SBI Capital Markets Limited (SBICAP Group)

Request for Proposal: RFP No. RFP/IS-01/2025

Managed Services for

Security Operations Centre (SOC) -

Security Information and Event Management (SIEM),

Security Orchestration, Automation and Response (SOAR) &

User and entity Behaviour Analytics (UEBA)

SBI Capital Markets Limited & Group companies (SBICAP Group) Unit No. 1501, 15th floor, A& B Wing, Parinee Crescenzo Building, Plot C- 38, G Block, Bandra Kurla Complex, Bandra (East), Mumbai- 400 051

RFP No. RFP/IS-01/2025 dated 6th August 2025

Request For Proposal (RFP) For Hiring of Managed Services for Security Operations Centre: Security Information and Event Management, Security Orchestration, Automation and Response & User and entity Behaviour Analytics (SOC: SIEM-SOAR-UEBA)

ACTIVITY SCHEDULE		
Sr No	**Activity**	**Details**
1.	RFP Number	RFP No. RFP/IS-01/2025
2.	Release of RFP	6th August 2025
3.	Pre Bid Queries on email	13th August 2025
4.	Online Technical & Commercial Bid submission	14th August 2025 - 14:00 Hrs
5.	Bid Evaluation and Presentation of shortlisted Service Providers	18th August to 21st August 2025 (tentative schedule)
6.	Method of Selection	The method of selection is Quality and Cost Base Selection. The weights given to the Technical and Commercial Proposals are: Technical = 70% and Commercial= 30%
7.	M/s. e-Procurement Technologies Ltd. – Contact Details	B-704, Wall Street – II Ahmedabad, Gujarat – 380006. Email: allocation@eptl.in Website : https://etender.sbi
8.	SBICAP Group - Contact Details	Krishna Mohan Ginjupalli (CISO) SBI Capital Markets Limited, Unit No. 1501, 15th floor, A& B Wing, Parinee Crescenzo Building, Plot C- 38, G Block, Bandra Kurla Complex, Bandra (East), Mumbai- 400 051 Email Id – ciso@sbicaps.com

Table of Contents

1. Introduction

1.1 Background

SBI Capital Markets Ltd and its Group companies ("SBICAP Group") are committed to improve its security posture and achieves this objective by updating its processes and technology periodically. Driven by this commitment, SBICAP Group is inviting bids from Managed Security Service Providers (MSSPs) to define, roll-out and support a comprehensive Security Operations Center (SOC) Framework which will provide assurance on the security posture and enhance SBICAP Group's capabilities to monitor, respond and mitigate threats against SBICAP Group. SBICAP Group Consist of:

i) SBI Capital Markets Ltd. (SBICAP) - Unit No. 1501, 15th floor, A& B Wing, Parinee Crescenzo Building, Plot C- 38, G Block, Bandra Kurla Complex, Bandra (East), Mumbai- 400 051
ii) SBICAP Group Trustee Co. Ltd. (STCL) - 04th Floor, Mistry Bhavan, 122 Dinshaw Vachha Road, Churchgate, Mumbai -400020.

SBICAP Group intends engaging with a Service Provider (SP) who has a sustainable and proven business model, recognized accreditation, established customer-base, distinguishable solution accelerators and enablers, high-performance personnel, while maintaining the ability to support SBICAP Group's evolving requirements.

SPs are advised to study the RFP document carefully. Submission of proposal shall be deemed to have been done after careful study and examination of the RFP document with full understanding of its implications.

The RFP will be conducted online by M/s e-Procurement Technologies Ltd. The response to this RFP should be full and complete in all respects. The SP must quote for all the items asked for in this RFP.

The SP shall bear all Prices associated with the preparation and submission of the proposal, including Price of presentation for the purposes of clarification of the proposal, if so desired by SBICAP Group. SBICAP Group will in no case be responsible or liable for those Prices, regardless of the conduct or outcome of the selection process.

1.2 Disclaimer:

1.2.1. The information contained in this RFP document or information provided subsequently to Bidder(s) whether verbally or in documentary form/email by or on behalf of SBICAP Group (Companies), is subject to the terms and conditions set out in this RFP document.

1.2.2. This RFP is not an offer by SBICAP Group, but an invitation to receive responses from the eligible Bidders. No contractual obligation whatsoever shall arise from the RFP process unless and until a formal contract is signed and executed by duly authorized official(s) of SBICAP Group with the selected Bidder.

1.2.3. The purpose of this RFP is to provide the Bidder(s) with information to assist preparation of their Bid 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 contained in this RFP and where necessary obtain independent advice/clarifications. Company may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFP.

1.2.4. SBICAP Group, its employees and advisors make no representation or warranty and shall have no liability to any person, including any Applicant or Bidder under any law, statute, rules or regulations or tort, principles of restitution or unjust enrichment or otherwise for any loss, damages, Price or expense which may arise from or be incurred or suffered on account of

anything contained in this RFP or otherwise, including the accuracy, adequacy, correctness, completeness or reliability of the RFP and any assessment, assumption, statement or information contained therein or deemed to form or arising in any way for participation in this bidding process.

1.2.5. SBICAP Group also accepts no liability of any nature whether resulting from negligence or otherwise, howsoever caused arising from reliance of any Bidder upon the statements contained in this RFP.

1.2.6. The issue of this RFP does not imply that the SBICAP Group is bound to select a Bidder or to appoint the Selected Bidder or Concessionaire, as the case may be, for the Project and the Company reserves the right to reject all or any of the Bidders or Bids without assigning any reason whatsoever.

1.2.7. The Bidder is expected to examine all instructions, forms, terms and specifications in the bidding Document. Failure to furnish all information required by the bidding Document or to submit a Bid not substantially responsive to the bidding Document in all respect will be at the Bidder's risk and may result in rejection of the Bid.

1.2.8. Proposed solution must be as per the detailed Technical Specifications and the Vendor should adhere to Scope of Work mentioned in this RFP.

1.2.9. The Purchase Order may be placed in part or full by SBICAP Group, the quantity or number of equipment to be purchased as mentioned in this RFP is only indicative. No guarantee or assurance is being provided hereby as to the exact quantity of equipment to be purchased or the minimum order quantity. SBICAP Group, however, reserves the right to procure extra quantity during the bid validity period of the offer and till 3 years from the date of project sign-off. The price of such procurement will be calculated on pro-rata basis of the balance period. The offer should be valid for SBICAP Group companies.

1.3. Definitions

Throughout this RFP, unless inconsistent with the subject matter or context:

1.3.1. **Vendor/ Service Provider/ System Integrator** – MSSP / SIEM Vendors.

1.3.2. **Supplier/ Contractor/ Vendor** – Selected Vendor/System Integrator under this RFP.

1.3.3. **Company/ Purchaser/ -** Reference to "Company" and "Purchaser" shall be determined in context and may mean without limitation "SBICAP / STCL

1.3.4. **Proposal/ Bid** – the Vendor's written reply or submission in response to this RFP

1.3.5. **RFP/Tender** – the request for proposal (this document) in its entirety, inclusive of any Addenda that may be issued by SBICAP Group.

1.3.6. **Solution/ Services/ Work/ System** – "Solution" or "Services" or "Work" or "System" all services, scope of work and deliverable to be provided by a Vendor as described in the RFP and include services ancillary for Security information Event Management - Security Operations Center (SIEM-SOC) for continuous log monitoring and analysis, co-relation of all logs, threats and vulnerabilities. Etc. covered under the RFP.

1.3.7. **Product** – "Product" means Security Information and Event Management, Security Orchestration, Automation and Response & User and entity Behaviour Analytics (SIEM, SOAR, UBA) Tools / services implemented for SOC monitoring and log collector as mentioned in the tender.

1.3.8. **Server / Network / Website** – As specified within the technical requirement section of this RFP document.

2. RFP Process

- The technical and commercial proposal with the relevant information/documents/acceptance of all terms and conditions as described in this RFP document will be submitted online through M/s e-

Procurement Technologies Ltd., Ahmedabad, the authorized agency approved by SBICAP Group for e-tendering on the website https://etender.sbi/SBI/.

- For any query related to e-tender and bid submission, the bidders may contact M/s eProcurement Technologies Ltd., Ahmadabad as mentioned below:

  e-Procurement Technologies Limited
  Email: allocation@eptl.in
  Website : https://etender.sbi

- The Bidders will have to upload the duly signed and scanned tender documents and all Annexure Forms as part of technical bid have to be submitted online.
- The tender document is not required to be sent to us in hard copy.
- Please find below the RFP schedule for submissions and evaluations.

1.	Release of RFP	6th August 2025
2.	Pre-Bid Queries on email	13th August 2025
3.	Online Technical & Commercial Bid submission	14th August 2025 - 14:00 Hrs
4.	Technical Bid Evaluation and Presentation of shortlisted Service Providers	18th August to 21st August 2025 (tentative schedule)

2.1 The bidders are requested to note that:

a) They cannot make their online submission after the time stipulated above, and no extension of time will be permitted for submission of bids.
b) It is mandatory to have a valid digital certificate issued by any of the valid Certifying Authority approved by Government of India to participate in the online bidding. The bidders are requested to ensure that they have the same, well in advance or if any assistance is required for the purpose, Bidders can contact our service provider (M/s e-Procurement Technologies Ltd.).

2.2 Terms & Conditions:

2.2.1. Tender should strictly confirm to the specifications. Tenders not conforming to the specifications will be rejected summarily. Any incomplete or ambiguous terms/ conditions/ quotes will disqualify the offer.
2.2.2. SBICAP Group reserves the right to accept in part or in full or reject the entire quotation and cancel the entire tender, without assigning any reason there for at any stage.
2.2.3. Any terms and conditions from the Vendors are not acceptable to the SBICAP Group.
2.2.4. SBICAP Group reserves the right to impose and recover penalty from the vendors who violate the terms & conditions of the tender including refusal to execute the order placed on them for any reasons.
2.2.5. Not with standing approximate quantity mentioned in the Tender the quantities are liable to alteration by omission, deduction or addition**.** Payment shall be regulated on the actual work done at the accepted rates and payment schedule.
2.2.6. The L1 rates finalized discovered will be valid for 36 months and the L1 vendor is bound to execute the orders placed at L1 rates during the duration of the contract.
2.2.7. The validity period may be extended at the discretion of SBICAP Group which will be binding on the vendors.
2.2.8. The prices quoted for SOC services should be for three years.

2.2.9. The prices should be **exclusive of all taxes**, the vendor should arrange for obtaining of permits wherever applicable.

2.2.10. The Vendor should attach all the related product literature, data sheets, handouts, evaluation reports etc., pertaining to the SOC for which the Vendor has quoted.

2.2.11. Vendor shall ensure that the SOC implemented have use cases with capabilities to detect both internal and external attacks/threats.

2.2.12. The tools used for SOC by the vendor should be licensed one.

2.2.13. Cloud based solution / tools and the channel being used, should be clearly stated.

2.2.14. Vendor shall conduct monthly meetings with SBICAP Group and develop use cases to be integrated on the SIEM solution. Vendor shall ensure that use cases are updated regularly to keep it relevant to emerging threats.

2.2.15. It would be binding upon the vendor to maintain security of SBICAP Group systems at all times.

2.2.16. SBICAP Group may changes the bid evaluation criteria at its own discretion after receipt of bids from competent bidder. SBICAP Group also reserves the rights to remove components from Commercial bid for evaluation purpose and for releasing the work order for partial scope.

2.2.17. SBICAP Group will notify successful Bidder in writing by way of issuance of purchase order through letter or email that its Bid has been accepted. The selected Bidder has to acknowledge by return email/letter in token of acceptance.

2.2.18. Penalties for Delayed Implementation - The SOC Implementation should be started immediately from the date of placing the letter of Intent / Purchase order whichever is earlier. If delayed, SBICAP Group will charge a penalty of 1% of order value for every week of delay, subject to a maximum of 5% of the order value or will lead to cancellation of the purchase order itself.

2.2.19. The Bidders will have to submit the Service Level Agreement as per Annexure - E and Nondisclosure Agreement as per Annexure – J together with acceptance of all terms and conditions of RFP, duly signed by the authorized signatory.

2.2.20. Copy of board resolution and power of attorney (POA wherever applicable) showing that the signatory has been duly authorized to sign the acceptance letter, contract and NDA should be submitted.

- The agreement shall remain in force from the date of entering contract, but it can be suspended/cancelled at any time and any stage by SBICAP Group during the validity of the contract without assigning any reason. No claim or damage on account of such cancellation/suspension of the contract/license shall be entertained.
- The renewal of the contract can, however, be done to the satisfaction of SBICAP Group about the performance, rates, etc.
- The bidders shall depute a senior officer of the company as a Project Manager who shall act as a single point of contact for all activities regarding this project. The Project Manager shall be capable to make on-site decisions regarding the scope of the work and any changes required thereon.
- The technical proposal shall be evaluated for technical suitability as well as for other terms and conditions.
- Selected bidders shall be awarded with work order as per terms and condition as has been defined in this document and subsequently an Agreement shall be executed between SBICAP Group and the selected bidders.
- Bidders should specify only a single solution which is cost-effective and meets SBICAP Group requirement and should not include any alternatives.
- The Bidders shall bear all costs associated with the preparation and submission of its proposal, attending Pre-Bid meeting or arranging proof of concept (POC)/Product Walk through etc. SBICAP Group shall provide no reimbursement for such costs.
- To assist in the scrutiny, evaluation and comparison of offers SBICAP Group may, at its discretion, ask some or all bidders for clarification of their offer.

- All design requirements should be worked around the requirements given by SBICAP Group.
- Bidders shall be responsible for Post implementation management, on-site support, Call centre services/help desk, etc.
- Bidders shall be responsible for knowledge transfer to the incoming company at the end of the contract period or at any stage in case of termination of the contract.
- Any effort by the applicant to influence SBICAP Group on any matter relating to the proposal, its evaluation, comparison, selection may result in the rejection of the bidder's proposal.
- In case of any upward change in transaction rates (excluding of taxes) on account of regulatory guidelines/directions, the same is to be absorbed by the bidders whereas in case the revision is downwards, the benefit is to be passed on to the SBICAP Group
- All guidelines issued by Central Government from time to time with respect to various activities of the sector under which the bidding company falls shall be mandatorily binding on the company. The bidders should keep themselves updated and ensure necessary up-gradations/enhancements for complying with the guidelines, without extra cost to SBICAP Group.
- The bidders shall be responsible for maintaining all security compliances necessary for their services.
- The bidders should not capture/store/use/share any of the stakeholders' information (like license number, name, phone number, card details etc.) for any purpose, other than the ones specified in this document.
- Bids submitted shall remain valid for 180 days from the date of opening of the bids.
- In case of complete failure of operations at DC, the Service provider has to ensure that the traffic coming to DC is pointed to DR.

2.3 Payment Terms:

Sl. No.	Details
1.	Payment would be done on quarterly-in-arrears basis at the end of the quarter upon receipt of invoice from vendor.

