIEM. Is the understanding correct?	SIEM - MDR Services is not part of the scope for this RFP. However, the bidder is expected to closely work and cordinate with existing StockHolding's MDR service provider.
56	NA	General Queries	General Queries	What services will be in scope of the MSSP with respect to EDR/MDR/SIEM?	As per RFP
57	NA	General Queries	General Queries	In addition to CrowdStrike MDR, what SIEM solution (cloud/on-prem) is currently deployed?	Details can be shared with the Selected bidder
58	NA	General Queries	General Queries	We understand that some level of update in existing playbooks is part of the scope, however, is there any preference or restriction on adding new SIEM/SOAR integrations?	As per RFP
59	NA	General Queries	General Queries	Will MSSP have admin rights to tune detection rules/use cases/threat feeds? or the MSSP will mainly suggest and some third party (or stockholding) will execute the changes via change requests	End to End Monitoring & Management will be done by the Selected Bidder
60	NA	General Queries	General Queries	Are there existing automation playbooks to migrate or rebuild?	As per RFP
61	NA	General Queries	General Queries	what are current baseline metrics e.g. alert volume, false positive rate etc.. of existing CrowdStrike MDR?	Details can be shared with the Selected bidder
62	NA	General Queries	General Queries	Is there any infrastructure expected to be added as part of MSSP service ? Like log storage infra ? We understand no infra will be owned by MSSP/bidder, please confirm.	Yes, understanding is correct
63	NA	General Queries	General Queries	The MSSP/bidder should not provide/manage device licenses or manage only client-owned? Is this understanding correct?	The RFP deals only with services, activities and manpower. However if the selected bidder is bringing any solution then the Software, License, Implementation & Support cost will be part of this RFP Bidder to manage all licenses which are StockHolding owned.
64	NA	General Queries	General Queries	From the inventory provided for firewall/IPS/WAF that are deployed, are there any upgrades or additional provisioning planned ?	As per RFP

65	NA	General Queries	General Queries	Is MSSP responsible for firmware upgrades and EOL planning? Or the scope is mainly for co-ordinating with responsible parties?	End to End Monitoring & Management will be done by the Selected Bidder
66	NA	General Queries	General Queries	Who coordinates whitelisting, test creds, rollbacks for tests? Are there test environments, test appliances available?	End to End Monitoring & Management will be done by the Selected Bidder in consultation with Stockholding
67	NA	General Queries	General Queries	For Security Testing scope, who is supposed to bring the tools ? Will the tools be MSSPs responsibility or will those be provided by Stock holding ?	The RFP deals only with services, activities and manpower. However if the selected bidder is bringing any solution then the Software, License, Implementation & Support cost will be part of this RFP
68	NA	General Queries	General Queries	How will policy reviews and new policy development be prioritized? Other that suggesting the new policies is the MSSP expected to carry out policy implementation?	As per RFP
69	NA	General Queries	General Queries	Will MSSP directly handle regulatory audit queries (CERT-In, SEBI, etc.)?	No
70	NA	General Queries	General Queries	Is MSSP expected to participate in DR/BCP tests beyond cyber drills?	Yes
71	NA	General Queries	General Queries	Can resources hold multiple roles or is strict separation mandatory?	As per RFP
72	NA	General Queries	General Queries	Is there flexibility in SLA penalties for false positives/vendor delays?	As per RFP
73	NA	General Queries	General Queries	How will penalties apply for incidents from client misconfig or 3rd party?	As per RFP
74	NA	General Queries	General Queries	Any legacy vendor or tool limitation that could affect transition?	Details can be shared with the Selected bidder
75	NA	General Queries	General Queries	What tools are expected to be deployed in point 10 as monitoring as service? Is this to monitor transition? We understand in the pre-bid call that no additional tool deployment is in scope of MSSP/bidder	There is no such word Monitoring as service mentioned in RFP. The RFP deals only with services, activities and manpower. However if the selected bidder is bringing any solution then the Software, License, Implementation & Support cost will be part of this RFP
76	NA	General Queries	General Queries	Do we need to integrate our ticketing tool with your SOC or we need to work on your ticketing tool for alert investigations, tracking, status updates etc	As per RFP
