State Bank Operations Support Services Pvt Ltd (SBOSS)
New Delhi

Request For Proposal (RFP)

From

(Managed Security Service Provider (MSSP)

For

Managed - SIEM-SOC
(Security Information and Event Management – Security Operations Centre)

State Bank Operations Support Service Pvt Ltd (SBOSS)

2 Floor, NBCC Place, South Wing, Bhisham, Pitamah Marg, Pragati Vihar,
Lodhi Road, New Delhi, India, 110003

RFP NO. SBOSS/24-25/009

Request For Proposal (RFP)

For Procurement of SIEM-SOC Services from managed security service provider (MSSP).

RFP SCHEDULE		
Sr No	**Activity**	**Details**
1.	RFP Number	**SBOSS/24-25/009**
2.	Bid Document Availability including changes/amendments, if any to be issued	RFP may be downloaded from Company's website https://www.sboss.net.in/notice
3.	Release of RFP	20th Sep, 2024
4.	Pre Bid	Queries on email
4.	Technical Bid submission End Date	4th Oct, 2024- 17:00 Hrs
5.	Technical Bid Opening	7th Oct, 2024 - 15:00 Hrs
6	Technical Bid Evaluation and Presentation of shortlisted Service Providers	8th Oct, 2024 – 11th Oct 2024 (tentative schedule)
7.	Opening of Commercial Bids	16th Oct, 2024 - 11:30 Hrs (tentative)
8.	Method of Selection	The method of selection is Quality and Price Base Selection. The weights given to the Technical and Commercial Proposals are: Technical = 70% and Commercial= 30%
9.	Reverse Auction	18th Oct, 2024 - 11:30 Hrs (tentative)
11	SBOSS - Contact Details	Mr. Susim Das (GM) M - 9674712267 email – fh1@sboss.net.in Mr. Prateek Saxena (VP & Head IT) M- 8800876090 email – ith1@sboss.net.in

Table of Contents

1. INTRODUCTION

1.1 Background

In order to improve the security posture by updating & implementing robust IT security processes and technologies periodically, State Bank Operations Support Services Pvt Ltd (SBOSS) inviting RFPs from reputed, experienced & technologically competent Firms, Service Providers (SP)/Companies/Agencies/Societies having adequate infrastructure and Experience to define, roll-out and support a comprehensive Security Operations Center (SOC) Framework which will provide assurance on the security posture and enhance SBOSS's capabilities to monitor, respond and mitigate cyber & IT threats against SBOSS.

SBOSS intends to engage 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 SBOSS's evolving requirements.

SP's 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 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 SBOSS. SBOSS will in no case be responsible for 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 SBOSS (Company), is subject to the terms and conditions set out in this RFP document.

1.2.2. This RFP is not an offer by SBOSS, 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 SBOSS 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 advices/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. SBOSS, 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. SBOSS 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 SBOSS 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 SBOSS, 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. SBOSS, however, reserves the right to procure extra quantity during the bid validity period of the offer and till 3 year from the date of project sign-off. The price of such procurement will be calculated on pro- rata basis of the balance period.

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/ SBOSS -** Reference to the "SBOSS", "Company" and "Purchaser" shall be determined in context and may mean without limitation "SBOSS Ltd.

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 SBOSS.

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 SIEM and Security Tools implemented for SOC 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

1. 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 only through sealed tenders under two bid system.
2. The Bidders will have to submit tender documents and all Annexure Forms as part of technical bid.
3. The bidders are requested to note that:

   They cannot make their submission after the time stipulated above and no extension of time will normally be permitted for submission of bids.

2.1 List of the Annexures to be submitted in sealed envelope as mentioned below :

S/N	Particulars	Annexure	To be submitted with
1	Technical Specification and Scope of Work	Annexure-A	Technical Bid
2	Inventory	Annexure-B	Technical Bid
3	Bidders Organization Profile & capability presentation to support the scope of work as per RFP and post implementation support.	Annexure-C	Technical Bid
4	Eligibility Criteria	Annexure-D	Technical Bid
5	Service Level Agreement	Annexure-E	Technical Bid
6	Pre-Bid Queries with SBOSS response to be submitted with Technical Bid.	Annexure-F	Technical Bid
7	Commercial Bid	Annexure-G	Commercial Bid
8	Tender Document duly signed		Technical Bid
9	Reverse Auction	Annexure-H	Offline
10	Final Price Break-up by L1 vendor	Annexure-I	L1 Bidder
11	NDA	Annexure-J	L1 Bidder

2.2 Terms & Conditions:

2.2.1. Tender should strictly conform 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. SBOSS reserves the right to accept in part or in full or reject the entire bid 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 SBOSS.

2.2.4. SBOSS reserves the right to impose and recover penalties 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 3 years 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 SBOSS which will be binding on the vendors.

2.2.8. The prices quoted for SIEM-SOC services should be for total three year which is subject to renew every year on mutual agreement.

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

2.2.10. During the validity period of tender quotes, any upward change in the exchange rate/ excise duty and customs duty are to be borne by the vendor. In the event of any downward revision of levies/duties etc., the same should be passed on to SBOSS, notwithstanding what has been stated in the quotation or in the Purchase Order.

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

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

2.2.13. The tools used for SIEM-SOC by the vendor should be licensed one in the name of SBOSS.

2.2.14. Cloud based or On-premise solution / tools and the channel being used, should be clearly stated.

2.2.15. Vendor shall conduct monthly meeting with SBOSS 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.

2.2.16. It would be binding upon the vendor to maintain security of SBOSS systems at all times.

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

2.2.18. SBOSS 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.

2.2.19. Penalties for Delayed Implementation - The SIEM- SOC Implementation should be started immediately from the date of placing the letter of Intent / Purchase order whichever is earlier. If delayed, SBOSS 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.

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

2.2.21. 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.

2.3 Payment Terms:

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

3. Submission of Bids

A two-stage bidding process will be followed for evaluating the bids. The bidders should submit their responses to this RFP in two parts, i.e., first Technical Bid and Commercial Bid and after techno- commercial evaluation, the short-listed bidders will be called for Reverse Auction.