2.4 Force MAJEURE

If any time, during the continuance of this Agreement, the performance in whole or in part by either party or any obligation under this Agreement shall be prevented or delayed by reason of any war, or hostility, fires, floods, explosions, epidemics, quarantine restrictions, or act of God (herein after referred to as events) provided notice of happenings, of any such eventuality is given by either party to the other within 21 days from the date of occurrence thereof, neither party shall by any reason of such event be entitled to terminate this Agreement nor shall either party have any such claim for damages against the other in respect of such non-performance or delay in performance, and deliveries under the Agreement shall be resumed as soon after such event may come to an end or cease to exist, and the decision of the SBICAP Group as to whether the delivery have been so resumed or not shall be final and conclusive, provided further that if the performance, in whole or part of any obligation under this contract is prevented or delayed by reason of any such event for a period exceeding 60 days SBICAP Group may, at its option terminate the Agreement.

Limitation of Liability

Vendor's aggregate liability under the contract shall be limited to a maximum of the contract value. This limit shall not apply to third party claims for: -

IP Infringement indemnity

The Services shall be provided by Bidder exclusive of any warranties whatsoever, whether express or implied, including but not limited to warranties of merchantability, noninfringement, fitness for a specific purpose or fitness for ordinary purpose.

In no event shall either party be liable to the other for any indirect, incidental, special, consequential, exemplary or punitive damages including, but not limited to, damages for lost revenue, lost profits, loss of goodwill, loss of data, technology, equipment or types of damages whatsoever, whether or not caused by any acts of omission or commission and regardless whether such party has been informed of the possibility or the likelihood of such damages. Under no circumstances will Bidder's liability for direct damages, whether arising out of tort or contract or any other doctrine of law, exceed the provisions as per this Clause 8 relating to Limitation of Liability.

REJECTION/TERMINATION OF AGREEMENT

1. Either party may terminate this Agreement if the other party breaches any material term or condition of this Agreement and the breaching party fails to cure such breach within thirty (30) days of receipt of written notice of the same from the other party, unless where such breach is irremediable in nature.
2. Either party may terminate this Agreement if the other party becomes the subject of an involuntary or voluntary petition in bankruptcy or any voluntary or involuntary proceeding relating to insolvency, receivership, liquidation or composition for the benefit of creditors, if such petition or proceeding has not been dismissed within sixty (60) days of filing or such prescribed period under the Insolvency and Bankruptcy Code of India.
3. In case the SBICAP Group terminates or downgrades any Service(s) under the Agreement for convenience (i.e. for any reason other than a material breach that is not remedied by Service Provider) prior to end of such initial Service term, SBICAP Group shall not be liable to pay any termination charge or penalty.
4. Subject to limitations of Clauses 3. above and clause 5 below, either party may terminate this Agreement for convenience by service of ninety (90) days written notice delivered at each other's notified addresses.
5. SBICAP Group understands and agrees that dedicated hardware and / or software [including but not limited to servers, routers, switches, firewalls, load balancers and storage devices ("Dedicated Service Provider's Equipment")], if any, provided to the SBICAP Group by Service Provider for Services are tailored to the SBICAP Group's individual or specific need by Service Provider and any early termination or downward revision of Services related to such Dedicated Service Provider's Equipment by SBICAP Group would be detrimental to Service Provider from commercials (including pricing) perspective. So if in the event SBICAP Group contracts for Dedicated Service Provider's Equipment and terminates, in part or full, or scales downwards any of the Services related thereto or this Agreement, without cause i.e. for convenience before the end of the Service Term, then SBICAP Group shall not be liable to pay any termination charge or penalty.

Confidentiality

This document contains information confidential and proprietary to SBICAP Group. Additionally, the Bidder will be exposed by virtue of the contracted activities to internal business information of SBICAP Group, the Associates, Subsidiaries and/or business partners. The Bidders agree and undertakes that they shall keep confidential all matters relating to this RFP and will not make any disclosure to any person who is under the obligation under this document, any information, data, and know-how, documents, secrets, dealings, transactions or the terms or this RFP (the "Confidential Information"). Disclosure of receipt of this RFP or any part of the aforementioned information to parties not directly involved in providing the services requested could be treated as breach of confidentiality obligations and SBICAP Group would be free to initiate any action deemed appropriate.
The restrictions on disclosure of confidential information shall not apply to any matter which is already available in the public domain; or any disclosures made under law.
No news release, public announcement, or any other reference to this RFP or any program there under shall be made without written consent from SBICAP Group. Reproduction of this RFP, without prior written consent of SBICAP Group, by photographic, electronic, or other means is strictly prohibited.

Non-Disclosure Agreement

The shortlisted bidder will be required to sign a Non-Disclosure Agreement with SBICAP Group. The Bidder shall treat all documents, information, data and communication of and with SBICAP Group as privileged and confidential and shall be bound by the terms and conditions of the Non-Disclosure Agreement.

Governing Law and Jurisdiction

All disputes and controversies arising out of this RFP and related bid documents shall be subject to the exclusive jurisdiction of the Courts in Mumbai and the parties agree to submit themselves to the jurisdiction of such court and the governing law shall be the laws of India.

Arbitration

All disputes and differences of any kind whatsoever shall be settled by Arbitration in accordance with the provisions of Arbitration and Conciliation Act, 1996 or any statutory amendment thereof. The dispute shall be referred to the sole arbitrator who shall be appointed by SBICAP Group. The venue of Arbitration proceedings shall be at Mumbai. The Arbitration proceedings shall be conducted in English Language. The award of the Arbitration shall be final and binding on both the Parties and shall be delivered in Mumbai in the English language. The fees of the Arbitrator and the cost of the Arbitration proceedings shall be equally borne by both the Parties.

Data Protection

The Bidders authorizes the release from time to time to SBICAP Group (and any of its Subsidiaries or Affiliates) all personal or professional data that is necessary or desirable for the administration of the RFP (the "Relevant Information"). Without limiting the above, the bidders permit SBICAP Group to collect, process, register and transfer to and aforementioned entities all Relevant Information. The Relevant Information will only be used in accordance with applicable law.

Intellectual Property

SBICAP Group shall have sole exclusive ownership to all its Intellectual property including and not limited to its trademarks, logos etc. This RFP shall in no way be considered as a transfer or assignment of the respective rights over any intellectual property owned, developed or being developed by SBICAP Group.

2.5 List of the Annexures: Annexure A to J to be submitted online.

Sr.No.	Particulars	Annexure	To be submitted
1	Technical Specification and Scope of Work	Annexure-A1	Yes (With Eligibility Criteria)
2	Scope of Work for offshore Resident Engineer	Annexure-A2	Yes (With Eligibility Criteria)
3	Inventory	Annexure-B	Yes (With Technical Bid)
4	Bidders Organization Profile	Annexure-C	Yes (With Technical Bid)
5	Eligibility Criteria	Annexure-D	Yes (Before Technical Bid)
6	SLA terms	Annexure-E	Yes (With Technical Bid)
7	Pre-Bid Queries	Annexure-F	Yes
8	Evaluation Process	Annexure-G	-
9	Technical Bid	Annexure-H	Yes
10	Tender Document duly signed		Yes (With Technical Bid)
11	Commercial Bid	Annexure-I	Yes
12	Final Price Break-up by L1 vendor	Annexure-J	Yes (For L1 Bidder)
13	NDA	Annexure-K	Yes (For L1 Bidder)
14	Service Level Agreement	Annexure-L	Yes (For L1 Bidder)

3. Annexure – A1 : Technical Specification and Scope of Work

Compliance: C – Fully compliant, P – Partially Compliant, N – Not compliant
Category: M – Mandatory, O - Optional

The key requirements of SOC Transformation are as follows:

Sr.No.	Requirements	Category	Compliance	Remarks
1	**Security Monitoring Requirements**			
1.1	Vendor should monitor security logs to detect malicious or abnormal events and raise the alerts for any suspicious events that may lead to security breach.	M		
1.2	Vendor should provide log baselines for all platforms under scope that are required to be monitored.	M		
1.3	Vendor platform should have capability to collect logs from most of the standard platforms like Windows, Linux, AIX, Solaris, Firewall, Network and other security devices or solution, etc.	M		
1.4	Vendor Platform should be able to collect logs from most of standard network, security devices, Data bases, Web servers and cloud services (Aws/Azure), SAAS Solutions, O365, etc.	M		
1.5	Vendor should have a tool capable of detecting both internal & external attacks. In addition to security attacks on IT infrastructure, vendors should also monitor for security events on databases and servers.	M		
1.6	Vendor should carry out correlations amongst the logs from multiple sources to detect multi-vector attacks.	M		
1.7	Vendor operations team should send alerts with details of mitigation steps to a designated distribution list provided SBICAP Group.	M		
1.8	The Vendor should bring workflows and solutions that can automate majority of the incident response activities such as false positive management, managing whitelists, escalation workflow, SLA management etc.	M		
1.9	Alerts should be notified to SBICAP Group only after proper triage process. Alerts from SIEM should be enriched with context data, environmental data, vulnerability data received from SBICAP Group, historical data, threat intelligence etc.	M		
1.10	Historical parameters should include and not limited to attack volume, attacker volume, and destination volume for every alert.	M		
1.11	Vendor should give long term solution to prevent such threats in future	M		
1.12	Define, Develop and implement Use Cases based on standard methodologies such as Cyber Kill Chain	M		

1.13	Service provider should have capability to integrate log from nonstandard application and devices and service provider platform should be able to process them for generating alerts and reports. This should be accomplished through standard or custom parsers as applicable.	M		
1.14	Service Provider should have a Remote SOC which is certified in Major Industry Certifications such as ISO, PCI, SOC1, SOC2, BCMS, ISMS, CERT-IN empanelled.	M		
1.15	Service provider to assist the organization to ensure the log retention is as per local regulatory requirement like SEBI, NSE, and BSE, etc and parallelly aligning with the Organisations log retention policy.	M		
1.16	Service Provider's solution should have capabilities to define rules on event logs captured from various sources to detect suspicious activities Examples • Failed login attempts • Successful Login attempts from suspicious locations or unusual systems • Authorization attempts outside of approved list • Vendor logins from unauthorized subnets • Vertical & Horizontal port scans • Traffic from blacklisted IPs • Login attempts at unusual timings	M		
1.17	Service provider solution should be able to provide charts for top attacks & attackers, OWASP based threat analysis, Trending threats, attack demographics etc. by utilizing the WAF solution deployed in SBICAP Group.	O		
1.18	The proposed system shall be able to capture all details in raw log, events and alerts and normalize them into a standard format for easy comprehension.	M		
1.19	The proposed solution should prevent tampering of any type of logs and log any attempts to tamper logs. It must provide encrypted transmission of log data to the log management by enabling required encryption methods needed.	M		
1.20	Any failures of the event collection infrastructure must be detected and operations personnel must be notified.	M		
1.21	The solution should be able to support enrichment of data with contextual information like Geo Data, malicious IPs, Domains, URLs, Threat Intel and custom specified tags and annotations. The enrichment fields should be indexed along with the event in real-time at an individual event level and not done as a separate lookup process.	M		
1.22	Vendor should have a tool capable of monitoring, detecting and managing incidents for the following minimum set of database security events. This is an indicative list and is not a comprehensive/complete set of events. Vendors should indicate their event list in proposal response. • Monitor Access to Sensitive Data (e.g. PII data)	M		

	• Database access including logins, client IP, server IP and source program information. • Track and audit administrative commands			
1.23	Vendor should monitor, detect and manage incidents for the following minimum set of IT infrastructure security events by integrating the WAF/Firewall solution deployed at SBICAP Group. This is indicative minimum list and is not a comprehensive/complete set of events. • Buffer Overflow attacks • Port and vulnerability Scans • Password cracking • Worm/virus outbreak • File access failures • Unauthorized service restarts • Unauthorized service/process creation • Unauthorized changes to firewall rules • Unauthorized access to systems • SQL injection • Cross site scripting • All layer 7 web attacks via internet / intranet	M		
1.24	Vendor should monitor, detect and manage incidents for the following minimum set of business application security events. This is an indicative list and is not a comprehensive / complete set of events. • Attempted segregation of duties violations • Attempted access violations • Critical user additions, deletions • Creation, deletion and modification of critical application roles/Groups • Changes to permissions or authorizations for critical application roles/Groups • Changes to account and password policies in the application • Changes to critical application parameters • Changes to audit parameters	M		
1.25	The SOC solution must provide Central Management of all components and administrative functions from a single web-based user interface for SIEM, NBAD, UBA.	M		
1.26	SIEM solution should be able to correlate Events & Flows together to generate incidents.	M		
2.	**Incident Analysis**			
2.1	Solution should support centralized incident management to prioritize and manage security incidents.	M		
2.2	Solution should support triaging of alerts from number of security products including SIEM, DLP, IPS, WAF, Anti-APT, ETDR, etc.	M		
2.3	Solution should support machine driven triaging algorithms that considers contextual parameters, historical behaviour and external threat intelligence to enrich and arrive at a	O		

	triage score in real time. Triage score should form the basis for prioritizing the alert and further action on the same • Environmental parameters should include and not limited to asset criticality, user criticality, and vulnerability status for every alert. • Historical parameters should include and not limited to attack volume, attacker volume, destination volume for every alert, severity of alert and so on. • Central Threat Intelligence feed should also be applied to identify threats through known bad actors			
2.4	Solution should support a rule engine for users to define custom triage rule. Rule engine should support asset data fields, event data fields, user data fields, triage score, and triage parameters	O		
2.5	Solution should enable investigation of triaged alert/custom alerts deemed critical	O		
2.6	Investigation module should integrate with log sources (SIEM, ETDR, EPP, Data Lake) on demand to pull data related to the investigated alert. It should also include charting and graphs to analyse data	M		
2.7	Solution should have features to analyse impact of the attack on the targeted asset including configurations, Indicators of Compromise (IOCs), external network connections, etc.	O		
2.8	Solution should support features to identify attacker attributes including threat intelligence score of attackers, who-is lookup information, geo-mapping in a single console.	M		
2.9	Solution should support models to build up the entire attack chain- from attack inception, progress of the attack and spread to attack in the network.	O		
2.10	Solution should provide run books for investigation steps corresponding to different types of attacks, derive attack inception and progress of the attack. i.e. Detect Patient Zero, Attack origin and Blast Radius.	O		
2.11	Solution should support integration with open source or commercial IOC sources. List the supported sources which can be integrated with Solution and brief on the integration approach. Solution should support features to analyse and identify the impact of this attack on other assets.	M		
2.12	Solution should support models to derive attack inception and progress of the attack. List the details of investigation models used in the Solution.	O		
2.13	Solution should provide case management features to store raw and analysed data for a specific alert or set of alerts. Provide details on what artefacts can be stored related to an investigation	M		
2.14	Solution should support quick search across stored datasets in the Solution. Provide details of search features supported.	M		
2.15	Solution should provide run books for investigation steps corresponding to different types of attacks.	M		