77	NA	General Queries	General Queries	What is an average Alert count from all security solutions in scope. Kindly provide solution wise average alert count.	Details can be shared with the Selected bidder
78	9	Eligibility Criteria	The bidder should have executed or managed from customer premise with atleast 1 project from BFSI segment, during any of the last 05 (five) years	Is it mandatory to have experience specifically with Indian clients, or will experience with global clients also be considered?	Only for Indian Clients
79	NA	General Queries	General Queries	Please share the high-level architecture diagram of their current SOC setup for better understanding and planning?	Please refer pg-26, Further details can be shared with the Selected bidder
80	9	Eligibility Criteria	The bidder should be a company registered under Indian Companies Act, 1956 or a Partnership Firm registered under Indian Partnership Act, 1932 with experience of managing SOC services for the period of 7 years	We request you to modify the clause as follow:- The bidder should be a company registered under Indian Companies Act, 1956 or a Partnership Firm registered under Indian Partnership Act, 1932 with experience of managing SOC services for the period of 5 years	No Change

81		Eligibility Criteria	The bidder should have executed or managed from customer premise with atleast 1 project from BFSI segment, during any of the last 05 (five) years with any one of the following: • 01 (one) SOC contract with network- security device management from customer premises having value not less than Rs. 5.6 Crores for any Corporate entity in India OR • 02 (two) SOC contract with network-security device management from customer premises having value not less than Rs. 3.5 Crores each for any Corporate entity in India OR • 03 (three) SOC contract with network-security device management from customer premises having value not less than Rs. 2.8 Crores each for any Corporate entity in India	We request you to modify clause as follow:- The bidder should have executed or managed from customer premise with atleast 1 project from Government /PUS /BFSI segment, during any of the last 05 (five) years with any one of the following: • 01 (one) SOC contract with network- security device management from customer premises having value not less than Rs. 5.6 Crores for any Corporate entity in India OR • 02 (two) SOC contract with network-security device management from customer premises having value not less than Rs. 3.5 Crores each for any Corporate entity in India OR • 03 (three) SOC contract with network-security device management from customer premises having value not less than Rs. 2.8 Crores each for any Corporate entity in India	No Change
82		Eligibility Criteria	The bidder Company should have at-least 15 valid qualified Information Security / Cyber Security professionals (CISA or CISM or CISSP or CEH or ISO/IEC 27001:2022 certified lead auditors) in their payroll.	We request you to modify the clause as below:- The bidder Company should have at-least 10 valid qualified Information Security / Cyber Security professionals (CISA or CISM or CISSP or CEH or ISO/IEC 27001:2022 certified lead auditors) in their payroll.	No Change
83	82	ANNEXURE – 3 – Technical Criteria	Projects of SOC implementation and/or managing SOC (onsite/from customer premises) to BFSI Sector in India during last 05 (five) years in India	We request you to modify the clause as below:- Projects of SOC implementation and/or managing SOC (onsite/from customer premises) to Government /PSU /BFSI Sector in India during last 05 (five) years in India	No Change
84	82	ANNEXURE – 3 – Technical Criteria	The number of professional staff in the area of Information Security (CISA/CISM/CISSP/CEH/ISO 27001 certified) certified person on bidder Payroll. 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. Atleast 15 nos. Certified person – 10 Marks • 16-40 Certified persons – 12 Marks • More than 41 Certified persons – 15 Marks	We request you to modify the clause as follow: The number of professional staff in the area of Information Security (CISA/CISM/CISSP/CEH/ISO 27001 certified) certified person on bidder Payroll. 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. Atleast 10 nos. Certified person – 10 Marks • 11-40 Certified persons – 12 Marks • More than 41 Certified persons – 15 Marks	No Change
85	84	ANNEXURE – 3 – Technical Criteria	Bidder having CERT-In Empanelled as on RFP Date	We request you to remove this cluase	No Change
86	9	Eligibility Criteria	General Queries	Requesting to please allow bidding as Consortium so then the RFP qualification criteria may be met jointly as Consortium partners; this will enhance the competitiveness of the bid	Consortium is not allowed for this tender.