3.1 Technical Specification and Scope of Work (Requirements of SBOSS) is detailed at **Annexure-A.**

3.2 Inventory for the scope of work is detailed at **Annexure – B.**

3.3 Bidders Organisation Profile as per **Annexure – C**.

3.4 Eligibility criteria alongwith supporting documents as per **Annexure D.**

3.5 Service Level Agreement - as per **Annexure – E.**

3.6 Clarification to RFP - The Bidder should carefully examine and understand the specifications/ requirements/ conditions of the RFP and may seek clarifications, if required, before submitting the bids. The Bidders are required to direct all communications in writing through email to the designated SBOSS officials as per the time schedule defined above, in the Pre-bid Queries format as per **Annexure – F**.

4. Bid Evaluation Process

4.1 Bidder Eligibility Criteria

4.1.1. Bidder Profile and experience in the industry.
4.1.2. Bidders capability to support the RFP scope and based on the presentation.
4.1.3. Bidder support facilities / proactive support/Profile/ Previous experience.
4.1.4. OEM post sale support experience.
4.1.5. SBOSS will evaluate the technical and functional specification of all the equipment quoted by the Bidder.
4.1.6. During evaluation and comparison of bids, SBOSS may, at its discretion ask the bidders for clarification of its bid. The request for clarification shall be in writing and no change in prices or substance of the bid shall be sought, offered or permitted. No post bid clarification at the initiative of the bidder shall be entertained.
4.1.7. SBOSS reserves the right to evaluate the bids on technical & functional parameters including vendor site visit and witness demos of the system and verify functionalities, response times, public documents, Market Share, OEM establishment blogs. Group Company experience with product etc.

4.2 Techno-Commercial evaluation

4.2.1. **Technical bids** will be examined by the Technical Committee of SBOSS which may call for clarifications/additional information from the Vendors which must be furnished to the Technical Committee in the time stipulated by the Technical Committee. E.g. Presentation, Demo or POC of the product.
4.2.2. Technical bids will be opened for eligibility criteria and technical evaluation.
4.2.3. Bids that are not substantially responsive are liable to be disqualified at the Company's discretion.
4.2.4. Technical evaluation will include technical information submitted as per technical Bid format, demonstration of proposed solution, reference calls and site visits, wherever required. The Bidder may highlight the noteworthy/superior features of their Services, Proposed solution features, guaranteed uptime, integration, underlying components' etc. Scalability / Capability of the proposed solution to meet future requirements not outlined in the RFP.
4.2.5. Support on open platforms and solution based on proposed technology (both software and hardware).
4.2.6. Management GUI for administration for proposed components
4.2.7. The Bidder will demonstrate/substantiate all claims made in the technical Bid to the satisfaction of the Company, the capability of the Services to support all the required functionalities at their Price in their lab or those at other organizations where similar Services is in use.
4.2.8. Vendor who have fulfilled the eligibility criteria will be evaluated as per the scoring parameters below : In this stage shortlisted Bidders will prepare

technical proposal which shall comprise of (at a minimum)

i)	Eligibility criteria	–	10 marks
ii)	Architecture & SIEM solution	–	30 marks
iii)	Technical Evaluation of SOC	–	30 marks
iv)	Project Plan with Timelines	–	15 Marks
v)	Vendor presentations	–	10 Marks
vi)	Security Certifications of vendor (SOC/ISO 27001)	-	5 Marks

4.2.9. The bidders who have attained the minimum technical score & have complied with the points of Technical Bid shall qualify for Commercial Bid evaluation.

i. Technical Bid will be assigned a technical weightage. Only the bidders whose overall Technical score is 70 % or more will qualify for commercial bid evaluation.

ii. The Final technical score of the Bidder shall be calculated as follows -

Normalized Technical Score of a Bidder = {Technical Score of that Bidder / Score of the Bidder with the highest technical score} X 100 (adjusted to 2 decimals)

4.3 Commercial Bid evaluation

i. The Commercial bids for the technically qualified bidders will then be opened and reviewed by the Technical & Price Negotiation Committee (TPNC) of SBOSS to determine whether the commercial bids are substantially responsive. Bids that are not substantially responsive are liable to be disqualified at owner's discretion.

ii. The Commercial Bids of the technically qualified bidders shall be calculated as follows -

2.2.4.

Normalized Commercial Score of a Bidder = {lowest discounted quote / Bidders discounted quote} X 100 (adjusted to 2 decimals)

iii. The final techno-commercial score will be Quality and Price based with the following weightage:

a) 70%: Final Technical Score
b) 30%: Final Commercial score

Final Score = (0.7*Final Technical Score) + (0.3*Final Commercial Score)

iv. The bidder will be given ranks in the descending order, i.e. the highest Final score shall be treated as Rank-1 bidder. Based on the rankings, the TPNC will shortlist the bidders for Reverse Auction round.

4.4 Reverse Auction :

4.1.1. All the Bidders who qualify in the techno-commercial evaluation process shall have to participate in the online reverse auction to be conducted by the Authorised service provider on behalf of SBOSS.

4.1.2. Shortlisted Bidders shall be willing to participate in the reverse auction process and must have a valid digital signature certificate. Bidders shall also be willing to abide by the e-business rules for reverse auction framed by the Authorised service provider. The details of e-business rules, processes and procedures will be provided by the Authorised service provider.

4.1.3. The Bidder will be selected as L1 on the basis of overall price package as quoted in the Reverse Auction.

4.1.4. Final Price Break-up details as per **Annexure – H**, should be submitted by the successful Bidder by next day of Reverse Auction.

4.1.5. Prices quoted must be "All Inclusive" except taxes as applicable.

4.1.6. SBOSS reserve the complete rights to issue a full or partial purchase order or to subtract any component from the proposed solution/ BILL OF MATERIAL at its own discretion.

5. GENERAL TERMS & CONDITIONS

5.1 Confidentiality

This document contains information confidential and proprietary to SBOSS. Additionally, the Bidder will be exposed by virtue of the contracted activities to internal business information of SBOSS, 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 SBOSS 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 SBOSS. Reproduction of this RFP, without prior written consent of SBOSS, by photographic, electronic, or other means is strictly prohibited.

5.2 Non-Disclosure Agreement

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

5.3 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 Delhi and the parties agree to submit themselves to the jurisdiction of such court and the governing law shall be the laws of India.

5.4 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 SBOSS. The venue of Arbitration proceedings shall be at Delhi. 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 Delhi in the English language. The fees of the Arbitrator and the cost of the Arbitration proceedings shall be equally borne by both the Parties.