3.	**Incident Response**			
3.1	• Solution should support quick response to an ongoing incident or serious threats with remote configuration of parameters in servers/desktops, Firewalls, AD (Active Directory), IPS, WAF, Network Switches & Routers etc. • Automated Remediation for responding to commodity threats (e.g. recall malicious mails from inboxes, block bad IPs in Firewall, Disable bad users in Active Directory, etc.) • Solution should support multiple configuration parameters to servers/desktops including removal/changes to services, users, registry keys, software, and browser plugins.	O		
3.2	Solution should support the full workflow for incident classification, incident coordination such as assigning activities to different teams and tracking for closure, escalation of tasks, and exception approvals.	M		
3.3	Solution should support the full workflow for incident coordination.	M		
3.4	Solution should support sending notifications to common distribution list provided by SBICAP Group	M		
3.5	Solution should support the workflow required to approve such auto mitigation action or have option to exempt certain auto mitigation from approval process.	O		
3.6	Solution should support escalation workflows. Provide details on the escalation matrix within Solution along with the levels and list the escalation medium (SMS/email using gateway provided by SBICAP Group)	M		
3.7	Solution should support tracking of security exception approvals for those threats and incidents for which remediation is not possible or compensating controls are available.	O		
3.8	SP to provide Ticketing tool – SOC operations access to SBICAP Group.	M		
3.9	Solution should provide alert details and investigation outcomes linked and viewable for relevant remediation tickets.	M		
3.10	Incident Report with classification, chronology of events, RCA, IOC	M		
3.11	Track impacted assets related to an incident	M		
3.12	Tools for Response based on data and analytics	M		
3.13	Ability for quick Counter Response by integrating with devices such as firewall and AD for blocking traffic or quarantine system	O		
3.14	Usage of Ticketing and case management workflow	M		
3.15	Classification of incidents	M		
3.16	Maintain track of first response and subsequent measures taken for the incident	M		

3.17	Maintain chronological order of events related to incident response	M		
3.18	Maintain IOC and artifacts related to incident	M		
3.19	Incident response should include investigation of end points if required to conclude the investigation	M		
3.20	Centralized incident management to prioritize and manage security incidents.	M		
3.21	SP should bring a platform which facilitates collaboration between SOC and SBICAP Group with features comments on incidents, maintaining a history of conversation with timeline, ability to add artifacts	M		
4	**Threat Hunting Requirements**			
4.1	Use algorithms and tools to actively hunt of attacks in large volume of data and create alerts that are passed on to analysts. Supports use of Big data platform for collection and analysis	M		
4.2	Define, develop, implement, update and maintain Hunting Framework which contains: • Create Strategic Hunt Missions which are objective based to identify malicious activity that has not triggered an alert • Search for Indicators of Compromise received from Threat Intelligence and Analytics	M		
4.3	Create knowledge base of IOCs	M		
4.4	Vendor should provide security solution to able to detect unknown attacks	M		
4.5	The Solution should have models that are able to detect attacks in various stages of a cyber kill chain	M		
4.6	The Solution should able to detect threats from various attacks vectors such as malware, web application attacks, network attacks, watering hole attacks, DNS attacks, insider threat, and data exfiltration. List the detection use cases which can detect above attacks using pre-built machine learning techniques and analytical models.	M		
4.7	Solution using machine learning techniques should use multiple sources to identify malicious activity. A minimum the following sources should be used: • Netflow • IPS/IDS • Proxy • WAF • Windows logs • DNS • FW	M		
4.8	Solution should have pre-built AI models to detect targeted attacks (unknown attacks from unknown threat actors).	O		
4.9	Solution should have models to detect attacks in different stages of Cyber Kill chain.	O		

4.10	Network Threat Hunting should leverage existing network sources for better detection of advanced attacks. Network sources should include Netflow, Proxy, DNS, IPS, VPN, Firewall, AD/Windows, Email logs	M		
4.11	Network threat hunting should enable hunting for attacks including but not limited to Lateral Movement, Malware Beaconing, Data Exfiltration, Watering Hole, Targeted network attacks, Dynamic DNS attacks	M		
4.12	The service must be capable of identifying suspicious or hitherto undiscovered communication patterns. The service must support detection of newly discovered pattern in future	M		
4.13	The service should identify network traffic from potentially risky applications (e.g. file sharing, peer-to-peer, etc.).	M		
5	**Endpoint Detection and Response**			
5.1	The Platform to be provided by the Service Provider should support Integration of the EDR platform to be provided by SBICAP Group and build use cases for detection of the below ask	O		
5.2	Endpoint threat hunting should hunt for Process anomalies, Service anomalies, Hash values, Connection anomalies and indicators of compromises.	O		
5.3	EDR hunting should help to detect anomalies at the end point such as: • Detect Command and control activities • Detect Data stealing activities • Assess weakness by looking at vulnerabilities. • Searching for IOCs • Outlier detection of active system process, driver, services, network connections, etc.	O		
5.4	EDR should help perform the following: • Collection of forensic artifacts (Name, Hash code, Size, Loaded DLLs) of all binaries running in organization. • Matching of forensic artifacts against known indicator of compromise. • Segregating unknown forensic artifacts from known forensics artifacts. • Clustering of unknown forensic artifacts to find outlier binaries. • Analysing outlier binaries using supervised neural network.	O		
5.5	EDR service should be able to take quick response actions such as: • Killing anomalous processes, deleting malicious binaries · Isolating end points	O		
5.6	Detect threats on endpoints by deploying EDR agents. The service should be able to take containment actions such as isolating infected endpoints	O		
5.7	Detect user anomalies using a combination of rules and machine learning model. Optionally provide sensors to capture network traffic to detect threats at the network level.	O		

6.	**User Behaviour Analysis**			
6.1	Solution should provide UBA dashboard based on various UBA models outcome. • UBA Dashboard should highlight risky users based on objective scoring of users based on composite risk score comprising all behaviour anomalies of the user • Organization should be able to define risk thresholds based on their risk appetite	M		
6.2	Detect malicious/illegal activities performed by users	M		
6.3	Solution to have capabilities to collect user data from variety of sources like Directory Services, IAM, VPN, Proxy, O365, etc.	M		
6.4	Service should be able to track user ‘s activities locally and remote network sites and should be able to report usage behaviour across the entire network.	M		
6.5	The service should incorporate multiple baseline behavioural models which cover behavioural risk categories like Data Exfiltration, Malicious Users, Illicit Behaviour, compromised credentials, etc.	M		
6.6	Solution should support business application threat hunting for application to detect access and authorization anomalies using application logs, NetFlow.	M		
6.7	Solution should be able to search proactively and iteratively through a network or logs data to detect and isolate advanced threats that evade Signature based systems (SIEM, IDS, DLP etc.)	M		
6.8	Service provider should submit a monthly threat hunting based on the threat hunting performed on the logs generated for SBICAP Group	M		
7.	**Threat Intelligence**			
7.1	Service should anticipate likely threats to the Organization based on global threat events and data and provide proactive measures to prevent such happenings in the Organization.	M		
7.2	Service should support integration of machine-readable threat intelligence from different open and commercial sources. It should support providing weightage against sources and support algorithms to reduce noise & false positives in threat intelligence feeds	M		
7.3	SBICAP Group team would provide strategic threat intelligence about incidents and breaches happening across the globe for SBI Group and the Service Provider should analyse and provide recommendations such as • Can SBICAP Group be susceptible to such an attack? • If yes, which assets in the organization are susceptible? • Provide IoC’s where relevant • Provide mitigation steps for each advisory	M		
7.4	Solution should support STIX/TAXII for automated integration of actionable intelligence with security technologies.	M		
7.5	Service should support 3rd party / external threat intelligence to aid incident response by bringing in	M		

	organizational context and internal information available in SIEM and other sources of security information			
8	**Vulnerability Management**			
8.1	Mitigation recommendation (for in-scope infrastructure) based on the Vulnerability report shared by SBICAP Group to be provided by Bidder	O		
8.2	Co-relation of vulnerability information with the Threat management system to get 360-degree view of the asset in Scope.	O		
9	**General Requirements**			
9.1	Service provider team supporting SBICAP Group should have the following skills sets: • Security analysts • Threat hunter • SIEM Administration	M		
9.2	The platform should have machine learning capabilities and other advanced analytics of structured as well as unstructured security & network data.	O		
9.3	The Log management solution (Centralized) is required at SBICAP Group for collection of logs from different log sources. Log collector tool shall be provided by the vendor to collect the logs at the SBICAP Group location. VMs and Storage for Log collector will provide by SBICAP Group. Vendors need to ensure logger hardware details incorporated. Vendor shall provide complete details of required Hardware (Compute / Storage) for Logger solution. Sizing and architecture required for this project should be endorsed by the OEM in writing and the proof of this will have to be submitted. SBICAP Group will arrange hardware as per specification shared by vendor. Any shortfall will have to be filled by the Vendor at its own cost.	M		
9.4	Vendor shall build the capacity of the SIEM solution that can handle the log retention as mentioned below: • Six months – Online • Two Years – Offline	M		
9.5	24x7x365 real time logs monitoring, analysis and correlation, Threat hunting, Threat Intelligence consisting of Indicators of Compromise (IOC) and other threat intel (vulnerabilities report, incident reports etc.).	M		
9.6	The proposed solution should provide end-to end capability to setup an SIEM SOAR for storage, indexing, searching, analysis, correlation, reporting, visualization, orchestration of different types of structured security data generated within the organization.	M		
9.7	The proposed system should support SAN, NAS and DAS for adding external storage as and when required. The bidder is expected to size the storage as per the requirements mentioned in this RFP. The bidder ‘s response should include the calculations/ logic used to arrive at the sizing. It is to be noted that proposed hardware should be based on	O		

	RAID 5. The solution should have adequate redundancy for handling disk failures.			
9.8	Vendor will be responsible to store logs in industry standard solution and format.	M		
9.9	If connectivity between log collection agents and logger is down, then the Log collector agents should store the logs of at least 3 days and send them once connectivity is established. This would be applicable if the Service Provider is proposing cloud-based solution or separate logger and processing units.	M		
9.10	Alerting events/incidents and recommending remedial actions.	M		
9.11	Incident analysis (Triage) to remove false positives, incident notification.	M		
9.12	Daily report of events/incidents, correlation, analysis and recommendations. The daily report shall cover the correlation analysis of all the devices included as part of scope.	M		
9.13	Monthly report summarizing the list of events/incidents reported, correlation analysis, recommendations, status of actions by SBICAP Group and other security advisories. It should include the trend analysis comparing the present month's data with the previous month data. Weekly advisory details should be provided by the vendor.	M		
9.14	Detect known as well as unknown threats by using machine learning and security analytics	O		
9.15	Consolidate data and extract actionable insight from a variety of intelligence sources and existing security technologies	M		
9.16	Service Provide to Proactively perform threat hunting, which otherwise gets undetected via signature-based systems on monthly basis	M		
9.17	Be Cyber-Ready to respond to attacks swiftly.	M		
9.18	Complete analysis and correlation of logs from all the devices/solutions under scope	M		
9.19	Provide and/or develop parsing rules for standard/ non-standard logs respectively. Pre-defined / custom parsers should be available for parsing logs for the following applications but not limited to: Oracle E-Business Suite, OpenText Documentum platform etc.	M		
9.20	The proposed solution should have available connectors to support the standard devices / applications, wherever required the vendor should develop customized connectors for all standard/custom devices/applications at no extra Price	M		
9.21	24x7x365 uninterrupted security monitoring operations. Submit a report in case of service non availability of the devices along with the status.	M		
9.22	Automate security processes to reduce resource drain and threat response times	M		

9.23	The bidder must have skilled OEM certified staff at various levels (L1/L2/L3). Skilled and capable staff with expertise in at least the following domains. • Event monitoring and analysis • Incident detection and response • Threat Intelligence • Use Case engineering and new integrations to increase visibility • Threat Hunting • Security Analytics	M		
9.24	Correlation of low priority alerts with subsequent alerts to detect multi-stage attacks.	M		
9.25	Reduction of remediation time • Automated real time prioritization of alerts • Automated data collection for investigation followed by quick analysis on a single window. • Assisted remediation steps (integration with security devices to push policy/configuration remotely) for faster mitigation of threats	M		
9.26	Provide central dashboard to capture risk posture and maturity levels of organization at any given point of time.	M		
9.27	Comprehensive security dashboard (web-based dashboard) for viewing real-time incidents/events, alerts, status of actions taken, tracking of key security metrics and provide security threat scorecards.	M		
9.28	Vendor shall provide different dashboard and screens for different roles as mentioned below for viewing real-time incidents / events, alerts, status of actions taken etc.: • Top Management (Company View) • IS Team (complete and detailed dashboard of security posture of the organization setup being monitored through this SOC) • Auditors (Internal auditor, External auditors etc.)	M		
9.29	The offered cyber security product shall ~~be~~ assisted in complying with SEBI guidelines on Cyber security for financial intermediaries.	M		
9.30	Vendor needs to ensure that SOC solution can integrate with the IT system using standard methods/ protocols/ message formats without affecting the existing functionality of SBICAP Group.	M		
9.31	SOC setup/infrastructure may be subjected to audit from SBICAP Group and/or third party and/or regulatory body. It shall be responsibility of the Vendor to co-operate and provide necessary information and support to the auditors. The Vendor must ensure that the audit observations are closed on top priority and to the satisfaction of SBICAP Group and its appointed auditors. Due care should be taken by the Vendor to ensure that the observations do not get repeated in subsequent Audits.	M		
9.32	The solution should consist of security monitoring, incident response, proactive threat hunting, threat Intelligence	M		

	consisting of Indicators of Compromise (IOC) SIEM engineering, User Behavioural Anomaly detection, and network threat detection.			
9.33	Service Providers should propose monitoring platforms, to best suit the requirements stated in the RFP.	M		
9.34	To Develop & recommend improvement plans for the SOC as needed to maintain an effective and secure computing environment	M		
9.35	For improvement of SOC Monitoring at SBICAP Group. SP should do the Firewall rules review half yearly basis and Network architecture review annually. This could be an optional service, but the Service Provider should have an in-house capability to provide this.	O		
9.36	Effective and Efficient Governance Model with fortnightly, monthly, quarterly and annual reviews	M		
9.37	SLA's and implementation timelines for the various activities would be mutually agreed while signing a contract with the selected SP. However, SP is expected to give an overall implementation and roll out plan as part of this proposal with templates of SLA, Project Plan, Governance meeting templates etc.	M		
9.38	UEBA shall be considered as part of MSSP services, monitoring devices which provides insight of anomalies and potential risk to the network.	M		
9.39	The applications and databases logs shall be considered for the correlation.	M		
9.40	Standard Operating Procedure (SOP) shall be developed for all the products /solutions /services provided including alert management, incident management, forensics, report management, log storage and archiving, SOC business continuity, operational documents, escalation matrix, change management, use cases, knowledge documents, playbook etc.	M		
9.41	Analytical reports on Daily, weekly and Monthly basis and Ad-hoc reports as and when to be provide by service provider	M		
9.42	IT Forensic services for root cause of incident and investigations as and when required. This could be an Optional Service, but the service provider should have an capability to provide this as and when asked by SBICAP Group.	O		
9.43	During the exit of the contract or services vendor should provide logs as per retention period from their end to SBICAP Group without any Price	M		
9.44	Service provider should have a comprehensive portfolio of platform-based security solutions to complement the SOC in the future	M		
9.45	Service provider should have experience to run SOC as a service	M		
9.46	Service provider should have expertise to provide next gen SOC solution like SOAR, EDR, WAF, DDOS etc.	M		

