Stock Holding Corporation of India Limited

(*StockHolding*)

RFP Reference Number: CPCM-20/2025-26

Date: 18-Nov-2025

GEM Reference No. - GEM/2025/B/6906136

REQUEST FOR PROPOSAL FOR SELECTION OF SERVICE PROVIDER FOR MANAGING ON-SITE SECURITY OPERATION CENTRE (SOC) FOR STOCKHOLDING

DISCLAIMER

The information contained in this Request for Proposal (RFP) document or information provided subsequently to bidder(s) or applicants whether verbally or in documentary form by or on behalf of Stock Holding Corporation of India Limited *(*StockHolding*)*, is provided to the bidder(s) on the terms and conditions set out in this RFP document and all other terms and conditions subject to which such information is provided.

This RFP document is not an agreement and is not an offer or invitation by StockHolding to any parties other than the applicants who are qualified to submit the bids ("bidders"). The purpose of this RFP is to provide the bidder(s) with information to assist the formulation of their proposals. This RFP does not claim to contain all the information each bidder may require. Each bidder should conduct its own investigations and analysis and should check the accuracy, reliability and completeness of the information in this RFP and where necessary obtain independent advice. StockHolding makes no representation or warranty and shall incur no liability under any law, statute, rules or regulations as to the accuracy, reliability or completeness of this RFP. StockHolding may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFP.

RFP Document Details

Sr. No.	Description	Remarks
1	Name of Organization	Stock Holding Corporation of India Limited
2	RFP Reference Number	CPCM-20/2025-26
3	Requirement	Request for proposal (RFP) for selection of Service Provider for managing On-Site Security Operation Centre (SoC) for Stockholding
4	Interest free Earnest Money Deposit (EMD) [*]	Rs. 35,00,000/- (Indian Rupees Thirty Five Lakhs only) to be paid to Stock Holding Corporation of India Limited as Earnest Money Deposit should be submitted separately before submission of online bids by way of RTGS/NEFT/BG/FDR on StockHolding's Bank Account No.: 004103000033442 Bank: IDBI Bank (Nariman Point Branch) IFSC: IBKL0000004. Please share the UTR details to us on below mentioned email address.
5	Email Id for queries up to Pre-Bid Meet	CPCM@stockholding.com
6	Date of Issue of RFP Document	18-Nov-2025
7	Date, Time and place for online Pre-bid meeting	25-Nov-2025 11:30 AM For participation in pre-bid meeting, please send mail for online meeting link to CPCM@stockholding.com before 24-Nov-2025 05:00 PM
8	Last Date for Submission of Online Bid	09-Dec-2025 06:00 PM
9	Date of opening bid	09-Dec-2025 06:30 PM

[*] - Bidders registered under Micro & Small Enterprises (MSE) for specific trade are exempted from EMD. Bidders shall upload the scanned copy of necessary documents as part of eligibility criteria documents.

This bid document is not transferable.

StockHolding reserves the right to modify/update activities/ dates as per requirements of the process.

Table of Contents

SUBMISSION OF PROPOSAL

StockHolding invites e-tender through GeM Portal, in two bid system (Technical and Commercial bid), from firm/company who has proven experience in the implementation, integration and managing of Security Operation Centre (SOC).

Submission of Bids:

The online bids will have to be submitted within the time specified on website https://gem.gov.in/ for:-

1. Eligibility/Technical Bid (.pdf files)
2. Commercial Bid (.pdf files)

Invitation for bids:

This "Invitation for bid" is meant for the exclusive purpose of "Managed Security Service (MSS) / Security Operation Centre (SoC) Operations management from Stockholding's Data centre location" for StockHolding as per the terms, conditions, and specifications indicated in this RFP and shall not be transferred, reproduced or otherwise used for purposes other than for which it is specifically issued.

The System Integrator shall understand StockHolding's overall Information Technology Infrastructure w.r.t. network and network-security architecture and device management of security solutions/ Services mentioned in this RFP and submit a response, to operate a 24*7 security operation centre integrated with Stockholding IT Systems, Servers, applications, network and network-security appliances and devices using standard methods / protocols/ message formats to support Stockholding's critical applications.

Objective of this RFP

The objective of this RFP is SOC Operations Management, Support for MDR Services integrations and also to comply with the circulars and advisories issued by, CERT-in, NCIIPC, SEBI, NSDL, CDSL, PFRDA, IRDA, RBI etc. and to implement a robust Security Operation Center (SOC) in StockHolding to prohibit/fight against Cyber Security Threats. The threat landscape will consist of the applications, servers, network appliance and other technologies that support the critical infrastructure.

Due Diligence:

The bidder is expected to examine all instructions, Forms, Terms, Conditions and Specifications in this RFP. Bids shall be deemed to have been made after careful study and examination of this RFP with full understanding of its Implications. The Bid should be precise, complete with all details required as per this RFP document. Failure to furnish all information required by this RFP or submission of Bid not as per RFP requirements will be at the bidder's risk and may result in rejection of the bid and the decision of StockHolding in this regard will be final and conclusive and binding.

Cost of Bidding:
The bidder shall bear all costs associated with the preparation & submission of its bid and StockHolding will in no case be held responsible or liable for these costs, regardless of the conduct or outcome of the bidding process.

Contents of this RFP Document:
The requirements, bidding procedure, general terms & conditions are prescribed in this RFP document with various sections

a Bidder Details – Annexure 1
b Format for Eligibility Criteria - Annexure 2
c Technical Bid – Annexure 3
d Format for Commercial Price Bid - Annexure 4
e Integrity Pact (Text) - Annexure 5
f Covering Letter on Bidder's Letterhead for Integrity Pact – Annexure 6
g Compliance Statement - Annexure 7
h Format for bank Guarantee – Annexure 8
i Format for Non-disclosure Agreement - Annexure 9
j Covering Letter on Bidder's Letterhead for Concentration Risk – Annexure 10

Clarifications regarding RFP Document:

a Before bidding, the bidders are requested to carefully examine the RFP Document and the Terms and Conditions specified therein, and if there appears to be any ambiguity, contradictions, gap(s) and/or discrepancy in the RFP Document, they should forthwith refer the matter to StockHolding for necessary clarifications.
b A bidder requiring any clarification for their queries on this RFP may be obtained via email to CPCM@stockholding.com
c StockHolding shall not be responsible for any external agency delays.
d StockHolding reserves the sole right for carrying out any amendments / modifications / changes in the bidding process including any addendum to this entire RFP
e At any time before the deadline for submission of bids / offers, StockHolding may, for any reason whatsoever, whether at its own initiative or in response to a clarification requested by bidders, modify this RFP Document.
f StockHolding reserves the rights to extend the deadline for the submission of bids, if required. However, no request from the bidders for extending the deadline for submission of bids, shall be binding on StockHolding.
g StockHolding reserves the right to amend / cancel / postpone / pre-pone the RFP without assigning any reasons.
h It may be noted that notice regarding corrigendum/addendums/amendments/response to bidder's queries etc., will be published on StockHolding's website only. Prospective

bidders shall regularly visit StockHolding's same website for any changes/development in relation to this RFP.

i It may be noted that bidder mentioned in the document may be either OEM/Distributor/System Integrator (SI).

Validity of offer:

The offer should remain valid for a period of at least **90 days** from the date of submission**.**

ELIGIBILITY CRITERIA (Documents to be Submitted Online)

The System Integrator must possess the requisite experience, strength and capabilities in providing the services necessary to meet the requirements, as described in the tender document. . The invitation to bid is open to all bidders who need to qualify the eligibility criteria as given below. Eligibility criteria are mandatory and any deviation in the same will attract bid disqualification.

Guidelines to be followed prior to submitting an application-

Bidder should upload all supporting documents at the time of submission duly signed and stamped on their company's letter head.

SI.	Criteria	Documents to be submitted by Bidder
1	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.	Copy of Certificate of Incorporation issued by the Registrar of Companies and Self-declaration by the bidder on it Letter Head duly signed by the Authorized Signatory along with supporting documents for SOC related PO on or before RFP Date
2	The bidder should have an average annual turnover of at least Rs. 14 Crores per annum for last 03 (three) financial years (i.e. 2022-23, 2023-24 and 2024-25). It should be of individual company and not of Group of Companies	Certificate from CA mentioning annual turnover for last three financial years.
3	The Bidder should have Positive Net worth minimum Rs. 3.5 crores for each of the last 03 (three) audited financial years (i.e. 2022-23, 2023-24 and 2024-25)	Certificate from CA mentioning networth for the past three financial years.
4	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	Copy of Purchase Order & Completion certificate with Customer Name and Address, Contact Person, Telephone Nos. Fax and e-mail Address and customer reference to be provided (or) Copy of Purchase Order & self- certificate attested by the authorized signatory of the bidder confirming "in-progress" status of cited project

	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	
5	Bidder should not be blacklisted by any Government, Government Body, PSU, Bank, Autonomous body and any other entity for any reasons within last 3 years from the RFP date.	Self-declaration by the bidder on it Letter Head duly signed by the Authorized Signatory
6	The bidder must possess at the time of bidding, following valid certifications: • ISO 9001:2008 or latest/ISO 20000 and • ISO 27001:2022 or SOC 2 Type 2	Relevant valid Certificates
7	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.	Declaration from HR Manager or authorized signatory on company letter head
8	Bidder shall have their own Security Operation Center situated in India with a ISO 27001 certification compliance	Self-declaration by the bidder on it Letter Head duly signed by the Authorized Signatory with ISO Certificate
9	Bidder should not be existing System Integrator for Network Infrastructure (NOC Services) and/or Cyber Security Consultant or Auditor for StockHolding to avoid conflict of interest	Self-declaration by the bidder on it Letter Head duly signed by the Authorized Signatory
10	Bidder should have Support office at Maharashtra.	Bidder to provide office address along with GST details.
11	Bidder to provide undertaking that no penalties, amounting to up to 5% of the contract value per year, have been imposed in the last 03 (three) years by any of its client(s).	Self-declaration from bidder on their letter head duly signed by authorized signatory
12	The bidder should not be under insolvency resolution, bankruptcy or liquidation proceedings under the Insolvency and Bankruptcy Code or any other applicable laws as on date of bid submission	Self-declaration from bidder on their letter head duly signed by authorized signatory
13	The Bidder must be CERT-In Empanelled as on RFP Date	Relevant valid Certificates

14	The Bidder to submit signed & stamped Integrity Pact as per Annexure - 5	Self-declaration from bidder on their letter head duly signed by authorized signatory

Eligibility Criteria (For On-site Manpower Assignment)

Sr. No.	Role	Professional Summary	Education	Work Experience	Certifications
1	Project Manager	Minimum 07 (Seven) years of experience in IT Network Security. Minimum 03 of years of experience as Project Manager in Infrastructure Security domain	Bachelor of Engineering / Bachelor of Science	• Web Application Firewalls • Intrusion Prevention Systems • Routing and L2 Switching • URL Filtering • Proxy • Next Generation firewalls (Checkpoint, Cisco ASA/Firepower, Fortigate, Palo Alto etc.) • Vulnerability assessment • Load Balancing • SSL Virtual Private Network (Juniper, Array, F5, Cisco, Checkpoint etc.) • Anti-Virus (Trend Micro OfficeScan/Apex One and Symantec Endpoint	Certified Information Security Manager (CISM)/ CISSP/CSPM)
2	Team Leader	Minimum 05 (Five) years of experience in IT Network Security. Minimum 03 of years of experience as Project Manager in Infrastructure Security domain	Bachelor of Engineering / Bachelor of Science	Web Application Firewalls Intrusion Prevention Systems Routing and L2 Switching URL Filtering Proxy Next Generation firewalls (Checkpoint, Cisco ASA/Firepower, Fortigate, Palo Alto etc.) Vulnerability assessment Load Balancing	Certified Information Security Manager (CISM) / CISSP

				SSL Virtual Private Network (Juniper, Array, F5, Cisco, Checkpoint etc.) Anti-Virus (Trend Micro OfficeScan/Apex One and Symantec Endpoint	
3	Sr. Security Consultants - SOC Operations	5 years of experience in IT Security and Networking. Working as Analyst – Infrastructure Security.	Bachelor of Engineering / Bachelor of Science	Web Application Firewalls Intrusion Prevention Systems Routing and L2 Switching URL Filtering Proxy Next Generation firewalls (Checkpoint, Cisco ASA/Firepower, Fortigate, Palo Alto etc.) Vulnerability assessment Load Balancing SSL Virtual Private Network (Juniper, Array, F5, Cisco, Checkpoint etc.) Anti-Virus (Trend Micro OfficeScan/Apex One and Symantec Endpoint Protection etc.) • Single Sign on Patch Management (Windows Server Update Services) Ticketing Tool	Certified Ethical Hacker (CEH) or Certified in Cyber Security (CC) and /or Any SIEM / Firewall / ADC / EDR-XDR OEM certified.
4	Security Consultants - SOC Operations	3 years of experience in IT Security and Networking. Working as Analyst – Infrastructure Security.	Bachelor of Engineering / Bachelor of Science	Web Application Firewalls Intrusion Prevention Systems Routing and L2 Switching URL Filtering Proxy Next Generation firewalls (Checkpoint, Cisco ASA/Firepower, Fortigate, Palo Alto etc.) Vulnerability assessment Load Balancing	Certified Ethical Hacker (CEH) or Certified in Cyber Security (CC) and /or Any SIEM / Firewall / ADC / EDR-XDR OEM certified.

				SSL Virtual Private Network (Juniper, Array, F5, Cisco, Checkpoint etc.) Anti-Virus (Trend Micro OfficeScan/Apex One and Symantec Endpoint Protection etc.) • Single Sign on Patch Management (Windows Server Update Services) Ticketing Tool	
5	Security Consultants – Active Directory Management	03 years of experience in Active Directory and SCCM Management	Bachelor of Engineering / Bachelor of Science	Experience in Installing, Managing and Configuring Domain Controller Maintain DNS Systems administration support Windows System Administration Skills Experience in creating create script in Batch, Powershell Experience in Promotion/decommission of domain controllers Plan and implement migration, upgrade /Updates /patching	Microsoft Certified IT Professional (MCITP)

BIDS PREPARATION AND SUBMISSION DETAILS

The online bids will have to be submitted within the time specified on website https://gem.gov.in/ . Bidders must familiarize (if not already) with the Portal and check/ fulfil the pre-requisites to access and submit the bid there.

1. Submission of Bids

a. The required documents for Eligibility Criteria, Commercial Bid must be submitted (uploaded) online on GeM portal. Eligibility Criteria and Commercial Bid should be complete in all respects and contain all information asked for in this RFP document

b. The offer should be valid for a period of at least **90 days** from the date of submission of bid.

c. The Bidder shall fulfil all statutory requirements as described by the law and Government notices. The Bidder shall be solely responsible for any failure to fulfil the statutory obligations and shall indemnify StockHolding against all such liabilities, which are likely to arise out of the agency's failure to fulfil such statutory obligations.

d. The bidders are expected to examine all instructions, forms, terms, project requirements and other information in the RFP document(s). Failure to furnish all information required as mentioned in the RFP document(s) or submission of a proposal not substantially responsive to the RFP document(s) in every respect will be at the bidder's risk and may result in rejection of the proposal.

e. Delayed and/or incomplete bid shall not be considered.

f. There may not be any extension(s) to the last date of online submission of Eligibility Criteria details and commercial Price bids. This will be at the sole discretion of StockHolding.

2. Evaluation of Bids

StockHolding will evaluate the bid submitted by the bidders under this RFP. The eligibility bid submitted by the Bidder will be evaluated against the Eligibility criteria set forth in the RFP. The Bidder needs to comply with all the eligibility criteria mentioned in the RFP to be evaluated for evaluation. Noncompliance to any of the mentioned criteria would result in outright rejection of the bidder's proposal. The decision of *StockHolding* would be final and binding on all the bidders to this document.

StockHolding may accept or reject an offer without assigning any reason what so ever. The bidder is required to comply with the requirement mentioned in the RFP. Non-compliance to this may lead to disqualification of a bidder, which would be at the discretion of *StockHolding*.

a. Please note that all the information desired needs to be provided. Incomplete information may lead to non-consideration of the proposal.

b. The information provided by the bidders in response to this RFP document will become the property of StockHolding.

Evaluation Process

First the 'Eligibility Criteria bid document' will be evaluated and only those bidders who qualify the requirements will be eligible for 'Technical bid'. In the second stage, for only those bidders who meets the 'Eligibility Criteria', technical bids will be evaluated, and a technical score would be arrived at. In third stage, only those bidders, who have qualified in the technical evaluation, shall be invited for commercial evaluation.

Eligibility Criteria Evaluation

The bidder meeting the Eligibility Criteria as per **Annexure 2** will be considered for Technical evaluation. Any credential/supporting detail mentioned in "Annexure 2 – Eligibility Criteria" and not accompanied by relevant proof documents will not be considered for evaluation. All credential letters should be appropriately bound, labelled and segregated in the respective areas. There is no restriction on the number of credentials a bidder can provide.

Technical Bid Evaluation

The Technical bids of only those bidders shall be evaluated who have satisfied the eligibility criteria bid. *StockHolding* may seek clarifications from the any or each bidder as a part of technical evaluation. All clarifications received by within stipulated time shall be considered for evaluation. In case a clarification is not received within the stipulated time, the respective technical parameter would be treated as non-compliant and decision to qualify the bidder shall be accordingly taken by the *StockHolding*.

The proposal submitted by the bidders shall, therefore, be evaluated on the following criteria:

Sl. No	Parameter	Scores	Qualifying Scores	Max Scores
A. BASED ON EXPERIENCE, TURNOVER & RESOURCE STRENGTH (70 MARKS)				
1	Average annual turnover of the bidder during last 03 (three) years (i.e. 2022-23, 2023-24 and 2024-25)	• 14 Crores >= 25 Crores : 10 Marks • >25 Crore but <= INR 50 Crore : 12 Marks • More than INR 50 crore : 15 Marks	10	15
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	10	15

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	5	10
3	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	10	15
4	Bidder having a ISO 27001 Certified SOC functional in India as on RFP date	• 5 Years : 7 marks • More than 5 Years - <= 8 Years : 8 Marks • More than 10 Years : 10 Marks	7	10
5	Bidder having CERT-In Empanelled as on RFP Date	• Not empanelled – 0 Marks • Less than or equal to 3 Years – 3 Marks • More than 3 Years : 5 Marks	3	5
B. BASED ON PROPOSED SOLUTION, APPROACH & PRESENTATION (30 MARKS)				
6	Bidder's technical presentation	• Understanding of the Project requirements • Bidder's SOC Capabilities • Relevant Experience • Proposed Solution for StockHolding • Approach and Methodology • Resource Deployment Plan • Proposed Project Manager / Team lead / resources experience & skillset • SLA Management Framework	15	30

Note:

- The bidder is required to provide documentary evidence for each of the above criteria.
- StockHolding shall verify the credentials submitted with the respective issuer and understand the credentials claimed for the purpose of evaluation and awarding marks.
- The bidder to submit appropriate credentials [other than self- certification] in respect of each of the item.
- The technical score will be allotted by StockHolding to each bidder against each section and will be considered final. Cumulative score of 60 marks in the Technical evaluation needs to be achieved.

Commercial Bid Evaluation (Stage 3)

The Commercial offers of only those Bidders, who are short-listed after technical evaluation, would be opened.