87	18	Understanding of Scope	General Queries	Requesting for explicit clarity on which tools, HW and SW must be procured, supplied and deployed by the bidder [VERSUS] which tools, HW and SW shall be re-used from SHCIL repository.	Please refer to page no. 26 for the list of Hardware and Software Components deployed at Stockholding. The RFP deals only with services, activities and manpower. However if the selected bidder is bringing any solution then the Software, License, Implementation & Support cost will be part of this RFP

88	NA	General Queries	General Queries	The RFP deals only with services, activities and manpower. No HW or SW or licensing or Capex. Kindly confirm	The RFP deals only with services, activities and manpower. However if the selected bidder is bringing any solution then the Software, License, Implementation & Support cost will be part of this RFP
89	14	Bid preparation and Submission Details	General Queries	As the scope is vast and extensive, the bid preparation must thoroughly take into account the upcoming SHCII technical answers to the pre-bid queries together with the associated corrigendum; therefore, kindly requesting to consider bid submission timeline somewhere near first or second week of Aug-2025.	Kindly check Corrigendum
90	NA	General Queries	General Queries	Is the current SIEM hosted on-premise, on cloud, or in a hybrid environment?	Details can be shared with the Selected bidder
91	NA	General Queries	General Queries	What is the licensed EPS (Events Per Second) capacity of the current SIEM infrastructure?	Details can be shared with the Selected bidder
92	NA	General Queries	General Queries	Are any integrations already in place with SOAR, DAM, or MDR platforms, or is integration part of the MSSP scope?	The SOC Infra related Solution and Device Integration is part of Selected Bidder's scope
93	NA	General Queries	General Queries	Are we expected to build new use cases, playbooks, and correlation rules, or manage existing ones only?	Not expected. MSSP to ensure that all the activities mentioned are monitored and cordinate with SIEM Vendor as per SIEM Contract SLA's
94	NA	General Queries	General Queries	Will the MSSP be responsible for log source onboarding and parsing optimization for new platforms (e.g., EDR, WAF, DLP)?	Not expected. MSSP to ensure that all the activities mentioned are monitored and cordinate with SIEM Vendor as per SIEM Contract SLA's
95	NA	General Queries	General Queries	Would StockHolding be open to optimization or modernization of the existing SIEM architecture based on our expert recommendations?	Not expected. MSSP to ensure that all the activities mentioned are monitored and cordinate with SIEM Vendor as per SIEM Contract SLA's
96	NA	General Queries	General Queries	Is it expected that the MSSP would be responsible for the platform health, backup, patching, and performance management of the SIEM as well?	Not expected. MSSP to ensure that all the activities mentioned are monitored and cordinate with SIEM Vendor as per SIEM Contract SLA's
97	NA	General Queries	General Queries	Could you share the list of current log sources integrated with the SIEM solution?	Details can be shared with the Selected bidder
98	NA	General Queries	General Queries	Are there any regulatory or internal audit expectations tied to SIEM reporting (e.g., SEBI CSCRF, RBI Cyber Security Framework)?	As per RFP
99	NA	General Queries	General Queries	In Eligibility Criteria - Point No 4 - can this criteria be changed instead of 2.8 cr each to 1 cr each PO value upto 2 PO's? Kindly confirm.	No Change
100	59	Service Level Agreement (SLA) and Penalty	MSSP needs to execute a Service Level Agreement with StockHolding covering all terms and conditions of this tender		Separate agreement will be executed with selected bidder
101	42	Resource Management	Minimum 11 resources [as per below table] for DC and DR Site should be available on site fulfilling all the shifts		Kindly check Corrigendum