5.5 Indemnification

The Bidder shall, at its own cost and expenses, defend and indemnify SBOSS against all losses, judgements, statutory and regulatory penalties, fines, damages, third-party claims on account of the any misrepresentation, infringement of intellectual property rights, fraud and breach of terms of this RFP/ violation by the Bidder of any or all national/international trade laws, norms, standards, procedures etc.

The Bidder shall expeditiously meet any such claims and shall have full rights to defend itself there from. If SBOSS is required to pay compensation to a third party on account of the Bidder or association with the Bidder, then the Bidder shall be fully responsible for the same, including all expenses and court and legal fees.

5.6 Force Majeure

In case of delay in implementation of the Project on account of conditions which are beyond the control of the shortlisted bidder such as war, floods, earthquakes, strikes, lockouts, epidemics, pandemic, riots, fire or Governmental regulations superimposed after the date of order/ contract, the Parties shall be permitted to terminate the contract / bid document, if such delay extends for a period beyond 15 days. SBOSS shall not be liable to make any payments in this case.

5.7 Termination

SBOSS reserves the right to abandon the current tender process and restart the bidding process at any point of time without assigning any reason whatsoever. SBOSS can cancel the award granted to the elected Bidder at any point of time and restart the bid process completely or select another Bidder. The Elected Bidders understands and agrees that SBOSS shall not be obligated in any manner whatsoever and is free to stop / modify the bidding process at any stage without any liability.

5.8 Data Protection

The Bidders authorizes the release from time to time to SBOSS (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 SBOSS 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.

5.9 Intellectual Property

SBOSS 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 SBOSS.

6. Annexure-A : Technical Specification and Scope of Work

Compliance: C – Fully compliant, P – Partially Compliant, N – Not

compliant The key requirements of SOC Transformation are follows:

S.No	Requirements	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.		
1.2	Vendor should provide log baselines for all platforms under scope that are required to be monitored.		
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.		
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.		
1.5	Vendor should detect both internal & external attacks. In addition to security attacks on IT infrastructure, vendors should also monitor for security events on databases and servers.		
1.6	Vendor should monitor, detect and manage 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) · Database access including logins, client IP, server IP and source program information. · Track and audit administrative commands		
1.7	Vendor should carry out correlations amongst the logs from multiple sources to detect multi-vector attacks.		
1.8	Vendor operations team should send alerts with details of mitigation steps to designated personnel as including any identified service provider of SBOSS.		
1.9	The Vendor should bring workflows and solutions that can automate majority of the incident response activities such as false positive management, managing white lists, escalation workflow, SLA management etc.		
1.10	Alerts should be notified to SBOSS only after proper triage process. Alerts from SIEM should be enriched with context data, environmental data, vulnerability data, historical data, threat intelligence etc.		
1.11	Historical parameters should include and not limited to attack volume, attacker volume, and destination volume for every alert.		
1.12	Vendor should give long term solution to prevent such threats in future		
1.13	Define, Develop and implement Use Cases based on standard methodologies such as Cyber Kill Chain		

1.14	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		
1.15	Service Provider reports are in compliance with industry best practice and international standards like ISO 27001, PCI, SOC1, SOC2 etc. and regulatory requirement like RBI.		
1.16	Service provider to assist the organization to ensure the log retention is as per local regulatory requirement like RBI, etc..		
1.17	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		
1.18	Service provider solution should be able to provide charts for top attacks & attackers, OWASP based threat analysis, Trending threats, attack demographics etc.		
1.19	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.		
1.20	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.		
1.21	Any failures of the event collection infrastructure must be detected and operations personnel must be notified.		
1.22	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.		

1.23	Using the outbound plugins architecture the Vendor must provide integrations with services like ticketing systems, messaging platforms, vulnerability scanners etc. to facilitate automation of workflows.		
1.24	Vendor should detect both internal and external attacks. In addition to security attacks on IT infrastructure, Vendor should also monitor for security events on critical business applications, databases and also identify network behavior, user behavior anomalies.		
1.25	Vendor should monitor, detect and manage incidents for the following minimum set of IT infrastructure security events. 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		
1.26	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		
2.	**Incident Analysis**		
2.1	Solution should support centralized incident management to prioritize and manage security incidents.		
2.2	Solution should support triaging of alerts from number of security products including SIEM, DLP, IPS, WAF, Anti-APT, ETDR.		
2.3	Solution should support machine driven triaging algorithms that considers contextual parameters, historical behavior and external threat intelligence to enrich and arrive at a 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		
2.5	Solution should enable investigation of triaged alert/custom alerts deemed critical		
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		

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,		
2.8	Solution should support features to identify attacker attributes including threat intelligence score of attacker, who-is lookup information, geo-mapping in a single console.		
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.		
2.10	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.		
2.11	Solution should support models to derive attack inception and progress of the attack. List the details of investigation models used in the Solution.		
2.12	Solution should provide case management features to store raw and analyzed data for a specific alert or set of alerts. Provide details on the what artefacts can be stored related to an investigation		
2.13	Solution should support quick search across stored datasets in the Solution. Provide details of search features supported.		
2.14	Solution should provide run books for investigation steps corresponding to different types of attacks.		
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 · 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.		
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		
3.3	Solution should support the full workflow for incident coordination.		

3.4	Solution should support assigning activities to different teams and tracking for closure.		
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.		
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)		
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.		
3.8	Solution should integrate with external service desks such as e.g. ServiceDeskPlus, Internal ticketing tool for leveraging existing service desk platform		
3.9	Solution should provide alert details and investigation outcomes linked and viewable for relevant remediation tickets.		
3.10	Incident Report with classification, chronology of events, RCA, IOC		
3.11	Track impacted assets related to an incident		
3.12	Tools for Response based on data and analytics		
3.13	Ability for quick Counter Response by integrating with devices such as firewall and AD for blocking traffic or quarantine system		
3.14	Usage of Ticketing and case management workflow		
3.15	Classification of incidents		
3.16	Maintain track of first response and subsequent measures taken for the incident		
3.17	Maintain chronological order of events related to incident response		
3.18	Maintain IOC and artifacts related to incident		
3.19	Incident response should include investigation of end points if required to conclude the investigation		
3.20	Centralized incident management to prioritize and manage security incidents.		
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		

4.2	Define, develop, implement, update and maintain Hunting Framework which contains:		
4.3	Create knowledge base of IOCs(Indicators of Compromise)		

4.4	Vendor should provide security analytics as a service to able to detect unknown attacks		
4.5	The analytics service should have models that are able to detect attacks in various stages of a cyber kill chain		
4.6	The analytics service 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.		
4.7	Analytics 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		
4.8	Solution should have pre-built AI models to detect targeted attacks (unknown attacks from unknown threat actors).		
4.9	Solution should have analytical models to detect different stages of Cyber Kill chain.		
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		
4.11	Network threat hunting should use AI on network sources and enable hunting for attacks including but not limited to Lateral Movement, Malware Beaconing, Data Exfiltration, Watering Hole, Targeted network attacks, Dynamic DNS attacks		
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		
4.13	The service should identify network traffic from potentially risky applications (e.g. file sharing, peer-to-peer, etc.).		