Best Value Bid Determination and Final Evaluation (Stage 4)

A composite score shall be calculated for those bidders whose bids are found to be in order.

The weightage for the composite evaluation is as described below:
a. Technical – 70%
b. Commercial – 30%

For Quality and Cost based Evaluation (QCBS), the following formula will be used for evaluation of the bids

Bn = 0.7 * (Tn/Thigh * 100) + 0.3 * (Cmin/Cb * 100)

Where;
Bn = Overall score of bidder under consideration
Tn = Technical score for the bidder under consideration
Thigh = Highest Technical score achieved against criteria among all eligible bids
Cb = Evaluated Bid Cost (as calculated above) for the bidder under consideration
Cmin = Lowest Evaluated Bid Cost (as calculated above) among the financial proposals under consideration.

The bidder achieving the maximum overall score will be selected for the project.

REQUIREMENT

Stockholding inviting bids from firm/company/organization who has proven experience in the implementation, integration and managing of StockHolding's Security Operation Centre (SoC) for the period of 02 (two) years.

Scope of Work (SOW)

StockHolding Corporation of India Limited (StockHolding) is floating a request for proposal for MSSP (Managed Security Service Provider) to provide managed security services (MSS) / Security Operation Centre (SoC) Operations management from Stockholding's Data Centre locations. Over the years, StockHolding has been scaling up as well as planning to scale up its cyber defense by deploying various technological controls like Cloud based Security Information and Event Management (SIEM), Managed Detection and Response (MDR) Services, Web Site Scanning Suite (WSS), Anti-phishing, Brand Monitoring and Brand Protection, Deep and Dark Web Monitoring, Next Generation (NGX) Firewalls, Intrusion Prevention System (IPS), Virtual Private Networks (VPN), Distributed Denial of Service (DDOS) Mitigation, Web Application Firewall (WAF), Hybrid Proxy Management, Endpoint Detection and Response (EDR), Data Leakage Protection (DLP), Application Delivery Controller (ADC), Management and maintenance of Secure Active Directory and Patch Management SCCM onsite setup and so on.

StockHolding is seeking a 24x7 managed service that can detect and respond to advanced cyber threats from both fast-moving threats such as ransomware, worms and from deliberate slower attacks that result in data exfiltration and threat. Additionally, MSSP must provide consulting services like Secure Network Architecture (SNA) activity, Risk Assessment and Risk Treatment, Remote Exposure Assessment, Policy and Procedure review etc. as per the detail methodology and deliverables mentioned in the RFP document. StockHolding also expects MSSP must conduct security testing activities like configuration audits, Internal and external Vulnerability assessments and penetration testing activities, Internal and External Red Team Assessment as per the detail methodology and deliverables provided in this RFP document.

Considering all these factors, StockHolding has bundled various services and Included a detailed scope of work in each of these services in the request for proposal (RFP) for SOC Services to be provided to StockHolding for a period of 02 (two) years. StockHolding may choose to extend the contract period for another one (01) year.

Understanding of Scope

Device Management:

Typical Daily Operation: The objective of device management service is to align cybersecurity operations and governance with existing and new initiatives. The operations include:

- Ensure updates for protection from the evolving threat landscape.
- Understand & mitigate risks present in the environment.

- SOC Internal planning, operations and maintenance of infrastructure devices.

Examples of Typical daily activities performed by the Device Management team for daily operations are listed below:

Perimeter Security / Branch Firewall

- Regular rule addition, modification on perimeter devices as per the request received from StockHolding team.
- Handling Change request with respect to Production, Pre-production or UAT environment post necessary approvals.
- Daily troubleshooting task related to any incident reported, pertaining to perimeter devices.
- Regular Backup Maintenance.
- Sharing regular health status-related reports which include status on CPU, Memory and disk utilization.
- Co-ordinate with stakeholders for Upgradation of devices based on new firmware available and also involving vendor support in critical cases.
- Vendor support handling for critical issues by creating, keeping records and continuous follow-up on cases related to support.
- Implementing NAT related policies on the firewall.
- Security Auditing and review of Perimeter devices.
- Creation, modification of new IPSEC tunnel/SSL VPN on the firewall.
- Performance configuration, tuning, and management.
- Coordinating with stakeholders for an understanding of new set-up of any technologies or any new changes in infrastructure and provide recommendation according to that.
- Capacity Planning of the SoC Infrastructure.
- Reporting unexpected trends observed on perimeter devices.
- Performing blacklisting of domains and IP addresses which are threats to the organization, based on data received from SOC analysis.

End point Security (On-premise and/or Cloud based)

Currently StockHolding has cloud based Endpoint detection and response (EDR) solution from Crowdstrike. MSSP services should be compatible with both cloud as well as on-premise (EDR-XDR). Following activities as a part of EDR and XDR Solution has been highlighted to be performed by on-premise device management team.

- Prepare Daily, Weekly, Monthly compliance reports.
- Co-ordinate with stakeholders for Upgradation of Servers / devices on the basis of new version upgrades / firmware available and also involving OEM and vendor support in critical cases.
- Sharing health status related reports which include status on CPU, Memory and disk utilization (on premises).
- Vendor support handling for critical issues by creating, keeping records and continuous follow-up on cases related to support.

- Incident management, Troubleshooting, and break-fix for devices.
- Management of installation/uninstallation, updation of end point agents,
- Daily/Weekly/Monthly & Ad-hoc and scheduled reporting for management and technical team.

Crowdstrike Endpoint Detection and Response: Cloud EDR Deployment & Maintenance:

- Deploy and maintain Crowdstrike EDR agents across cloud workloads (VMs, containers etc.)
- Ensure workloads remain updated with the latest antivirus patterns and detection rules.
- Leverage cloud-native integration with private cloud platforms like VMware & Oracle PCA for seamless agent deployment and monitoring.
- Protect endpoints (on or off-network) from malware, trojans, worms, and ransomware.
- Adapt to evolving threats by using real-time threat intelligence.
- Automate responses like quarantining instances or blocking malicious IPs to reduce downtime.
- Use Indicators of Attack (IOAs) and behavioural analysis rules to detect file-less attacks and advanced threat indicators.
- Perform sweeping searches using IOCs or YARA rules for indicators like malware signatures, registry modifications, or running processes.
- Develop custom attack discovery rules to identify threats proactively.
- Conduct detailed RCA to identify the origin of the threat, patient zero, and its spread.
- Contain compromised resources by isolating or halting cloud instances and blocking malicious credentials or IPs.
- Create post-incident RCA reports detailing the findings and resolutions.
- Consolidate and analyze logs from all endpoints (Windows, Linux servers) via a unified dashboard.
- Assess the full impact of threats, including compromised users, systems, and lateral movement.
- Automate workflows for rapid detection and mitigation before sensitive data is lost.
- Prevent data exfiltration by monitoring and blocking unauthorized data transfers.
- Secure critical data in motion and at rest within cloud or hybrid environments.
- Protect against vulnerabilities using virtual patching for both cloud and legacy systems.
- Limit executable and application access to reduce the attack surface.
- Use Server Protect for Windows/Linux and Deep Security for AIX workloads to ensure consistent coverage.
- Prioritize and investigate high-priority alerts within SLA parameters.
- Collaborate with stakeholders to resolve incidents and ensure timely communication.
- Automate response measures like instance quarantine, forensic snapshot capture, or credential rotation.

- Minimize the attack impact by providing support for integrating EDR with SIEM/SOAR platforms for faster resolution.
- Generate regular security reports highlighting threats, response metrics, and overall system health.
- Update detection rules and security playbooks based on lessons learned from previous incidents.

Web Application Firewall (On-premise and/or Cloud based WAF)

- Creating new policies as per the requirement from StockHolding.
- Creating change tickets and implementing changes by taking approval on POA.
- Performance configuration, tuning, and management.
- Regular Backup Maintenance.
- Managing Certificate status on individual WAF.
- Troubleshooting of incidents reported from the StockHolding end.
- Performing blacklisting of domains and IP addresses which are threats to the organization based on the data received from SOC analysis and whitelisting of the domain.
- Analysis of frequent attack alerts on WAF and share it with the stakeholder on a regular basis.
- Coordinate with stakeholders for upgrade of devices based on new firmware available and also involving vendor support in critical cases.
- Vendor support handling for ALL issues by creating, keeping records and continuous follow-up on cases related to support.

Email Security (On-premise and/or Cloud based)

- Check mail content, Mail body /subject for Suspicious content such as Profanity, Racial content, sexual content, Social engineering attempts.
- Blacklisting of Domain and IP address of the sender on E-mail security products on the basis of reputation on various threat investigation portal.
- Verifying the attachments and web links embedded in the mail on portals like as "virustotal.com" & "ipvoid.com"
- Addition of transport rules on Email security gateways for better security from attacks like Spoofing.
- Categorization of attacks after analyzing the email contents and sharing the consolidated data to customer weekly.
- Co-ordinate with OEM and support for critical issues.
- Header analysis of mail which includes originating Source IP, DMARC, SPF value, the domain name for better understanding the attacks and then suggesting appropriate steps to the stakeholders for remediation.
- Analyzing of mail and sharing relevant remediation steps in the form of Advisory mail to users directly.
- Coordinate with stakeholders for upgrade of devices based on new firmware available and also involving vendor support in critical cases.

Application Delivery Controller (ADC) Appliances

- Creating change tickets and implementing changes by taking approval on POA.
- Performance configuration, tuning, and management.
- Regular Backup Maintenance.
- Managing Certificate status on individual WAF.
- Troubleshooting of incidents reported from the stakeholder end.
- Coordinate with stakeholders for upgrade of devices based on new firmware available and also involving vendor support in critical cases.
- Vendor support handling for all issues by creating, keeping records and continuous follow-up on cases related to support.

On Premises Hybrid and/or Cloud Based Proxy Support

- Creating new policies as per the requirement from StockHolding.
- Creating change tickets and implementing changes by taking approval on POA.
- Performance configuration, tuning, and management.
- Regular Backup Maintenance.
- Managing Certificate status on individual proxies and Cloud based proxies.
- Support to on-premise users for proxy support and remote users with Hybrid proxy support.
- Co-ordinate with OEM and support for critical issues.
- Coordinate with stakeholders for upgrade of devices based on new firmware available and also involving vendor support in critical cases.

Data Security

- Analyzing incidents daily and share with the stakeholders on a regular basis.
- Tracking and verifying regular Backup Maintenance.
- Creating new policies as per the requirement from customer.
- An incident, Troubleshooting, and break-fix for devices.
- Co-ordinate with Vendor supports for critical issues and keep track of it for an immediate closure of issues.
- Integration with multiple channels like email, endpoints, etc. for monitoring and analyzing incidents.

Active Directory Management (Standalone as well as on Private cloud deployment)

- Installation and Configuring Domain Controller.
- Maintain Domain Name Services (DNS) and Lightweight Directory Access Protocol (LDAP) databases.
- DNS Scavenging & Aging
- Experience with system monitoring, design, maintenance, and administration duties
- Demonstrated Windows System Administration Skills (Windows 10)
- Ability to create script in Batch, Powershell
- DNS server Health check
- Promote/demote of domain controllers.

- Plan and implement migration, upgrade /Updates /patching.
- Sound Knowledge on PKI infra management, Certificate infra management
- Domain controller health monitoring, Backup and restore
- Configure and Manage Active Directory Site and Services.
- Configure & Manage Active Directory and Group Policy.
- Migration active directory to latest version as and when applicable.
- Deployment of group policies as per business requirement.
- Deployment of hardening settings via group policies to UAT and production servers.
- User account creating, unlocking, and password reset from the active directory.
- Active Directory Recycle Bin
- Enabling and disabling user account and system host from the active directory.
- DNS record creation and modification activity like Host A Record, PTR, CName
- Object creation and domain joining in active directory and support AD client application support.
- Participate in DR activities AD
- Maintain incident management, Change Management and SOPs.
- Server integrate in domain and reboot, Migration of SOC servers in Domain.
- Checking the replication of all ADC on daily basis.

Microsoft System Centre Configuration Manager (SCCM) – (Standalone as well as on private cloud deployment)

- Configuration and management of Windows operating systems and installation/loading of operating system software.
- Experience with System monitoring, design, maintenance, and administration duties.
- Demonstrated Windows System Administration Skills (Windows 10)
- Application installation
- Manage patching of virtual and physical servers with windows server OS
- Plan and implement migration, upgrade /Updates /patching.
- SCCM Infrastructure health monitoring
- SCCM server backup and restoration.
- Microsoft windows server patching (Server Patch management)
- Maintain incident management, Change Management and SOPs.
- PAN India Providing technical support (software installation)
- Updating servers with latest service packs and hot fixes.
- Knowledge on SCCM upgrade/Migration and site implementation
- Periodical health checks of SCCM environment and site backup.
- Troubleshooting SCCM infrastructure, primary server and SCCM client remediation
- Monthly patch testing on UAT systems, installation of SCCM client, SCCM Client Upgradation Policy
- Monthly patch deployment on production endpoints, Monthly patch testing and deployment on uat servers
- Troubleshooting on no client and unhealthy endpoints and servers
- Software distribution and OSD/Win10/Win11 servicing process.

- Experience in Feature upgrades /IN place upgrade
- Experience in Baseline configuration
- Deploy all software from SCCM tools
- patch Management with SCCM, WSUS
- SCCM package, SCCM backup monitoring
- Power Plan policy to disable sleep mode and wake-on on endpoints
- Report Administration i.e. Installed software and Hardware reports
- Preparing customized reports in SCCM console and SQL

Dynamic Host Configuration Protocol (DHCP) deployment - (Standalone as well as on Private Cloud Environment)

- Configuration of DHCP Server
- Maintains a pool of IP addresses and leases an address to any DHCP-enabled client
- DHCP server health monitoring, Backup and restore
- Create, delete, and manage different areas of the server's scope
- Experience with system monitoring, design, maintenance, and administration duties
- Demonstrated Windows System Administration Skills (Windows 10/Windows 11)

Support for Secure Network Virtualization NSX-T/NSG with VMware/Oracle PCA for StockHolding's private Cloud

- NSX-T Distributed Firewall Policy configuration via Firewall Rule table, using GUI or REST API via NSX-T Manager.
- Static & Dynamic grouping based on compute objects & Tags.
- Enforce FW rules regardless of network transport -Overlay or LAN
- vMotion-Policy move with VM
- Simplified UI & Workflows with categorise available for Distributed firewall and Gateway firewall.
- Configuration of Global rules – AD, DNS, NTP, DHCP, Backup, Mgmt Servers.
- Rules between Zones – Production V/s Development, PCI v/s Non PCI, Inter BU rules.
- Rules between Apps, App tiers or the rules or between Micro-services.
- NSX integration with SIEM-MDR platform and creation of use cases as per the requirements

SOC Operations:

MSSP 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. MSSP will develop documents such as Standard Operating procedures for smooth functioning of SOC.

MSSP will coordinate and assist MDR Service provider to establish full featured cloud based Managed Detection and Response (MDR) Services along with Incident Management capabilities. In future, MSSP will configure and integrate Database Activity Monitoring (DAM), Privileges Identity Management (PIM), any other new security device, and Cloud based services in consultation with StockHolding and MDR team to generate meaningful

incidents/reports and reduce the generation of false positives and operate the SOC Operations. MSSP will manage SOC operations in consultation with StockHolding's team.

StockHolding will also have a right to use the services of the tools from different locations. MSSP has to keep a note of the same and integrate the devices from centralized location.

StockHolding reserves the right to get the SOC services audited once in a year by external CERT-In empaneled auditor.

Functional Principles

The intent for SOC device management is covered in the below functional principles:

- Device Management, Prevention & Identification of Information Security Vulnerabilities: The SOC device management solution should be able to identify information security vulnerabilities in StockHolding's environment and prevent these vulnerabilities.
- Incident Management: Reporting of information security incidents through the use of appropriate tool centrally managed dashboard to track and monitor the closure of these information security incidents and escalation of these incidents to appropriate teams/ individuals in StockHolding.
- Continuous Improvement: Continuously improve SOC device management / Services / Solutions.

Scalability Principles

The services/ solutions offered are modular, scalable, and are able to address StockHolding's equipment during the period of contract.

Availability Principles

The services/ solutions in scope designed with adequate redundancy and fault tolerance to ensure compliance with SLAs for uptime as outlined in this RFP.

Performance Principles:

The services/ solutions offered should not have any significant impact on the existing Infrastructure/business of StockHolding either during integration or during operation of SOC. Based on the above principles, the following services/ solutions have been identified to enhance the security posture of StockHolding:

- Security Intelligence Services.
- Security Advisory Services.
- Anti-Malware Services.

Devices under Scope of Device Management

Devices		Mahape	Bangalore	Fort	Branches
Application Delivery Controllers (ADC Appliances)		3	2	0	0
Checkpoint Firewall Management		1	1	0	0
Cisco FMC		1	1	0	0
Forti Manager & Analyzer		4	0	0	0
Firewall Appliances	Checkpoint	4	4	0	0
	Cisco FPD	4	2	2	0
	Fortinet	4	0	1	14
Email Security Appliance Cisco IronPort		1	1	0	0
Imperva WAF Management		1	0	0	0
Imperva WAF Appliance		1	1	0	0
Array VPN Appliances.		2	2	0	0
Linux Servers					
Tenable SC		1	0	0	0
Nessus Scanner		1	0	0	0
Nessus Manager		1	0	0	0
Force point Proxy Gateway		2	1	0	0
Syslog Server		1	1	0	0
SIEM LEC server		1	0	0	0
SIEM Logger server		1	1	0	0
Windows Servers					
Smart protection Server		1	1	0	0
DSM Database		1	1	0	0
Force point Proxy Management		1	1	0	0
SIEM LEC server		1	1	0	0
Active Directory Management		2	1	0	0
SCCM		1	1	0	0
DHCP		2	0	0	0
Total Number of devices		**43**	**23**	**3**	**14**

Note:

1) The above OEM brands are as of now in production in StockhHolding's environment. The OEM brands are subject to change in the near future.
2) Some of the above devices may move to a cloud based solution in the near future.
3) The above devices mentioned are as on today deployed. This count may increase/decrease in the near future to the extent of 10% variation to the existing count.

Security Testing

Sr. No.	ACTIVITY	SCOPE	FREQUENCY
1	Network Penetration Testing	Internal - Up to 200 IP Addresses	Twice a Year (2 Initial Test + 2 Confirmatory Test)
2	Firewall rule base review - To be performed by device Management team.	Checkpoint – 2; Cisco FPD – 8 and FMC – 2	Twice a Year (2 Initial Test + 2 Confirmatory Test)
3	Red Team Assessment (Internal + External)	Internet facing and Internal Assets	Once a Year (Initial +Confirmatory)
4	Cyber Security Drill (Hybrid Scenario based Drills)	IT Assets	Once a Year (Initial +Confirmatory)
5	Remote Exposure and Breach Assessment (External + Internal)	IT Assets	Once a Year (Initial +Confirmatory)
6	SOP Review	In-Scope Devices	Device Specific on Monthly basis. (Initial + Confirmatory)
7	Configuration Audit (CA), Vulnerability Assessments (VA) & Penetration Testing (PT) - (As per CIS Benchmark and close the gap's and provide the clean report)	200 IP addresses	Twice a Year (2 Initial Test + 2 Confirmatory Test)
8	IPS Review - To be performed by device Management team.	On Firewall blades	Once a Year (Initial +Confirmatory)
9	AdHoc network security assessment	Up to 5 IP Addresses / 5 Apps in a year PT: 5 IP's Black / Grey Box Scan – app – 5 apps	Twice a Year (2 Initial Test + 2 Confirmatory Test)
10	Vulnerability Assessment and External PT (With White listing and Without White listing)	50 IP Addresses + Additional 10	Twice a Year (2 Initial Test + 2 Confirmatory Test)
11	Adhoc Revalidation post any planned / unplanned audits findings implementation	Up to 10 Units PT	Initial Test + Confirmatory
12	Report Analysis	VA PT Audits (Initial and Confirmatory)	Quarterly / Half yearly
13	Backup and Restoration.	In-Scope Devices	Device Specific Monthly rotation.

