Response to Pre-Bid Queries for RFP					Date:02/Dec/2025
RFP Ref. No.	**CPCM-20/2025-26 (GEM Reference No. - GEM/2025/B/6906136)**				
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	27	Scope of Work - Security Testing	ACTIVITY - Network Penetration Testing SCOPE - Internal - Up to 200 IP Addresses FREQUENCY - Twice a Year (2 Initial Test + 2 Confirmatory Test)	> 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 /bidder]" > Regulation Compliance (if any)	**Clarification** 1. Authenticated Scanning for internal scanning, Non-Authenticated for External Scanning. 2. Yes, based on the need of the respective regulations and criticality. 3. Bidder has to bring their own tool. 4. Yes SEBI CSCRF Framework, PFRDA, IRDA, etc.
2	27	Scope of Work - Security Testing	ACTIVITY - Firewall rule base review SCOPE - Checkpoint – 2; Cisco FPD – 8 and FMC – 2 FREQUENCY - Twice a Year (2 Initial Test + 2 Confirmatory Test)	Approx how many rules per firewall.	**Clarification** Details to be shared with winning bidder. The bidder has to bring their own firewall analyzer tool.
3	27	Scope of Work - Security Testing	ACTIVITY - Red Team Assessment (Internal + External SCOPE - Internet facing and Internal Assets FREQUENCY - Once a Year (Initial +Confirmatory)	> Phishing to be considered under red teaming or separately > Any specific scenario to be implemented , please specify	**Clarification** Phishing is part of Red-Teaming. Please refer Pages 35-37 on the scope of the activity

4	27	Scope of Work - Security Testing	ACTIVITY - Remote Exposure and Breach Assessment (External + Internal) SCOPE - IT Assets FREQUENCY - Once a Year (Initial +Confirmatory)	> Need more clarity on the requirement. What is the deliverable in the report? Is there is a scenario to be tested in red teaming? Is this separate than Red teaming?	**Clarification** 1. External Exposure Assessment and Internal Breach Assessment 2. Deliverables: Attack Surface and Path Mapping, Vulnerability Assessment, Credential & Dark Web Exposure, Risk Rating + Exploitation Evidence, Impact Demonstration, Compromise Spread Risk, Mitigation Recommendations 3. It is separate than Red Teaming. Refer Pages 41-42 on the scope and deliverables.
5	27	Scope of Work - Security Testing	ACTIVITY - SOP Review SCOPE - In-Scope Devices FREQUENCY - Device Specific on Monthly basis. (Initial + Confirmatory)	> Need more clarity on the requirement. Which SOP for which processes?	**Clarification** Security Devices related SOP's are to be reviewed. Please refer Pages- 28 & 29
6	27	Scope of Work - Security Testing	ACTIVITY - Configuration Audit (CA), Vulnerability Assessments (VA) & Penetration Testing (PT) - (As per CIS Benchmark and close the gap's and provide the clean report) SCOPE - 200 IP addresses FREQUENCY - Twice a Year (2 Initial Test + 2 Confirmatory Test)	> 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	**Clarification** 1. VA Numbers: Yes, Both Internal and External Please refer to Page - 27 & 28 2. PT IP's: Both Internal and External 3. Type of Scan: Authenticated for Internal, unauthenticated for external 4. False Positive Validation and Removal: Required 5. Customization in Reports: Yes, As per Regulatory requirements 6. Scanning Tool: Bidder to

				tool: [Nessus / SAINT / Qualys / Other – Please specify] > Who will provide the scanning tool? [SHCIL/ bidder] > Regulation Compliance (if any)	bring their own Tool. 7. Regulation: SEBI CSCRF, Internal StockHolding Policies
7	27	Scope of Work - Security Testing	ACTIVITY - IPS Review SCOPE - On Firewall blades FREQUENCY - Once a Year (Initial +Confirmatory)	What is the coverage required in IPS review? IPS will be managed by the device management team. Over that what is the Review required?	**Clarification:** 1. IPS policy review, Signature coverage & effectiveness, Performance impact analysis, Logging & SIEM integration review, Optional exploit testing, Firewall rulebase integration, Compliance mapping, HA behaviour analysis, Full remediation report. 2. To be managed by Device Management Team
8	27	Scope of Work - Security Testing	ACTIVITY - AdHoc network security assessment SCOPE - Up to 5 IP Addresses / 5 Apps in a year PT: 5 IP's Black / Grey Box Scan – app – 5 apps FREQUENCY - Twice a Year (2 Initial Test + 2 Confirmatory Test)	5 Ips Black /Grey Box - Is this Black + Grey Box testing? > Is this only Scan requirement or full testing?	**Clarification:** 1. Yes, Black + Grey Box Testing 2. Full Testing