9.47	The solution proposed should be in the Gartner's Magic Quadrant for SIEM for the last 5 years	M		
9.48	The bidder should have implemented Security Information and Event Management (SIEM) /any other security solutions and it should be currently running as on the date of the RFP in any one of i. BFSI sector organizations/ Listed companies globally. OR ii. Government organizations / PSUs/Schedule Commercial Banks in India.	M		
9.49	The solution must provide 'canned' out-of-the-box reports for specific compliance regulations (PCI, SOX, FISMA) and control frameworks including (NIST, COBIT, ISO).	M		
9.50	The solution should have a single portal which would provide dashboards, reports, incidents and ability to raise and update incidents	M		
9.51	The solution should have a mobile app which will allow ability to raise and update tickets on the go	O		
10	**Security Incident and Crisis Management services – This would need to be provided as a one-time service at the start of the contact.**			
10.1	Alignment of Security Incident management plan in line with SBICAP Group Cyber Crisis Management Plan (CCMP) and Cyber Security Policy	M		
10.2	The Incident and Cyber crisis management support shall be (preferred offsite and, in case of emergency, onsite support is mandatory) provided by MSSP	O		
10.3	MSSP will provide a detailed process for managing cyber incidents - describing each phase of the process – prepare, identify, contain, eradicate, recover and learn from the incidents	O		
10.4	Develop response plan/ strategy which will describe the prioritization of incidents based on the organizational impact	M		
10.5	The incident management solution should be able to register any security event and generate alerts	O		
10.6	Establishing process for identifying, preventing, detecting, analysing & reporting all Information Security incidents as per the best practices, this may revise time to time as per the requirements	O		
10.7	Incident and problem Management, resolution, root cause analysis, and reporting within time limit as per the requirement	O		
10.8	Describe the incident response process including the roles and responsibilities and scope of action in line with CCMP	O		
10.9	MSSP should do root cause analysis for security incidents and recommend implementation of controls to prevent reoccurrence	M		
10.10	MSSP must provide on demand timely support by performing investigation and forensic analysis on the logs by doing the necessary analysis on the logs and providing required data on a timely fashion	M		
10.12	MSSP shall provide backend professional incident management team support in case of severe incident occurs	M		

11	**Packet Capture Analysis – Optional: The Service Provider platform should be capable of integrating and supporting this as and when required by SBICAP Group cos.**			
11.1	Solution should enable network visibility with high-speed packet capture. Solution should provision reconstruction of network traffic using packet capture and make it available in formats including PCAP	O		
11.2	Solution should support Deep Packet Inspection (DPI) to classify protocols & applications by capturing packet.	O		
11.3	Solution should have capabilities for packet capture analysis for zero-day threat detection, retrospection & metadata extraction feed into analytics engine for contextual enrichment & forensic analysis.	O		

4. Annexure - A2: Scope of Work for Resident Engineer

Deliverables:

- Co-ordinate with SBICAP's internal teams to optimize SOC operations and Infosec activities.
- Ensure smooth and complete migration from existing SOC service platform.
- Manage and prepare SOC process and technical documentations
- Provide monthly progress reports in terms of new integration, enhancements and SOC maturity model.
- Provide SOC Efficacy Testing Report on half yearly basis as mentioned in SEBI CSCRF.
- Escalate critical issues to SBICAP's representatives.
- Liaise and engage with SBICAP's technology specific SPOC for onboarding, key troubleshooting issues that shall enable delivery to SOC.
- Assisting Infosec activities
- Ensure resolution of the identified issues

5. Annexure- B: Inventory

List of devices / servers (Total devices)

Company	Device count
SBICAP Group	20
STCL	16

6. Annexure-C: Bidder's Organization Profile

(to be printed on Bidder's Letter Head and included with the Technical Bid Envelope)
Date: _____
To: Chief Information Security Officer
SBI Capital Markets Limited, Unit No. 1501, 15th floor, A& B Wing, Parinee Crescenzo Building, Plot C-38, G Block,
Bandra Kurla Complex, Bandra (East), Mumbai- 400 051

Dear Sir,
Ref: **RFP No. RFP/IS-01/2025 dated 17/07/2025** Details of the Bidder:

S/N	Particulars	Bidders Comment
1	Name of Bidders Company	
2	Registered Office Address	
3	Date of Incorporation	
4	Contact Person Phone and Email	
5	Director, MD & CEO Name and contacts	
6	Total Employee count PAN India	
7	Brief description of the Bidder including details of its main line of Business	
8	Company /firms website URL	
9	Of the Authorized Signatory of the Bidder (i.e. Name, Designation, address, contact no., email)	
10	Income Tax. No. (GST/PAN/GIR). Please enclosed photocopy of latest income tax clearance certificate	
11	Bidders support office presence at Mumbai, Hyderabad, Chennai, New Delhi, Kolkata)	If not available, how bidder will support remote locations
12	Total No. of clients in India for the bidder for similar implementation SIEM-SOC	
13	Total number of clients in for similar implementations (active engagements) SIEM -SOC	
14	No. of Years of experience, Bidder has been providing managed services	
15	Number of technicians available in for proposed solution and its components	
16	The Organisation certificated with process ISO 9001/20000,27001/ITIL etc. (Certificate to be provided)	
17	Capability to support 24/7	

7. Annexure-D: Eligibility Criteria

(to be printed on Bidder's Letter Head and included with the Technical Bid Envelope)

Sr. No.	Eligibility Criteria	Compliance (Compliant/ Not Compliant)	Supporting Evidence
1.	The MSSP should be a current legal entity in India and should have the experience of owning and managing a well-established Security Operations Centre (SOC) for at least five years. Vendor shall provide the details of the SOC including the location, infrastructure, tools used, companies served, process and methodology, staff employed in India.	Y/N	Certificate of Incorporation and Appropriate Supporting Document on providing SOC services for minimum 5 years (PO copy)
2.	The MSSP should have performed managed SOC services for at least five clients during the last 3 financial years, with at least Two of which should preferably be in the BFSI.	Y/N	Copies of Purchase Orders or Self Declaration signed by Authorized Signatory
3.	The MSSP's Account should not have been declared as a Non-Performing Asset (NPA) in the Books of any bank or financial institution as on 31.03.2025.	Y/N	Self-Declaration
4.	The MSSP must submit an undertaking that no Government / undertaking organizations have blacklisted the bidder for any reason. Past/present litigations, disputes, if any (Adverse litigations could result in disqualification, at the sole discretion of the SBICAP Group)	Y/N	Undertaking by Bidder.
5	Minimum Annual Turnover should be Rs. 50 Crores in each of the Preceding three financial years.	Y/N	Auditors Certificate or CA certificate
6	Financial statements i.e. Audited Balance sheet and Profit & Loss accounts for last three years (FY2022-23 and FY2023- 24, FY2024-25)	Y/N	Auditors Certificate or CA certificate
7	The Bidder should be a profit-making entity. The bidder must be a profitable organisation in 2 years out of past 3 financial years. Average turnover of Rs. 100 Crores in last 3 financial years.	Y/N	Appropriate Supporting Document
8	MSSP should have a remote SOC which is certified in major industry certifications like: 1.ISO- 27001:2013 (ISMS), 2.ISO-20000-1:2011 (ITSM), 3.ISO-9001:2015 (QMS), 4.ISO 22301:2012 (BCMS) 5.PCI-DSS v3.2.1 6.CERT-In Empanelment 7.Service Organization Control (SOC) 2 Type 2 Report	Y/N	Copy of certification including validity to be provided

9	An undertaking that, no penalties/fines have been imposed on their entities by any Regulator or Govt Agency or any Authority for breach of any Regulations or Laws.	Y/N	Supporting Document
10	MSSP to have approved Business Continuity Plan to support SBICAP Group cos. for continuity of SOC Operations	Y/N	Self-Declaration by Authorized Signatory as SOC being part of BCP Plan
11	MSSP should be complying with all the requirement mentioned in SEBI CSCRF as per applicability.	Y/N	Compliance certificate and audit report by CERT-IN empanelled vendor.
12	MSSP should comply and submit the compliance to SBICAPS along with eligibility criteria for all the mandatory requirements mentioned in Annexure A1 and for requirement in Annexure A2 respectively to be eligible for technical and commercial bid.	Y/N	Compliance to Annexure A1 and A2.

8. Annexure – E: SLA Terms

SBICAP Group to be contacted when bidder's SOC team is tracking a problem in the event that an alarm is triggered based on predefined correlation rules/policies and be kept abreast of problem resolution status. Following SLA will be applicable for Security Incident Alerting & Reporting:

Sr. No.	SLA Metric	Description	SLA			
			Critical (P0)	High Priority (P1)	Med Priority (P2)	Low Priority (P3)
1	TTN	**Time to Notify** This is the acceptable time a System/analyst shall take to send out an Incident notification to the customer.	10 Minutes	15 Minutes	30 Minutes	60 Minutes
2	TTR	**Time to Triage** This is the acceptable time an SOC Analyst will take to perform and conduct first responder processes as documented (run - books)	45 Minutes	60 Minutes	90 Minutes	120 Minutes
3	TTD	**Time to Diagnose** This is the acceptable time an SOC Analyst will take to perform a detailed analysis of the Incident and update the customer with recommendation and response steps.	90 Minutes	120 Minutes	180 Minutes	240 minutes

Event	Penalty, INR*
For delay in reporting Severity incidents (as per SOW)	99% Responses within SLA commitments - No Credit 98.99% - 98% - 5% of MRC 97.99% - 96% - 10% of MRC Below 96% - 20% of MRC

*Aggregate penalties will be capped at 20% of ARC
*Penalty payout will be in terms of service credits offered to customer

Severity Categorization

Critical (P0)

Successful penetration or Denial of Service attacks detected with significant impact on operations; ransomware attack; exfiltration of market sensitive data; widespread instances of data corruption causing impact on operations; significant risk of negative financial or public relations impact, etc.

High Severity (P1):

Penetration or Denial of Service attacks attempted with limited impact on operations; widespread instances of a new malwares not handled by anti-virus software; unauthorized access to servers and network devices; unauthorized or unexpected configuration changes on network devices detected; impersonation of SEBI officials in email communications; data exfiltration; unusually high count of phishing emails; instances of outbound phishing emails; some risk of negative financial or public relations impact, etc.

Medium Severity (P2):

Target recon or scans detected; penetration or Denial of Service attacks attempted with no impact on operations; widespread instances of known malwares easily handled by antivirus software; isolated instances of a new malwares not handled by anti-virus software; instances of phishing emails that were not recognized by employees and were clicked by them; instances of data corruption, modification and deletion being reported, etc.

Low Severity (P3):

Events that produce no effect on system operations or result in significant business impact, and is System probes or scans detected on external systems; intelligence received concerning threats to which systems may be vulnerable; intelligence received regarding username password compromise; isolated instances of known malwares easily handled by antivirus software, etc.

SLA Key Notes –

1. SLAs shall always be calculated basis the first base event of the alert as alerted in the SIEM. SLA calculation shall be done on a quarterly basis
2. All timelines are calendar minutes/hours
3. Classification of Severity of incidents will be based on agreement.
   - 3.1 Alerts not triggered by SIEM will not be part of the SLA calculation
   - 3.2 Daily report of events/incidents, correlation, analysis, recommendations and closure status by next business day.
   - 3.3 Monthly report by 7th day of every month (including excel based reports).
   - 3.4 Information must be shared as stated above of getting validated information about the potential security threats/vulnerabilities new global security threats/zero-day attacks in circulation to the designated SBICAP Group official and suggest suitable countermeasures to safeguard against such evolving threats/attacks along with the analysis. The advisories should be customized to SBICAP Group Infrastructure. Report pertaining to the same should be part of the monthly report.
   - 3.5 Report on recommendations regarding enhancement of security of SBICAP Group should be part of the monthly report.
   - 3.6 24*7*365 dashboard availability to be ensured.
   - 3.7 **VALIDITY OF AGREEMENT:** The Agreement/ SLA will be valid for the period of three years. The SBICAP Group reserves the right to terminate the Agreement as per the terms of RFP/ Agreement.
   - 3.8 For purpose of calculating penalty, uptime is calculated as under:

$$\text{Uptime (\%)} = \frac{\text{Sum of total hours during quarter - Sum of downtime hours during quarter}}{\text{Sum of total hours during the quarter}} * 100$$

Total hours during the quarter = No. of working days i.e. 90 * 24 hours = 2160 hours

$$\text{Uptime (\%)} = \frac{2160 \text{ - Sum of downtime hours during quarter}}{2160} * 100$$

Note: L1 Bidder shall utilize the Non-Disclosure Agreement (NDA) and Service Level Agreement (SLA) formats as specified in Annexure K and Annexure L, respectively in sole discretion of SBICAP Group.

9. Annexure - F: Pre-Bid Queries

S. No.	Page No	Section (Name & No.)	Statement as per tender document	Query by bidder	Reason for Query
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					

10. Annexure - G: Evaluation Process

Method of Selection: Selection of bidder consists of two stages:

I. Eligibility Criteria Evaluation
II.QCBS Evaluation (Quality and Cost Based Selection)

- Only the bidders qualified under Eligibility Criteria evaluation will be considered for QCBS evaluation. Shortlisted Service Providers will be called for presentations/demos.
- Commercial bid of only those bidders **who obtain minimum 70% in** the overall technical score shall be opened. Total Cost of ownership shall be calculated based on the commercial formats given in the Price bid
- Evaluation of the Bids will be done on the Quality cum Cost based (QCBS) in proportion of 70: 30 (70% technical and 30% Financial weightage).
- Selection of the bidder shall be based on Quality & Cost Based Selection (QCBS) criteria.
- The Evaluation Committee will review the technical bids to determine whether the technical bids are substantially responsive. Bids of substantially responsive bidders will be considered as technically qualified. Bids that are not substantially responsive are liable to be disqualified.
- The Commercial bids for the technically qualified bidders will then be opened for identification of successful bidder on the basis of lowest price bid (L1) as per QCBS.

The Commercial bids shall be evaluated based on the total amount quoted by the Bidder as per commercial Bid in the prescribed Performa given online in the RFP and QCBS formula.