14	Network and Network-Security devices Failover Testing as per calendar schedule.	In-Scope Devices	Monthly
15	BAS (Breach and Attack Simulation)	200 IP addresses	Upto twice in a year
16	CART(Continuous Automated Red Teaming	200 IP addresses	Upto twice in a year
17	Honey pot Exercise		Upto twice in a year
***Mode - Any testing/activity, if internal, independent team should conduct it onsite. If external, independent team should conduct it off site.**			

Consulting Services

Sr. No.	ACTIVITY	SCOPE	DELIVERABLES	FREQUENCY	LOCATION
1	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.	200 IP Addresses	SNA Report	Onsite & Yearly	Navi Mumbai
2	Risk Assessment of network security devices on yearly basis and reporting with proper analysis with industry supported guidelines.	200 IP Addresses	Risk Assessment Report	Onsite & Yearly	Navi Mumbai
3	Ensuring adequate, appropriateness and concurrency of	15 Policies & Procedure s to be reviewed &	15 Policies & Procedures to be reviewed & 5 new	Onsite & Yearly	Navi Mumbai

	various policies and guidelines in place and shall provide Information Security consultancy for newer technology deployment for new and existing applications and products.	5 new policies and procedures Development	Policies Development		
4	Assisting StockHolding in planning, execution, and implementation of information security related initiatives / projects / Preparation of request for proposals programs in StockHolding.	Handholding & Assistance to StockHolding in implementing Information Security	Advisory Support	OffSite / Onsite & Monthly	Navi Mumbai
5	Cyber Security Drill	IT Assets	No Table Top exercised. Scenario based Drill Live Simulation	Onsite & Yearly Once	Navi Mumbai
6	Remote Exposure and Breach Assessment	IT Assets		Onsite & Yearly Once	Navi Mumbai
7	Active Directory Risk Assessment Programme (AD RAP) Assessment	Active Directory & Related Setup	AD RAP Assessment Report	Onsite & Half Yearly Once	Navi Mumbai
8	Secure Active Directory , DNS and DHCP Setup Management	IT Infrastructure Assets	User Management. Group Management. Policy Management. DNS Management. DHCP Management. Managing Site. Managing Trust.	Ongoing with Onsite Team	Navi Mumbai

			Managing Forest. Managing FSMO roles. Managing Replication. Remote user logon permissions.		

Note: Any modifications in security testing's and consulting services as per the compliance requirement, needs to adhered and factored. Policies count may vary in the future upto variation of 10%.

Deliverables for Security Testing

Network Penetration Testing – External/Internal

SERVICE HIGHLIGHTS

- Provides hacker's view of network vulnerabilities in organizational assets.
- Comprehensive methodology from Information Gathering, Fingerprinting to Vulnerability Detection, Exploitation and Reporting.
- Tool driven automated scans for discovering breadth of security issues.
- Expert executes in-depth manual penetration exploit steps.
- Detailed Solution Repository for different technology platforms.

SCOPE

Public & Internal IP address count or Net Blocks as documented during estimation process

METHODOLOGY

REPORT EXPECATION: A Penetration Testing Report containing Executive Summary, Vulnerability Details with screenshot evidences, Impact, Risk Rating, case-specific Solutions and Good Reads.

Frequency: This activity required to be perform on half-yearly basis with confirmatory to be perform 3 months after initial assessment report.

Vulnerability Scanning

SERVICE HIGHLIGHTS

- Automated Scans performed for faster turn-around cycle.
- Scan option is available in both authenticated and un-authenticated mode.
- More information like missing patches, confirmation of certain potential vulnerabilities is possible with authenticated mode.
- Assurance that basic VM program is in place and basic security level is complied.

METHODOLOGY

SCOPE: All IP addresses as documented during initiation process.

REPORT EXPECTATION: A Network Vulnerability Scan Report containing Executive Summary, Vulnerability Details, Impact, Risk Rating and Solutions in excel as well as in pdf formats. This activity required to be perform on yearly basis with review of action taken on last year's assessment report.

Configuration Review- Nessus Based Compliance Scan

APPROACH: Configuration Audit will be done against CIS Derived Controls. Customization of CIS benchmarks is out of scope.

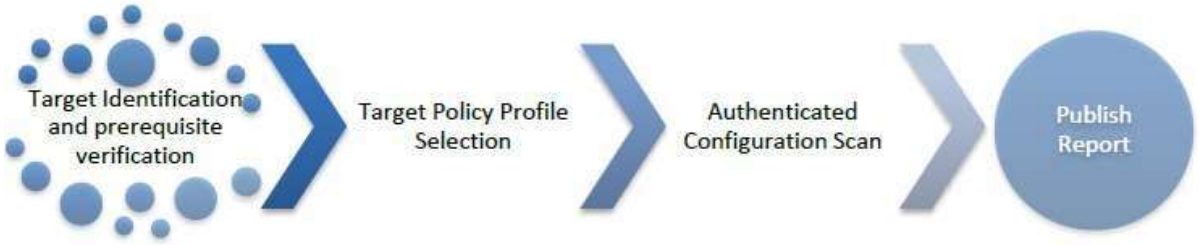
Assumptions: Bidder is allowed to setup and run Nessus scanner. Provide required pre-requisites for each system to be reviewed.

List of activities	Deliverables
Implementation of software	

Testing scan prerequisites	Scan report for each system with the indication of noncompliant settings as compared to CIS Benchmarks and recommended fixes/settings to secure the system
Scanning of target systems	
Report generation	

AUTOMATION APPROACH FOR SECURITY CONFIGURATION AUDIT

Configuration Audit is a process to identify insecure features present in the system & the configuration settings for devices (such as servers, databases, routers, etc.). These insecure features are detected by performing scans using Nessus. Exhaustive methodology is used to perform these scans. Authenticated Configuration Scanning process as shown below.



STEP 1: TARGET IDENTIFICATION

First step is to identify the scan targets with the platform and verify scan prerequisites. The outcome of this step is:

- Identification of Asset Type \ Platform
- Verification of
  - Network Connectivity
  - Credentials
  - Other configuration details (like instance name etc.)
- In this step, valid administrator credentials will have to be supplied in Nessus.
- If prerequisite verification stage is passed, then the target is ready for scanning.

STEP 2: TARGET POLICY PROFILE SELECTION

Depending upon the platform of target a base policy profile will be selected which includes Policy Profile Selection for target

STEP 3: AUTHENTICATED CONFIGURATION SCAN

Using Nessus, configuration scan is scheduled which takes some time to collects the value of technical controls (configuration settings) from target and compares them against a selected policy baseline; and provides compliance reporting by leveraging a comprehensive knowledgebase that is mapped to prevalent security regulations, industry standards and compliance frameworks. The knowledge base of the tools is updated regularly.

STEP 4: PUBLISH REPORT

A detailed report is prepared for the verified scan results. The vulnerabilities identified are detailed with description, severity level, solution details etc.

PRE-REQUISITES FOR SCANNING

- IP addresses of the server / device
- Nessus needs to be provided with Administrator Username & password of each server/ device (OS, DB etc.)
- Nessus needs complete access to the servers that are behind firewalls over required network protocols.
- Few more settings on servers need to be adjusted (only for scan duration) to enable successful scanning by tools (e.g. Group Policy, powershell enablement, services tweaking etc.).
- RDP access on the server where Nessus is installed to login and perform the scans.

Report Expectation: A CONFIGURATION REVIEW Scan Report containing Executive Summary, Vulnerability Details, Impact, Risk Rating and Solutions in excel as well as in pdf formats.

Frequency: Please refer to the Table '**Security Testing – Point 10'** on Page 27 for details.

APPLICATION PENETRATION TESTING- GRAY BOX

SERVICE HIGHLIGHTS

- Detect Application level vulnerabilities via Gray Box approach.
- Application specific Threat Profile.
- OWASP Top 10 attacks like Injection flaws, XSS,
- Authentication, and Session flaws etc.
- Leverage both open source tools and commercial tools.
- Employs manual testing on top of automated tools for specific test cases like business logic bypass.

METHODOLOGY

SCOPE

- Scope of this test is to discover web application vulnerabilities in the application under scope.
- A gray box test scope includes all internal protected pages and the APIs that are reachable from the web application front end.

REPORT EXPECTATION: Application Security Testing Report containing Executive Summary, Vulnerability Details with screenshot evidences, Impact, Risk Rating, Solutions and Good Reads.

Frequency: This activity required to be perform on yearly basis with review of action taken on last year's assessment report.

FIREWALL RULEBASE REVIEW

SERVICE HIGHLIGHTS

- Review of the configured Firewall Rule base to discover common configuration weaknesses
- Assurance via audit approach that the firewall basic security level is complied

METHODOLOGY

SCOPE: All Firewalls (and rule counts) as documented during initiation process.

REPORT EXPECTATION: A Firewall Rule based Review Report containing Insecure Rules, its Impact and Solutions.

Frequency: This activity required to be perform on half-yearly basis with review of action taken on last assessment report.

RED TEAM ASSESSMENT

SERVICE HIGHLIGHTS

- Provides a holistic view of organization's potential for a security breach.
- Emulates real world attack scenarios that spread across the gamut of people, process and technology of an organization to achieve defined objectives
- Comprehensive MITRE ATT&CK framework-based methodology that delivers a controlled, bespoke, intelligence driven security test
- Enhances visibility into effectiveness of security controls leading to better ROI
- Help improve detection and response capabilities of the SOC.

Scoping for Internal Red Team Assessment

- Compromise Active Directory and upto 2 Critical Applications.
- Compromise any one of the cloud services setup and configured by the client.
- Perform Data Exfiltration from compromised applications/ Servers.
- Attempt to erase logs from the compromised systems.

METHODOLOGY: The primary intent of an organization to perform a Red Team Assessment is to understand the current weaknesses in the environment that could allow an attacker to breach the network and applications. To meet this intent, bidder needs to first define a set of objectives that are to be achieved to measure the outcome of the Red Team Assessment.

The typical objectives recommend to organization are:

- Test effectiveness of existing security controls
- Test detection and response capabilities
- Test effectiveness of response procedures

REPORT EXPECTATION:

- A detailed Technical report covering Executive summary, List of vulnerabilities with severities, Impact and ease of exploitation of each finding, List of exploits attempted and their status, Screen shots / Proof of concepts wherever possible and Recommended solutions.
- Status updates shall be provided over an email.

Frequency

- This activity required to be perform on yearly basis with review of action taken on last year's assessment report.

RED TEAM OBJECTIVES

#	Domain / Area	Target Objectives	Evidence Example
1	Identity and Access Management	Access to a Domain Admin Account	Change a user's properties / Add a new user account/ Screenshot
2	Communication Infrastructure	Compromise Email Infrastructure	Send Phishing emails from a company Internal account
		Compromise Messaging Infrastructure	Send messages with malicious links from a legitimate account

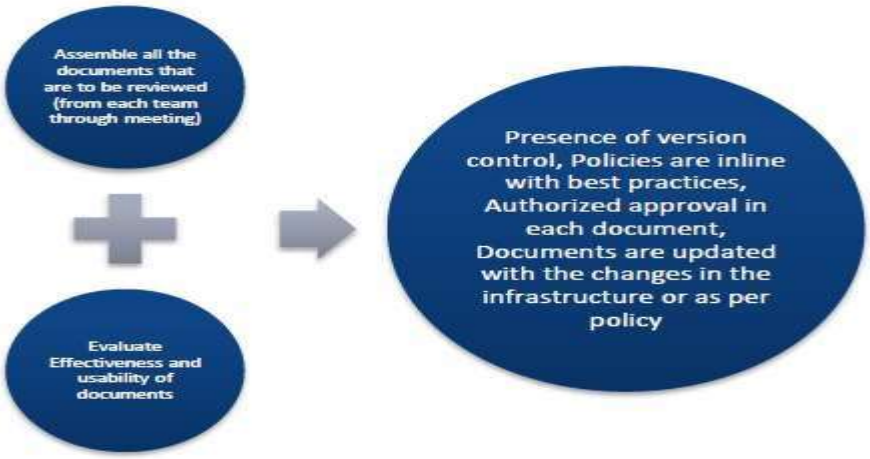
3	Compromise Internal Collaboration Portals.	Privileged access to Cloud portal	Access to restricted content / Portal admin access / Host malicious files.
4	Security Infrastructure	Privileged Access to IPS	Privileged Access to IPS Logs
		Access to SIEM	Access to Collected Logs
		Privileged access to Perimeter Firewall	Firewall admin access screenshot.
5	Internal Project Management Systems	Access to Sensitive Corporate Data	Account admin access / Portal admin access / Record tampering / Access to financial reports or customer details
6	Network Routing Infrastructure	Privileged access to DNS servers	Poison DNS with a malicious record
		Privileged access to edge routers	Root access
7	Enterprise Segregation Controls	Access sensitive systems	Sensitive systems' contents
8	Transaction Systems	Compromise Transactional Systems	Access to tamper with inputs for transactional systems
9	Customer PII	Compromise PII in RM (Relationship management) systems	List of PII database / table
10	Source Code Control	Code change access to source code repository	Tampered dummy source code file in the repository

CONSULTING SERVICES & DELIVERABLES

METHODOLOGY: Bidder has to follow a approach for performing review & redrafting of the policies and procedures, as depicted below

Process Study: The scope of assessment needs to be defined clearly in terms of organizational units and the internal/external parties that interact with the structure, processes, people & technology. SPOCs will be identified from each team for effective coordination.

Policy Review: All relevant documents will be identified and collected from each department during the course of discussions after which, review of these documents will be carried out.



The policies and processes will be studied and its understanding and adequacy will be assessed as part of the document review activities. As part of the documentation review, all policies, processes and records will be identified and reviewed.

Policy Validation: After the policies and procedures are assessed against worldwide standards such as ISO 27001:2013, ISO 27001:2022 etc. and industry best practices, all the identified gaps and recommendations for the same will be documented in a draft report for the purpose of discussion with the management. After obtaining approval on the same, the corresponding changes will be made in the policies. The validated policy drafts will be presented to the management and upon their approval, the drafts will be finalized.

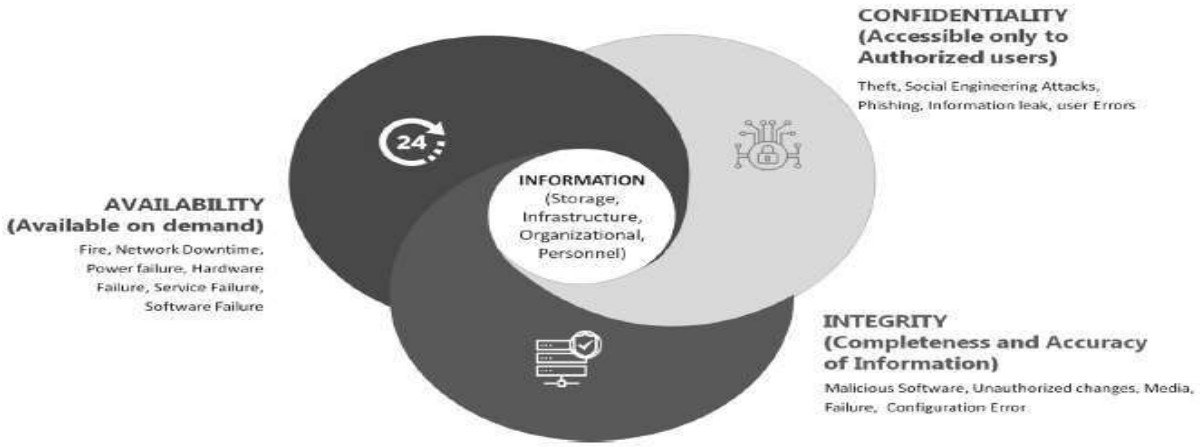
REPORT EXPECTATION: Reviewed and Updated Policies.

Frequency: This activity required to be perform on yearly basis with review of action taken on last year's assessment report.

RISK ASSESSMENT AND RISK TREATMENT

METHODOLOGY: The objective of Risk Assessment activity is to develop robust and comprehensive standards and supporting materials to enhance IT security. These materials include a framework of specifications, tools, measurements and support resources to help organizations ensure the safe handling of organization's IT at every step.

INFORMATION ASSET REGISTER PREPARATION



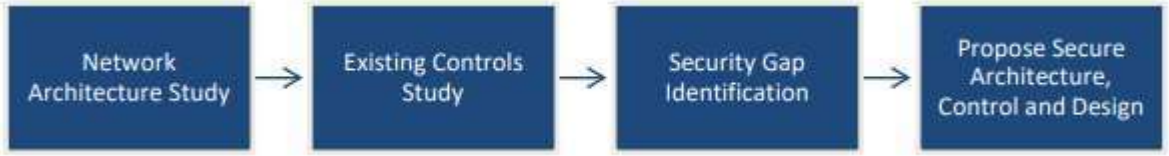
REPORT EXPECTATION:

- Information Assets Register
- Risk Management Methodology
- Risk Assessment Report
- Risk Treatment Plan Document

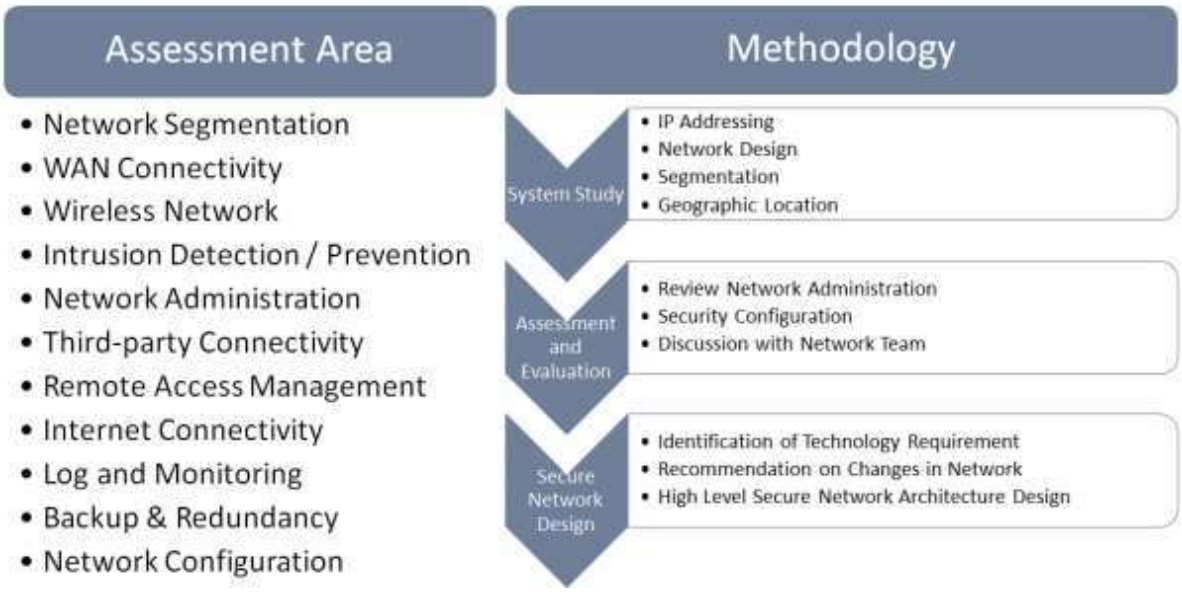
Frequency: This activity required to be perform on yearly basis with review of action taken on last year's assessment report.