9	27	Scope of Work - Security Testing	ACTIVITY - Vulnerability Assessment and External PT (With White listing and Without White listing) SCOPE - 50 IP Addresses + Additional 10 FREQUENCY - Twice a Year (2 Initial Test + 2 Confirmatory Test)	> Is this all 60 Ips to be considered for with and without white listing? = 60*2? For each activity VA and PT?	**Clarification:** 1. IP's mentioned in the requirement are part of VA&PT exercise with whitelisting 2. Yes, for each activity of VA & PT
10	27	Scope of Work - Security Testing	ACTIVITY - Adhoc Revalidation post any planned / unplanned audits findings implementation SCOPE - Up to 10 Units PT FREQUENCY - Initial Test + Confirmatory	> Kindly clarify the 10 Units definition? Each Unit means how many Ip?	**Clarification:** Each unit is an IP
11	27	Scope of Work - Security Testing	ACTIVITY - Report Analysis SCOPE - VA PT Audits (Initial and Confirmatory) FREQUENCY - Quarterly / Half yearly	> Kindly clarify the expectation. What kind of analysis is needed? What is the deliverablke of this actovity and in what format?	**Clarification:** Complete and Separate report to be provided on the VA and PT exercise along with the recommendations
12	27	Scope of Work - Security Testing	ACTIVITY - Backup and Restoration. SCOPE - In-Scope Devices FREQUENCY - Device Specific Monthly rotation.	Please clarify on the frequency of this test for **each device (e.g. 12 Firewalls - all 12 firewalls will be done on Monthly baisis or 1 firewall per month only)) please help with the clear frequency per device type. Do all the** devices (e.g. 58 over all devices (exclusing Servrs) in scope of RFP) need to be tested.	**Clarification:** Monthly frequency per device

13	27	Scope of Work - Security Testing	ACTIVITY - Network and Network-Security devices Failover Testing as per calendar schedule. SCOPE - In-Scope Devices FREQUENCY - Monthly	Please clarify on the frequency of this test for each device type and count of devices wherein this testing will be performed	**Clarification:** Monthly frequency per device. Please refer Page 26 for count of devices

14	27	Scope of Work - Security Testing	ACTIVITY - BAS (Breach and Attack Simulation) SCOPE - 200 IP addresses FREQUENCY - Upto twice in a year	> Kindly clarify the expectations. > Scenarios expectated	**<u>Clarification For BAS:</u>** A. Attack Simulation Artifacts Library of Playbooks covering: - MITRE ATT&CK techniques - Email phishing simulations - Malware delivery simulations - Lateral movement scenarios - Privilege escalation tests - Data exfiltration simulations - Execution Logs for each simulation - Detection Coverage Reports B. Security Control Effectiveness Reports 1. EDR Performance Report - Detection - Prevention - Response time 2. SIEM Detection Mappings - Which alerts fired - Detections missed - MITRE technique-to-alert mapping 3. SOC Performance Metrics - Time to detect - Time to respond - Analyst workflow analysis C. Gap & Improvement Insights 1. Gap Analysis Report

					- Missed alerts - Incomplete log sources - Uninstrumented endpoints 2. False Positive / False Negative Report 3. Actionable Recommendations - Detection rule enhancements - Log source improvement - EDR policy tuning - Network control hardening Reporting should be (Initial + Confirmatory) and should be customised as per Regulatory requirements

15	27	Scope of Work - Security Testing	ACTIVITY - CART(Continuous Automated Red Teaming SCOPE - 200 IP addresses FREQUENCY - Upto twice in a year	> Kindly clarify the expectations. > Scenarios expectated	**<u>Clarification For CART:</u>** A. Autonomous Red Team Campaign Reports - End-to-End Attack Path Reports - Initial access → foothold → privilege escalation → lateral movement → objective achieved - Kill Chain Mapping - Evidence of Exploitation (screenshots, logs, command artifacts) B. Continuous Attack Surface Visibility - Live Attack Surface Map - Exposure Analysis - Credentials exposure - Open ports - Shadow IT - Misconfigured IAM paths - Risk Prioritization Dashboard C. Remediation Validation - Automated Retesting Reports - Fixed - Partially fixed - Not fixed - Regression introduced - Continuous Validation Score D. SOC & Detection

					Engineering Insights - SOC Behavior Analysis - Did SOC detect CART attacks in real time? - Detection Gaps Report - Missing Sigma/EDR rules - Incident Readiness Score E. Governance & Strategic Deliverables - Purple Team Collaboration Reports - Security Maturity Scorecard (Before vs After) - Roadmap for Hardening & Improved Detection Reporting should be (Initial + Confirmatory) and should be customised as per Regulatory requirements