5.	**Endpoint Detection & Response Service – It should support**		
5.1	Endpoint threat hunting should hunt for Process anomalies, Service anomalies, Hash values, Connection anomalies and indicators of compromises.		
5.2	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.		

5.3	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. · Analyzing outlier binaries using supervised neural network.		
5.4	EDR service should be able to take quick response actions such as: · Killing anomalous processes, deleting malicious binaries · Isolating end points		
5.5	Detect threats on endpoints by deploying EDR agents. The service should be able to take containment actions such as isolating infected endpoints		
5.6	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.		
6.	**User Behavior 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 behavior anomalies of the user · Organization should be able to define risk thresholds based on their risk appetite		
6.2	Detect malicious/illegal activities performed by users		
6.3	Solution to have capabilities to collect user data from variety of sources like Directory Services , IAM, VPN, Proxy,O365, etc.		
6.4	Service should be able to track user‘s activities locally and remote network sites and should be able to report usage behavior across the entire network.		
6.5	The service should incorporate multiple baseline behavioral models which cover behavioral risk categories like Data Exfiltration, Malicious Users, Illicit Behavior, compromised credentials, etc.		

6.6	Solution should support business application threat hunting for application to detect access and authorization anomalies using application logs, NetFlow.		
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.)		
6.8	Solution should support applying AI models on WAF events to detect targeted web application attacks		
6.9	Service provider should submit a daily threat hunting based on the threat hunting models deployed at the organization		
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.		

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		
7.3	Service should provide strategic threat intelligence about incidents and breaches happening across the global and provide actionable intelligence such as · Can SBOSS 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		
7.4	Service should apply the threat intelligence to Organization assets, network traffic, security event and users to provide actionable report on likely impact on each entity and recommend pre-emptive measures.		
7.5	Solution should track status of assets against IoCs, CVEs and support the workflow for remediation. As an example, CVEs related to shadow broker release should be used to identify affected assets. Workflow should enable tracking the CVEs to closure through patching/other activities. Service provider should track closure and corresponding risk reduction		
7.6	Service should have machine algorithms to auto-evaluate an asset and assign a business value to the asset		
7.7	Solution should support STIX/TAXII for automated integration of actionable intelligence with security technologies.		
7.8	Service should support 3rd party / external threat intelligence to aid incident response by bringing in organizational context and internal information available in SIEM and other sources of security information		
8	Vulnerability Management		
8.1	Reports Should be provided on vulnerability status along with mitigation recommendations.		
8.2	Integration of vulnerability information with the Threat management system to get 360 degree view of the asset.		
9	**General Requirements**		

9.1	Service provider team should have the following skills: · Security analysts · Incident investigator · Threat hunter · Data scientists · Threat intelligence analytics · Incident responders · Specialized security team for IOC collection, deeper analysis, forensic investigation		
9.2	Solution should provision reconstructing common file formats including word document, image, Web page.		
9.3	The platform should have machine learning capabilities and other advanced analytics of structured as well as unstructured security & network data.		

9.4	The Log management solution (Centralized) is required at SBOSS for collection of logs from different log sources. VMs and Storage for Log collector will provide by SBOSS. Vendor to provide required specification document for log collector.		
9.5	Vendor shall build the capacity of the SIEM solution that can handle the log retention as mentioned below: · Three months – Online · Two Years – Offline		
9.6	24x7x365 real time logs monitoring, analysis and correlation using security analytics, Threat hunting, Threat Intelligence consisting of Indicators of Compromise (IOC) and other threat intel (vulnerabilities report, incident reports etc.).		
9.7	The proposed solution should provide end-to end capability to setup an SIEM, Big Data Security Analytics Platform and SOAR for storage, indexing, searching, analysis, correlation, reporting, visualization, orchestration of different types of structured / semi-structured data generated within the organization.		
9.8	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 RAID 5. The solution should have adequate redundancy for handling disk failures.		
9.9	Vendor will be responsible to store logs in industry standard solution and format.		
9.1	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.		
9.10	Alerting events/incidents and recommending remedial actions.		
9.11	Incident analysis (Triage) to remove false positives, incident notification.		
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.		

9.13	Monthly report summarizing the list of events/incidents reported, correlation analysis, recommendations, status of actions by SBOSS and other security advisories. It should include the trend analysis comparing the present month's data with the previous month data.		
9.14	Detect known as well as unknown threats by using machine learning and security analytics		
9.15	Consolidate data and extract actionable insight from a variety of intelligence sources and existing security technologies		
9.16	Proactive threat hunting on daily basis, which otherwise gets undetected via signature based systems.		
9.17	Be Cyber-Ready to respond to attacks swiftly.		

9.18	Complete analysis and correlation of logs from all the devices/solutions under scope		
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.		
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		
9.21	24x7x365 uninterrupted security monitoring operations. Submit a report in case of service non availability of the devices along with the status.		
9.22	Automate security processes to reduce resource drain and threat response times		
9.23	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		
9.24	Correlation of low priority alerts with subsequent alerts to detect multi-stage attacks.		
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		
9.26	Provide central dashboard to capture risk posture and maturity levels of organization at any given point of time.		

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. Vendor shall also provide customized dashboard to suit as per SBOSS requirements.		
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.)		
9.29	The offered cyber security product shall be complying with the Indian government regulations.		