SECURE NETWORK ARCHITECTURE REVIEW

METHODOLOGY: This activity will involve 4 steps, that helps understand the security gaps in the IT Network architecture and recommend the solutions for fixing the security gaps.



Following assessment areas to be covered in the service.



Bidder's consultant should propose and review a secure network architecture and implementation approach on yearly basis. It should cover following things.

REPORT EXPECTATION:

- High Level Network Architecture Design
- Suitable changes in access controls on, routers, switches, modems and other network devices to prevent unauthorized users.
- Stronger schemes for authentication for critical and sensitive information assets.
- Means to improve the security of IT environment.
- Recommendations on industry trusted technologies for fortifying security using the defense-in-depth approach.
- Recommendation on security monitoring and intrusion detection.
- Suggestions on relocation of critical existing network elements for improved security and performance.
- Review of adequacy of business continuity, capacity and threat management aspect of the network.
- Detailed Secure Network Architecture Review Report.
- Network Architecture Security Risks & recommendations.

Frequency: This activity required to be perform on yearly basis with review of action taken on last year's assessment report.

REMOTE EXPOSURE ASSESSMENT

METHODOLOGY

DELIVERABLES

Scope	**Remote - People, Process and Technology**	**Up to 25 Assets**	**Up to 3 processes and 1 application**	**Process Review**	**Existing BCP (review of RTO & RPO) & DR plan**
Coverage	Current state - People, Process and Technical understanding - Interview business stakeholders to identify crown jewels and establish confidentiality, integrity, and availability requirements - Inventory of asset register & risk registers	Inventory of Data register	DLP Process Review	Existing BCP Plan, 1 DR Plan	

Deliverables	Establishing the Business context - Asset Register with confidentiality, integrity, and availability rating - List of threat scenarios with inherent exposure rating	- Data Classification Register rating - RBAC Review (Role-based access control) – Report - Data Flow diagram for one application	DLP Process Review – Report	Report on BCP & DR Plan	Remote Exposure Gap Assessment Report

Resource Management

All team resources included in SOC Operations and device management should be on the payroll of MSSP.

MSSP can design and implement the optimal team size to manage the SOC operations. However, at DC Site - Project Manager and Team Leader is mandatory to be allocated as part of the team size and there should be minimum one resource of Sr. Security Consultant, Security Consultant at DC site across each shift and one Security Consultant at DR Site. Security Consultants – Active Directory Management should cover 2 shifts.

Minimum 11 resources [as per below table] for DC and DR Site should be available on site fulfilling all the shifts.

Shifts	Resources per Day
1st Shift 7 AM to 2 PM	DC 1 no - Sr. Security Consultant 1 no - Security Consultant 1 nos- Security Consultant AD
2nd Shift 2 PM to 10 PM	DC 1 no - Sr. Security Consultant 1 no - Security Consultant 1 nos- Security Consultant AD
3rd Shift 10 PM to 7 AM	DC 1 nos - Security Consultant

General Shift 09 AM to 06 PM	DC 1 no - Sr. Security Consultant Team Lead and Project Manager will be in General shift Monday to Saturday
General Shift 09 AM to 06 PM	DR 1 nos - Security Consultant Support from Monday to Saturday

MSSP has to factor resources accordingly to take care of shifts, weekly off's, emergency / Planned leaves Holidays and resource replacement (in case of resignation) allocated for StockHolding for the full project contract duration. They should have requisite professional qualifications for the product/ solution available in StockHolding. Resume/CV for each of these members should be provided to StockHolding for completing screening of such candidates. StockHolding reserved the right to select / reject the candidates without giving any reason at our sole discretion. Candidates should have an experience in a Financial Institution for SOC implementation / device management of at least 2 years each, with the Services/ Solutions mentioned in the RFP. MSSP shall submit the proof of the experience.

- Notice Period: For all proposed resources notice period is 60 days from the date of information to StockHolding.
- The MSSP proposed team shall be deployed onsite to provide device management services 24x7x365.
- DC Site: Support Window: 24x7x365.
- DR Site: Support from Monday to Saturday: 9:00AM to 18:00PM
- Support on Sunday and StockHolding Holidays: All 3 shifts should be covered with atleast 2 resources available at Mahape Navi Mumbai Site.
- 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.
- SOC team shall support any changes to be implemented based on recommendations of MDR team. MSSP shall propose their team strength in their proposal and the same team strength shall continue during the entire contract period. MSSP must factor number of shadow resources required to managed the Network-Security operations and accordingly include the same. Regarding shadow resource, if StockHolding is not satisfied with the performance of the standby personnel, StockHolding may not accept such standby manpower and in such cases, charges on actual basis of manpower support will be charged to the System Integrator subject to adherence of SLA conditions.
- MSSP should ensure that none of the resources working in any shift should work in consecutive shifts.

Sr. No.	Role	Experience	Location	Shift Type
1	Project Manager	7 Years working experience in Information Security domain	Navi Mumbai	9x6
2	Team Leader	5 Years working experience in Information Security domain	Navi Mumbai	9x6
3	Sr. Security Consultants	5 Years in Information Security domain	Navi Mumbai	24x7
4	Security Consultants	3 Years in Information Security domain	Navi Mumbai	24x7
5	Security Consultants for Active Directory	5 Years in Active Directory domain.	Navi Mumbai	16x6
6	Security Consultant	3 Years in Information Security domain	Bangalore	9x6

TEAM PROFILES

Sr. No.	Role	Professional Summary	Education	Work Experience	Certifications
1	Project Manager	Minimum 07 (Seven) years of experience in IT Network Security. Minimum 03 of years of experience as Project Manager in Infrastructure Security domain	Bachelor of Engineering / Bachelor of Science	• Web Application Firewalls • Intrusion Prevention Systems • Routing and L2 Switching • URL Filtering • Proxy • Next Generation firewalls (Checkpoint, Cisco ASA/Firepower, Fortigate, Palo Alto etc.) • Vulnerability assessment • Load Balancing • SSL Virtual Private Network (Juniper, Array, F5, Cisco, Checkpoint etc.)	Certified Information Security Manager (CISM)/ CISSP/CSPM)

				• Anti-Virus (Trend Micro OfficeScan/Apex One and Symantec Endpoint	
2	Team Leader	Minimum 05 (Five) years of experience in IT Network Security. Minimum 03 of years of experience as Project Manager in Infrastructure Security domain	Bachelor of Engineering / Bachelor of Science	Web Application Firewalls Intrusion Prevention Systems Routing and L2 Switching URL Filtering Proxy Next Generation firewalls (Checkpoint, Cisco ASA/Firepower, Fortigate, Palo Alto etc.) Vulnerability assessment Load Balancing SSL Virtual Private Network (Juniper, Array, F5, Cisco, Checkpoint etc.) Anti-Virus (Trend Micro OfficeScan/Apex One and Symantec Endpoint	Certified Information Security Manager (CISM) / CISSP
3	Sr. SECURITY CONSULTANTS - SOC Operations	5 years of experience in IT Security and Networking. Working as Analyst – Infrastructure Security.	Bachelor of Engineering / Bachelor of Science	Web Application Firewalls Intrusion Prevention Systems Routing and L2 Switching URL Filtering Proxy Next Generation firewalls (Checkpoint, Cisco ASA/Firepower, Fortigate, Palo Alto etc.)	Certified Ethical Hacker (CEH) or Certified in Cyber Security (CC) and /or Any SIEM / Firewall / ADC / EDR-XDR OEM certified.

				Vulnerability assessment Load Balancing SSL Virtual Private Network (Juniper, Array, F5, Cisco, Checkpoint etc.) Anti-Virus (Trend Micro OfficeScan/Apex One and Symantec Endpoint Protection etc.) • Single Sign on Patch Management (Windows Server Update Services) Ticketing Tool	
4	SECURITY CONSULTANTS - SOC Operations	3 years of experience in IT Security and Networking. Working as Analyst – Infrastructure Security.	Bachelor of Engineering / Bachelor of Science	Web Application Firewalls Intrusion Prevention Systems Routing and L2 Switching URL Filtering Proxy Next Generation firewalls (Checkpoint, Cisco ASA/Firepower, Fortigate, Palo Alto etc.) Vulnerability assessment Load Balancing SSL Virtual Private Network (Juniper, Array, F5, Cisco, Checkpoint etc.) Anti-Virus (Trend Micro OfficeScan/Apex One and Symantec Endpoint Protection etc.) • Single Sign on	Certified Ethical Hacker (CEH) or Certified in Cyber Security (CC) and /or Any SIEM / Firewall / ADC / EDR-XDR OEM certified.

				Patch Management (Windows Server Update Services) Ticketing Tool	
5	Security Consultants – Active Directory Management	03 years of experience in Active Directory and SCCM Management	Bachelor of Engineering / Bachelor of Science	Experience in Installing, Managing and Configuring Domain Controller Maintain DNS systems administration support Windows System Administration Skills Experience in creating create script in Batch, Powershell Experience in Promotion/decommission of domain controllers Plan and implement migration, upgrade /Updates /patching	Microsoft Certified IT Professional (MCITP)

JOB DESCRIPTION

Role	Professional Summary
Project Manager Project Lead	1. Managed Detection and Response Administration. Monitoring and analyzing the High and Medium Severity tickets raised for the IT Assets integrated with MDR. 2. Track Incident detection and reporting. 3. Incident closure. 4. Incident escalation. 5. Identify new alert requirement. 6. Ensure services are being provided within SLA parameters. 7. Performing periodic DR drill. 8. Follow-up up departments for closure of various reports / Incidents and escalate the long outstanding issues / Change Management / Problem Management. 9. Create and Submit Weekly Activity Summary Report, Monthly Security Report pertaining to Managed SOC services and technologies, Monthly Incident Reports, Monthly shift schedule. 10. Reviewing Daily, Weekly, Monthly and Quarterly all SOC reports.

	11. Perform review of Firewall Requests and provide recommendations before approving. 12. Involvement during POC conducted by customer for new security solutions. 13. Perform Vulnerability Assessments of Network, Security, Windows and Linux technologies. Assist team while performing closures related to these technologies. Sending report of closures performed vs open observations vs exception needed. 14. Giving implementation sign off as a service provider to customer for new solution implementations that are done. 15. Reviewing customer policies and aligning the technical aspects of on premise technologies with respect to it. 16. Conduct Weekly and Monthly meetings with customer thereby presenting achievements, next plans and improvement areas. 17. Investigate and streamline Security Incidents. 18. Reviewing SOPs and knowledge base articles. 19. Reviewing Security alerts like virus activity, network security events, application compliance, asset monitoring and firewall alerts. 20. Reviewing Firewall Access Policy Rules review, Router ACL review, WAF & IPS Signature Review, Websense URL Filtering policy reviews Review closure report of Cisco Router and Switches closure plan review. 21. Review action plan of Risk Assessment prepared by Team and track closures.
Sr. Security Consultants Security Consultants - SOC Operations	1. Managed Detection and Response Administration. Monitoring and analyzing the Critical, High, Medium and Low Severity tickets raised for the IT Assets integrated with MDR and closed the same by coordinating with respective IT Team as per SLA parameters. 2. Management and Administration of Security Network Devices like firewall, Remote VPN, Proxy, Routers, Switches and WAF. 3. Performing analysis of network security needs and contribution in design, integration, hardening and installation of hardware and software. 4. Firewall implementation for integration of 3rd Party vendor connectivity as per client requirement. 5. Formulating the security architecture for various application implementations. 6. Performing Vulnerability Assessments of network and security devices as per requirement. 7. Handling Escalation of Team and troubleshooting 8. Monitoring security environment; identifying security gaps; evaluating and implementing enhancements as per client requirement. 9. Creating and submitting daily, weekly reports as per client requirement. 10. Following up with MDR team from Call initiation till call closure in MDR Dashboard for all the IT assets integrated with MDR. 11. Incident Validation.

	12. Detailed analysis of attacks and Incident Response. 13. Solution recommendation for IT Assets vulnerabilities. 14. Implementation of patches and secure configuration of servers. 15. Manage security devices. 16. Risk analysis for change management for security devices. 17. Escalation point for device issue resolution. 18. Resolve escalation. 19. Identify missed incidents. 20. Maintain knowledge base. 21. VA Tool administration.
Security Consultants – Active Directory Management	1. Installing and Configuring Domain Controller. 2. Maintain Domain Name Services (DNS) and Lightweight Directory Access Protocol (LDAP) databases. 3. DNS Scavenging & Aging 4. Configures and manages Windows operating systems and installs/loads operating system software, 5. Provide systems administration support for new and existing infrastructure for the client 6. Experience with system monitoring, design, maintenance, and administration duties 7. Demonstrated Windows System Administration Skills (Windows 10) 8. Application installation, support, testing, and troubleshooting skills 9. Manage virtual and physical servers with windows server 2016,2019,2022 or latest available. 10. Ability to create script in Batch, Powershell 11. Should have very good communication skill 12. DNS server Health check 13. Promotion/decommission of domain controllers. 14. Plan and implement migration, upgrade /Updates /patching. 15. Sound Knowledge on pki infra management, Certificate infra management 16. Infrastructure health monitoring, Backup and restore 17. Troubleshooting and Monitoring Windows 2012 Servers, 2016 Server, 2019 Server. 2022 Server or latest available. 18. Configure and Manage Active Directory Site and Services. 19. Configure & Manage Active Directory and Group Policy. 20. Active directory server backup and restoration. 21. Migration of Active directory from 2016 to 2019 & from 2019 to 2022 or latest available 22. Installing & configuring network printer and other software / hardware devices • Responsible for Management and delivery of windows based services. 23. Perform day to day routine task as mentioned in the checklist OS Services, Events & hardware monitoring. 24. To add client system into domain and support end user for application troubleshooting.

	25. Providing day-to-day technical support - Analyzing, Troubleshooting and addressing technical issues related to servers and client. 26.Deployment of group policies as per business requirement. 27.Deployment of hardening settings via group policies to UAT and production servers. 28.User account creating, unlocking, and password reset from the active directory. 29.Active Directory Recycle Bin 30.Enabling and disabling user account and system host from the active directory. 31.Knowledge about RAID. 32.DNS record creation and modification activity like Host A, PTR, CName 33.OS deployment, Hardening and Application installation for windows servers. 34.Object creation and domain joining in active directory and support AD client application support. 35.Microsoft windows server patching(Server Patch management) 36.Knowledge of Operating systems Windows Installation 37.Participate in DR activities AD 38.Maintain incident management, Change Management and SOPs. 39.Server integrate in domain and reboot, Migration of all servers in Domain. 40. PAN India Providing technical support (software installation & configuration, managing update patches) 41.Updating servers with latest service packs and hot fixes. 42.Checking the replication of all ADC on daily basis. 43.Knowledge of Virtualization Technology like Hyper-V. 44.AD Computer Disable and Deletion, AD user Disable and deletion. Weekly Report 45.Knowledge of database server, application server, SMTP, IIS for windows. 46.Knowledge on SCCM upgrade/Migration and site implementation 47.Periodical health checks of SCCM environment and site backup. 48.Troubleshooting SCCM infrastructure, primary server and SCCM client remediation 49.Preparing customized reports in SCCM console and SQL. 50. Monthly patch testing on UAT systems, Installation of SCCM client, SCCM Client Upgradation Policy 51. Monthly patch deployment on production endpoints, Monthly patch testing and deployment on UAT servers. 52.Troubleshooting on no client and unhealthy endpoints and servers 53.Software distribution and OSD/Win10 servicing process. 54.Experience in Feature upgrades /IN place upgrade 55.Experience in Baseline configuration. 56.Deploy all software from SCCM tools.

	57.Patch Management with SCCM, WSUS. 58.SCCM package, SCCM backup monitoring. 59.Power Plan policy to disable sleep mode on endpoints.

Other Conditions:

- In case of exigencies, Security consultants and Project Manager / Team Leader should be available on Sundays and Holidays as well.
- StockHolding will conduct resume screening of each of the MSSP's selected resource before deployment in the project.
- MSSP has to ensure shadow resources are also incorporated as part of overall team strength to take care of leaves / emergencies etc. These shadow resources shall have the same skillsets and certifications as that of the replaced resources.
- A Technical Program Manager shall be appointed & be responsible for execution and compliance of entire Scope of Work. Although the Technical Program Manager for the project would not be stationed at StockHolding but he or she shall be required to visit StockHolding for attending the meetings, taking feedback, review of policies, consultation etc. and giving recommendations there of as and when required by StockHolding as well as to meet the project requirement.
- The Technical Project Manager (7yrs Exp in SOC program Management-Certified Information Security Manager (CISM) or CISSP/CSPM) within shall visit StockHolding at least 2 times per month or as directed by StockHolding officials to review the project. The number of visits may increase during important activities or as and when required.
- MSSP's personnel's deployed for SOC Operation and device management having access to information on StockHolding's security programs and systems received or generated under this contract shall ensure that they meet StockHolding's requirements.
- MSSP shall conduct adequate background checks of the personnel who will be deputed at positions handling StockHolding's sensitive information. MSSP shall submit an undertaking that they have conducted adequate background screening of their employees who will be assigned for this project. The background check report for each personal deputed at StockHolding's site has to be submitted to StockHolding till contract expiration period.
- MSSP shall maintain confidentiality of StockHolding's information accessed by them.
- MSSP shall sign Confidentiality cum Non- Disclosure Agreement on behalf of all such employees.
- Once MSSP's personnel are removed from the project, whether on termination / resignation etc. the same should be immediately informed to StockHolding and preclude any further access to all information to such person. Prior approval should be obtained from StockHolding before granting access to StockHolding's information either at MSSP's site or at StockHolding's sites.

- MSSP should not transfer any of its onsite resources (Security Consultants and Active Directory Support Consultants) from StockHolding's premises within 12 months of deployment without written consent of the designated StockHolding official. In case of inevitable circumstances, MSSP shall deploy an eligible employee with an equivalent or higher work experience at least one month prior to replacement of the deployed resource.