16	27	Scope of Work - Security Testing	ACTIVITY - Honey pot Exercise FREQUENCY - Upto twice in a year	What is your key goal of this exercise? Will the tool be provided by SHCIL? Which network segments can the honeypot be deployed in (internal, external, cloud, DMZ)? What systems, network segments, or environments should the honeypot emulate, and are there any restrictions regarding placement or data collection? Should the honeypot be low-interaction or high-interaction? How long should the honeypot run (week, month)	**Clarification:** 1. Key Goal : Threat Detection & Early Warning, Threat Intelligence Collection, Lateral Movement Monitoring, Security Posture Validation, Decoy to Mislead Attackers 2. Bidder has to bring their own tool for this activity and set it up in the StockHolding enviornment. Servers will be provided by StockHolding and deception technology/tool and architecture setup to be provided by bidder 3. External (Internet-facing) and DMZ Servers 4. Available servers in DMZ which will be a combination of Windows, Linux, Web-Servers, API, etc. 5. Restrictions Usually Include: No real production data, No user credentials, Cannot expose sensitive internal architecture, Logs and captured data must stay in SOC environment, No outbound connections unless allowed for research 6. High-Interaction Honeypot 7. Duration: 24x7x365. However, the review has to be done twice a year

17	28	Scope of Work - Consulting Services	Activity - Network-security Infrastructure architecture (functionality and security) is put in place, and conduct methodical reviews / assessments on a yearly basis (to identify any gaps / loopholes OR areas of concern and Improvement. Scope - 200 IP Addresses Deliverable - SNA Report Frequency - Onsite & Yearly Location - Navi Mumbai	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.	**Clarification** 1. High level Information has been shared on page -26, other Details will be shared with winning bidder 2. Yes, upto 10 applications has to be reviewed 3. Details will be shared with winning bidder. No cloud apps in scope 4. Internal StockHolding Policies 5. Has to be done Onsite

18	28	Scope of Work - Consulting Services	Activity - Risk Assessment of network security devices on yearly basis and reporting with proper analysis with industry supported guidelines. Scope - 200 IP Addresses Deliverable - Risk Assessment Report Frequency - Onsite & Yearly Location - Navi Mumbai	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.	**Clarification** 1. It is for Network and Security Device 2. No. We expect the bidder to bring their own templates 3. No specific regulation. It is to implement industry best practices 4. Yes. Centralized Repository is available 5. Yes, details mentioned on page 39 & 40 6. Has to be done Onsite

19	28	Scope of Work - Consulting Services	Activity - Ensuring adequate, appropriateness and concurrency of various policies and guidelines in place and shall provide Information Security consultancy for newer technology deployment for new and existing applications and products. Scope - 15 Policies & Procedures to be reviewed & 5 new policies and procedures Development Deliverable - 15 Policies & Procedures to be reviewed & 5 new Policies Development Frequency - Onsite & Yearly Location - Navi Mumbai	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?	**Clarification** 1. No reference to any regulation apart from what is mentioned in the RFP 2. Yes. Wherever available and applicable 3. No. Activity has to be done Onsite
20	28	Scope of Work - Consulting Services	Activity - Assisting StockHolding in planning, execution, and implementation of information security related initiatives / projects / Preparation of request for proposals programs in StockHolding. Scope - Handholding & Assistance to StockHolding in implementing Information Security Deliverable - Advisory support Frequency - OffSite / Onsite & Monthly Location - Navi Mumbai	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.	**Clarification** 1. Bifurcation is not possible since this is As and When Required 2. Please share the Block rate

21	28	Scope of Work - Consulting Services	Activity - Cyber Security Drill Scope - IT Assets Deliverable - No Table Top exercised. Scenario based Drill Live Simulation Frequency - Onsite & Yearly Once Location - Navi Mumbai	1. What exact type of live simulation are you expecting—red team activity, incident simulation, attack injection, or blue-team response drill? 2. Which systems or environments may be targeted or simulated during the drill, and which ones must be excluded? 3. What business processes or crisis-response teams must be involved during the simulation? 4. What core capability do you want to test? (Detection, response, SOC workflow, internal communication, user behavior, incident escalation, resilience, etc.) 5. Which departments must participate? (SOC, IT, HR, Legal, Finance, Management, PR) 6. Should C-suite decision-making be tested?	**Clarification** 1. Bidder should be capable to conduct all kinds of simulation 2. Stockholding will share the details for Cyber Drill exercise 3. As per CCMP Plan the repossible team will be part of this simulation 4. Bidder should be capable to conduct all kinds of test 5. Multiple Departments will participate, Department Details will be shared to the winning bidder 6. Yes
22	28	Scope of Work - Consulting Services	Activity - Remote Exposure and Breach Assessment Scope - IT Assets Frequency - Onsite & Yearly Once Location - Navi Mumbai	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?	**Clarification** 1. Team Details will be shared to the winning bidder 2. Team Details will be shared to the winning bidder, Please refer page - 26 for Technology related assets