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 SBOSS.		
9.31	SOC setup/infrastructure may be subjected to audit from SBOSS 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 SBOSS and its appointed auditors. Extreme care should be taken by the Vendor to ensure that the observations do not get repeated in subsequent Audits. Such non-compliance by Vendor shall attract penalty as defined in SLA.		
9.32	The solution should consist of security monitoring, incident response, security analytics, proactive threat hunting, threat Intelligence consisting of Indicators of Compromise (IOC) and other threat intel (vulnerabilities, strategic, tactical etc.), SIEM engineering, Endpoint Detection & Response, User Behavioral Anomaly detection, vulnerability scanning and network threat detection.		
9.33	Service Providers should propose monitoring platforms, to best suit the requirements stated in the RFP.		
9.34	To Develop & recommend improvement plans for the SOC as needed to maintain an effective and secure computing environment		
9.35	For improvement of SOC Monitoring at SBOSS. SP should done the Firewall rules review half yearly basis and Network architecture review along with VAPT (External VA, External PT, Internal VA and Internal PT)for critical assets on quarterly basis.		
9.36	Effective and Efficient Governance Model with fortnightly, monthly, quarterly and annual reviews		
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.		

9.38	NBAD and UEBA shall be considered as part of MSSP services, monitoring devices which provides insight of anomalies and potential risk to the network.		
9.39	The applications and databases logs shall be considered for the correlation.		
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.		
9.41	Analytical reports on Daily, weekly and Monthly basis and Ad-hoc reports as and when to be provide by service provider		
9.42	IT Forensic services for root cause of incident and investigations as and when required		

9.43	During the exit of the contract or services vendor should provide logs as per retention period from their end to SBOSS without any Price		
10	**Security Incident and Crisis Management services**		
10.1	Alignment of Security Incident management plan in line with SBOSS Cyber Crisis Management Plan (CCMP) and Cyber Security Policy		
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		
10.3	MSSP will provide a detailed process for managing cyber incidents - describing each phases of the process – prepare, identify, contain, eradicate, recover and learn from the incidents		
10.4	Develop response plan/ strategy which will describe the prioritization of incidents based on the organizational impact		
10.5	The incident management solution should be able to register any security event and generate alerts		
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		
10.7	Incident and problem Management, resolution, root cause analysis, and reporting within time limit as per the requirement		
10.8	Describe the incident response process including the roles and responsibilities and scope of action in line with CCMP		
10.9	MSSP should do root cause analysis for security incidents and recommend implementation of controls to prevent reoccurrence		
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 by doing the necessary analysis and log review and providing required data on a timely fashion		
10.11	Faster incident response by replacing purely ad-hoc activities with Advanced playbooks, analytical tools, incident management tools and reporting, which liberates security analysts to spend less time doing research and more time doing analysis		
10.12	MSSP shall provide backend professional incident management team		

	support in case of severe incident occurs		
11	**Packet Capture Analysis – Optional**		
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		
11.2	Solution should support Deep Packet Inspection (DPI) to classify protocols & applications by capturing packet.		
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.		
12	**Managed SOC Project Team for implementation and operation (offsite)**		
12. 1	The Project team must include following project structure with one dedicated SOC/SIEM Manager for real-time response mechanism throughout the engagement with SBOSS. SOC Manager (5+ Yrs) - CISSP/CISA/ISO 27001 Implementer or LA		

7. Annexure-B : Inventory

List of devices / servers (Approximate and indicative, this may increase over a period of time)

Sr. No.	Model	IOS / OS Version	Qty
1.	Network Devices	Firewall, Proxy (UTM), Routers, Aps, Switches, Load Balancer, VPN, etc..	5
2.	Systems	AD, AV, DLP, Email, Application, etc.	5
3.	Servers	OS & DB, VMs	2
4	End Points	Laptop Desktop	200 (tentative)

8. Annexure – C : Bidder's Organization Profile

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

To:

GM-SBOSS

Delhi 110003

Dear Sir,

Ref: **SBOSS/24-25/009** dated: 19/08/2024 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 Delhi, 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 in System Integration and 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	

9. Annexure – D : Compliance For Eligibility Criteria

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

MSE bidders shall be given relaxation from Prior Turnover Criteria, provided the bidder submits document such as MSE registration certificate. The registration certificate submitted by MSMEs must be valid as on close date of the RFP.

#	Eligibility Criteria	Compliance (Compliant/ Not Compliant)	Supporting Evidence
1.	The MSSP should be a current legal entity with a minimum 5 years of experience in India.	Y/N	Certificate of Incorporation or Appropriate Supporting Document
2.	The vendor should have experience of owning and managing a well-established Security Operations Centre (SOC) for at least three years. Vendor shall provide the details of the SOC including the location, infrastructure, tools used, companies served, process and methodology, staff employed, period of service	Y/N	Self-Declaration
3.	The MSSP should have performed managed SOC services for at least two clients during the last 3 financial years, with at least one of which should preferably be in the BFSI. Kindly furnish details of the same in the Technical Proposal. Size of SOC services must be similar or larger than SBOSS	Y/N	Customer references to be provided & Copies of Purchase Orders
4.	The service provider shall not sub-contract the assignment or to any other person/firm.	Y/N	Self-Declaration
5.	The bidder should be a company registered in India as per Company Acts. The bidder should have experience of minimum 3 years as SP of SIEM-SOC solution in India.	Y/N	Incorporation Certificate
6.	The Bidder's Account should not have been declared as a Non-Performing Asset (NPA) in the Books of any bank or financial institution as on 31.03.2023.	Y/N	Certificate from Bank/ Auditor
7.	The bidder 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 SBOSS)	Y/N	Undertaking by Bidder.
8	Average Annual Turnover should be INR 10 Crores in any of the Preceding last three financial years ie 2020-	Y/N	Auditors Certificate or CA certificate

	21, 2021-22, 2022-23 and or 2023-24.		
9	Financial statements i.e. Audited Balance sheet and Profit & Loss accounts for last three years (FY2020-21, FY2021-22 and FY2022- 23 and or 2023-24)	Y/N	Auditors Certificate or CA certificate
10	The participant should be a profit-making entity for minimum of Preceding Three years. It should not have incurred / reported losses during any of the last Three financial years.	Y/N	Appropriate Supporting Document
11	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
12	MSSP to have a functioning Disaster Recovery site and approved Business Continuity Plan to support SBOSS for continuity of SOC Operations	Y/N	Supporting Document
13	The MSSP should have permanent office in India	Y/N	Appropriate Supporting Document

ANNEXURE – E

SERVICE LEVEL AGREEMENT (SLA)

To be executed on non-judicial stamp of appropriate value.