Deliverables

Device Management

As a part of 24x7 device management project, MSSP will carry out the following activities:

S.N.	Activity	Deliverables
1	Device Onboarding (One Time)	1) System Study -Understanding current Architecture -Understanding current SOPs -Understanding Escalation current Utilization thresholds 2) Credentials and Logon Process, Backup Management Process 3) Service Request, Change Management, and Incident Management processes 4) Key Stakeholders and alignment 5) Draw Escalation Matrix 6) Get Vendor Support details 7) Perform Issue tracker review
2	Service Request Management	Addition / deletion of rules / policies Reports
3	Change Management	Administer rules/signatures, access controls, and other configurations
		Configure the custom Use cases on request and as applicable
4	Availability Management	Monitor health of device and related components
		Take proactive measure to maintain maximum uptime
		Respond and resolve availability related issues
		Provide periodic update on key parameters
5	Incident Management	Troubleshoot/Resolve issues
		Interface with IT Contacts for resolving issues/faults
		Interface with OEM for support
		Securely configure devices/console to ensure minimum vulnerabilities Regularly update the product to the latest versions (assistance of OEM / SI Required)

		Patch & Policy Management Coordinate with OEM for Preventive Maintenance Check Ups and take remediation actions
		Securely configure devices/console to ensure minimum vulnerabilities Regularly update the product to the latest versions (assistance of OEM / SI Required)
		Patch & Policy Management Coordinate with OEM for Preventive Maintenance Check Ups and take remediation actions
6	Version Upgrades & Agent Compliance Monitoring (Version, Definitions)	• Securely configure devices/console to ensure minimum vulnerabilities • Regularly update the product to the latest versions (assistance of OEM / SI Required)
7	Other Activities	• Patch & Policy Management • Coordinate with OEM for Preventive Maintenance Check Ups and take remediation actions

Network Security and related Services

Areas	Activities	Deliverables
Security Monitoring	Log Monitoring; Server Monitoring; Security and Network Device monitoring	1. 24*7*365 log monitoring 2. Detection of threats from integrated log sources and based on the use cases defined. 3. Event Analysis 4. Alerts as per defined escalation matrix
Network Threat Hunting	Analytics Based Hunting & IOC Based	Ongoing continuous process. Notification of alerts generated through analytical models on Threat Hunting enabling hunting for attacks including but not limited to Lateral Movement, Malware Beaconing, Data Exfiltration, Watering Hole, Targeted network attacks, Dynamic DNS attacks etc.
Incident Management	Incident Analysis, Identification of all components of the incident, root cause analysis and mitigation plans	1. Provide logs and incident report for any identified security incident. Coordinate with StockHolding's team and help to contain attack/incident. 2. Provide evidences for legal and regulatory purpose in the form of log data.

SOC Maturity Improvement		Quarterly briefings on Analysis and insights from data: trends, high risks areas, roadmap for strategic improvements, security posture benchmarking. Briefings on global threat trends, regulatory trends and cyber technology trends.
Report Management	Periodic reports; Trend analysis; Customized reports	1. Review multiple reports including top attackers, attacks, attack targets, trends. 2. Monthly MIS reports for monitored devices. 3. Recommendation for improvement of security posture and threat landscape.
Global Intelligence Feeds	Continuous and regular global feeds from external known agencies.	Threat & Vulnerability advisories in form of E-mails. Recommendations for security improvements. Provide Historical, Operational, Analytical and predictive Analysis.

Security Intelligence Services

MSSP shall regularly track and advise StockHolding about new global security threats and Vulnerabilities. The advisories shall be customized to suit StockHolding's network and information security infrastructure. MSSP shall advise upgrades/ changes in the security infrastructure of StockHolding against evolving threats and vulnerabilities. Onsite team shall conduct impact analysis of new vulnerabilities and threats to StockHolding's assets and take necessary action on immediate basis for High and Medium Severity Vulnerabilities.

MSSP should advise and coordinate implementation of controls to mitigate new threats. MSSP or their onsite team shall ensure 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. Onsite Team shall track and support implementation and coordinate for closure of vulnerabilities on assets that are affected. MSSP shall provide a security dashboard for online view of the global vulnerabilities and threats applicable to StockHolding's environment, number of assets affected and status of mitigation.

MSSP shall guide and recommend StockHolding with respect to any change required in the existing infrastructure of StockHolding for deployment of new application and services, which can have security implication to StockHolding, like- changing of rule in Firewall, Router, IPS, and application/ server configurations OR redesign of the existing Network & Security Architecture.

SOC team shall identify evolving vulnerabilities and threats to IT infrastructure assets, deployed in StockHolding. This includes:

- Top global attack sources
- Top global attack targets
- New Vulnerabilities and advisories
- New Attack vectors

- Worms & Virus outbreaks

MSSP should provide countermeasures, patches and recommended workarounds or Solution to remediate vulnerabilities as and when they are discovered for StockHolding IT Assets.

Security Advisory Services

- MSSP should regularly track and advise StockHolding about new global security threats and vulnerabilities.
- The advisories should be customized to suit StockHolding's security infrastructure. Advise upgrades / changes in the security infrastructure of StockHolding against evolving threats and vulnerabilities.
- MSSP shall providing Risk Assessment and Risk Treatment Services to StockHolding on yearly basis.
- MSSP shall assist StockHolding in formulation and review of various Policies and Plans, like- IT Security Policy, BCP-DR Plan, Cyber Fraud Policy, Digital Evidence Policy, Migration Policy, MDM Policy, Hardening Policy, and IS Audit Policy etc. MSSP shall also assist StockHolding in development of necessary procedures for the same.
- Evaluation of Information Security related audit observations of StockHolding and facilitating the rectification thereof.
- MSSP shall assist StockHolding in planning, execution, and implementation of information security related initiatives/projects/programs in StockHolding.
- MSSP shall assist StockHolding in development/review, monitoring, testing, and implementation of BCP and DR Planning related to network and network security devices.
- MSSP shall participate in the periodic DC-DR Drill activity of StockHolding and suggest and assist in implementation of enhancements in the DC-DR Drill process related to network-security.
- For any new applications rollout by StockHolding, MSSP shall do network-security requirement assessment and advise StockHolding.

Transition Management (On-boarding and During-Exit)

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.

MSSP should ensure the smooth transfer of the services so as to continue to meet StockHolding's business requirements in a way that minimizes unplanned business interruptions.

MSSP will be responsible for planning, preparing and submitting a Transition Plan to StockHolding. MSSP will fully cooperate and work with any and all StockHolding's Third Party Contractors/Vendors/Consultant in a manner that will result in a seamless transfer of Services, and such transfer of Services shall be in accordance with the Transition Plan. During the Transition Period, MSSP will be responsible for implementation of the Governance Model. MSSP will identify the suitable personnel for the roles defined under the governance structure for implementation. MSSP will also be responsible for appointing its representative members to the newly established governance forums.

MSSP will have the sole responsibility for implementation of the new MSSP's delivery organization structure. All preparation and planning for such implementation must be completed during the Transition Period.

MSSP will explain how and when it will implement the transition activities, describe how it will transition Services from StockHolding's current environment. MSSP will include a project plan ("Transition Project Plan") indicating the tasks, timeframes, resources, and responsibilities associated with the transition activities.

MSSP has to develop a detailed transition plan covering at least the following key areas:

- Transition Schedules, Tasks and Activities
- Transition activities
- Operations and Support
- Maintenance
- Resource Requirements
- Software Resources
- Hardware Resources
- Facilities
- Personnel
- Other Resources
- Relationships to StockHolding's other Teams / Projects
- Management Controls
- Reporting Procedures
- Risks and Contingencies- Key Risks, issues, dependencies and mitigation plans.
- Transition Team Information
- Transition Impact Statement and assessment
- Review Process
- Configuration Control
- Plan Approval
- Describe tools, methodologies and capabilities of the teams deployed for transition.

MSSP is required to ensure that their framework for transition of proposed services from StockHolding IT team/current Service Provider, at a minimum should include the following phases and allied activities:

Service Requirements	Description
Initiation	Kick off the transition based on the agreed transition plan
Planning	This phase takes care of all the planning activities required for successful transition of services
Execution	Execute the transition of services while ensuring near zero risk and no disruption to business.
Closure	Create all the transition documents and submit to the client for review and sign off and start off with MIS & SLA reporting.
Transition Document	To be made available monthly for review.

MSSP's Roles & Responsibility

A	**Initiation**
1	Project kick- off
2	Team mobilization
B	**Planning**
3	Project charter
4	Communications plan
5	Set- up transition management process (risk, issues, changes, dependencies, reporting etc.)
6	Agreement on acceptance criteria and sign- offs
C	**Execution**
7	Discover and study existing practice, process, assets etc.
8	Define service delivery process
9	Define processes; develop SOPs, checklists, escalation matrix and flow charts. The defined processes and SOP's should be in line with Stockholding's ISMS Policies and procedures. (MSSP has to obtain StockHolding's sign off on documentation prior to completion of transition phase)
10	Deploy tools Monitoring tools as a service
11	Configuration of monitoring parameters and SLAs
12	Shadow support
D	**Transition Closure**
13	Primary Takeover
14	Business as usual to be delivered by successful MSSP's operations team as per scope of work
15	Finalized run- books
16	Hand- over document
17	Finalize the Service transfer process document

18	Submit the Transition documents to StockHolding for review and sign off
19	MIS report generation and SLA reporting
20	The scope of work mentioned is illustrative and not exhaustive. MSSP needs to comply with StockHolding's requirements and any statutory or regulatory guidelines

- MSSP to ensure proper documentation during each phase of transition and get them approved by StockHolding Networking team.
- Maintain steady operation of Transition period will have to be done within 90 days from the date of the order from the existing MSSP
- MSSP has to provide sufficient staff during the transition period however the payment for services shall start after the transition period and formal handover of service to the MSSP.
- All SLA's and associated penalties shall be applicable to the new MSSP post transition period of 3 months
- Finalize the reporting mechanism in consultation with StockHolding.

Periodic Review of the project

StockHolding officials will hold a meeting with the senior officials of MSSP once in a Quarter or as decided by StockHolding on a later date to review the progress and to take necessary steps/decisions for performance improvement. The scope of the meeting includes but not limited to the following.

- Taking decisions on network-security architecture designs.
- Making necessary Policies/ changes as part of change management.
- Examining the level of SLA compliance achieved and taking steps for improvement.
- Attending to dispute resolution.
- Suggesting extra reports based on SLA requirement.
- Transition process planning.
- Health monitoring of the network-security appliances and devices.
- Any other issues that arise from time to time.

Service Level Agreement (SLA) and Penalty

MSSP needs to execute a Service Level Agreement with StockHolding covering all terms and conditions of this tender. MSSP need to strictly adhere to Service Level Agreements (SLA). Services delivered by MSSP should comply with the SLA mentioned in the table below.

MSSP should generate SLA reports for tracking the delivery of services. SLA will be reviewed on a monthly basis, and based on the review, payments for the services will be made. Thus enabling StockHolding to continuously track the SLA. Penalty amount applicable for the services will be estimated and reported every month. The total estimated penalty amount will be shared with StockHolding.

In all other Operational conditions - The maximum penalty applicable will be 10% of the monthly contract value.

Service Level Targets Metric Calculation and Penalty Calculation: High level service level targets are described in sections below.

- SLA deviation calculation to be considered on monthly basis.
- The penalty will be calculated on the monthly contract value.

Monitoring and Management of Network Devices: Uptime Commitment for Network Security Devices under Device Management.

Table - A

Penalty Calculation Table (A)		
Category	**Breach Condition**	**Penalty**
Network Uptime	Uptime falls below 99.5%	1% of monthly contract value per hour of breach less than the uptime of 99.5%
Configuration & Capacity Management	Delayed implementation of network device changes	1% of monthly contract value for each instance of breach
Capacity Planning Review	Review delayed beyond 5th day of the quarter	
Lost Network Assets	Loss due to omission or negligence or failure	1% of monthly contract per incident + full recovery of asset cost

Incident Response Time	Ticket response delayed beyond SLA Time	INR 5,000 per missed response
Incident Resolution Time	Resolution exceeds SLA limit	INR 5,000 per breach
OEM Call Logging Delay	Call not logged within 30 min	INR 5,000 per day of delay
Incident Management - Security Intelligence	Breach beyond SLA time limit. To be applied for every 24 hours delay	INR 5,000 per breach
Problem Management	Ticket response delayed beyond SLA Time for each Priority Level i.e. P0, P1, P2 and P3	INR 5,000 per missed response
Change Management – Schedule Adherence	Change not performed / implemented below the SLA Metric	INR 5,000 for every change not performed / implemented
Change Management – Efficiency		
Change Management – Failed Changes	Failed change rollback beyond the SLA metric	INR 5,000 for every failed change rollback
Compliance Management – Schedule Adherence	Change not performed / implemented below the SLA Metric	INR 5,000 for every change not performed / implemented
Compliance Management – Efficiency		
Compliance Management – Failed Changes	Failed change rollback beyond the SLA metric	INR 5,000 for every failed change rollback
Reports Submission - Daily Security Reports	To be submitted by end of each day	INR 1,000 per missed report
Reports Submission - Weekly Reports	To be submitted by end of the week	INR 1,000 per missed report
Reports Submission - Monthly Reports	To be submitted by 10th of the month	INR 5,000 per missed report
Reports Submission - Compliance Reports	To be submitted by 15th of the month	INR 5,000 per missed report
Reports Submission - Quarterly Security Audit Reports	To be submitted by the 7th of the following quarter	INR 5,000 per missed report
Reports Submission - Half-Yearly Vulnerability Reports	To be submitted by the end of the period	INR 5,000 per missed report

Security Testing	For each missed deliverables for the said period	INR 10,000 per missed deliverable for every month of delay for the activities defined in the monthly calendar (will be shared to the winning bidder)
Consulting Services	For each missed deliverables for the said period	INR 10,000 per missed deliverable for every month of delay for the activities defined in the monthly calendar (will be shared to the winning bidder)

- Exclusions: Preventive maintenance, scheduled outages, LAN cabling faults, infrastructure issues.
- Total Monthly Penalty = Sum of All Penalties (excluding penalty on resource management), Capped at 10% of Monthly contract value
- For resource management, separate penalty is applicable as per penalty terms and conditions
- If Monthly Penalty > 5% for Two Consecutive Months → 10% Deduction in Second Month
- Business Hours Window: (24 * 7 * 365 Support = 24 hours in a day * 30 days = 720 hours.
- Uptime shall be calculated at the end of each month as follows.
  Uptime: {(Actual Uptime in Hrs. – Downtime in Hrs.) / Schedule Hrs.} x 100.
- Actual Uptime means, of the scheduled hours, the aggregate number of hours in any month during which each defined and supported equipment is actually available for use.
- Downtime in Hrs. means the aggregate number of hours in any month during which each defined and supported equipment and service is down during scheduled hours other than due to preventive maintenance, scheduled outages, Upgrades and updates, LAN cabling faults, infrastructure problems or any other situation which is not attributable to MSSP's failure to exercise due care in performing its responsibilities.
- Scheduled hours means the days of the week and the hours per day for which the MSSP has committed to an availability service level for a system or network and during which periods such Availability Service Level will apply.

Configuration and Capacity Management of Network Devices: SLA and Penalty Structure

Event	Criticality	Timeframe	Benchmark	Penalty Calculation

Create, modify and delete configurations in network devices after obtaining approval from the StockHolding Team.	As per device / Application risk severity rating.	Response Time : 30 min	Resolution time: 2 hour	Please Refer the above Penalty Calculation Table (A)
Review of capacity planning of in scope network and Network-security devices, appliances and Servers.	As per device / Application risk severity rating.	Response: starting on the 1st day of the first month of the Start of every Quarter.	Resolution: within 5th day of the first month of the start of every Quarter.	Please Refer the above Penalty Calculation Table (A)
Loss of any network assets, under the control of the MSSP's onsite team, due to omission or negligence or failure, to follow the due process in handling and updating the network inventory.	High			Please Refer the above Penalty Calculation Table (A)

Incident Management and Investigation Metric Calculation and Penalty

Incident Management aims to restore normal service operation as quickly as possible and minimize the adverse effect on business operations, thus ensuring that the best possible levels of service-quality are maintained. 'Normal service operation' is defined here as service operation within service level agreement limits.

Incident management can be defined as any event which is not part of the standard operation of the service and which causes, or may cause, an interruption or a reduction of the quality of the service.

The objective of incident management is to restore normal operations as quickly as possible with the least possible impact.

Severity	Severity Definition	Response Time	Resolution Time*	Penalty Structure
P0	An outage which impacts a large number of people or critical business process (i.e. Internet Link Outage, Firewall Down, misconfiguration issues etc.)	15 min	30mins	Please Refer the above Penalty Calculation Table (A)
P1	An outage which impacts a small group of people (i.e. SOC Infrastructure, Services and Components etc.)	15 min	60 mins	
P3	An impact for individual end user (login issues, ID lockout, Proxy issue etc.)	30 min	90 mins	
P4	A request for service (Firewall rules)	30 min	24 hours	

Incidents pertaining to Managed Detection and Response and Other Services:

Sr. No	Service Area	Criticality	Service Level
1	Incidents to be actioned based on alerts raised by SIEM-MDR Team	Post raising alerts from MDR Team for any suspicious events Incident, - Initial response should be Initiated by SOC team after notification from MDR Team a) Within 15 minutes for Critical (P0) and high priority (P1) incidents for all In-scope and other devices. b) Within 30 minutes for others (P2) priority incidents for all In-scope and other devices.	Please Refer the above Penalty Calculation Table (A) for Incident Response and Incident Resolution

3	Anti-Malware and Anti Trojan scanning Services	• Alerts generated from monitoring and detection systems should be suitably investigated in order to determine activities that are to be performed to prevent expansion of such incident of cyber-attack or breach, mitigate its effect and eradicate the incident. • SOC team should have implement measures to prevent unauthorized access or copying or transmission of data / information held in contractual or fiduciary capacity. It should be ensured that confidentiality of information is not compromised during the process of exchanging and transferring information to external parties. • The response and recovery plan of the SOC team should have plans for the timely restoration of systems affected by incidents of cyber- attacks or breaches • Any incident of loss or destruction of data or systems should be thoroughly analysed and lessons learned from such incidents should be incorporated to strengthen the security mechanism and improve recovery planning and processes.	Please Refer the above Penalty Calculation Table (A) for Incident Response and Incident Resolution
4	Security Intelligence	Initiation & Resolution of remedial/ migratory measures to thwart such security vulnerabilities within 24 hours.	Please Refer the above Penalty Calculation Table (A) for Incident Management

Problem Management

Parameter	Metric	Metric Calculation	Unit of Measure	Reporting Frequency	Penalty Calculation

Root Cause	% of RCA report submitted (Critical) >95%	Total number of RCAs submitted within 48Hrs./ Total number of RCAs	Percentage	Monthly	Refer to the penalty table below.

Priority	SLA for RCA Completition	Penalty Structure
P0	<=48 hours	Please Refer the above Penalty Calculation Table (A) for Problem Management
P1	<=72 hours	
P2	<=96 hours	
P3	<=96 hours	

Change Management

Change management aims to ensure that standardized methods and procedures are used for efficient handling of all changes; a change is "an event that results in a new status of one or more configuration items approved by management and enhances business process changes (fixes) - with a minimum risk to IT infrastructure. The main aims of change management include:

- Minimal disruption of services
- Reduction in back-out activities.
- Economic utilization of resources involved in the change
- Change Management Terminology
- Change: the addition, modification or removal of CIs
- Forward Schedule of Changes (FSC): schedule that contains details of all forthcoming changes.