The Bidder who's Commercial Bid has the lowest total quoted amount for the Project ("L1 Bidder") shall be given a Commercial Score of 100 marks. The Commercial scores of other Technically Qualified Bidders shall be computed as follows:

- Commercial Score of Bidder for the Project (Y) = 100 x total amount quoted by the L1 Bidder (in INR) / total amount quoted by the Bidder (in INR)
- The marks secured based on evaluation of the Commercial Bid as per Clause above shall be the Commercial Score of the Bidder for the Project ("Financial Score")

Composite Score of the Bidders shall be worked out as under:

Score Type	Bidder's Scores (A)	Weightage (B)	Weighted Score [(C) = (A) x (B)]
Technical Score	X	70%	(0.7)(TS)
Commercial Score	Y	30%	(0.3)(FS)
Composite Score of the Bidder			(0.7)(TSX) + (0.3)(FSY)

Evaluation for Preferred **Bidder**

The Bidder who has secured the highest Composite Score as calculated above shall be declared the Preferred Bidder for the Project.

Total marking criteria for Technical evaluation:

Sr No	Criteria	Scoring parameter for technical evaluation	Max Marks	Documentation required
1	Number of years of experience in the field of managed security solutions & services in India.	**No of Years** -Between 5 years to 9 years: **4 Marks** -More than 9 years: **10 Marks**	**10**	Copy of Work Order with Self Certification/ letter from customer
2	In the last 5 years the bidder should have 2 (two) captive SOC / Managed SOC implementations in govt/FSI/PSU in India.	**No. of Clients** - 2 to 4 Clients: **4 Marks** - More than 4 Clients: **10 Marks**	**10**	Copy of PO or Client Undertaking
3	The bidder should have reference of currently providing Managed Security Services for clients in India	**No. of Clients** -More than 10 Clients: **5 Marks** - 3 to 10 Clients: **3 Marks** - Minimum 3 Clients: **2 Marks**	**5**	Copy of PO or Client Undertaking
4	The bidder must have skilled OEM certified staff at various levels (L1/L2/L3) for MSSP services.	-More than 20 engineers - **10 Marks** -More than 10 less than 20: **5 Marks** -Minimum 10: **3 Marks**	**10**	Certificate from Bidder's HR along with OEM certificate copy
5	MSSP should have a remote SOC which is certified in major industry certifications including: 1.ISO- 27001:2013 (ISMS), 2.ISO-20000-1:2011 (ITSM), 3.ISO-9001:2015 (QMS), 4.ISO 22301:2012 (BCMS) 5.PCI-DSS v3.2.1 6.CERT-In Empanelment 7.Service Organization Control (SOC) 2 report	- 3 out of 7: **5 Marks** - 5 out of 7: **10 Marks** - All 7: **15Marks**	**15**	Certificate to be Attached
6	Compliance to Optional (Marked as "O") Technical Specification and Scope of Work (refer Annexure A)	- 98 -100%: 10 **Marks** - 95 – 97%: **5 Marks** - 92- 94%: 3 **Marks** - Below 92% **- Dis-Qualified**	**10**	Data Sheets
7	Bidder should have Cyber Security Skilled manpower (not outsourced or franchised)	**No of Engineers** - >200 Engineers: **10 Marks** - >100 to 200 Engineers: **4 Marks** - 50 to 100 engineers: **2 Marks - <** 50: **0 Marks**	**10**	Undertaking by Bidders HR on Letter Head
8	Bidder profile	-Understanding of SBICAP's requirement -Approach methodology -Quality of the presentation	**10**	Solution Presentation Evaluation & timelines
9	Product/ Services Functionality, and compliance with SBICAP's requirement	Device integrations, Use case hunting, Dashboards, Detect & Response ticketing, SOC services, etc.	**20**	Solution Presentation Evaluation & timelines

Total	**100**	

11. Annexure - H: Technical Bid

Part – 1: SIEM Hardware for Logger/ Collector –

S.N.	Item	Server / VM Config (Core, Memory, Disk-Space, no of servers)	Storage capacity for logger	OS Details	Any other item
1	SBICAP				
2	STCL				

Part – 2: Optional components, if any –

S.N.	**Company**	**Device count**	**Optional Items - 1**	**Optional Items-2**	**Optional Items-3**
1	SBICAP	20			
2	STCL	16			

12. Annexure - I: Commercial Bid

Part-1: SOC MSSP services

S.N.	Company	Device count	1st Yearly Price (excl. Tax) (in INR) (a)	2nd Yearly Price (excl. Tax) (in INR) (b)	3rd Yearly Price (excl. Tax) (in INR) (c)	Total price (in INR) (a+b+c)
1	SBICAP	20				
2	STCL	16				
	Total Package price					

Part – 2: Optional components, if any –

S.N.	Company	Device count	Optional Items - 1	Optional Items-2	Optional Items-3
1	SBICAP	20			
2	STCL	16			
	Total Package price				

Part-3: Rate Discovery for Resident Engineer

	Rate Discovery	Qty	Price excl. taxes - Yearly
1	Resident Engineerfor SBICAP – L1 resource	1	
2	Resident Engineerfor SBICAP – L2 resource	1	

Part-4: Rate Discovery for Incremental Devices / EPS during the contract period

	Rate Discovery	EPS/ Device count	Price excl. taxes - Yearly
1	Managed SOC services for additional 100 EPS over and above usages of Subscribed EPS or additional devices	100 EPS unit or one device unit	

Note:

- L1 will be reckoned based on the package price quoted in Part-1.
- This Price shall remain valid during the entire contract period of three years.

13. Annexure - J: Final Price Break-up: To be submitted by the L1 Vendor

Part-1: SOC MSSP services

S.N.	Company	Device count	1st Yearly Price (excl. Tax) (in INR) (a)	2nd Yearly Price (excl. Tax) (in INR) (b)	3rd Yearly Price (excl. Tax) (in INR) (c)	Total price (in INR) (a+b+c)
1	SBICAP	20				
2	STCL	16				
	Total Package price					

Part – 2: Optional components, if any –

S.N.	Company	Device count	Optional Items - 1	Optional Items-2	Optional Items-3
1	SBICAP	20			
2	STCL	16			
	Total Package price				

Part-3: Rate Discovery for Resident Engineer

	Rate Discovery	Qty	Price excl. taxes - Yearly
1	Resident Engineerfor SBICAP – L1 resource	1	
2	Resident Engineerfor SBICAP – L2 resource	1	

Part-4: Rate Discovery for Incremental Devices / EPS during the contract period

	Rate Discovery	EPS/ Device count	Price excl. taxes - Yearly
1	Managed SOC services for additional 100 EPS over and above usages of Subscribed EPS or additional devices	100 EPS unit or one device unit	

14. Annexure - K: Non-Disclosure Agreement

THIS RECIPROCAL NON-DISCLOSURE AGREEMENT (the "Agreement") is executed at _____this _____ day of _____Unit No. 1501, 15th floor, Parinee Crescenzo, Bandra Kurla Complex, Bandra (East), Mumbai- 400 051 hereinafter referred to as "SBICAPS" which expression includes its successors and assigns) of the ONE PART;
And
< Company Name >incorporated under the_____ provisions of the Companies Act, 1956/ Limited Liability Partnership Act 2008/ Indian Partnership Act 1932 having its registered office at _____ hereinafter referred to as " service provider_____" which expression shall unless repugnant to the subject or context thereof, shall mean and include its successors and permitted assigns) of the OTHER PART;
And Whereas

1. < Company Name > is the Managed Security Service Providers (MSSPs) to define, roll-out and support a comprehensive Security Operations Center (SOC) Framework which will provide assurance on the security posture and enhance SBICAP Group's capabilities to monitor, respond and mitigate threats against SBICAP Group as per the terms of RFP No. _____ dated _____.
2. For purposes of Security Operations Center services, SBICAPS would need to disclose certain valuable confidential information to the service provider (the Party receiving the formation being referred to as the "Receiving Party" and the Party disclosing the information being referred to as the "Disclosing Party. Therefore, in consideration of covenants and agreements contained herein for the mutual disclosure of confidential information to each other, and intending to be legally bound, the parties agree to terms and conditions as set out hereunder.

NOW IT IS HEREBY AGREED BY AND BETWEEN THE PARTIES AS UNDER 1.

Confidential Information and Confidential Materials:

(a) "Confidential Information" means non-public information that Disclosing Party designates as being confidential or which, under the circumstances surrounding disclosure ought to be treated as confidential. "Confidential Information" includes, without limitation, information relating to developed, installed or purchased Disclosing Party software or hardware products, the information relating to general architecture of Disclosing Party's network, information relating to nature and content of data stored within network or in any other storage media, Disclosing Party's business policies, practices, methodology, policy design delivery, and information received from others that Disclosing Party is obligated to treat as confidential. Confidential Information disclosed to Receiving Party by any Disclosing Party Subsidiary and/ or agents is covered by this agreement

(b) Confidential Information shall not include any information that:
   (i) is or subsequently becomes publicly available without Receiving Party's breach of any obligation owed to Disclosing party.
   (ii) becomes known to Receiving Party free from a confidentiality obligation prior to Disclosing Party's disclosure of such information to Receiving Party.

(iii) became known to Receiving Party from a source other than Disclosing Party other than by the breach of an obligation of confidentiality owed to Disclosing Party and without confidentiality restrictions on use and disclosure; or

(iv) is independently developed by Receiving Party.

(c) "Confidential Materials" shall mean all tangible materials containing Confidential Information, including without limitation written or printed documents and computer disks or tapes, email messages, whether machine or user readable.

1. Restrictions

(a) The Service Provider (Receiving Party)shall treat as confidential the Contract and any and all information ("confidential information") obtained from the SBICAPS (Disclosing party) pursuant to the Contract and shall not divulge such information to any person (except to such party's "Covered Person" which term shall mean employees, contingent workers and professional advisers of a party who need to know the same) without the other party's written consent provided that this clause shall not extend to information which was rightfully in the possession of such party prior to the commencement of the negotiations leading to the Contract, which is already public knowledge or becomes so at a future date (otherwise than as a result of a breach of this clause). Receiving Party will have executed or shall execute appropriate written agreements with Covered Person, sufficient to enable it to comply with all the provisions of this Agreement. If Service Provider appoints any Sub-Contractor (if allowed) then Service Provider may disclose confidential information to such Subcontractor subject to such Subcontractor giving SBICAP an undertaking in similar terms to the provisions of this clause. Any breach of this Agreement by Receiving Party's Covered Person or Sub- Contractor shall also be constructed a breach of this Agreement by Receiving Party.

(b) Receiving Party may disclose Confidential Information in accordance with judicial or other governmental order to the intended recipients (as detailed in this clause), provided Receiving Party shall give Disclosing Party reasonable notice (provided not restricted by applicable laws) prior to such disclosure and shall comply with any applicable protective order or equivalent. The intended recipients for this purpose are:

i. the statutory auditors of the either party and

ii. government or regulatory authorities regulating the affairs of the parties and inspectors and supervisory bodies thereof SBI

(c) Receiving Party agrees to segregate all such Confidential Material from the confidential material of others in order to prevent mixing.

2. Rights and Remedies

(a) Receiving Party shall notify Disclosing Party immediately upon discovery of any unauthorized, fraudulent or intentional or unintentional misuseor disclosure of Confidential Information and/ or Confidential Materials, or any other breach of this Agreement by Receiving Party and will cooperate with Disclosing Party in every reasonable way to help Disclosing Party regain possession of the Confidential Information and/ or Confidential Materials and prevent its further unauthorized use.

(b) Receiving Party shall return all originals, copies, reproductions and summaries of Confidential Information or Confidential Materials at Disclosing Party's request, or at Disclosing Party's option, certify destruction of the same.

(c) Receiving Party acknowledges that monetary damages may not be the only and / or a sufficient remedy for unauthorized disclosure of Confidential Information and that disclosing party shall be entitled, without waiving any other rights or remedies (including but not limited to as listed below), to injunctive or equitable relief as may be deemed proper by a Court of competent jurisdiction. i. Suspension of access privileges ii. Change of personnel assigned to the job iii. Termination of contract

(d) Disclosing Party may visit Receiving Party' s premises, with reasonable prior notice and during normal business hours, to review Receiving Party's compliance with the term of this Agreement.

3. Miscellaneous

(a) All Confidential Information and Confidential Materials are and shall remain the sole and of Disclosing Party. By disclosing information to Receiving Party, Disclosing Party does not grant any expressed or implied right to Receiving Party to disclose information under the Disclosing Party' s patents, copyrights, trademarks, or trade secret information.

(b) Confidential Information made available is provided " As Is," and disclosing party disclaims all representations, conditions and warranties, express or implied, including, without limitation, representations, conditions or warranties of accuracy, completeness, performance, fitness for a particular purpose, satisfactory quality and merchantability provided same shall not be construed to include fraud or wilful default of disclosing party.

(c) Neither party grants to the other party any license, by implication or otherwise, to use the Confidential Information, other than for the limited purpose of information security audit as per the agreed scope defined by both the parties, or any license rights whatsoever in any patent, copyright or other intellectual property rights pertaining to the Confidential Information.

(d) This Agreement constitutes the entire agreement between the parties with respect to the subject matter hereof. It shall not be modified except by a written agreement dated subsequently to the date of this Agreement and signed by both parties. None of the provisions of this Agreement shall be deemed to have been waived by any act or acquiescence on the part of Disclosing Party, its agents, or employees, except by an instrument in writing signed by an authorized officer of Disclosing Party. No waiver of any provision of this Agreement shall constitute a waiver of any other provision(s) or of the same provision on another occasion.

(f) In case of any dispute, both the parties agree for neutral third-party arbitration. Such arbitrator will be jointly selected by the two parties and he/she may be an auditor, lawyer, consultant or any other person of trust. The said proceedings shall be conducted in English language at Mumbai and in accordance with the provisions of Indian Arbitration and Conciliation Act 1996 or any Amendments or Re-enactments thereto. Nothing in this clause prevents a party from having recourse to a court of competent jurisdiction for the sole purpose of seeking a preliminary injunction or any other provisional judicial relief it considers necessary to avoid irreparable damage. This Agreement shall be governed by and construed in accordance with the laws of Republic of India. Each Party hereby irrevocably submits to the exclusive jurisdiction of the courts of Mumbai.

(g) Subject to the limitations set forth in this Agreement, this Agreement will inure to the benefit of and be binding upon the parties, their successors and assigns.

(h) If any provision of this Agreement shall be held by a court of competent jurisdiction to be illegal, invalid or unenforceable, the remaining provisions shall remain in full force and effect.

(i) The Agreement shall be effective from _____ ("Effective Date") and shall be valid for a period of _____year(s) thereafter (the "Agreement Term"). The foregoing obligations as to confidentiality shall survive the term of this Agreement and for a period of five (5) years thereafter provided confidentiality obligations with respect to individually identifiable information, customer's data of Parties or software in human-readable form (e.g., source code) shall survive in perpetuity.

Dated this day of (Month) 22 at _(place)

For and on behalf of SBI Capital Markets Ltd

Name	Krishna Mohan Gijupalli	
Designation	SVP, Group Head, CRO and CISO	
Place	Mumbai	
Signature		

For and on behalf of < Company Name>

Name		
Designation		
Place		
Signature		

15. Annexure - L : Service Level Agreement

Agreement for Managed Security Services (MSS) for Security Operations Centre (SOC) - Security Information and Event Management (SIEM), Security Orchestration, Automation and Response (SOAR) & User and entity Behaviour Analytics (UBA)

BETWEEN

SBI CAPITAL MARKETS LTD, CUFFE PARADE
AND

_____

Date of Commencement: _____

Date of Expiry : _____

AGREEMENT

This agreement ("Agreement") is made on _____ day of _ 20 .