This agreement ("Agreement") is made at Delhi (Place) on this day of 2024

BETWEEN

State Bank Operations Support Services Pvt Ltd, constituted under the Indian Companies Act 2013, having its Registered Office at 2nd Floor, NBCC Place, South Wing, Bhisham Pitamah Marg, Pragati Vihar, Lodhi Road, New Delhi, Delhi, India, 110003, hereinafter referred to as "SBOSS" which expression shall, unless it be repugnant to the context or meaning thereof, be deemed to mean and include its successors in title and assigns of the First Part:

AND

M/s----------, a private limited company incorporated under the provisions of the Companies Act, 2013, having its registered office at ----------, hereinafter referred to as "Service Provider" or "Vendor" or "----------", which expression shall mean to include its successors in title and permitted assigns of the Second Part:

WHEREAS "SBOSS" is carrying on business in extending operations support services to State Bank of India (SBI), in India and desirous to avail services for procurement and use of a front-end IT Application for the Feet-on-Street (FOS) executives;

AND WHEREAS the Service Provider being in a business of providing ---------- to various clients & in terms of SBOSS's Request for Proposal (RFP) No. ---------- dated ---------- along with its clarifications/ corrigenda, referred hereinafter as a "RFP".

NOW THEREFORE, in consideration of the mutual covenants, undertakings and conditions set forth below, and for valid consideration the acceptability and sufficiency of which are hereby acknowledged, the Parties hereby agree to the following terms and conditions hereinafter contained:

1. DEFINITIONS & INTERPRETATION

Definitions - Throughout this RFP, unless inconsistent with the subject matter or context:
Vendor/ Service Provider/ System Integrator – MSSP / SIEM Vendors.
Supplier/ Contractor/ Vendor – Selected Vendor/System Integrator under this RFP.
Company/ Purchaser/ SBOSS - Reference to the "SBOSS", "Company" and "Purchaser" shall be determined in context and may mean without limitation "SBOSS Ltd.
Proposal/ Bid – the Vendor's written reply or submission in response to this RFP
RFP/Tender – the request for proposal (this document) in its entirety, inclusive of any Addenda that may be issued by SBOSS.
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.
Product – "Product" means SIEM and Security Tools implemented for SOC and log collector as mentioned in the tender.
Server / Network / Website – As specified within the technical requirement section of this RFP document.

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 understood in technical sense in accordance with the industrial practices.

2. Commencement, Term & Change in Terms

2.1 This Agreement shall commence from its date of execution mentioned above/ be deemed to have commenced from ----------(Effective Date).

2..2 This Agreement shall be in force for a period of one (1) year from Effective Date, unless terminated by either party by notice in writing in accordance with the termination clauses of this Agreement.

2.3 SBOSS shall have the right at its discretion to renew this Agreement in writing, for a further term of Two (2) year on the same terms & conditions (total 3 years maximum).

2.4 Either Party can propose changes to the scope, nature or time schedule of services being performed under this Service Level Agreement. Such changes can be made upon mutually accepted terms & conditions maintaining the spirit (Purpose) of this Service Level Agreement.

3. SCOPE OF WORK

3.1 The scope and nature of the work/ Services which Service Provider must provide to SBOSS is described in Annexure-A.

Service Provider and/or its employee/representative shall be required to furnish. an undertaking and/or information security declaration on SBOSS's prescribed format before such remote access is provided by SBOSS.

3.2 Service Provider shall ensure that services are performed in a physically protected and secure environment which ensures confidentiality and integrity of SBOSS's data and artefacts, including but not limited to information (on customer, account, transactions, users, usage, staff, etc.), architecture (information, data, network, application, security, etc.), programming codes, access configurations, parameter settings, executable files, etc., which SBOSS representative may inspect. Service Provider shall facilitate and/ or handover the Device to SBOSS or its authorized representative for investigation and/or forensic audit.

3.3 Service Provider shall be responsible for protecting its network and subnetworks, f from which remote access to SBOSS's network is performed, effectively against unauthorized access, malware, malicious code and other threats in order to ensure SBOSS's information technology system is not compromised in the course of using remote access facility.

4. Bank Guarantee and Penalties -

4.1 Service Provider shall furnish performance security in the form of Bank Guarantee for an amount of Rs. 10%/of the order value valid for a period of Three (3) year(s) zero (0) month(s) from a Scheduled Commercial Bank other than State Bank of India in a format provided/ approved by SBOSS.

4.2 Bank Guarantee is required to protect the interest of SBOSS against delay in supply/installation and/or the risk of non-performance of Service Provider in respect of successful implementation of the project; or performance of the material or services sold; or breach of any terms and conditions of the Agreement, which may warrant invoking of Bank Guarantee.

4.3 If at any time during performance of the Contract, Service Provider shall encounter unexpected conditions impeding timely completion of the Services under the Agreement and performance of the services, Service Provider shall promptly notify SBOSS in writing of the fact of the delay, it's likely duration and its cause(s). As soon as practicable, after receipt of Service Provider's notice, SBOSS 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.

4. 4 Performance of the obligations under the Agreement shall be made by the Service Provider in accordance with the time schedule specified in this Agreement.

4.5 Service Provider shall be liable to pay penalty at the rate mentioned in Annexure 'F' in respect of any delay beyond the permitted period in providing the Services and attributable to Service Provider.

4.6 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.

4.7 No penalty shall be levied in case of delay(s) in deliverables or performance of the contract for the reasons solely and directly & indirectly (example SBOSS's 3rd party vendors) attributable to SBOSS. On reaching the maximum of penalties specified SBOSS reserves the right to terminate the Agreement.

5. REPRESENTATIONS & WARRANTIES:

5.1 Service Provider warrants that the technical quality and performance of the Services provided will be consistent with the mutually agreed standards. Warranty shall cover the entire period of this Agreement from the date of acceptance. Service Provider will also provide twelve weeks of post production support for rollout of each phase.

5.2 Any defect found will be evaluated mutually to establish the exact cause of the defect. Service Provider to provide technical support to SBOSS for related deficiencies.

5.3 Service Provider warrants that at the time of delivery, the Software or its component is free from malware, free from any obvious bugs, and free from any covert channels in the code (of the versions of the applications/software being delivered as well as any subsequent versions/modifications delivered).