Parameter	Metric	Metric Calculation	Unit of Measure	Reporting Frequency	Penalty Calculation
Schedule Adherence	Schedule Adherence – Change, >=95%	Total number of Changes Implemented by total number of changes planned for the month	Percentage	Monthly	Please Refer the above Penalty Calculation Table (A) for Change Management

Change Management Efficiency	Successful Changes, >=95%	Total number of Changes implemented successfully by total number of changes implemented	Percentage	Monthly	
Failed Changes	% changes rolled back, <=5%	Total number of changed rolled back due to failure by total number of changes implemented successfully	Percentage	Monthly	Please Refer the above Penalty Calculation Table (A) for Change Management

Compliance Management Terminology and Action from SOC Team

(Applicable for Audits / Configuration Audits / Vulnerability Assessment and Penetration Testing / Secure Network Architecture / Remote Assessment / Red Team Assessments / Monthly Security Advisories – CERT-in, NCIIPC, SEBI, NSDL, CDSL, PFRDA, IRDA, SEBI CSCRF and RBI etc. closures for the observations reported by them)

- Compliance action: The addition, modification of changes.
- Forward Schedule of Changes (FSC): schedule that contains details of all forthcoming changes.
- Vulnerability Assessment and Penetration Testing reports (Internal and external) can be provided to SOC team on quarterly basis by respective internal and external vendors. Analysis and action taken to be completed on such VA/PT in the 1st month for "Critical" and "High" severity vulnerabilities. Post Medium severity vulnerabilities to be close in the 2nd month. All the "Low" Severity vulnerabilities to be close in 3rd month i.e. before initiating the confirmatory test for VA/PT from respective vendor.
- Internal and external audit related findings to be close on priority basis within a stipulated period provided by StockHolding.

Parameter	Metric	Metric Calculation	Unit of Measure	Reporting Frequency	Penalty Calculation
Schedule Adherence	Schedule Adherence – Change, >=95%	Total number of Changes Implemented by total	Percentage	Monthly	Please Refer the above Penalty Calculation Table (A) for

		number of changes planned for the month			Compliance Management
Change Management Efficiency	Successful Changes, >=95%	Total number of Changes implemented successfully by total number of changes implemented	Percentage	Monthly	
Failed Changes	% changes rolled back, <=5%	Total number of changed rolled back due to failure by total number of changes implemented successfully	Percentage	Monthly	Please Refer the above Penalty Calculation Table (A) for Compliance Management

Resource Management:

Event	Criticality	Penalty Calculation
Unavailability of agreed resources on site. (For 1 resource) for a day.	Low	For each instance of breach, penalty will be 0.5% of monthly contract value. i.e. (A)
Unavailability of agreed resources on site. (For 2 resource) for a day.	Medium	Additional 1% of monthly contract value. i.e. B = (A) + 1%
Unavailability of agreed resources on site. (For More than 2) for a day.	High	Additional 2% of monthly contract value. i.e. C = (B) + 2% for subsequent instances and increase in unavailability of resources.
Unavailability of Project Manager and Team Leader on site for same days.	Medium	For each instance of breach, penalty will be 2% of monthly contract value.
Late Coming/Early departures will be considered as absent for the day.	High	For each instance of breach, penalty will be 0.25% of monthly contract value.

Separation of duties (i.e. use of email ids and login ids across roles)	Medium	For each instance of Breach/resource, penalty will be 0.25% of monthly contract value.

Reports

All automatic and manual reports generated through various devices / tools required to be analyse on Daily / Weekly and Monthly basis and after analyzing reports should be provided to StockHolding

S/N.	Activity	Reports	Frequency
1	Firewall Appliances	Top 10 Inbound Allowed Traffic by IP Destination Address and analysis done and action taken by MSSP.	Daily
2		Top 10 Inbound Allowed Traffic by IP Destination. Port and analysis done and action taken by MSSP.	Daily
3		Top 10 Inbound Denied Traffic by IP Destination Port and analysis done and action taken by MSSP.	Daily
4		Top 10 Inbound Denied Traffic by IP Source Address and analysis done and action taken by MSSP.	Daily
5		Top 10 Outbound Allowed Traffic by IP Destination Port and analysis done and action taken by MSSP.	Daily
6		Top 10 Outbound Denied Traffic by IP Destination Address and analysis done and action taken by MSSP.	Daily
7		Top 10 Outbound Denied Traffic by IP Destination Port and analysis done and action taken by MSSP.	Daily
8		Top 10 Outbound Denied Traffic by IP Source Address and analysis done and action taken by MSSP.	Daily
9		Top 10 Outbound Allowed Traffic by IP Source Address and analysis done and action taken by MSSP.	Daily
10		Top 10 Inbound Denied Traffic by IP Destination Address and analysis done and action taken by MSSP.	Daily
11	IPS Blade	Top 10 Events by Signature and analysis done and action taken by MSSP.	Daily
12		Top 10 Inbound Events by IP Destination Address and analysis done and action taken by MSSP.	Daily

13		Top 10 Inbound Events by IP Destination Port and analysis done and action taken by MSSP.	Daily
14		Top 10 Inbound Events by IP Source Address and analysis done and action taken by MSSP.	Daily
15		Top 10 Outbound Events by IP Destination Address and analysis done and action taken by MSSP.	Daily
16		Top 10 Outbound Events by IP Destination Port and analysis done and action taken by MSSP.	Daily
17		Top 10 Outbound Events by IP Source Address and analysis done and action taken by MSSP.	Daily
18	Cisco FMC and FPD appliance.	Top 20 Accepted Events by Destination Address and analysis done and action taken by MSSP.	Daily
19		Top 20 Accepted Events by Destination Port and analysis done and action taken by MSSP.	Daily
20		Top 20 denied Events by Destination Address and analysis done and action taken by MSSP.	Daily
21		Top 20 denied Events by Destination port and analysis done and action taken by MSSP.	Daily
22	Proxy + URL filtering	Spyware Activity Summary and analysis done and action taken by MSSP.	Daily
23		Top Sites by Bandwidth and analysis done and action taken by MSSP.	Daily
24		Top Sites by Browse Time and analysis done and action taken by MSSP.	Daily
25		Top Users by Bandwidth and analysis done and action taken by MSSP.	Daily
26		Top Users by Browse Time and analysis done and action taken by MSSP.	Daily
27	Antivirus Reports	Daily Antivirus Outdated client list Report and analysis done and action taken by MSSP.	Daily
28		Weekly Antivirus Outdated client list Report and analysis done and action taken by MSSP.	Weekly
29		Systems without Antivirus connected in network and shared report to IT SPOC.	Daily

30		Monthly Antivirus outdated client list report along with Analysis	Monthly
31	Real Time reporting – Alerts view security	Denied Inbound / Outbound connection. (At the end of the day) and analysis done and action taken by MSSP.	Real Time
32		Severity Summary (At the end of the day) and analysis done and action taken by MSSP.	Real Time
33		Top Intruders (At the end of the day) and analysis done and action taken by MSSP.	Real Time
34		Top Attacks (At the end of the day) and analysis done and action taken by MSSP.	Real Time
35		Suspected Security Issues. (At the end of the day) and analysis done and action taken by MSSP.	Real Time
36		Attack Identification report. (At the end of the day) and analysis done and action taken by MSSP.	Real Time
37	ILL Link Testing Report	Speed Test report to test ILL link Bandwidth	Weekly basis
38	MDR Monthly Review Report	Monthly SIEM tickets review with validation and closure comments.	Monthly Basis.
39	Active Directory and SCCM Reports	AD Computer Disable and Deletion, AD user Disable and Deletion.	Weekly Report
40	Other Reports	Vulnerability Assessment / PT Services. (Internal Security Assessment Services.) and analysis done and action taken by MSSP.	Half-yearly Analysis and Reports.
41		Vulnerability Assessment / PT Services. (External Security Assessment Services. – Through Vendors office) and analysis done and action taken by MSSP.	Half-yearly Analysis and Reports
42	Daily Operational Calls Summary	Daily Operational calls – Completed / Ongoing / Pending to submit at the end of the day to StockHolding.	Daily
43	Monthly Compliance Report	Adherences to regulatory and certifications (e.g. SEBI, ISO27001:2022, SOC 2 Type 2 Report, Cert-In etc.) SOC Services opted and the commitment to effective network security.	Monthly
44	VA / PT Report	Vulnerability- Action Taken Report	Half Yearly
45	Process Reviews	Yearly and as on need basis.	Yearly and as on need basis
46	Tactical Review	Project Feedback / SLA Review.	Quarterly

47		Escalations and Service Improvements.	Quarterly
48	Operational Review	Activity Review and deadline tracking.	Monthly
49		Technical and Resource Issues.	Monthly

Report Type	Submission Deadline	Penalty Calculation
Daily Security Reports	End of each day	Please Refer the above Penalty Calculation Table (A) for Reports Submission
Weekly Reports	End of the week	
Monthly Reports	By the 10th of the month	
Compliance Reports	By 15th of the month	
Quarterly Security Audit Reports	By the 7th of the following quarter	
Half-Yearly Vulnerability Reports	By the end of the period	

Contract Duration

1) 02 (Two) years.
2) StockHolding may choose to extend the contract period for another 1 year based on satisfactory performance from the successful bidder.

Terms and Conditions

A. Payment:

SI.	Description	Payment Terms
1	Initial 3 months post acceptance of PO and during the transition period	Payment will be released after completion of transition period
2	Device Management and Activity Execution	Monthly Payment after deduction of applicable penalties

Note:

a. Applicable penalty will / may be recovered from the monthly payment.
b. Applicable TDS and/or CESS will be recovered (deducted) from the payment.
c. First Payment will be released only after signing of Integrity Pact and Non-Disclosure Agreement.
d. Payments will be released only after submission and verification of the required Bank Guarantee (BG). No payment will be made to successful bidder, until the BG verification is done.

B. Taxes & levies:

a. Applicable GST payable at actual as per prevailing rate of taxes as per Government notification
b. In case of tax exemption or lower TDS; Bidder has to submit letter from Government Authority for tax exemption or lower TDS (to be submitted along with each of the invoice(s) (c) Applicable TDS will be deducted from payment(s).

C. Bidder to abide by labour laws, human rights and regulations in their regions of business. Bidder to adhere to laws addressing child, forced or trafficked labour

Refund of Earnest Money Deposit (EMD):

a. EMD will be refunded through NEFT or return of BG/FDR to the successful bidder on providing an acceptance confirmation against the PO issued by StockHolding.
b. In case of unsuccessful bidders, the EMD will be refunded to them through NEFT or return of BG/FDR within 30 days after selection and confirmation of successful bidder, subject to internal approval of StockHolding.

Performance Bank Guarantee (PBG):

Successful Bidder shall, at own expense, deposit with the *StockHolding*, within Fifteen (15) days on issuance of PO, a Bank Guarantee (BG) for the value of 5% (Five per cent) of the Contract value (including GST) from scheduled commercial banks as per Annexure - 8. This Bank Guarantee shall be valid up to 60 days beyond the completion of the contract period. The BG claim period will be 12 months from BG expiry date. No payment will be due to the successful bidder based on performance, until the BG verification is pending. A penalty of ₹5,000 per day will be imposed on for any delay in issuing the PBG within the specified timeline

Bank Guarantee may be discharged / returned by *StockHolding* upon being satisfied that there has been due performance of the obligations of the Bidder under the contract. However, no interest shall be payable on the Bank Guarantee. *StockHolding* reserves the right to invoke the BG in the event of non-performance by the successful bidder.

Force Majeure

Neither StockHolding nor the Bidder shall be responsible for any failure to fulfil any term or condition of the CONTRACT if and to the extent that fulfilment has been delayed or temporarily prevented by a Force Majeure occurrence, defined as "Force Majeure". For purposes of this clause, "Force Majeure" mean an event beyond the control of the Parties and which prevents a Party from complying with any of its obligations under this Contract, including but not limited to: acts of God not confined to the premises of the Party claiming the Force Majeure, flood, drought, lightning or fire, earthquakes, strike, lock-outs beyond its control, labour disturbance not caused at the instance of the Party claiming Force Majeure, acts of government or other competent authority, war, terrorist activities, military operations, riots, epidemics, civil commotions etc.

The Party seeking to rely on Force Majeure shall promptly, within 5 days, notify the other Party of the occurrence of a Force Majeure event as a condition precedent to the availability of this defence with particulars detailed in writing to the other Party and shall demonstrate that it has taken and is taking all reasonable measures to mitigate the events of Force Majeure. And, all Parties will endeavor to agree on an alternate mode of performance in order to ensure the continuity of service and implementation of the obligations of a party under the Contract and

to minimize any adverse consequences of Force Majeure. Each PARTY shall bear its own cost in relation to the force majeure occurrence.

However, any failure or lapse on the part of the Bidder to mitigate the damage that may be caused due to the above-mentioned events or the failure to provide adequate disaster management/recovery or any failure in setting up a contingency mechanism would not constitute force Majeure, as set out above.

If the duration of delay exceeds ninety (90) consecutive or one hundred eighty (180) cumulative days, StockHolding and the Bidder shall hold consultations with each other in an endeavour to find a solution to the problem. Notwithstanding above, the decision of the StockHolding, shall be final and binding on the bidder.

Dispute Resolution

In the event of any dispute arising out of or in connection with this Order, the parties shall use their best endeavour to resolve the same amicably AND if the dispute could not be settled amicably, the matter shall be settled in the court under Mumbai jurisdiction only. The final payment will be released only after the Bidder complies with above-mentioned clause.

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.

Integrity Pact

The Bidder will have to enter in to an Integrity Pact with StockHolding. The format (text) for the Integrity Pact is provided as Annexure-5. The Bidder will have to submit a signed and stamped copy of the Integrity Pact by the authorized signatory of the Bidder.

Non-Disclosure Agreement (NDA)

The successful Bidder will sign a Non-Disclosure Agreement (NDA) as per Annexure-9 with StockHolding for the contract period. The draft text of the NDA will have to be approved by legal department of StockHolding. All the expenses related to execution of the document such as the applicable stamp duty and registration charges if any shall be borne by the successful bidder.

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.

Subcontracting

As per scope of this RFP, sub-contracting is not permitted. The bidder shall not assign or sub-contract the assignment or any part thereof to any other person/firm.

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;

Exit Management

a. Purpose: In the case of termination of the Contract, the Exit Management procedure should start 90 days before the expiry or termination of contract.
b. Plan: An Exit Management Plan, provided in writing by the Bidder to the StockHolding within 60 days of the acceptance of the Purchase Order/Contract, will outline the Bidder's support during the termination or expiration of the contract, along with the company's exit strategy. Following this, the exit plan must be reviewed and updated annually.
c. Bidder shall provide the Termination/Expiration Assistance regardless of the reason for termination or expiration.
d. Bidder shall fully and timely comply with the Exit Plan.
e. Bidder shall not make any changes to the Services under this Agreement and shall continue to provide all Services to comply with the Service Levels.
f. Confidential Information, Security and Data: The Bidder will promptly on the commencement of the exit management period supply to StockHolding the following:
    - Information relating to the current services rendered.
    - Documentation relating to Project's Intellectual Property Rights.
    - Project Data and Confidential Information.
    - All current and updated project data as is reasonably required for purposes of transitioning the services to its Replacement Bidder in a readily available format specified by StockHolding.

Assignment

Either Party may, upon written approval of the other, assign its rights and obligations hereunder to: (i) its Parent Corporation (as defined below) or an Affiliate; and (ii) a third party entity in connection with the transfer of all or substantially all of the business and assets of that party to such entity. For purposes of this Agreement, a "Parent Corporation" shall mean a company or entity owning over 50% of a Party and an "Affiliate" shall mean a company directly or indirectly controlling, controlled by, or under common control with, a Party. Except

as provided above in this Section, either Party may assign its rights and obligations under this Agreement to a third party only upon receiving the prior written consent of the other Party, which consent may be reasonably conditioned but will not be unreasonably withheld or delayed. The Parties agree that no assignments will be made unless the assignee agrees to accept in full the responsibilities and obligations of the assigning Party.

Information Sharing with Regulators Clause

1. **Regulatory Compliance and Information Sharing:**
   1.1. **Obligation to Comply with Laws -** The Bidder agrees to comply with all applicable laws, regulations, and guidelines set forth by relevant regulatory bodies, including but not limited to financial, privacy, and data protection regulations.
   1.2. **Cooperation with Regulatory Authorities -** The Bidder acknowledges that StockHolding may be subject to periodic audits, inspections, or inquiries by regulatory authorities. The Bidder agrees to fully cooperate with such regulatory authorities and provide, upon request, all necessary information, documentation, or data related to the services being provided under this SLA, to the extent permitted by applicable laws and regulations.
   1.3. **Disclosure of Information to Regulators -** In the event that StockHolding or the Bidder is required by law or regulation to disclose information to regulators, the Bidder agrees to promptly notify StockHolding in writing of such requirements. The Bidder shall provide StockHolding with reasonable access to the information being disclosed and cooperate with StockHolding in fulfilling any regulatory obligations.
   1.4. **Confidentiality of Regulatory Disclosures -** Where required by regulators, the Bidder will share information in accordance with applicable confidentiality agreements, ensuring that StockHolding is aware of the regulatory requirements surrounding such disclosures. If information shared with regulators contains confidential or proprietary information of StockHolding, the Bidder will take appropriate steps to protect StockHolding's interests, including requesting the inclusion of confidentiality provisions in any regulatory disclosure requests.
   1.5. **Regulatory Reporting and Notifications -** The Bidder agrees to promptly inform StockHolding if the Bidder or its subcontractors are subject to any investigations, fines, sanctions, or enforcement actions by regulatory bodies that could materially impact the Bidder's ability to perform its obligations under this SLA. This includes any changes in the Bidder's regulatory standing that might affect the services provided to StockHolding.

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.

3. **Data Protection and Privacy:**

3.1. **Data Sharing with Regulators** - If any personal data, confidential information, or proprietary data is required to be shared with regulators, both parties agree to comply with applicable data protection laws, including any necessary prior consultation or notification requirements with data protection authorities.

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.

ANNEXURE - 1 - Details of Bidder's Profile

(To be submitted along with technical bid on Company letter head)

Details filled in this form must be accompanied by sufficient documentary evidence, in order to verify the correctness of the information.