Between

SBI Capital Markets Limited, constituted under the Companies Act, 1956 having its Corporate Centre Unit No. 1501, 15th floor, Parinee Crescenzo, Bandra Kurla Complex, Bandra (East), Mumbai- 400 051 - hereinafter referred to as "**SBICAP**" which expression shall unless repugnant to the context or meaning thereof shall include its successors & assigns of the First Part

And

_____, a private limited company incorporated under the provisions of the Companies Act, 1956 having its registered office at _____ hereinafter referred to as "Service Provider" which expression shall unless repugnant to the context or meaning thereof shall include its successor, executor & permitted assigns of the Second Part.

SBICAP and Service Provider are sometimes individually referred to as a" Party" and collectively as "Parties" throughout this Agreement, and the words Party and Parties shall be construed accordingly.

RECITALS

WHEREAS

SBI Capital Markets Ltd and its Group companies ("SBICAP Group") are committed to improve its security posture and achieves this objective by updating its processes and technology periodically. Driven by this commitment, SBICAP Group is procuring Managed Security Services to define, roll-out and support a comprehensive Security Operations Center (SOC) Framework which will provide assurance on the security posture and enhance SBICAP Group's capabilities to monitor, respond and mitigate threats against SBICAP Group.

v) SBI Capital Markets Ltd. (SBICAP) - Unit No. 1501, 15th floor, A& B Wing, Parinee Crescenzo Building, Plot C- 38, G Block, Bandra Kurla Complex, Bandra (East), Mumbai- 400 051

vi) SBICAP Group Trustee Co. Ltd. (STCL) - 04th Floor, Mistry Bhavan, 122 Dinshaw Vachhan Road, Churchgate, Mumbai -400020.

and

Service Provider is in the business of providing **Managed Security Services (MSS) for Security Operations Centre (SOC)** and has agreed to provide the services as may be required by SBICAP mentioned in the **Techno Commercial Proposal for RFP No. RFP/IS-01/2025** dated 25/06/2025 submitted by _____ and same shall be part of this Agreement.

NOW THEREFORE, in consideration of the mutual covenants, undertakings and conditions set forth below, and for other valid consideration the acceptability and sufficiency of which are hereby acknowledged, the Parties hereby agree as follows:

1. DEFINITIONS & INTERPRETATIONS

1.1 Definitions

1.1.1. Vendor/ Service Provider/ System Integrator – MSSP / SIEM-SOC Vendors.

1.1.2. **Supplier/ Contractor/ Vendor** – Selected Vendor/System Integrator under this RFP.

1.1.3. **Company/ Purchaser/ -** Reference to "Company" and "Purchaser" shall be determined in context and may mean without limitation "SBICAP / STCL.

1.1.4. **Proposal/ Bid** – the Vendor's written reply or submission in response to this RFP

1.1.5. **RFP/Tender** – the request for proposal (this document) in its entirety, inclusive of any Addenda that may be issued by SBICAP Group.

1.1.6. **Solution/ Services/ Work/ System** – "Solution" or "Services" or "Work" or "System" all services, scope of work and deliverable to be provided by a Vendor as described in the RFP and include services ancillary for Security information Event Management - Security

Operations Center (SIEM-SOC) for continuous log monitoring and analysis, co-relation of all logs, threats and vulnerabilities. Etc. covered under the RFP.

1.1.7. **Product** – "Product" means Security Information and Event Management, Security Orchestration, Automation and Response & User and entity Behaviour Analytics (SIEM, SOAR, UBA) Tools / services implemented for SOC monitoring and log collector as mentioned in the tender.

1.1.8. **Server / Network / Website** – As specified within the technical requirement section of this RFP document.

1.1.9. **Applicable Law**: means Information Technology Act, 2000, the Data Protection legislation and all applicable SEBI and other statutory body's regulations, guidelines, notices, circulars, notifications published and/or circulated and respective amendments to these from time to time.

1.2. **Interpretations**:

1.2.1 Reference to a person includes any individual, firm, body corporate, association (whether incorporated or not) and authority or agency (whether government, semi government or local).

1.2.2 The singular includes the plural and vice versa.

1.2.3 Reference to any gender includes each other gender.

1.2.4 The provisions of the contents table, headings, clause numbers, italics, bold print and underlining is for ease of reference only and shall not affect the interpretation of this Agreement.

1.2.5 The Schedules, Annexures and Appendices to this Agreement shall form part of this Agreement.

1.2.6 A reference to any documents or agreements (and, where applicable, any of their respective provisions) means those documents or agreements as amended, supplemented or replaced from time to time provided they are amended, supplemented or replaced in the manner envisaged in the relevant documents or agreements.

1.2.7 A reference to any statute, regulation, rule or other legislative provision includes any amendment to the statutory modification or re-enactment or, legislative provisions substituted for, and any statutory instrument issued under that statute, regulation, rule or other legislative provision.

1.2.8 Any agreement, notice, consent, approval, disclosure or communication under or pursuant to this Agreement is to be in writing.

1.2.9 The terms not defined in this Agreement shall be given the same meaning as given to them in the RFP. If no such meaning is given technical words shall be **Date** understood in technical sense in accordance with the industry practices.

2. COMMENCEMENT & TERM

2.1 This Agreement shall commence from its date of execution mentioned above/ be deemed to have commenced from _____.

2.2 This Agreement shall be in force for a period of three years from Effective Date, unless terminated by SBICAP by notice in writing in accordance with the termination clauses of this Agreement.

2.3 SBICAP shall have the right at its discretion to renew this Agreement in writing, for a further terms on the same terms and conditions.

2.4 Unless terminated earlier in accordance with this Agreement, the Agreement shall come to an end on completion of the term specified in the Agreement or on expiration of the renewed term.

3. SCOPE OF SERVICES

3.1 The scope and nature of the work which Service Provider must provide to SBICAP (Services) is as follows:

3.1.1 SOC MSSP services for 3 years period,

3.1.2 Other services as Detailed in Proposal submitted for RFP No. RFP/IS-01/2025

4. REPRESENTATIONS AND WARRANTIES

4.1 Each of the Parties represents and warrants in relation to itself to the other that:

4.1.1 It has all requisite corporate power and authority to execute, deliver and perform its obligations under this Agreement and has been fully authorized through applicable corporate process to do so.

4.1.2 The person(s) signing this agreement on behalf of the Parties have the necessary authority and approval for execution of this document and to bind his/their respective organization for due performance as set out in this Agreement. It has all necessary statutory and regulatory permissions, approvals and permits for the running and operation of its business.

4.1.3 It has full right, title and interest in and to all software, copyrights, trade names, trademarks, service marks, logos symbols and other proprietary marks (collectively **'IPR'**) (including appropriate limited right of use of those owned by any of its vendors, affiliates or subcontractors) which it provides to the other Party, for use related to the services to be provided under this Agreement.

4.1.4 It will provide such cooperation as the other Party reasonably requests in order to give full effect to the provisions of this Agreement.

4.1.5 The execution and performance of this Agreement by either of the Parties does not and shall not violate any provision of any of the existing Agreement with any of the party and any other third party.

4.2 Additional Representation and Warranties by Service Provider

4.2.1 Service Provider shall perform the Services and carry out its obligations under the Agreement with due diligence, efficiency and economy, in accordance with generally accepted techniques and practices used in the industry and with professional standards recognized by international professional bodies and shall observe sound management practices. It shall employ appropriate advanced technology and safe and effective equipment, machinery, material and methods.

4.2.2 Service Provider has the requisite technical and other competence, sufficient, suitable, qualified and experienced manpower/personnel and expertise in providing the Services to SBICAP.

4.2.3 Service Provider shall duly intimate to SBICAP Group immediately, the changes, if any in the constitution of Service Provider.

4.2.4 Service Provider warrants that to the best of its knowledge, as on the Effective Date of this Agreement, the products and services provided by Service Provider to SBICAP Group do not violate or infringe any patent, copyright, trademarks, trade secrets or other Intellectual Property Rights of any third party.

4.2.5 Service provider shall ensure that all persons, employees, workers and other individuals engaged by or sub-contracted (if allowed) by Service Provider in rendering the Services under this Agreement have undergone proper background check, police verification and other necessary due diligence checks to examine their antecedence and ensure their suitability for such engagement. No person shall be engaged by Service provider unless such person is found to be suitable in such verification and Service Provider shall retain the records of such verification and shall produce the same to SBICAP Group as when requested.

4.2.6 Service Provider warrants that it shall be solely liable and responsible for compliance of applicable Labour Laws in respect of its employee, agents, representatives and subcontractors (if allowed) and in particular laws relating to terminal benefits such as pension, gratuity, provided fund, bonus or other benefits to which they may be entitled

and the laws relating to contract labour, minimum wages, etc., and SBICAP Group shall have no liability in this regard.

5. RESPONSIBILITIES OF SBICAP

5.1 Processing and authorising invoices

5.2 Approval of information

6. RESPONSIBILITIES OF SERVICE PROVIDER

6.1 Service Provider agrees and declares that it shall be the sole responsibility of Service Provider to comply with the provisions of all the applicable laws including but not limited to RBI Guidelines/circular, SEBI Guideline/Circular, Digital Protection and Data Privacy Act and applicable Guideline/Circular by any body of Government of India, concerning or in relation to rendering of Services by Service Provider as envisaged under this Agreement.

6.2 Service Provider shall procure and maintain all necessary licenses, permissions, approvals from the relevant authorities under the applicable laws throughout the currency of this Agreement, require for performing the Services under this Agreement.

6.3 Service Provider shall ensure that Service Provider's personnel and its sub-contractors (if allowed) will abide by all reasonable directives issued by SBICAP Group, including those set forth in the current standards, policies and procedures (to the extent applicable), all on-site rules of behaviour, work schedules, security procedures and other standards, policies and procedures as established by SBICAP Group from time to time.

6.4 Roles and responsibilities of contractors, employees and third-party users shall be documented as they relate to information assets and security.

6.5 SBICAP Group shall communicate its Privacy Policy and the consequences of noncompliance with such policies, at least annually, to Service Provider's personnel responsible for collecting, using, retaining, and disclosing personal information.

6.6 Service Provider shall identify and document the risk in delivering the services. Service Provider shall identify the methodology to monitor and prevent the risk and shall also document the steps taken to manage the impact of the risks.

6.7 Service Provider would be responsible for Data Purging. Service Provider to inform and take explicit approval from SBICAP Group before every data purge incidence and also inform the purging details to SBICAP Group after the data purge incidence. In the event of any premature exit, must purge all data of SBICAP Group after taking prior approval and the purging logs to be shared with SBICAP Group prior to the exit.

6.8 Data retention and purging certificate shall be sent to SBICAP Group as per stipulated time communicated by SBICAP Group. The certificate should be issued by the authorized signatory in the format as specified by SBICAP Group and should capture the details of data received, data purged, period of the certificate, and evidence in support to purging.

6.9 Business Continuity and Backup - Service provider shall have defined Business Continuity Management, Disaster Recovery Plan and backup processes.

6.10 SBICAP Group to be contacted when bidder's SOC team is tracking a problem in the event that an alarm is triggered based on predefined correlation rules/policies and be kept abreast of problem resolution status. Following Service Level Agreement (SLA) will be applicable for Security Incident Alerting & Reporting:

Sr. No.	SLA Metric	Description	SLA			
			Critical (P0)	High Priority (P1)	Med Priority (P2)	Low Priority (P3)
1	TTN	**Time to Notify** This is the acceptable time a System/analyst shall take to send out an	10 Minutes through email	15 Minutes	30 Minutes	60 Minutes

		Incident notification to the customer.				
2	TTR	**Time to Triage** This is the acceptable time an SOC Analyst will take to perform and conduct first responder processes as documented (run - books)	45 Minutes	60 Minutes	90 Minutes	120 Minutes
3	TTD	**Time to Diagnose** This is the acceptable time an SOC Analyst will take to perform a detailed analysis of the Incident and update the customer with recommendation and response steps.	90 Minutes	120 Minutes	180 Minutes	240 minutes

Event	**Penalty, INR***
For delay in reporting Severity incidents (as per SOW)	99% Responses within SLA commitments - No Credit 98.99% - 98% - 5% of MRC 97.99% - 96% - 10% of MRC Below 96% - 20% of MRC

*Aggregate penalties will be capped at 20% of ARC
*Penalty payout will be in terms of service credits offered to customer

Severity Categorization

Critical (P0)

Successful penetration or Denial of Service attacks detected with significant impact on operations; ransomware attack; exfiltration of market sensitive data; widespread instances of data corruption causing impact on operations; significant risk of negative financial or public relations impact, etc.

High Severity (P1):

Penetration or Denial of Service attacks attempted with limited impact on operations; widespread instances of a new malwares not handled by anti-virus software; unauthorized access to servers and network devices; unauthorized or unexpected configuration changes on network devices detected; impersonation of SEBI officials in email communications; data exfiltration; unusually high count of phishing emails; instances of outbound phishing emails; some risk of negative financial or public relations impact, etc.

Medium Severity (P2):

Target recon or scans detected; penetration or Denial of Service attacks attempted with no impact on operations; widespread instances of known malwares easily handled by antivirus software; isolated instances of a new malwares not handled by anti-virus software; instances of phishing emails that were not recognized by employees and were clicked by them; instances of data corruption, modification and deletion being reported, etc.

Low Severity (P3):

Events that produce no effect on system operations or result in significant business impact, and is System probes or scans detected on external systems; intelligence received concerning threats to which systems may be vulnerable; intelligence received regarding username password compromise; isolated instances of known malwares easily handled by antivirus software, etc.

6.11 SLA Key Notes

6.11.1 SLAs shall always be calculated basis the first base event of the alert as alerted in the SIEM. SLA calculation shall be done on a quarterly basis.
6.11.2 All timelines are calendar minutes/hours
6.11.3 Classification of Severity incidents will be based on agreement
6.11.4 Alerts not triggered by SIEM will not be part of the SLA calculation
6.11.5 Daily report of events/incidents, correlation, analysis, recommendations and closure status by next business day.
6.11.6 Monthly report by 7th day of every month (including excel based reports).
6.11.7 Information must be shared as stated above of getting validated information about the potential security threats/vulnerabilities new global security threats/zero-day attacks in circulation to the designated SBICAP Group official and suggest suitable countermeasures to safeguard against such evolving threats/attacks along with the analysis. The advisories should be customized to SBICAP Group Infrastructure. Report pertaining to the same should be part of the monthly report.
6.11.8 Report on recommendations regarding enhancement of security of SBICAP Group should be part of the monthly report.
6.11.9 24*7*365 dashboard availability to be ensured. In case the dashboard/SOC portal is working fine but not accessible by SBICAPS then it will be considered under downtime.
6.11.10 **VALIDITY OF AGREEMENT:** The Agreement/ SLA will be valid for the period of three years. The SBICAP Group reserves the right to terminate the Agreement as per the terms of RFP/ Agreement.
6.11.11 For purpose of calculating penalty, uptime is calculated as under:

$$\text{Uptime (\%)} = \frac{\text{Sum of total hours during quarter - Sum of unplanned downtime hours during quarter}}{\text{Sum of total hours during the quarter}} * 100$$

Total hours during the quarter = No. of working days i.e. 90 * 24 hours = 2160 hours

$$\text{Uptime (\%)} = \frac{2160 - \text{Sum of unplanned downtime hours during quarter}}{2160} * 100$$

6.11.12 Submit compliance certificate which certifying compliance with SEBI Cyber Security and Cyber Resilience Framework dated 20th Aug 2024 before onboarding and every year till the expiration of contract.
6.11.13 Submit the SOC efficacy testing on half yearly as mentioned in the SEBI Cyber Security and Cyber Resilience Framework dated 20th Aug 2024 as per format.