5.4 Service Provider represents and warrants that its personnel shall be present at SBOSS premises or any other place as SBOSS may direct, only for the Services and follow all the instructions provided by SBOSS; Act diligently, professionally and shall maintain the decorum and environment of SBOSS; Comply with all occupational, health or safety policies of SBOSS.

5.5 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 sub-contractors (if allowed) and in particular laws relating to terminal benefits such as pension, gratuity, provident fund, bonus or other benefits to which they may be entitled and the laws relating to contract labour, minimum wages, etc., and SBOSS shall have no liability in this regard.

5.6 Each Party represents and warrants that it has all requisite power and authorization to enter into and perform this Agreement and that nothing contained herein or required in the performance hereof conflict or will conflict with or give rise to a breach or default under, or permit any person or entity to terminate, any contract or instrument to which the party is bound.

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

5.8 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.

5.9 Service Provider has the requisite technical and other competence, sufficient, suitable, qualified and experienced manpower/personnel and expertise in providing the Services as scoped under this RFP to SBOSS.

5.10 Service Provider shall duly intimate to SBOSS immediately, the changes, if any in the constitution of Service Provider.

5.11 Service Provider warrants that to the best of its knowledge, as on the Effective Date of this Agreement, the Software does not violate or infringe any patent, copyright, trademarks, trade secrets or other Intellectual Property Rights of any third party.

5.12 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 SBOSS as and when requested.

5.13 During the Warranty Period, if any software or any component thereof supplied by Service Provider is inoperable or suffers degraded performance not due to causes external to the software / SBOSS / SBOSS's other vendors, Service Provider shall, at SBOSS's request, promptly replace the software or specified component with new software of the same type and quality on its own cost. Such replacement shall be accomplished without any adverse impact on SBOSS's operations within agreed time frame.

6. Service Level Requirements, Penalties & Escalation Matrix:

1.1. SLAs for 24 x 7 Threat Detection & Response Services will be applied as below:
1.2. Daily report of events/incidents, correlation, analysis, recommendations and closure status by next business day.
1.3. Monthly report by 7th day of every month (including excel based reports).
1.4. 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 SBOSS official and suggest suitable countermeasures to safeguard against such evolving threats/attacks along with the analysis. The advisories should be customized to SBOSS Infrastructure. Report pertaining to the same should be part of the monthly report.
1.5. Report on recommendations regarding enhancement of security of SBOSS should be part of the monthly report.
1.6. 24*7*365 dashboard availability to be ensured.
1.7. For purpose of calculating penalty, uptime is calculated as under:

$$\text{Uptime (\%)} = \frac{\text{Total Monthly Minutes} - \text{Total downtime minutes in month}}{\text{Total monthly Minutes during the month}} \times (100)$$

Sr No	Service Area	Service Level	SLA
1	Monitoring & Incident Alerting	1. Log Analysis Services 2. 24x7 monitoring of all in- scope devices. 3. Categorization of Incidents into High, Medium and Low priority shall be carried out in consultation with the selected bidder during the contract period. 4. All High and Medium priority incident should be logged as incident tickets and alerted as per SL. • High Criticality security alerts within 30 minutes of the event identification. • Medium priority security alerts within 3 hours of the event identification. • Low priority security alerts within 8 hours of the event identification	1. High Criticality Security Alerts (Priority 1) to be reported within 30 minutes and resolved within 1 hour 2. Medium Criticality Security Alerts (Priority 2) to be responded within 3 hours and resolved within 6 hours 3. Low Criticality Security Alerts (Priority 3) to be responded within 8 hours and resolved within 24 hours 4. SLs pertaining to new use cases, request of logs, new devices integrations will also be used in below table calculations

2	1. Threat Hunting 2. EDR 3. Incident Analysis & response 4. Investigation Reports and Closure 5. UBA	Sending out detailed investigation report post alert notification. Action plan/ mitigation steps should be alerted to designated bank personnel as per the below SL: • High Criticality incident within 1 hour of the event identification. • High priority incident within 6 hours of the event identification. • Medium priority incident within 24 hours of the event identification	1. High priority incident within 1 hours 2. Medium priority incident within 6 hours 3. Low priority incident within 24 hours
3	Reports and Dashboard	1. Daily Reports: By 10:00 AM everyday 2. Weekly Reports: By 10:00 AM, Monday 3. Monthly Reports: 5thworking day of each month	Threshold: SL compliance 95%, measured per month Penalty: 5% of monthly payment.

Penalty for Service Area 1 to 2 shall be calculated as follows-

Service Uptime Penalty.

Service Level Compliance /Month	**Penalty**
99.5% and above	NA
Greater than 97% but less than 99.5%	3 % monthly payment
Greater than 95% but less than 97%	5 % monthly payment
Greater than 90% but less than 95%	10% of monthly payment
Less than 90 percent	100% of monthly payment

Escalation Matrix

During the period of agreement following escalation matrix is to be used

For SBOSS

Level	Name	Email ID	Mobile No	Designation
Level 1				
Level 2				
Level 3				

For ----------

Level	Name	Email ID	Mobile No	Designation
Level 1				
Level 2				
Level 3				

7. GENERAL INDEMNITY

7.1 Service Provider agrees and hereby keeps SBOSS indemnified against all claims, actions, loss, damages, costs, expenses, charges, including legal expenses (Attorney, Advocates fees included) which SBOSS may suffer or incur on account of (i) Service Provider's breach of its warranties, covenants, responsibilities or obligations; or (ii) breach of confidentiality obligations mentioned in this Agreement; or (iii) any willful 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 SBOSS.

7.2 Service Provider hereby undertakes the responsibility to take all possible measures, at no cost, to avoid or rectify any issues which thereby results in non-performance of software within reasonable time. SBOSS shall report as far as possible all material defects to Service Provider without undue delay. Service Provider also undertakes to co-operate with other Service Providers thereby ensuring expected performance covered under scope of work.

8. CONTINGENCY PLANS

Service Provider shall arrange and ensure proper data recovery mechanism, attrition plan and other 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 SBOSS. Service Provider at SBOSS's discretion shall co-operate with SBOSS in case on any contingency.