Sl. No	Parameters	Response	
1	Name of the Firm/Company		
2	Year of Incorporation in India		
3	Names of the Partners/Directors		
4	Company PAN no		
5	Company GSTN no. (please attach annexures for all states)		
6	Addresses of Firm/Company		
	a) Head Office		
	b) Local Office in Mumbai(if any)		
7	Authorized Contact person		
	a) Name and Designation		
	b) Telephone number		
	c) E-mail ID		
8	Years of experience of Managing on-site SOC services		
9	**Financial parameters**		
	Business Results (last three years)	Annual Turnover	Networth
		(Rs. in Crores)	(Rs. in Crores)
	2022-23		
	2023-24		
	2024-25		
	(Only Company figures need to be mentioned not to include group/subsidiary Company figures)	(Mention the above Amount in INR only)	

N.B. Enclose copies of Audited Balance Sheet along with enclosures

Dated this..... Day of 2025

(Signature)

(In the capacity of)

ANNEXURE - 2 – Eligibility Criteria

To be submitted as part of Technical Bid

SI.	Criteria	Documents to be submitted by Bidder
1	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.	Copy of Certificate of Incorporation issued by the Registrar of Companies and Self-declaration by the bidder on it Letter Head duly signed by the Authorized Signatory along with supporting documents for SOC related PO on or before RFP Date
2	The bidder should have an average annual turnover of at least Rs. 14 Crores per annum for last 03 (three) financial years (i.e. 2022-23, 2023-24 and 2024-25). It should be of individual company and not of Group of Companies	Certificate from CA mentioning annual turnover for last three financial years.
3	The Bidder should have Positive Net worth minimum Rs. 3.5 crores for each of the last 03 (three) audited financial years (i.e. 2022-23, 2023-24 and 2024-25)	Certificate from CA mentioning networth for the past three financial years.
4	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	Copy of Purchase Order & Completion certificate with Customer Name and Address, Contact Person, Telephone Nos. Fax and e-mail Address and customer reference to be provided (or) Copy of Purchase Order & self- certificate attested by the authorized signatory of the bidder confirming “in-progress” status of cited project

5	Bidder should not be blacklisted by any Government, Government Body, PSU, Bank, Autonomous body and any other entity for any reasons within last 3 years from the RFP date.	Self-declaration by the bidder on it Letter Head duly signed by the Authorized Signatory
6	The bidder must possess at the time of bidding, following valid certifications: • ISO 9001:2008 or latest/ISO 20000 and • ISO 27001:2022 or SOC 2 Type 2	Relevant valid Certificates
7	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.	Declaration from HR Manager or authorized signatory on company letter head
8	Bidder shall have their own Security Operation Center situated in India with a ISO 27001 certification compliance	Self-declaration by the bidder on it Letter Head duly signed by the Authorized Signatory with ISO Certificate
9	Bidder should not be existing System Integrator for Network Infrastructure (NOC Services) and/or Cyber Security Consultant or Auditor for StockHolding to avoid conflict of interest	Self-declaration by the bidder on it Letter Head duly signed by the Authorized Signatory
10	Bidder should have Support office at Maharashtra.	Bidder to provide office address along with GST details.
11	Bidder to provide undertaking that no penalties, amounting to up to 5% of the contract value per year, have been imposed in the last 03 (three) years by any of its client(s).	Self-declaration from bidder on their letter head duly signed by authorized signatory
12	The bidder should not be under insolvency resolution, bankruptcy or liquidation proceedings under the Insolvency and Bankruptcy Code or any other applicable laws as on date of bid submission	Self-declaration from bidder on their letter head duly signed by authorized signatory
13	The Bidder must be CERT-In Empanelled as on RFP Date	Relevant valid Certificates
14	The Bidder to submit signed & stamped Integrity Pact as per Annexure - 5	Self-declaration from bidder on their letter head duly signed by authorized signatory

Eligibility Criteria (For On-site Manpower Assignment)

Sr. No.	Role	Professional Summary	Education	Work Experience	Certifications
1	Project Manager	Minimum 07 (Seven) years of experience in IT Network Security. Minimum 03 of years of experience as Project Manager in Infrastructure Security domain	Bachelor of Engineering / Bachelor of Science	• Web Application Firewalls • Intrusion Prevention Systems • Routing and L2 Switching • URL Filtering • Proxy • Next Generation firewalls (Checkpoint, Cisco ASA/Firepower, Fortigate, Palo Alto etc.) • Vulnerability assessment • Load Balancing • SSL Virtual Private Network (Juniper, Array, F5, Cisco, Checkpoint etc.) • Anti-Virus (Trend Micro OfficeScan/Apex One and Symantec Endpoint	Certified Information Security Manager (CISM)/ CISSP/CSPM)
2	Team Leader	Minimum 05 (Five) years of experience in IT Network Security. Minimum 03 of years of experience as Project Manager in Infrastructure Security domain	Bachelor of Engineering / Bachelor of Science	Web Application Firewalls Intrusion Prevention Systems Routing and L2 Switching URL Filtering Proxy Next Generation firewalls (Checkpoint, Cisco ASA/Firepower, Fortigate, Palo Alto etc.) Vulnerability assessment Load Balancing SSL Virtual Private Network (Juniper, Array,	Certified Information Security Manager (CISM) / CISSP

				F5, Cisco, Checkpoint etc.) Anti-Virus (Trend Micro OfficeScan/Apex One and Symantec Endpoint	
3	Sr. Security Consultants - SOC Operations	5 years of experience in IT Security and Networking. Working as Analyst – Infrastructure Security.	Bachelor of Engineering / Bachelor of Science	Web Application Firewalls Intrusion Prevention Systems Routing and L2 Switching URL Filtering Proxy Next Generation firewalls (Checkpoint, Cisco ASA/Firepower, Fortigate, Palo Alto etc.) Vulnerability assessment Load Balancing SSL Virtual Private Network (Juniper, Array, F5, Cisco, Checkpoint etc.) Anti-Virus (Trend Micro OfficeScan/Apex One and Symantec Endpoint Protection etc.) • Single Sign on Patch Management (Windows Server Update Services) Ticketing Tool	Certified Ethical Hacker (CEH) or Certified in Cyber Security (CC) and /or Any SIEM / Firewall / ADC / EDR-XDR OEM certified.
4	Security Consultants - SOC Operations	3 years of experience in IT Security and Networking. Working as Analyst – Infrastructure Security.	Bachelor of Engineering / Bachelor of Science	Web Application Firewalls Intrusion Prevention Systems Routing and L2 Switching URL Filtering Proxy Next Generation firewalls (Checkpoint, Cisco ASA/Firepower, Fortigate, Palo Alto etc.) Vulnerability assessment Load Balancing SSL Virtual Private Network (Juniper, Array,	Certified Ethical Hacker (CEH) or Certified in Cyber Security (CC) and /or Any SIEM / Firewall / ADC / EDR-XDR OEM certified.

				F5, Cisco, Checkpoint etc.) Anti-Virus (Trend Micro OfficeScan/Apex One and Symantec Endpoint Protection etc.) • Single Sign on Patch Management (Windows Server Update Services) Ticketing Tool	
5	Security Consultants – Active Directory Management	03 years of experience in Active Directory and SCCM Management	Bachelor of Engineering / Bachelor of Science	Experience in Installing, Managing and Configuring Domain Controller Maintain DNS Systems administration support Windows System Administration Skills Experience in creating create script in Batch, Powershell Experience in Promotion/decommission of domain controllers Plan and implement migration, upgrade /Updates /patching	Microsoft Certified IT Professional (MCITP)

Note:

a. Letter of Authorization shall be issued by either Managing Director having related Power of Attorney issued in his favour or a Director of the Board for submission of Response to RFP
b. All self-certificates shall be duly signed and Stamped by Authorized signatory of the Bidder Firm unless specified otherwise.
c. Bidder response should be complete, Yes/No answer is not acceptable.
d. Details of clients and relevant contact details are mandatory. Bidders may take necessary approval of the clients in advance before submission of related information. StockHolding will not make any separate request for submission of such information.

Dated this..... Day of 2025
(Signature)

(In the capacity of)

Duly authorized to sign bid with seal for & on behalf of (Name & Address of the Bidder)

ANNEXURE – 3 – Technical Criteria

Sl. No	Parameter	Scores	Qualifying Scores	Max Scores
A. BASED ON EXPERIENCE, TURNOVER & RESOURCE STRENGTH (70 MARKS)				
1	Average annual turnover of the bidder during last 03 (three) years (i.e. 2022-23, 2023-24 and 2024-25)	• 14 Crores >= 25 Crores : 10 Marks • >25 Crore but <= INR 50 Crore : 12 Marks • More than INR 50 crore : 15 Marks	10	15
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	10	15
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	5	10
3 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.	The number of professional staff in the area of Information Security (CISA/CISM/CISSP/CEH/ISO 27001 certified) certified person on bidder Payroll.	• Atleast 15 nos. Certified person – 10 Marks • 16-40 Certified persons – 12 Marks • More than 41 Certified persons – 15 Marks	10	15
4	Bidder having a ISO 27001 Certified SOC functional in India as on RFP date	• 5 Years : 7 marks • More than 5 Years - <= 8 Years : 12 Marks • More than 10 Years : 10 Marks	7	10

5	Bidder having CERT-In Empanelled as on RFP Date	• Not empanelled – 0 Marks • Less than 3 Years – 3 Marks • More than 3 Years : 5 Marks	3	5
B. BASED ON PROPOSED SOLUTION, APPROACH & PRESENTATION (30 MARKS)				
6	Bidder's technical presentation	• Understanding of the Project requirements • Bidder's SOC Capabilities • Relevant Experience • Proposed Solution for StockHolding • Approach and Methodology • Resource Deployment Plan • Proposed Project Manager / Team lead / resources experience & skillset • SLA Management Framework	15	30

Note:

a. Letter of Authorization shall be issued by either Managing Director having related Power of Attorney issued in his favour or a Director of the Board for submission of Response to RFP
b. All self-certificates shall be duly signed and Stamped by Authorized signatory of the Bidder Firm unless specified otherwise. Cumulative score of 60 marks in the Technical evaluation needs to be achieved.
c. Bidder response should be complete, Yes/No answer is not acceptable.
d. Details of clients and relevant contact details are mandatory. Bidders may take necessary approval of the clients in advance before submission of related information. StockHolding will not make any separate request for submission of such information.

Dated this..... Day of 2025
(Signature)

(In the capacity of)
Duly authorized to sign bid with seal for & on behalf of (Name & Address of the Bidder)

ANNEXURE - 4 - Commercial Price Bid Format

Commercial Price Bid Format

SI.	Description	Year 1 Cost (₹)	Year 2 Cost (₹)
1	Cost for Device Management		
2	Cost for Activity Execution		
Total Per Year Cost (₹) without GST			
GST Charges (₹)			
Total Per Year Cost (₹) with GST			
Total 2 Years Cost with GST (₹)			

Notes:

a Price to be quoted is for 02 (two) years including GST while uploading financial bids on GeM portal.

b Contract will be awarded to the bidder achieving the maximum overall score.

c StockHolding may choose to extend the contract period for another 1 year based on satisfactory performance from the successful bidder.

d Bidder must take care in filling price information in the Commercial Offer, to ensure that there are no typographical or arithmetic errors. All fields must be filled in correctly. Please note that any Commercial Offer, which is conditional and / or qualified or subjected to suggestions, will also be summarily rejected. This offer shall not contain any deviation in terms & conditions or any specifications, if so such an offer will also be summarily rejected.

e All payments will be made in INR.

ANNEXURE - 5 – Integrity Pact

(_____ Name of the Department / Office) RFP No._____ for_____

This pre-bid pre-contract Integrity Pact (Agreement) (hereinafter called the Integrity Pact) (IP) is made on _____ day of the _____, between, on one hand, StockHolding ., a company incorporated under Companies Act, 1956, with its Registered Office at 301, Centre Point Building, Dr. B R Ambedkar Road, Parel, Mumbai – 400012 , acting through its authorized officer, (hereinafter called **Principal**), which expression shall mean and include unless the context otherwise requires, his successors in office and assigns) of the First Part **And** M/s._____ _____(with complete address and contact details)represented by Shri _____ (i.e. Bidders hereinafter called the **`Counter Party'**) which expression shall mean and include , unless the context otherwise requires, his successors and permitted assigns) of the Second Part.

AND WHEREAS the PRINCIPAL/Owner values full compliance with all relevant laws of the land, rules, regulations economic use of resources and of fairness/transparency in its relation with Bidder(s) /Contractor(s)/Counter Party(ies).

AND WHEREAS, in order to achieve these goals, the Principal/Owner has appointed Independent External Monitors (IEM) to monitor the Tender (RFP) process and the execution of the Contract for compliance with the principles as laid down in this Agreement.

WHEREAS THE Principal proposes to procure the Goods/services and Counter Party is willing to supply/has promised to supply the goods OR to offer/has offered the services and WHEREAS the Counter Party is a private Company/Public Company/Government Undertaking/ Partnership, constituted in accorded with the relevant law in the matter and the Principal is a Government Company performing its functions as a registered Public Limited Company regulated by Securities Exchange Board of India. **NOW THEREFORE**, To avoid all forms of corruption by following a system that is fair, transparent and free from any influence prejudiced dealings prior to, during and subsequent to the tenor of the contract to be entered into with a view to "- Enabling the PRINCIPAL to obtain the desired goods/services at competitive price in conformity with the defined specifications by avoiding the high cost and the distortionary impact of corruption on public procurement, and Enabling the Counter Party to abstain from bribing or indulging in any type of corrupt practice in order to secure the contract by providing assurance to them that their competitors will also abstain from bribing and other corrupt practices and the PRINCIPAL will commit to prevent corruption, in any form, by its officials by following transparent procedures. The parties hereto hereby agree to enter into this Integrity Pact and agree as follows**:**

I. Commitment of the Principal / Buyer

1. The Principal Owner commits itself to take all measures necessary to prevent corruption and to observe the following principles:-

a) No employee of the Principal/Owner, personally or through any of his/her family members, will in connection with the Tender (RFP) or the execution of the contract, procurement or services/goods, demand, take a promise for or accept for self or third person, any material or immaterial benefit which the person not legally entitled to.

b) The Principal/Owner will, during the Tender (RFP) Process treat all Bidder(s)/Counter Party(ies) with equity and reason. The Principal / Owner will, in particular, before and during the Tender (RFP) Process, provide to all Bidder(s) / Counter Party (ies) the same information and will not provide to any Bidder(s)/Counter Party (ies) confidential / additional information through which the Bidder(s)/Counter Party (ies) could obtain an advantage in relation to the Tender (RFP) Process or the Contract execution.

c) The Principal / Owner shall endeavor to exclude from the Tender (RFP) process any person, whose conduct in the past been of biased nature.

2. If the Principal / Owner obtains information on the conduct of any of its employees which is a criminal offence under the Indian Penal Code (IPC) / Prevention of Corruption Act, 1988 (PC Act) or is in violation of the principles herein mentioned or if there is a substantive suspicion in this regard, the Principal / Owner / StockHolding will inform the Chief Vigilance Officer through the Vigilance Officer and in addition can also initiate disciplinary actions as per its internal laid down policies and procedures.

II. Commitments of Counter Parties/Bidders

1. The Counter Party commits itself to take all measures necessary to prevent corrupt practices, unfair means and illegal activities during any stage of bid or during any pre-contract stage in order to secure the contract or in furtherance to secure it and in particular commit itself to the following. Counter Party (ies) / Bidders commits himself to observe these principles during participation in the Tender (RFP) Process and during the Contract execution.
2. The Counter Party will not offer, directly or through intermediaries, any bribe, gift, consideration, reward, favour, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of the PRINCIPAL, connected directly or indirectly with the bidding process, or to any person organization or third party related to the contract in exchange for any advantage in the bidding, evaluation, contracting and implementation of the contract.
3. The Counter Party further undertakes that it has not given, offered or promised to give directly or indirectly any bribe, gift, consideration, reward, favour, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of the Principal / StockHolding or otherwise in procurement the Contract or forbearing to do or having done any act in relation to the obtaining or execution of the contract or any other contract with the

Principal / StockHolding for forbearing to show favour or disfavor to any person in relation to the contract or any other contract with the Principal / StockHolding.

4. Bidder / Counter Party shall disclose the name and address of agents and representatives, if any, handling the procurement / service contract.
5. Bidder / Counter Party shall disclose the payments to be made by them to agents / brokers; or any other intermediary if any, in connection with the bid / contract.
6. The Bidder / Counter Party has to further confirm and declare to the Principal / StockHolding that the Bidder / Counter Party is the original integrator and has not engaged any other individual or firm or company, whether Indian or foreign to intercede, facilitate or in any way to recommend to Principal / StockHolding or any of its functionaries whether officially or unofficially to the award of the contract to the Bidder / Counter Party nor has any amount been paid, promised or intended to the be paid to any such individual, firm or company in respect of any such intercession, facilitation or recommendation.
7. The Bidder / Counter Party has to submit a Declaration along with Eligibility Criteria, as given at **Annexure**. If bids are invited through a Consultant a Declaration has to be submitted along with the Eligibility Criteria as given at **Annexure**.
8. The Bidder / Counter Party, either while presenting the bid or during pre- contract negotiation or before signing the contract shall disclose any payments made, is committed to or intends to make to officials of StockHolding /Principal, or their family members, agents, brokers or any other intermediaries in connection with the contract and the details of services agreed upon for such payments.
9. The Bidder / Counter Party will not collude with other parties interested in the contract to impair the transparency, fairness and progress of bidding process, bid evaluation, contracting and implementation of the Contract.
10. The Bidder / Counter Party shall not accept any advantage in exchange for any corrupt practice, unfair means and illegal activities.
11. The Bidder shall not use improperly, for purposes of competition or personal gain, or pass on to others, any information provided by the Principal / StockHolding as part of the business relationship, regarding plans, proposals and business details, including information contained in any electronic data carrier. The Bidder / Counter Party also Undertakes to exercise due and adequate care lest any such information is divulged.
12. The Bidder / Counter Party commits to refrain from giving any complaint directly or through any other manner without supporting it with full and verifiable facts.
13. The Bidder / Counter Party shall not instigate or cause to instigate any third person including their competitor(s) of bidding to commit any of the actions mentioned above.
14. If the Bidder / Counter Party or any employee of the Bidder or any person acting on behalf of the Bidder / Counter Party, either directly or indirectly, is a relative of any of the official / employee of Principal / StockHolding, or alternatively, if any relative of an official / employee of Principal / StockHolding has financial interest / stake in the Bidder's / Counter Party firm, the same shall be disclosed by the Bidder / Counter Party at the time of filing of tender (RFP).

15. The term `relative" for this purpose would be as defined in Section 2 Sub Section 77 of the Companies Act, 2013.
16. The Bidder / Counter Party shall not lend to or borrow any money from or enter into any monetary dealings or transactions, directly or indirectly, with any employees / officials of the Principal / StockHolding
17. The Bidder / Counter Party declares that no previous transgression occurred in the last three years immediately before signing of this IP, with any other Company / Firm/ PSU/ Departments in respect of any corrupt practices envisaged hereunder that could justify Bidder / Counter Party exclusion from the Tender (RFP) Process.
18. The Bidder / Counter Party agrees that if it makes incorrect statement on this subject, Bidder / Counter Party can be disqualified from the tender (RFP) process or the contract, if already awarded, can be terminated for such reason.

III. Disqualification from Tender (RFP) Process and exclusion from Future Contracts

1. If the Bidder(s) / Contractor(s), either before award or during execution of Contract has committed a transgression through a violation of Article II above or in any other form, such as to put his reliability or credibility in question, the Principal / StockHolding is entitled to disqualify the Bidder / Counter Party / Contractor from the Tender (RFP) Process or terminate the Contract, if already executed or exclude the Bidder / Counter Party / Contractor from future contract award processes. The imposition and duration of the exclusion will be determined by the severity of transgression and determined by Principal / StockHolding. Such exclusion may be for a period of 1 year to 3 years as per the procedure prescribed in guidelines of the Principal / StockHolding.
2. The Bidder / Contractor / Counter Party accepts and undertake to respect and uphold the Principal / StockHolding's absolute right to resort to and impose such exclusion.
3. Apart from the above, the Principal / StockHolding may take action for banning of business dealings / holiday listing of the Bidder / Counter Party / Contractor as deemed fit by the Principal / Owner / StockHolding.
4. The Bidder / Contractor / Counter Party can prove that it has resorted / recouped the damage caused and has installed a suitable corruption prevention system, the Principal / Owner/ StockHolding may at its own discretion, as per laid down organizational procedure, revoke the exclusion prematurely.