23	28	Scope of Work - Consulting Services	Activity - Active Directory Risk Assessment Programme (AD RAP) Assessment Scope - Active Directory & related Setup Deliverable - AD RAP Assessment Report Frequency - Onsite and Half Yearly basis Location - Navi Mumbai	1. How many ADs are available? 2. Can you share AD forest/domain design documents or high level details (if available)? 3. Is the AD on-prem or on Cloud?	**Clarification** 1. 1 Domain with 3 Domain Controllers. 2. Remaining details will be shared with the winning bidder 3. AD is on-prem
24	Page 11 and 12 (Points 3 and 4)	Eligibility Criteria (For On-site Manpower Assignment)	Certified Ethical Hacker (CEH) or Certified in Cyber Security (CC) and /or Any SIEM / Firewall / ADC / EDR[1]XDR OEM certified	Does this mean any one of the mentioned certifications?	**Clarification** Yes. Any one certification
25	Page 26	Scope of Work	Devices under Scope of Device Management	Count of Crowdstrike modules to be managed is not added under this point but is mentioned in detailed scope. Please specify which services from Crowdstrike have been availed.	**Clarification** Crwodstrike Services : Falcon Endpoint Protection, Thread Graph, Falcon Firewall management, Overwatch, Falcon Prevent, Falcon Insight, Falcon Device Control, Data Protection, Data Replicator, Spotlight, Discover, File Vintage, FDR
26	Page 42	Scope of Work - Resource Management	Resource Management	Is the count of 11 resources to be maintained on Saturday and Sunday as well	**Clarification** Refer Resource Management Section in Page 42

27	Page 43	Scope of Work - Resource Management	Resume/CV for each of these members should be provided to StockHolding for completing screening of such candidates.	Will SHCIL take interview of proposed candidates or only screen resumes of proposed candidates?	**Clarification** Screening and Interview will be done by StockHolding
28	Page 43	Scope of Work - Resource Management	Support on Sunday and StockHolding Holidays: All 3 shifts should be covered with atleast 2 resources available at Mahape Navi Mumbai Site.	2 resources per shift is needed on Sundays and Public Holidays?	**Clarification** Refer Resource Management Section in Page 42
29	Page 53 and 54	Scope of Work - Network Security and related Services	Security Monitoring and SOC Maturity Improvement is out of scope	This deliverable is more related to SOC monitoring. Please clarify the scope for this actionable	**Clarification** Scope is already mentioned in the RFP
30			Ticketing and monitoring tool	Is there a monitoring and ticketing tool being used for Device Management scope in SHCIL?	**Clarification** Yes
31			Rebadging of resources	Will SHCIL allow rebadging of existing resources to new Vendor?	**Clarification** Yes. As long as the Education Qualifications, Experience and Certifications are met as per RFP Terms
32	Pages 11, 12 and 13	Eligibility Criteria (For On-site Manpower Assignment)	Degree of Resources	Will SHCIL allow resources who have relevant experience but may have a different degree than one mentioned in RFP?	**Clarification** No
33	Pages 11, 12 and 13	Eligibility Criteria (For On-site Manpower Assignment)	Certification of Resources	Will SHCIL allow a grace period of 3 months for resources who have relevant experience and expertise to complete relevant certification?	**Clarification** No

34	11	Scope of Work (SOW) - SOC Operations	Functional Principles	What is your current SIEM platform and its deployment model?	**Clarification** Details to be shared with winning bidder
35	11	Scope of Work (SOW) - SOC Operations	Functional Principles	What is your average and peak EPS obsevred per month?	**Clarification** Details to be shared with winning bidder
36	11	Scope of Work (SOW) - SOC Operations	Functional Principles	What is the number of log sources integrated with SIEM ?	**Clarification** Details to be shared with winning bidder
37	11	Scope of Work (SOW) - SOC Operations	Functional Principles	What is total number of usecases configuered on SIEM ?	**Clarification** Details to be shared with winning bidder
38	11	Scope of Work (SOW) - SOC Operations	Functional Principles	What is your average number of monthly SOC incidents? Please provide bifurcation of P1, P2 & P3 incidents.	**Clarification** Details to be shared with winning bidder
39	11	Scope of Work (SOW) - SOC Operations	Functional Principles	What is the threat intel feed available?	**Clarification** Yes, Threat Intel platform is available at StockHolding
40	11	Scope of Work (SOW) - SOC Operations	Functional Principles	What is your SOAR platfrom ?	**Clarification** Details to be shared with winning bidder
41	11	Scope of Work (SOW) - SOC Operations	Functional Principles	How many automation playbooks are configured ?	**Clarification** Details to be shared with winning bidder
42	11	Scope of Work (SOW) - SOC Operations	Functional Principles	What is your ITSM platform ?	**Clarification** Details to be shared with winning bidder