7 CONFIDENTIALITY

7.1 For the purpose of this Agreement, Confidential Information shall mean

i. Information of all kinds, whether oral, written or otherwise recorded including, without limitation, any analyses, compilations, forecasts, data, studies or other documents, regarding the past, current or future affairs, business, plans or operations of a Party to which the other Party will have access,
ii. The existence of the contemplated terms and the fact that discussions or negotiations are taking place or have taken place between the Parties concerning the contemplated terms,
iii. Any and all information regarding the contemplated terms and any agreements that may be entered into in relation thereto and
iv. Any customer details or other data received by a Party from the other Party or its customer(s) or otherwise shared between the Parties in connection with the Service.

7.2 In consideration of each Party providing the other Party or its' representatives with the Confidential Information, the Parties agree as follows:

7.2.1 Each Party shall keep confidential and shall not, directly or indirectly, disclose, except as provided in sub-clauses below, in any manner whatsoever, in whole or in part, the Confidential Information without the other Party's prior written consent.

7.2.2 Each Party shall hold the Confidential Information in confidence and shall exercise all reasonable diligence in ensuring that the Confidential Information is not disclosed to third parties and will refrain from using the Confidential Information for any purpose whatsoever other than for the purposes of this Agreement or for the purpose for which such information is supplied.

7.2.3 Notwithstanding the above, each Party may reveal the Confidential Information to those of its representatives, those of its' holding company and those of its subsidiaries who are involved in the negotiation or evaluation of the project and shall procure and ensure that each of them complies with the obligation to keep the Confidential Information secret, private and confidential and strictly observes the terms of this Agreement.

7.2.4 The confidentiality obligation shall not apply to such portions of the Confidential Information which one of the Parties can demonstrate (i) are or become generally available to the public other than as a result of any breach of this Agreement; (ii) were in its possession on a non-confidential basis prior to the date hereof; (iii) have been rightfully received from a third party after the date hereof without restriction on disclosure and without breach of this Agreement, said third party being under no obligation of confidentiality to the other Party with respect to such Confidential Information; or (iv) Where Confidential Information is independently developed by receiving party without any reference to or use of disclosing party's Confidential Information.

7.2.5 In the event that a Party becomes legally compelled pursuant to any statutory or regulatory provision, court or arbitral decision, governmental order, or stock exchange requirements to disclose any of the Confidential Information, the compelled Party, as far as possible will provide the other Party with prompt written notice to the extent not prohibited by law. In any case, the compelled Party will furnish only that portion of the Confidential Information which is legally required and will exercise all reasonable efforts to obtain reliable assurance that confidential treatment will be accorded to the Confidential Information.

7.2.6 In the event of termination or expiry of this Agreement, each Party shall either (i) promptly destroy all copies of the written (including information in electronic form) Confidential Information in its possession or that of its representatives; or (ii) promptly deliver to the other Party at its own expense all copies of the written Confidential Information in its possession or that of its representatives, provided, however, each Party shall be permitted to retain one copy of the Confidential Information for the purposes of dispute resolution, compliance with regulatory agency or authority and internal compliance procedures, provided such copies being held and kept confidential.

7.2.7 By furnishing the Confidential Information, no Party makes an express or implied representation or warranty as to the accuracy or completeness of the Confidential Information that it has disclosed and each Party expressly disclaims any liability that may be based on the Confidential Information, errors therein or omissions there from, save in the case of fraud or wilful default.

7.3 Receiving party undertakes to promptly notify disclosing party in writing any breach of obligation of the Agreement by its employees or representatives including confidentiality obligation. Receiving party acknowledges that monetary damages may not be the only and / or a sufficient remedy for unauthorized disclosure of Confidential Information and that disclosing party shall be entitled, without waiving any other rights or remedies, to injunctive or equitable relief as may be deemed proper by a Court of competent jurisdiction.

7.4 Service Provider shall not, without the SBICAP's prior written consent, disclose the Agreement, or any provision thereof, or any specification, plan, drawing, pattern, sample or information furnished by or on behalf of SBICAP in connection therewith, to any person other than a person employed by Service Provider in the Performance of the Contract. Disclosure to any such employed person shall be made in confidence and shall extend only so far, as may be necessary to purposes of such performance.

7.5 Service Provider shall not, without SBICAP's prior written consent, make use of any document or information received from SBICAP except for purposes of performing the services and obligations under this Agreement.

7.6 Any document received from SBICAP shall remain the property of SBICAP and subject to clause 8.2.6 shall be returned (in all copies) to SBICAP on completion Service Provider ' s Performance under the Agreement.

7.7 The foregoing obligations (collectively referred to as "Confidentiality Obligations") set out in this Agreement shall survive the term of this Agreement and for a period of Six (6) years thereafter provided Confidentiality Obligations with respect to individually identifiable information, customer's data of Parties or software in human-readable form (e.g., source code) shall survive in perpetuity.

8 RELATIONSHIP BETWEEN THE PARTIES

8.1 It is specifically agreed that Service Provider shall act as independent service provider and shall not be deemed to be the Agent of SBICAP except in respect of the transactions/services which give rise to Principal-Agent relationship by express agreement between the Parties.

8.2 Neither Service Provider nor its employees, agents, representatives, Sub- Contractors shall hold out or represent as agents of SBICAP.

8.3 None of the employees, representatives or agents of Service Provider shall be entitled to claim permanent absorption or any other claim or benefit against SBICAP.

8.4 This Agreement shall not be construed as joint venture. Each Party shall be responsible for all its obligations towards its respective employees. No employee of any of the two Parties shall claim to be employee of other Party.

8.5 All the obligations towards the employee(s) of a Party on account of personal accidents while working in the premises of the other Party shall remain with the respective employer

and not on the Party in whose premises the accident occurred unless such accident occurred due to gross negligent act of the Party in whose premise's accident occurred.

8.6 For redressal of complaints of sexual harassment at workplace, Parties agree to comply with the policy framed by SBICAP (including any amendment thereto) in pursuant to the Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013 including any amendment thereto.

9 SUB-CONTRACTING

As per the scope of this Agreement sub-contracting is not permitted.

10 LIQUIDATED DAMAGES

If Service Provider fails to deliver product and/or perform any or all the Services within the stipulated time, schedule as specified in this Agreement, SBICAP may, without prejudice to its other remedies under the Agreement, and unless otherwise extension of time is agreed upon without the application of liquidated damages, deduct from the Project Cost, as liquidated damages a sum equivalent to 0.5% of total Project Cost for delay of each week or part thereof maximum up to 5 % of total Project Cost. Once the maximum deduction is reached, SBICAP may consider termination of the Agreement.

11 BANK GUARANTEE & PENALTY

11.1 Performance of the obligations under the Agreement shall be made by Service Provider in accordance with the time schedule specified in this Agreement.

11.2 Subject to clause 17 of this Agreement, any unexcused delay by Service Provider in the performance of its Contract obligations shall render this Agreement to be terminated.

11.3 If at any time during performance of the Contract, Service Provider should encounter unexpected conditions impeding timely completion of the Services under the Agreement and performance of the services, Service Provider shall promptly notify SBICAP in writing of the fact of the delay, its likely duration and its cause(s). As soon as practicable, after receipt of Service Provider's notice, SBICAP shall evaluate the situation and may at its discretion extend Service Provider's time for performance, in which case the extension shall be ratified by the Parties by amendment of the Agreement.

11.4 No penalty shall be levied in case of delay(s) in deliverables or performance of the Contract for the reasons solely and directly attributable to SBICAP. On reaching the maximum of penalties specified SBICAP reserves the right to terminate the Agreement.

12 FORCE MAJEURE

12.1 Notwithstanding anything else contained in the Agreement, neither Party shall be liable for any delay in performing its obligations herein if and to the extent that such delay is the result of an event of Force Majeure.

12.2 For the purposes of this clause, 'Force Majeure' means and includes wars, insurrections, revolution, civil disturbance, riots, terrorist acts, public strikes, hartal, bundh, fires, floods, epidemic, quarantine restrictions, freight embargoes, declared general strikes in relevant industries, Vis Major, acts of Government in their sovereign capacity, impeding reasonable performance of the Contractor and/or Sub-Contractor but does not include any foreseeable events, commercial considerations or those involving fault or negligence on the part of the party claiming Force Majeure.

12.3 If a Force Majeure situation arises, Service Provider shall promptly notify SBICAP in writing of such conditions, the cause thereof and the likely duration of the delay. Unless otherwise directed by SBICAP in writing, Service Provider shall continue to perform its

obligations under the Agreement as far as reasonably practical and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event.

12.4 If the event of Force Majeure continues beyond 30 (thirty) days, either Party shall have the right to terminate this Agreement by giving a notice to the other Party. Neither party shall have any penal liability to the other in respect of the termination of this Agreement as a result of an Event of Force Majeure. However, Service Provider shall be entitled to receive payments for all services actually rendered up to the date of the termination of this Agreement.

13 INSPECTION AND AUDIT

13.1 It is agreed by and between the Parties that Service Provider be subject to annual audit by internal/external Auditors appointed by SBICAP/ inspecting official from the CAG or any regulatory authority, covering the risk parameters finalized by SBICAP/ such auditors in the areas of products (IT hardware/ software) and services etc. provided to SBICAP and Service Provider shall submit such certification by such Auditors to SBICAP. Service Provider and or his / their outsourced agents / sub-contractors (if allowed by SBICAP) shall facilitate the same. SBICAP can make its expert assessment on the efficiency and effectiveness of the security, control, risk management, governance system and process created by Service Provider. Service Provider shall, whenever required by such Auditors, furnish all relevant information, records/data to them. All costs for such audit shall be borne by SBICAP. Except for the audit done by CAG or any statutory/regulatory authority, SBICAP shall provide reasonable notice not less than 7 (seven) days to Service Provider before such audit and same shall be conducted during normal business hours.

13.2 Where any Deficiency has been observed during audit of Service Provider on the risk parameters finalized by SBICAP or in the certification submitted by the Auditors, it is agreed upon by Service Provider that it shall correct/ resolve the same at the earliest and shall provide all necessary documents related to resolution thereof and the auditor shall further certify in respect of resolution of the Deficiencies. It is also agreed that Service Provider shall provide certification of the auditor to SBICAP regarding compliance of the observations made by the auditors covering the respective risk parameters against which such Deficiencies observed.

13.3 Service Provider further agrees that whenever required by SBICAP, it will furnish all relevant information, records/data to such auditors and/or inspecting officials of SBICAP/ Reserve Bank of India and/or any regulatory authority(ies). SBICAP reserves the right to call for and/or retain any relevant information/ audit reports on financial and security review with their findings undertaken by Service Provider. However, Service Provider shall not be obligated to provide records/data not related to Services under the Agreement (e.g. internal cost break-ups etc.).

13.4 In the event data/application code is stored at the Service Provider premises, audits shall be performed bi-annually by Service Provider appointed third party CERT-IN empanelled External Auditors in order to verify the strength of information security and to validate the compliance with Service Recipient's information security policies and standards. Compliance certificate shall be issued in the format as specified by Service Recipient and submitted to Service Recipient on bi-annually basis from an authorized signatory.

14 FEES, TAXES DUTIES & PAYMENTS

14.1 Service Provider shall be paid fees and charges, the same shall be subject to deduction of income tax thereon wherever required under the provisions of the Income Tax Act by SBICAP. The remittance of amounts so deducted and issuance of certificate for such deductions shall be made by SBICAP as per the laws and regulations for the time being in force. Nothing in the Agreement

shall relieve Service Provider from his responsibility to pay any tax that may be levied in India on income and profits made by Service Provider in respect of this Agreement.

14.2 **Payments:**

14.2.1 SBICAP will pay properly submitted valid invoices within reasonable period but not exceeding 30 (thirty) days after its receipt thereof. All payments shall be made in Indian Rupees.

14.2.2 SBICAP may withhold payment of any product/services that it disputes in good faith and may set-off penalty amount or any other amount which Service provider owes to SBICAP against amount payable to Service provider under this Agreement. However, before levying penalty or recovery of any damages, SBICAP shall provide a written notice to Service Provider indicating the reasons for such penalty or recovery of damages. Service Provider shall have the liberty to present its case in writing together with documentary evidence, if any, within 21 (twenty-one) days. Penalty or damages, if any, recoverable from Service Provider shall be recovered by SBICAP through a credit note or revised invoices. In case Service Provider fails to issue credit note/ revised invoice, SBICAP shall have right to withhold the payment or set-off penal amount from current invoices.

15 GENERAL INDEMNITY

15.1 Service Provider agrees and hereby keeps SBICAP indemnified against all claims, actions, loss, damages, costs, expenses, charges, including legal expenses (Attorney, Advocates fees included) which SBICAP may suffer or incur on account of (i) Services Provider's breach of its warranties, covenants, responsibilities or obligations; or (ii) breach of confidentiality obligations mentioned in this Agreement; or (iii) any wilful misconduct and gross negligent acts on the part of employees, agents, representatives or sub-contractors (if allowed) of Service Provider. Service Provider agrees to make good the loss suffered by SBICAP.

15.2 Subject to clause 15.2.1 and 15.2.2 of this Agreement, Service Provider, at its own expenses without any limitation, indemnify and keep fully and effectively indemnified SBICAP against all costs, claims, damages, demands, expenses and liabilities of whatsoever nature arising out of or in connection with all claims of infringement of Intellectual Property Rights, including patent, trade mark, copyright, trade secrets or industrial design rights of any third party arising from the Services or use of software/product under this Agreement.

15.2.1 SBICAP will give (a) notice to Service Provider of any such claim without delay/provide reasonable assistance to Service Provider in disposing of the claim and will at no time admit to any liability for or express any intent to settle the claim provided that (i) Service Provider shall not partially settle any such claim without the written consent of SBICAP, unless such settlement releases SBICAP fully from such claim; (ii) Service Provider shall promptly provide SBICAP with copies of all pleadings or similar documents relating to any such claim; (iii) Service Provider shall consult with SBICAP with respect to the defence and settlement of any such claim; and (iv) in any litigation to which SBICAP is also a party, SBICAP shall be entitled to be separately represented by a counsel of its own selection at the expense of the service provider.