IV. Consequences of Breach Without prejudice to any rights that may be available to the Principal / StockHolding / Owner under Law or the Contract or its established policies and laid down procedure, the Principal / StockHolding / Owner shall have the following rights in case of breach of this Integrity Pact by the Bidder / Contractor(s) / Counter Party:-

1. Forfeiture of EMD / Security Deposit : If the Principal / StockHolding / Owner has disqualified the Bidder(s)/Counter Party(ies) from the Tender (RFP) Process prior to the award of the Contract or terminated the Contract or has accrued the right to terminate the Contract according the Article III, the Principal / StockHolding / Owner apart from exercising any legal

rights that may have accrued to the Principal / StockHolding / Owner, may in its considered opinion forfeit the Earnest Money Deposit / Bid Security amount of the Bidder / Contractor / Counter Party.

2. Criminal Liability: If the Principal / Owner / StockHolding obtains knowledge of conduct of a Bidder / Counter Party / Contractor, or of an employee of a representative or an associate of a Bidder / Counter Party / Contractor which constitute corruption within the meaning of PC Act, or if the Principal / Owner / StockHolding has substantive suspicion in this regard, the Principal /
StockHolding / Owner will inform the same to the Chief Vigilance Officer through the Vigilance Officer.

IV. Equal Treatment of all Bidders/Contractors / Subcontractors / Counter Parties

1. The Bidder(s) / Contractor(s) / Counter Party (ies) undertake (s) to demand from all subcontractors a commitment in conformity with this Integrity Pact. The Bidder / Contractor / Counter-Party shall be responsible for any violation(s) of the principles laid down in this Agreement / Pact by any of its sub-contractors / sub-bidders.
2. The Principal / StockHolding / Owner will enter into Pacts on identical terms as this one with all Bidders / Counterparties and Contractors.
3. The Principal / StockHolding / Owner will disqualify Bidders / Counter Parties / Contractors who do not submit, the duly signed Pact, between the Principal / Owner / StockHolding and the Bidder/Counter Parties, along with the Tender (RFP) or violate its provisions at any stage of the Tender (RFP) process, from the Tender (RFP) process.

VI. Independent External Monitor (IEM)

1. The Principal / Owner / StockHolding has appointed Shri Shekhar Prasad Singh, IAS (Retd.) as Independent External Monitor (s) (IEM) for this Pact. The task of the Monitor is to review independently and objectively, whether and to what extent the parties comply with the obligations under this Integrity Pact.
2. The IEM is not subject to instructions by the representatives of the parties and performs his functions neutrally and independently. He reports to the Chief Executive Officer and Managing Director, StockHolding Ltd.
3. The Bidder(s)/Contractor(s) / Counter Party(ies) accepts that the IEM has the right to access without restriction, to all Tender (RFP) documentation related papers / files of the Principal / StockHolding / Owner including that provided by the Contractor(s) / Bidder / Counter Party. The Counter Party / Bidder / Contractor will also grant the IEM, upon his request and demonstration of a valid interest, unrestricted and unconditional access to his or any of his Sub-Contractor"s Tender (RFP) Documentation / papers / files. The IEM is under contractual obligation to treat the information and documents of the Bidder(s) / Contractor(s) / Sub-Contractors / Counter Party (ies) with confidentiality.
4. In case of tender (RFP)s having value of 50 lakhs or more, the Principal / StockHolding / Owner will provide the IEM sufficient information about all the meetings among the parties related to

the Contract/Tender (RFP) and shall keep the IEM apprised of all the developments in the Tender (RFP) Process.

5. As soon the IEM notices, or believes to notice, a violation of this Pact, he will so inform the Management of the Principal / Owner /StockHolding and request the Management to discontinue or take corrective action, or to take other relevant action. The IEM can in this regard submit nonbinding recommendations. Beyond this, the IEM has no right to demand from the parties that they act in a specific manner, refrain from action or tolerate action.
6. The IEM will submit a written report to the CEO&MD, StockHolding. Within 6 to 8 weeks from the date of reference or intimation to him by the Principal / Owner / StockHolding and should the occasion arise, submit proposals for correcting problematic situations.
7. If the IEM has reported to the CEO&MD, StockHolding Ltd. a substantiated suspicion of an offence under the relevant IPC/PC Act, and the CEO&MD, StockHolding has not within reasonable time taken visible action to proceed against such offence or reported it to the Chief Vigilance Officer, the IEM may also transmit the information directly to the Central Vigilance Officer.
8. The word `IEM" would include both singular and plural.

VII. Duration of the Integrity Pact (IP)

This IP begins when both the parties have legally signed it. It expires for the Counter Party / Contractor / Bidder, 12 months after the completion of work under the Contract, or till continuation of defect liability period, whichever is more and for all other Bidders, till the Contract has been awarded. If any claim is made / lodged during the time, the same shall be binding and continue to be valid despite the lapse of this Integrity Pact as specified above, unless it is discharged / determined by the CEO&MD StockHolding

VIII. Other Provisions

1. This IP is subject to Indian Law, place of performance and jurisdiction is the Head Office / Regional Offices of the StockHolding /Principal / Owner who has floated the Tender (RFP).
2. Changes and supplements in any Procurement / Services Contract / Tender (RFP) need to be made in writing. Change and supplement in IP need to be made in writing.
3. If the Contractor is a partnership or a consortium, this IP must be signed by all the partners and consortium members. In case of a Company, the IP must be signed by a representative duly authorized by Board resolution.
4. Should one or several provisions of this IP turn out to be invalid; the remainder of this Pact remains valid. In this case, the parties will strive to come to an agreement to their original intentions.
5. Any dispute or difference arising between the parties with regard to the terms of this Agreement / Pact, any action taken by the Principal / Owner / StockHolding in accordance with this Agreement / Pact or interpretation thereof shall not be subject to arbitration.

IX. Legal and Prior Rights

All rights and remedies of the parties hereto shall be in addition to all the other legal rights and remedies belonging to such parties under the Contract and / or law and the same shall be deemed to be cumulative and not alternative to such legal rights and remedies aforesaid. For the sake of brevity, both the Parties agrees that this Pact will have precedence over the Tender (RFP) / Contract documents with regard to any of the provisions covered under this Integrity Pact.

IN WITHNESS WHEREOF the parties have signed and executed this Integrity Pact (IP) at the place and date first above mentioned in the presence of the following witnesses:-

---

(For and on behalf of Principal / Owner / StockHolding

(For and on behalf of Bidder / Counter Party / Contractor)

WITNESSES:

1._____ (Signature, name and address)

2._____ (Signature, name and address)

Note: In case of Purchase Orders wherein formal agreements are not signed references to witnesses may be deleted from the past part of the Agreement.

ANNEXURE - 6 - Covering Letter on bidder's Letterhead of Integrity Pact

To,

---------- ----------

Sub: RFP REF NO: CPCM-20/2025-26 dated 18-Nov-2025 for Selection of Service Provider for Managing On-Site Security Operation Centre (SOC) for Stockholding

Dear Sir,

DECLARATION

Stock Holding Corporation of India Limited (StockHolding) hereby declares that StockHolding has adopted Integrity Pact (IP) Program as advised by Central Vigilance Commission vide its Letter No. ---------- Dated ---------- and stands committed to following the principles of transparency, equity and competitiveness in public procurement. The subject Notice Inviting Tender (RFP) (NIT) is an invitation to offer made on the condition that the Bidder will sign the Integrity Agreement, which is an integral part of tender (RFP) documents, failing which the tender (RFP)er / bidder will stand disqualified from the tender (RFP)ing process and the bid of the bidder would be summarily rejected. This Declaration shall form part and parcel of the Integrity Agreement and signing of the same shall be deemed as acceptance and signing of the Integrity Agreement on behalf of the StockHolding

Yours faithfully,

For and on behalf of StockHolding Corporation of India Limited
(Authorized Signatory)

ANNEXURE – 7 – Compliance Statement

(To be submitted on Company Letter Head)

Subject: **RFP REF NO:** CPCM-20/2025-26 dated 18-Nov-2025 for Selection of Service Provider for Managing On-Site Security Operation Centre (SOC) for Stockholding

DECLARATION

We understand that any deviations mentioned elsewhere in the bid will not be considered and evaluated by the StockHolding. We also agree that the StockHolding reserves its right to reject the bid, if the bid is not submitted in proper format as per subject RFP.

Sr. No.	Item / Clause of the RFP	Compliance (Yes / No)	Remarks/Deviations (if any)
1	Objective of the RFP		
2	Scope of Work		
3	Eligibility Criteria		
4	Service Level Agreement (SLA) / Scope of Work		
5	Non-Disclosure Agreement		
6	Payment Terms		
7	Bid Validity		
8	Integrity Pact		
9	All General & Other Terms & Conditions in the RFP		
10	Requirement		

(If Remarks/Deviations column is left blank it will be construed that there is no deviation from the specifications given above)

Date: Signature with seal

Name & Designation:

ANNEXURE – 8 – Format of Bank Guarantee

This Bank Guarantee is executed by the ---------- (Bank name) a Banking Company incorporated under the Companies Act, 1956 and a Scheduled Bank within the meaning of the Reserve Bank of India Act, 1934 and having its head office at ---------- and branch office at _____(hereinafter referred to as the "Bank", which term shall mean and include, unless to repugnant to the context or meaning thereof, its successors and permitted assigns) and Branch office at _____ in favour of Stock Holding Corporation of India Limited, a Company incorporated under the Companies Act, 1956 and having its Registered Office at 301, Centre Point, Dr. Babasaheb Ambedkar Road, Parel, Mumbai 400 012 (hereinafter referred to as "StockHolding", which term shall mean and include, unless to repugnant to the context or meaning thereof, its successors and permitted assigns) at the request of _____, a Company incorporated under the Companies Act, 1956 and having its Registered Office at (hereinafter referred to as the "Service Provider", which term shall mean and include, unless to repugnant to the context or meaning thereof, its successors and permitted assigns).

Whereas

A. StockHolding has, pursuant to the Tender No. _____, issued the Purchase Order dated _____ to the Service Provider for providing _____
B. In terms of the said Tender, the Service Provider has agreed to furnish to StockHolding, a Bank guarantee for Rs. _____ /- (Rupees _____ only) till _____ (date).
C. The Bank has, at the request of the Service Provider**,** agreed to give this guarantee as under.

NOW IN CONSIDERATION OF THE FOREGOING:

1. We, the Bank, at the request the Service Provider, do hereby unconditionally provide this guarantee to StockHolding as security for due performance and fulfilment by the Service Provider of its engagements, commitments, operations, obligations or liabilities including but not limited to any sums / obligations / claims due by the Service Provider to StockHolding for meeting, satisfying, discharging or fulfilling all or any obligation or liability of the Service Provider, under the said Tender / Purchase Order.

2. We, the Bank, hereby guarantee and undertake to pay StockHolding up to a total amount of Rs. _____/- (Rupees _____ only) under this guarantee, upon first written demand of StockHolding and without any demur, protest and without any reference to the Service Provider**.**
3. Any such demand made by StockHolding shall be conclusive and binding on the Bank as regards the amount due and payable notwithstanding any disputes pending before any court, Tribunal, or any other authority and/ or any other matter or thing whatsoever as the liability of the Bank under these presents being absolute and unequivocal.
4. We, the Bank, agree that StockHolding shall have the fullest liberty without consent of the Bank to vary the terms of the said Tender/ Purchase Order or to postpone for any

time or time to time exercise of any powers vested in StockHolding against the Service Provider and to forbear or enforce any of the Terms & Conditions relating to the said Tender / Purchase Order and the Bank shall not be relieved from its liability by the reason of any such variation, or extension being granted to the Service Provider or for any forbearance, act or omission or any such matter or thing whatsoever.

5. We, the Bank, agree that the guarantee herein contained shall be irrevocable and shall continue to be enforceable until it is discharged.
6. This Guarantee shall not be affected by any change in the Constitution of the Bank or the Service Provider or StockHolding.

NOTWITHSTANDING ANYTHING CONTAINED HEREIN ABOVE:

1. The liability of the bank under this guarantee is restricted to a sum of Rs. _____/- (Rupees _____ only).
2. This Bank Guarantee will be valid for a period up to _____ (date).
3. A written claim or demand for payment under this Bank Guarantee on or before _____ (date) is the only condition precedent for payment of part/full sum under this guarantee.

For Issuing Bank

Name of Issuing Authority:

Designation of Issuing Authority:

Employee Code:

Contact Number:

Email ID:

ANNEXURE – 9 – Format of Non-Disclosure Agreement

This Non-Disclosure Agreement (hereinafter "Agreement") is executed on this _____ day of _____, **20xx** by and between

Stock Holding Corporation of India Limited, a company incorporated under the Companies Act, 1956 and having its registered office at 301, Centre Point, Dr. Babasaheb Ambedkar Road, Parel, Mumbai 400012 (hereinafter referred to as "**StockHolding**" which expression shall mean and include its successors and assigns), of the One Part;

And

Company Name, a company incorporated under the Companies Act, 1956 and having its registered office / corporate office at **Complete Address** (hereinafter referred to as "**Company Name**" which expression shall mean and include its successors and assigns), of the Other Part.

(StockHolding and **Company Name** are individually referred to as 'Party' and collectively as 'Parties'.)

The Party disclosing Confidential Information under this Agreement shall be referred to as Disclosing Party and the Party receiving Confidential Information shall be referred to as Receiving Party.

1. **Purpose**: Whereas, the Parties wish to explore possible business opportunity, during which either Party will be required to disclose certain Confidential Information to the other.
2. **Confidential Information and Exclusions**: Confidential Information shall mean and include (a) any information received by the Receiving Party which is identified by Disclosing Party as confidential or otherwise; (b) all information including technical, data security , cyber security business, financial and marketing information, data, analysis, compilations, notes, extracts, materials, reports, drawings, designs, specifications, graphs, layouts, plans, charts, studies, memoranda or other documents, know-how, ideas, concepts, strategies, trade secrets, product or services, results obtained by using confidential information, prototype, client or vendor list, projects, employees, employees skills and salaries, future business plans disclosed by Disclosing Party whether orally or as embodied in tangible materials. Confidential Information shall however exclude any information which a) is in the public domain; (b) was known to the Party of such disclosure or becomes known to the Party without breach of any confidentiality agreement; (c) is independently developed by the Party without use of Confidential Information disclosed herein; (d) is disclosed pursuant judicial order or requirement of the governmental agency or by operation of law, provided that the recipient party gives disclosing party a written notice of any such requirement within ten (10) days after the learning of any such requirement, and takes all reasonable measure to avoid disclosure under such requirement.
3. **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. 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 Disclosing Party in the event of any unauthorized use or disclosure of the Confidential Information and reasonably support Disclosing Party in taking necessary remedial action.

4. **No Warranty**: All Confidential Information is provided 'as is.' Neither Party makes any warranty, express, implied or otherwise, regarding its accuracy, completeness or performance.
5. **No License**: Each Party recognizes that nothing in this Agreement is construed as granting it any proprietary rights, by license or otherwise, to any Confidential Information or to any intellectual property rights based on such Confidential Information.
6. **Return**: The Receiving Party who receives the Confidential Information and Confidential Materials agrees that on receipt of a written demand from the Disclosing Party:
    a. Immediately return all written Confidential Information, Confidential Materials and all copies thereof provided to, or produced by it or its advisers, as the case may be, which is in Receiving Party's possession or under its custody and control; (SUCH RETURN OF DOCUMENTS SHOULD BE DONE BY SIGNING A LETTER).
    b. To the extent practicable, immediately destroy all analyses, compilations, notes, studies, memoranda or other documents prepared by it or its advisers to the extent that the same contain, reflect or derive from Confidential Information relating to the Disclosing Party;
    c. So far as it is practicable to do so immediately expunge any Confidential Information relating to the Disclosing Party or its projects from any computer, word processor or other device in its possession or under its custody and control; and
    d. To the extent practicable, immediately furnish a certificate signed by its director or other responsible representative confirming that to the best of his/her knowledge, information and belief, having made all proper enquiries the requirements of this paragraph have been fully complied with.

e. Receiving party will attempt to maintain, to the best possible extent, physical and logical segregation of the Confidential Information of the data of the Receiving party from data of any third party.

7. **Term**: The term of this Agreement shall be ____ (___) years from _____ (the Effective Date). Either Party may terminate this Agreement by giving a thirty (30) days written notice to the other. The confidentiality obligations stated in this Agreement shall survive for a period of three (3) years from the date of termination or expiration of this Agreement.
8. **Remedies**: The Confidential Information and Confidential Materials and all copies thereof, in whatsoever form shall at all times remain the property of the Disclosing Party and its disclosure hereunder shall not confer on the Receiving Party any rights whatsoever beyond those contained in this document.
   The Parties acknowledge and agree that the Disclosing Party will suffer substantial and irreparable damage, not readily ascertainable or compensable in monetary terms, in the event of any breach of any provision of this Agreement by the Receiving Party. The Receiving Party therefore agrees that, in the event of any such breach, the Disclosing Party shall be entitled, without limitation of any other remedies otherwise available to it, to obtain an injunction or other form of equitable relief from any court of competent jurisdiction.
9. **Governing Law and Jurisdiction**: This Agreement may be governed and construed in accordance with the laws of India and shall be subject to the jurisdiction of courts in Mumbai, India.
10. **Miscellaneous**: This Agreement constitutes the entire agreement between the Parties with respect to the subject matter hereof and supersedes all prior commitments/ understanding in this regard and may not be amended or modified except by a writing signed by a duly authorized representative of the respective Parties. This Agreement may be executed in several counterparts (physical or electronic form), each of which shall be deemed an original, but all of which together shall constitute one and the same instrument. This Agreement may not be assigned or transferred except by a mutual written consent of both the Parties.

For Stock Holding Corporation of India Limited	**For Company Name**
Name:	Name:
Title:	Title:
In the Presence of	
Name:	Name:
Title:	Title:

ANNEXURE - 10 - Covering Letter on bidder's Letterhead for Concentration Risk

To,

Sub: RFP REF NO: CPCM-20/2025-26 dated 18-Nov-2025 for Selection of Service Provider for Managing On-Site Security Operation Centre (SOC) for Stockholding

Dear Sir,

DECLARATION

The bidder hereby declares the following regarding their concentration risk:

1. **Do you rely on any single customer, supplier, or service provider for more than 20% of your revenues or operational capacity?**
   [ ] Yes
   [ ] No

   If yes, please describe the potential risk, mitigation strategies, and contingency plans related to this concentration:
   [Bidder's Response]

2. **Do you have any reliance on a particular geographic region or market that could cause an over-concentration risk?**
   [ ] Yes
   [ ] No

   If yes, please provide details regarding the potential risks and any mitigation strategies in place:
   [Bidder's Response]

3. **Diversification Measures**
   Please describe any steps or measures your organization has taken to reduce concentration risks, such as diversification of suppliers, customers, or geographical spread:
   [Bidder's Response]

4. **Risk Mitigation and Continuity Plans**
   Please provide details of your contingency plans in case of disruption from any major supplier or customer:
   [Bidder's Response]

   Have you implemented any risk assessment or monitoring systems to track concentration risks regularly?

[ ] Yes
[ ] No

If yes, please describe the system or process in place:
[Bidder's Response]

5. Certification

I, the undersigned, certify that the information provided above is accurate and truthful to the best of my knowledge. I understand that any failure to disclose material concentration risks may result in the reconsideration of the vendor relationship.

Authorized Representative Name: _____
Designation: _____
Signature: _____
Date: _____