43	11	Scope of Work (SOW) - SOC Operations	Functional Principles	Have you integrated SIEM with SOAR & ITSM ?	**Clarification** Details to be shared with winning bidder
44	11	Scope of Work (SOW) - SOC Operations	Functional Principles	Is bidder expected to bring another SIEM or provide SOC services using StockHolding existing SIEM ?	**Clarification** Bidder is expected to provide SOC Services using Existing SIEM. SIEM comes with MDR services which is provided by the SIEM OEM
45	11	Scope of Work (SOW) - SOC Operations	Functional Principles	What is your current L1, L2, L3, SME resource count in SOC ?	**Clarification** Details to be shared with winning bidder
46	11	Scope of Work (SOW) - SOC Operations	Functional Principles	We understand as a part of SOC offering, our scope will be complete SOC operations and management including L1,L2, L3 SOC support, platform engineering and management with continous improvement. Please clarify if otherwise.	**Clarification** Yes
47	11	Scope of Work (SOW) - SOC Operations	Functional Principles	Do you have a Threat Intel Platform (TIP) ? Please provide details.	**Clarification** Yes, Threat Intel platform is available at StockHolding
48	11	Scope of Work (SOW) - SOC Operations	Functional Principles	What is your DC & DR setup ?	**Clarification** Yes. DC, DR and NDR sites are present
49	11	Scope of Work (SOW) - SOC Operations	Functional Principles	Can you provide your asset inventory ?	**Clarification** Details to be shared with winning bidder

50	11	Scope of Work (SOW) - SOC Operations	Functional Principles	What is the total number of users for UEBA ?	**Clarification** UEBA is not mentioned in the RFP
51	11	Scope of Work (SOW) - SOC Operations	Functional Principles	Is there a requirement of multi-tenancy, please clarify.	**Clarification** No Multi-tenancy required
52	11	Scope of Work (SOW) - SOC Operations	Functional Principles	please provide the list of domains to be considered for sizing Brand Monitoring & Dark Web monitoring efforts,	**Clarification** There is a separate platform which StockHolding has onboarded for Brand Monitoring and Dark Web Monitoring. Bidder is not required to provide this platform
53	11	Scope of Work (SOW) - SOC Operations	Functional Principles	What is the total number of digital assets for EASM ?	**Clarification** EASM is not mentioned in the RFP
54	11	Scope of Work (SOW) - SOC Operations	Functional Principles	Is bidder expected to bring in BM, DW & EASM tool or shall leverage StockHolding existing solutions. Please clarify along with OEM name.	**Clarification** BM, DW & EASM is not mentioned in the RFP

55	73	Indemnity Category - Legal	**Indemnity:-** The Bidder should hereby indemnify, protect and save StockHolding against all claims, losses, costs, damages, expenses, action suits and other proceedings, resulting from infringement of any patent, trademarks, copyrights etc. or such other statutory infringements in respect of all the equipment offered by the Bidder. Any publicity by Bidder in which name of StockHolding is used should be done only with the explicit permission of StockHolding.	**Comment/ Suggestion-** **We propose adding an exception to the existing indemnity clause as below:-** **Indemnity:-** Exceptions to Indemnity Provided that the Bidder complies with its obligations under this Agreement, the Bidder shall not be liable to indemnify StockHolding for any claim or infringement arising from (i) any misuse, alteration, or unauthorized modification of the equipment or services by StockHolding; (ii) any use of the equipment or services in combination with third-party products not supplied or recommended by the Bidder; (iii) StockHolding's failure to follow the Bidder's operating instructions or specifications; or (iv) any materials, data, or specifications provided or mandated by StockHolding that result in an infringement claim. **Justification -** This exception is proposed to prevent the Bidder from being held liable for matters beyond its control and to maintain a fair allocation of contractual risk.	No Change

56	74	Termination Clause Category - Legal	**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;	**Comment/ Suggestion- We propose addition to the existing clause as below:-** **Termination Clause:-** For Temination 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. **Justification -** This addition ensures the Bidder has a fair and reciprocal right to terminate the Agreement in case of an uncured material breach by StockHolding.	No Change