15.2.2 Service Provider shall have no obligations with respect to any infringement claims to the extent that the infringement claim arises or results from: (i) Service Provider's compliance with SBICAP's specific technical designs or instructions (except where Service Provider knew or should have known that such compliance was likely to result in an Infringement Claim and Service Provider did not inform SBICAP of the same); or (ii) any unauthorized modification or alteration of the product by SBICAP.

16 TERMINATION

16.1 SBICAP may, without prejudice to any other remedy for breach of Agreement, by written notice of not less than 30 (thirty) days, terminate the Agreement in whole or in part:

(i) If Service Provider fails to deliver any or all the obligations within the time period specified in the Agreement, or any extension thereof granted by SBICAP;

(ii) If Service Provider fails to perform any other obligation(s) under the Agreement;

(iii) Violations of any terms and conditions stipulated in the RFP;

(iv) On happening of any termination event mentioned herein above in this Agreement.

Prior to providing a written notice of termination to Service Provider under clause 16.1(i) to 16.1 (iii), SBICAP shall provide Service Provider with a written notice of 30 (thirty) days to cure such breach of the Agreement. If the breach continues or remains unrectified after expiry of cure period, SBICAP shall have right to initiate action in accordance with above clause.

16.2 SBICAP, by written notice of not less than 90 (ninety) days, may terminate the Agreement, in whole or in part, for its convenience. In the event of termination of the Agreement for SBICAP's convenience, Service Provider shall be entitled to receive payment for the Services rendered (delivered) up to the effective date of termination.

16.3 In the event SBICAP terminates the Agreement in whole or in part for the breaches attributable to Service Provider, it may procure, upon such terms and in such manner as it deems appropriate, products and services similar to those undelivered, and subject to clause 17 Service Provider shall be liable to SBICAP for any increase in cost for such similar products and/or services. However, Service Provider shall continue performance of the Agreement to the extent not terminated.

16.4 SBICAP shall have a right to terminate the Agreement immediately by giving a notice in writing to Service Provider in the following eventualities:

16.4.1 If any Receiver/Liquidator is appointed in connection with the business of Service Provider or Service Provider transfers substantial assets in favour of its creditors or any orders / directions are issued by any Authority / Regulator which has the effect of suspension of the business of Service Provider.

16.4.2 If Service Provider applies to the Court or passes a resolution for voluntary winding up of Service Provider or any other creditor / person files a petition for winding up or dissolution of Service Provider.

16.4.3 If any acts of commission or omission on the part of Service Provider or its agents, employees, sub-contractors or representatives, in the reasonable opinion of SBICAP tantamount to fraud or prejudicial to the interest of SBICAP or its employee(s).

16.4.4 Any document, information, data or statement submitted by Service Provider in response to RFP, based on which Service Provider was considered eligible or successful, is found to be false, incorrect or misleading.

16.5 In the event of the termination of the Agreement, Service Provider shall be liable and responsible to return to SBICAP all records, documents, data and information including Confidential Information pertains to or relating to SBICAP in its possession.

16.6 In the event of termination of the Agreement for material breach, SBICAP shall have the right to report such incident in accordance with the mandatory reporting obligations under the applicable law or regulations.

16.7 Upon termination or expiration of this Agreement, all rights and obligations of the Parties hereunder shall cease, except such rights and obligations as may have accrued on the date of termination or expiration; the obligation of confidentiality and indemnity; obligation of payment; Governing Law clause; Dispute resolution clause; and any right which a Party may have under the applicable Law.

17 LIMITATION OF LIABILITY

17.1 The maximum aggregate liability of Service Provider, subject to clause 17.3, in respect of any claims, losses, costs or damages arising out of or in connection with this Agreement shall not exceed the total Project Cost.

17.2 Under no circumstances shall either Party be liable for any indirect, consequential or incidental losses, damages or claims including loss of profit, loss of business or revenue.

17.3 The limitations set forth in clause 17.1 shall not apply with respect to:

17.3.1 Claims that are the subject of indemnification pursuant to infringement of third-party Intellectual Property Right;

17.3.2 damage(s) occasioned by the Gross Negligence or Wilful Misconduct of Service Provider;

17.3.3 damage(s) occasioned by Service Provider for breach of Confidentiality Obligations;

17.3.4 Regulatory or statutory fines imposed by a Government or Regulatory agency for noncompliance of statutory or regulatory guidelines applicable to SBICAP, provided such guidelines were brought to the notice of Service Provider.

For the purpose of clause 17 a party which was in reckless disregard of or gross indifference to the obligation of the party under this Agreement and which causes injury, damage to life, personal safety, real property, harmful consequences to the other party, which such party knew, or would have known if it was acting as a reasonable person, would result from such act or failure to act for which such Party is legally liable. Notwithstanding the forgoing, Gross Negligence shall not include any action taken in good faith. "Wilful Misconduct" means any act or failure to act with an intentional disregard of any provision of this Agreement, which a party knew or should have known if it was acting as a reasonable person, which would result in injury, damage to life, personal safety, real property, harmful consequences to the other party, but shall not include any error of judgment or mistake made in good faith.

18 CONTINGENCY PLANS & CONTINUITY ARRANGEMENTS.

18.1 Service Provider shall arrange and ensure proper contingency plans to meet any unexpected obstruction to Service Provider or any employees or sub-contractors (if allowed) of Service Provider in rendering the Services or any part of the same under this Agreement to SBICAP.

18.2 Service Provider agrees for the following continuity arrangements to ensure the business continuity of SBICAP.

18.2.1 In the event of failure of Service Provider to render the Services or in the event of termination of Agreement or expiry of term or otherwise, without prejudice to any other right, SBICAP at its sole discretion may make alternate arrangement for getting the Services contracted with another vendor. In such case, SBICAP shall give prior notice to the existing Service Provider. The existing Service Provider shall continue to provide services as per the terms of the Agreement until a 'New Service Provider' completely takes over the work.

18.2.2 During the transition phase, the existing Service Provider shall render all reasonable assistances to the new Service Provider within such period prescribed by SBICAP, at no extra cost to SBICAP, for ensuring smooth switch over and continuity of Services, provided where transition services are required by SBICAP or New Service Provider beyond the term of this Agreement, reasons for which are not attributable to Service Provider, payment shall be made to Service Provider for such additional period on the same rates and payment terms as specified in this Agreement. If existing vendor is found to be in breach of this obligation, they shall

be liable for paying a penalty of 10% of the total project cost on demand to SBICAP, which may be settled from the payment of invoices or bank guarantee for the contracted period.

19 ARBITRATION

19.1 Any and all disputes, controversies and conflicts ("Disputes") arising out of this Agreement or in connection with this Agreement or the performance or non- performance of the rights and obligations set forth herein, or the breach, termination, invalidity or interpretation thereof shall be referred for arbitration in terms of the Arbitration and Conciliation Act, 1996 (Arbitration Act) or any amendments thereof. Prior to submitting the Disputes to arbitration, the parties shall make all endeavors to settle the dispute/s through mutual negotiation and discussions. In the event that the said dispute/s are not settled within 30 days of the arising thereof as evidenced through the first written communication from any party notifying the other regarding the disputes, the same shall finally be settled and determined by arbitration as above.

19.2 The place of arbitration shall be at Mumbai and the language used in the arbitral proceedings shall be English. Arbitration shall be conducted by a mutually appointed sole arbitrator. If the Parties are unable to agree upon a sole Arbitrator, each Party shall appoint one arbitrator and the two arbitrators so appointed by the Parties shall appoint the third arbitrator, who shall be the Chairman of the Arbitral Tribunal.

19.3 The arbitral award shall be in writing and subject to the provisions of the Arbitration and Conciliation Act, 1996 Act shall be enforceable in any court of competent jurisdiction.

19.4 Pending the submission to arbitration and thereafter, till the Arbitrator or the Arbitral Tribunal renders the award or decision, the Parties shall, except in the event of termination of this Agreement or in the event of any interim order/award is granted under the afore stated Act, continue to perform their obligations under this Agreement.

20 GOVERNING LAW & JURISDICTION

20.1 The Agreement shall be governed and construed in accordance with the Laws of Republic of India.

20.2 The Parties agree to submit to the exclusive jurisdiction of the appropriate court in Mumbai in connection with any dispute between the Parties under the Agreement.

21 SEVERABILITY

If any part or any provision of this Agreement is or becomes illegal, invalid or unenforceable, that part or provision shall be ineffective to the extent of such invalidity or unenforceability only, without in any way affecting the validity or enforceability of the remaining parts of said provision or the remaining provisions of this Agreement. The Parties hereby agree to attempt to substitute any invalid or unenforceable provision with a valid or enforceable provision, which achieves to the greatest extent possible the economic, legal and commercial objectives of the invalid or unenforceable provision.

22 POWER TO VARY OR OMIT WORK

22.1 No alterations, amendments, omissions, additions, suspensions or variations of the work (hereinafter referred to as variation) under the Agreement shall be made by Service provider except as directed in writing by Bank. SBICAP shall have full powers, subject to the provision herein after contained, from time to time during the execution of the Agreement, by notice in writing to instruct Service Provider to make any variation without prejudice to the Agreement. Service Provider shall carry out such variations and be bound by the same conditions, though the said variations occurred in the Agreement documents. If any suggested variations would, in the opinion of Service Provider, if carried out, prevent them from fulfilling any of their obligations under the Agreement, they shall notify SBICAP, thereof, in writing with reasons for holding such opinion and Bank shall instruct Service Provider to make such other modified variation without

prejudice to the Agreement. Service Provider shall carry out such variations and be bound by the same conditions, though the said variations occurred in the Agreement documents. If SBICAP confirms their instructions Service Provider's obligations will be modified to such an extent as may be mutually agreed. If such variation involves extra cost, any agreed difference in cost occasioned by such variation shall be mutually agreed between the parties. In any case in which Service Provider has received instructions from SBICAP as to the requirement of carrying out the altered or additional substituted work, which either then or later on, will in the opinion of Service Provider, involve a claim for additional payments, such additional payments shall be mutually agreed in line with the terms and conditions of the order.

22.2 If any change in the work is likely to result in reduction in cost, the parties shall agree in writing so as to the extent of reduction in payment to be made to Service Provider, before Service provider proceeding with the change.

23 ENTIRE AGREEMENT

23.1 This Agreement constitutes the entire agreement between the Parties with respect to the subject matter hereof and supersedes all prior written agreements, undertakings, understandings and negotiations, both written and oral, between the Parties with respect to the subject matter of the Agreement, except which are expressly annexed or attached to this Agreement and saved by this Agreement. No representation, inducement, promise, understanding, condition or warranty not set forth herein has been made or relied upon by any Party hereto.

23.2 The following documents along with all addenda issued thereto shall be deemed to form and be read and construed as integral part of this Agreement and in case of any contradiction between or among them the priority in which a document would prevail over another would be as laid down below beginning from the highest priority to the lowest priority:

23.2.1 This Agreement;

23.2.2 Annexure of Agreement;

23.2.3 Purchase Order No. dated ; and

23.2.4 SBI Capital Proposal _____ submitted by _____

24 NOTICES

24.1 Any notice or any other communication required to be given under this Agreement shall be in writing and may be given by delivering the same by hand or sending the same by prepaid registered mail, postage prepaid, telegram or facsimile to the relevant address set forth below or such other address as each Party may notify in writing to the other Party from time to time. Any such notice given as aforesaid shall be deemed to be served or received at the time upon delivery (if delivered by hand) or upon actual receipt (if given by postage prepaid, telegram or facsimile).

24.2 A notice shall be effective when it is delivered or on the effective date of the notice, whichever is later.

24.3 Address for communication to the Parties are as under:

24.3.1 To SBICAP

SBI Capital Market Ltd,
Unit No. 1501, 15th floor, Parinee Crescenzo, Bandra Kurla Complex,
Bandra (East), Mumbai- 400 051

24.3.2 To Service Provider

_____

_____

24.4 In case there is any change in the address of one party, it shall be promptly communicated in writing to the other party.

25 INFORMATION SECURITY CLAUSES

25.1 Service Provider shall adhere to "Service Recipient IT and IS Policy", "Service Recipient Policy on Information Security Requirements for Third-Party", "Service Recipient Acceptable Usage policy", and any equivalent standards and in line with Service Recipient's information security policies, procedures and requirements. Service Provider shall ensure that they have information security organization in place to implement the provisions of Service Recipient's information security requirements.

25.2 Service Recipient may update from time to time, security related policies, guidelines, standards and requirements and will incorporate such updates by reference which shall be notified in writing by Service Recipient to Service Provider promptly. Service Provider is deemed to accept all the updates.

25.3 Service Provider shall have a documented policies and procedures to discharge the security requirements detailed within the Agreement.

25.4 Service Provider personnel working on Service Recipient project shall have adequate industry knowledge and standard certifications relevant to cyber security / cloud computing /etc.

26 MISCELLANEOUS

26.1 Any provision of this Agreement may be amended or waived, if, and only if such amendment or waiver is in writing and signed, in the case of an amendment by each party, or in this case of a waiver, by the Party against whom the waiver is to be effective.

26.2 No failure or delay by any Party in exercising any right, power or privilege hereunder shall operate as a waiver thereof nor shall any single or partial exercise of any other right, power of privilege. The rights and remedies herein provided shall be cumulative and not exclusive of any rights or remedies provided by law.

26.3 Neither this Agreement nor any provision hereof is intended to confer upon any person/s other than the Parties to this Agreement any rights or remedies hereunder.

26.4 If this Agreement is signed in counterparts, each counterpart shall be deemed to be an original.

26.5 Service Provider shall not assign or transfer all or any of its rights, benefits or obligations under this Agreement without the approval of SBICAP. SBICAP may, at any time, assign or transfer all or any of its rights, benefits and obligations under this Agreement.

26.6 Service Provider agrees that they shall not use the logo, trademark, copy rights or other proprietary rights of SBICAP in any advertisement or publicity materials or any other written communication with any other party, without the prior written consent of SBICAP.

26.7 The Parties agree that SBICAP shall have the right, but without any obligation to monitor and assess the Services to enable SBICAP to take necessary corrective measures, provided any such monitoring shall not amount to supervision of any of the jobs of Service Provider or the employees of Service Provider.

26.8 Service Provider agrees that the complaints/feedback, if any received from the customers of SBICAP in respect of the Services by Service Providers shall be recorded and Bank/Reserve Bank of India shall have access to such records and redressal of customer complaints by Service Provider.

26.9 Service Provider agrees that SBICAP shall have the right to disclose the details of this Agreement and the details of Services covered herein to the Reserve Bank of India and Indian Banks Association.

IN WITNESS WHEREOF, the parties hereto have caused this Agreement to be executed by their duly authorized representatives as of the date and day first mentioned above.

	SBI CAPITAL Markets Limited	**Service Provider**
By		
Name		
Title		
Date	xx-xxxx-25	xx-xxxx-25