57	75	Category - Legal	**2. Limitation of Liability:-** 2.1. No Liability for Regulatory Disclosures - Neither StockHolding nor the Bidder shall be held liable for any consequences arising from disclosures made in compliance with regulatory requirements, provided that such disclosures are made in good faith and in accordance with applicable laws and regulations. However, the Bidder agrees to notify StockHolding promptly of any potential regulatory action that could materially affect the Bidder's ability to meet the terms of this SLA.	**Comment/ Suggestion-** **We propose adding an exception to the existing indemnity clause as below:-** **Limitation of Liability:-** NEITHER PARTY SHALL BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, EXEMPLARY OR PUNITIVE DAMAGES OR ANY DAMAGES FOR LOST PROFITS, LOST REVENUES, LOSS OF GOODWILL, LOSS OF ANTICIPATED SAVINGS, LOSS OF CUSTOMERS, OR LOSS OF DATA, OR INTERFERENCE WITH BUSINESS, ARISING OUT OF THE PERFORMANCE OR FAILURE TO PERFORM UNDER THIS AGREEMENT, WHETHER OR NOT CAUSED BY THE ACTS OR OMISSIONS OR NEGLIGENCE (INCLUDING GROSS NEGLIGENCE OR WILLFUL MISCONDUCT) OF ITS EMPLOYEES OR AGENTS, AND REGARDLESS OF WHETHER SUCH PARTY HAS BEEN INFORMED OF THE POSSIBILITY OR LIKELIHOOD OF SUCH DAMAGES. In no event, regardless of the form of the claim or cause of action (whether based in contract, negligence, strict liability, tort or otherwise) shall either Party's aggregate liability to the other Party under this	No Change

				Agreement exceed the fees actually paid under a relevant Purchase Order or Statement of Work which is subject matter of claim **Justification** - This clause ensures fair risk allocation by preventing either party from being exposed to excessive or unforeseeable indirect or consequential damages	

58	76	Right to Audit and Due Diligence Category - Legal	**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.	**Comment/ Suggestion-** **We propose to amend 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 authorized auditors ~~at any time~~ upon prior written notice (not less than 20 days') 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~~ required 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 privacypolicies that meet the industry standards. Justification - This addition ensures	Revised Clause in RFP: **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 **upon prior written notice (not less than 48 hours)** 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

				that audits are conducted in an orderly, non-disruptive manner while limiting access to only relevant records necessary for compliance	privacy policies that meet the industry standards.

59	-	Category - Legal	We recommend including a Non-Solicitation clause in the RFP	**<u>Comment/ Suggestion- We recommending below clause under the RFP:- Non-Solicitation:-</u>** 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 Associates are equally restricted from poaching or soliciting or inducing any employees of other Party to leave their employment or engagement with such other Party. **Justification** - To protect both Parties from	New Clause added in RFP: ***Non-Solicitation:-*** *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 Associates are equally restricted from poaching or soliciting or inducing any employees of other Party to leave their employment or engagement with such other Party.*

				employee poaching and to ensure workforce stability during and after the engagement	

60	84	ANNEXURE – 3 – Technical Criteria Point 4	Bidder having a ISO 27001 Certified SOC functional in India as on RFP date	Contradictory scoring bands (12 marks where max is 10) and duplicate numbering.	**Rectification of Clause in Annexure -3 Technical Criteria Point 4:** Parameter: Bidder having a ISO 27001 Certified SOC functional in India as on RFP date Scores: 5 Years : 7 marks More than 5 Years - <= 8 Years **: 8 Marks** More than 8 Years : 10 Marks Qualifying Scores: 7 Max. Scores: 10
61	82	Eligibility Criteria (For On-site Manpower Assignment)	Eligibility table requires 03 years for "Security Consultants – Active Directory Management" (Eligibility – manpower), but Resource section (Team Profiles) demands 5 years.	Align to single requirement (e.g minimum 3 years with preference for 5+)	**Clarification** Security Consultants – Active Directory Management across the RFP to be read as 3+ years Experience
62	43	Resource Management	For Active Directory Management: 16x6x365 (Sunday Holiday): 2 shifts should cover with atleast 1 resources available at Mahape Navi Mumbai Site from Monday to Saturday.	Ambiguous—"x365" implies 365 days while "Sunday Holiday" removes Sundays. Clarify to 16x6 (Mon–Sat), no Sundays	**Clarification** For Active Directory Management: 16hrs x 6 days (Sunday Holiday): 2 shifts should cover with atleast 1 resources available at Mahape Navi Mumbai Site from Monday to Saturday.
63	19	End point Security (On-premise and/or Cloud based)	Currently StockHolding has cloud based Endpoint detection and response (EDR) solution from Crowdstrike.	SOW states CrowdStrike is the current EDR; later skills/deliverables require deep knowledge of Trend Micro OfficeScan/Apex One/ServerProtect/Deep Security and even AIX Deep Security. Confirm current endpoint stack	**Clarification** Current EDR is Crowdstrike. However, in the future there is no guarantee which EDR will be running. Hence other options are also included

64	63	Incident Management and Investigation Metric Calculation and Penalty Point 1	P0 resolution 30 mins for outages like "Firewall Down, misconfiguration issues"; P1 resolution 60 mins. Its Operationally infeasible for enterprise firewalls/WAF/IPS where RCA, approvals, and remediations exceed 30–60 mins, especially with change windows.	Request to adopt realistic restoration targets (e.g., P0 2–4 hrs, P1 4–8 hrs) with interim workarounds	**Clarification** No Change
65	59	Monitoring and Management of Network Devices Table - A	99.5% → 1% of monthly contract value per hour of breach; monthly penalties capped at 10% (excluding resource penalties).	Even brief outages can max out the cap quickly while root causes may be outside MSSP control (links, DC infra). Also resource penalties are separate, so total deductions can far exceed 10%. Request you to Cap aggregate penalties (including resource) at 10%; exclude clear non-MSSP causes with evidence.	**Clarification** Infra related outages are not in SLA scope.
66	71	Payment Terms Point 1	Transition is 3 months; MSSP must provide "sufficient staff" and 24x7 service setup, payment starts after transition.	Significant cost for 90 days with no payment; also penalties apply post transition, but expectations during transition are extensive. Request to exclude performance penalties during transition period.	**Clarification** Refer RFP Page No. 58 - "All SLA's and associated penalties shall be applicable to the new MSSP post transition period of 3 months"
67	42	Resource Management	Minimum 11 resources across all shifts	With leaves, weekly offs, and AD two-shift coverage, 11 headcount is insufficient to cover all patterns without consecutive shifts Provide a staffing matrix; likely 14–18 FTE minimum including spares/shadows to meet rules.	**Clarification** For any given day covering all the shifts, 11 resources have to be available wherever mentioned in the RFP. The bidder has to decide how many additional resources to

					be included to cover leaves, weekly off's etc.
68	26	Device Management - SIEM LEC / Logger Server		Please confirm the OEM and version of the SIEM platform currently in use.	**Clarification** Details will be shared with the Winning Bidder
69	26	Device Management	Can you provide the split of on-prem vs cloud-based security tools		**Clarification** All tools and platforms are on premise, except Threat Intelligence, SIEM and EDR platform
70		General		Please share the ticket volumetric details last 6 month for reference	**Clarification** Details to be shared with winning bidder
71	55	Transition Preiod	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.	**Clarification** No Change
72	59	Service Level Agreement (SLA) and Penalty	In all other Operational conditions - The maximum penalty applicable will be 10% of the monthly contract value.	Request for Penalty capping at 5%	No change
73	27	Security Testing		What is the count for SOP review	**Clarification** Refer Section : Consulting Services Page 28-29 of the RFP

74	27	Security Testing		In Cyber Security Drill could you please let us know details on hybrid scenarios	**Clarification** Hybrid Scenarios include Technical (cyber attack) and Non-Technical (physical, human, process-related)
75	27	Security Testing		For Continuous Automated Red Team Assessment, our understanding is Internal red team assessment twice in a year. Is this correct	**Clarification** Yes

76	27	Security Testing		What is the expectation in terms of deliverables for both BAS and CART Assessment	**<u>Clarification For BAS:</u>** A. Attack Simulation Artifacts Library of Playbooks covering: - MITRE ATT&CK techniques - Email phishing simulations - Malware delivery simulations - Lateral movement scenarios - Privilege escalation tests - Data exfiltration simulations - Execution Logs for each simulation - Detection Coverage Reports B. Security Control Effectiveness Reports 1. EDR Performance Report - Detection - Prevention - Response time 2. SIEM Detection Mappings - Which alerts fired - Detections missed - MITRE technique-to-alert mapping 3. SOC Performance Metrics - Time to detect - Time to respond - Analyst workflow analysis C. Gap & Improvement Insights 1. Gap Analysis Report

					- Missed alerts - Incomplete log sources - Uninstrumented endpoints 2. False Positive / False Negative Report 3. Actionable Recommendations - Detection rule enhancements - Log source improvement - EDR policy tuning - Network control hardening Reporting should be (Initial + Confirmatory) and should be customised as per Regulatory requirements Clarification For CART: A. Autonomous Red Team Campaign Reports - End-to-End Attack Path Reports - Initial access → foothold → privilege escalation → lateral movement → objective achieved - Kill Chain Mapping - Evidence of Exploitation (screenshots, logs, command artifacts) B. Continuous Attack Surface Visibility - Live Attack Surface Map - Exposure Analysis

					- Credentials exposure - Open ports - Shadow IT - Misconfigured IAM paths - Risk Prioritization Dashboard C. Remediation Validation - Automated Retesting Reports - Fixed - Partially fixed - Not fixed - Regression introduced - Continuous Validation Score D. SOC & Detection Engineering Insights - SOC Behavior Analysis - Did SOC detect CART attacks in real time? - Detection Gaps Report - Missing Sigma/EDR rules - Incident Readiness Score E. Governance & Strategic Deliverables - Purple Team Collaboration Reports - Security Maturity Scorecard (Before vs After) - Roadmap for Hardening & Improved Detection Reporting should be (Initial +

					Confirmatory) and should be customised as per Regulatory requirements

77	22	Device Management		Data Security - Which product and vendor is refferred here? Does MSSP need to bring licnese for the same ?	**Clarification** No license or product. Needs to be monitored using existing StockHolding's tools/platforms
78	24	SOC Operation		Is MSSP expected to bring DAM & PIM license in future ? If yes, what is expected time frame ?	**Clarification** No
79	26	Cloud components		Several controls may move to cloud soon. Please specify target cloud(s) (e.g., Oracle PCA private cloud, VMware, any public cloud), and clarify if MSSP must design migration, bear migration effort, and re-platform policies under the same commercials.	**Clarification** All Devices under Scope of Device Management will remain on Prem. Some of the components might move to cloud under Saas platforms or to Onprem VM's hosted on Vmware. SOC Team has to assist in migration related activities.
80	22/23	AD/SCCM responsibilities		Will UAT environments be provided by StockHolding, and whether monthly patch windows are pre-approved change slots to meet SLA	**Clarification** Yes
81	63	Severity Definition		Severity list includes P0, P1, P3, P4, with P2 missing in the table, though referred elsewhere. Please confirm complete severity matrix, definitions, and SLA times for P2	**Clarification** P3 to be read as P2 and P4 to be read as P3
82	24-25	MDR		Who will be responsible for author, maintain, and own SOAR playbooks/use-cases	**Clarification** There is no SOAR platform
83	20	EDR		Please confirm whether MSSP is responsible for policy design for EDR/XDR	**Clarification** No. However, consultation assistance might be taken as

					and when required and needed.
84	16	A. BASED ON EXPERIENCE, TURNOVER & RESOURCE STRENGTH (70 MARKS)	2) Projects of SOC implementation and/or managing SOC (onsite/from customer premises) of value more than Rs. 5.6 Crores each during last 05 (five) years in India · 1-3 Projects – 10 Marks · 4-5 Projects – 12 Marks · More than 5 Projects – 15 Marks	As multiple clauses of marking over another such as On premise SOC or value of SOC implementation narrow downs the competitive participation and confines the bidders. Therefore, we request that Stockholding kindly reconsider the clause below: · 1 Projects – 10 Marks · 2 Projects – 12 Marks · 3 Projects – 15 Marks	No Change
85	16	A. BASED ON EXPERIENCE, TURNOVER & RESOURCE STRENGTH (70 MARKS)	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 · 1 Project – 5 Marks · 2-3 Projects – 7 Marks More than 3 Projects – 10 Marks	As multiple clauses of marking over another such as On premise SOC or value of SOC implementation narrow downs the competitive participation and confines the bidders. Therefore, we request that Stockholding kindly reconsider the clause below: 3) Projects of SOC implementation and/or managing SOC (onsite/from customer premises) to BFSI/PSU/Government Sector in India during last 05 (five) years in India · 1 Projects – 10 Marks · 2 Projects – 12 Marks · 3 Projects – 15 Marks	No Change

86	4	ELIGIBILITY CRITERIA (Documents to be Submitted Online)	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	Request stock holding to government/PSU vertical in below clause 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	No Change
87	24	SOC Operations:	The System Integrator will develop the work flow process for attending to the various functions at the SOC including the work flow for attending to the incidents generated with network-security device management.	Request Stockholding to confirm existing ITSM for bi-directional integration and ticket workflow Management	**Clarification** Details to shared with winning bidder

88	53	Network Security and related Services	• Threat Hunting:	Please confirm frequency for threat hunting	**Clarification** Duration : As per RFP Page 53, it is mentioned "Ongoing continuous process". However, the review has to be done twice a year
89	27	D. Security Testing Network Penetration Testing Configuration Audit (CA), Vulnerability Assessments (VA) & Penetration Testing (PT) - (As per CIS Benchmark and close the gap's and provide the clean report)	D. Security Testing Network Penetration Testing Configuration Audit (CA), Vulnerability Assessments (VA) & Penetration Testing (PT) - (As per CIS Benchmark and close the gap's and provide the clean report)	Does the bidder utilize the existing VM solution for Vulnerablity Management for security testing. Please confirm.	**Clarification** Bidder has to onboard their own VM solution
90	48	MDR Sizing	10.Following up with MDR team from Call initiation till call closure in MDR Dashboard for all the IT assets integrated with MDR	Kindly confirm does the dashboard will be provide by stockholding for SOC KPI management.	**Clarification** MDR Dashboard is already existing and will be given to SOC Team
91	70	Point no. 37 ILL Link Testing Report	Speed Test report to test ILL link Bandwidth	Pls. suggest specific speed test methdology to be adopted for speed test, also need clarfication for who will conduct the speed test amongst the resource demanded in RFP.	**Clarification** StockHolding has a tool which displays ILL Speeds. This verification has to be done by SOC team as a weekly activity.

92	27	Point 13. Backup and Restoration.	In-Scope Devices	Pls. confirm existing backup & restoration mechanism /methodology and backup frequency if any.	**Clarification** Details will be shared with the Winning Bidder