9. TRANSITION REQUIREMENT

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, SBOSS at its sole discretion may make alternate arrangement for getting the Services contracted with another Service Provider/vendor. In such a case, SBOSS 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. During the transition phase, the existing Service Provider shall render all reasonable assistance to the new Service Provider within such period prescribed by SBOSS, at no extra cost to SBOSS, for ensuring smooth switch over and continuity of Services, provided where transition services are required by SBOSS 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 the existing Service Provider is in breach of this obligation, they shall be liable for paying a penalty of Rs.5,00,000/- on demand to SBOSS, which may be settled from the payment of invoices or Bank Guarantee for the contracted period. Transition & Knowledge Transfer plan is as per Annexure G.

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, SBOSS 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 implementation & integration fee for delay of each week or part thereof maximum up to 5% of total implementation & integration fee. Once the maximum deduction is reached, SBOSS may consider termination of the Agreement.

11. RELATIONSHIP BETWEEN THE PARTIES

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

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

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

11.4 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.

11.5 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 accidents occurred

due to gross negligent act of the Party in whose premises the accident occurred.

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

12. SUB-CONTRACTING

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

13. INTELLECTUAL PROPERTY RIGHTS

13.1 For any technology / Software / solution developed/used/supplied by Service Provider for performing Services or licensing and implementing Software and solution for SBOSS as part of this Agreement, Service Provider shall have right to use as well right to license for the outsourced services or third-party product. SBOSS shall not be liable for any license or IPR violation on the part of Service Provider.

13.2 Without SBOSS's prior written approval, Service Provider will not, in performing the Services, use or incorporate, link to or call or depend in any way upon, any software or other intellectual property that is subject to an Open Source or Copy-left license or any other agreement that may give rise to any third-party claims or to limit SBOSS's rights under this Agreement.

13.3 Subject to clause 13.4 and 13.5 of this Agreement, Service Provider shall, at its own expenses without any limitation, indemnify and keep fully and effectively indemnified SBOSS against all cost, claims, damages, demands, expenses and liabilities whatsoever nature arising out of or in connection with all claims of infringement of Intellectual Property Right, including patent, trademark, copyright, trade secret or industrial design rights of any third party arising from use of the technology/ Software/ products or any part thereof in India or abroad, for Software licensed/developed as part of this engagement. In case of violation/ infringement of patent/ trademark/ copyright/ trade secret or industrial design or any other Intellectual Property Right of third party, Service Provider shall, after due inspection and testing, without any additional cost (a) procure for SBOSS the right to continue to using the Software supplied; or (b) replace or modify the Software to make it non-infringing so long as the replacement to or modification of Software provide substantially equivalent functional, performance and operational features as the infringing Software which is being replaced or modified; or (c) to the extent that the activities under clauses (a) and (b) above are not commercially reasonable, refund to SBOSS all amounts paid by SBOSS to Service Provider under this Agreement.

13.4 SBOSS will give (a) notice to Service Provider of any such claim without delay/provide reasonable assistance to Service Provider in disposing of the claim; (b) sole authority to defend and settle such claim and; (c) 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 SBOSS, unless such settlement releases SBOSS fully from such claim, (ii) Service Provider shall promptly provide SBOSS with copies of all pleadings or similar documents relating to any such claim, (iii) Service Provider shall consult with SBOSS with respect to the defense and settlement of any such claim, and (iv) in any litigation to which SBOSS is also a party, SBOSS shall be entitled to be separately represented at its own expenses by counsel of its own selection..

13.5 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 SBOSS'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 SBOSS of the same); (ii) any unauthorized modification or alteration of the Software by SBOSS; or (iii) failure to implement an update to the licensed software that would have avoided the infringement, provided Service Provider has notified SBOSS in writing that use of the update would have avoided the claim.

13.6 Service Provider hereby grants SBOSS a fully paid-up, irrevocable, unlimited, exclusive license (for the annual duration from license activation date) throughout the territory of India to access and use Software licensed/developed including its upgraded versions available during the term of this Agreement by Service Provider as part of this engagement, including all inventions, designs and trademarks embodied therein.

15. INSPECTION AND AUDIT:

15.1 It is agreed by and between the parties that Service Provider shall be subject to annual audit by internal/external Auditors appointed by SBOSS/ inspecting official from SBI or Reserve Bank of India or any regulatory authority, covering the risk parameters finalized by SBOSS/ such auditors in the areas of products (IT hardware/ Software) and services etc. provided to SBOSS. Service Provider shall submit such certification by such Auditors to SBOSS. Service Provider and or his / their outsourced agents /sub – contractors (if allowed by SBOSS) shall facilitate the same. SBOSS 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 SBOSS. Except for the audit done by Reserve Bank of India or any statutory/regulatory authority, SBOSS 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.

15.2 Where any deficiency has been observed during audit of Service Provider on the risk parameters finalized by SBOSS 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 SBOSS regarding compliance of the observations made by the auditors covering the respective risk parameters against which such deficiencies observed.

15.3 Service Provider further agrees that whenever required by SBOSS, it will furnish all relevant information, records/data to such auditors and/or inspecting officials of SBOSS/ Reserve Bank of India and/or any regulatory authority. SBOSS 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.).

16. CONFIDENTIALITY

16.1 "Confidential Information" mean all information which is material to the business operations of either party or its affiliated companies, designated as being confidential or which, under the circumstances surrounding disclosure out to be treated as confidential, in any form including, but not limited to, proprietary information and trade secrets, whether or not protected under any patent, copyright or other intellectual property laws, in any oral, photographic or electronic form, whether contained on computer hard disks or floppy diskettes or otherwise without any limitation whatsoever. Without prejudice to the generality of the foregoing, the Confidential Information shall include all information about the party and its customers, costing and technical data, studies, consultants reports, financial information, computer models and programs, software Code, contracts, drawings, blue prints, specifications, operating techniques, processes, models, diagrams, data sheets, reports and other information with respect to any of the foregoing matters. All and every information received by the parties and marked confidential hereto shall be assumed to be confidential information unless otherwise proved. It is further agreed that the information relating to SBOSS and its customers is deemed confidential whether marked confidential or not.

16.2 All information relating to the accounts of SBOSS's customers shall be confidential information, whether labelled as such or otherwise.

16.3 All information relating to the infrastructure and Applications (including designs and processes) shall be deemed to be Confidential Information whether labelled as such or not. Service Provider personnel/resources responsible for the project are expected to take care that their representatives, where necessary, have executed a Non-Disclosure Agreement to comply with the confidential obligations under this Agreement.

16.4 Each party agrees that it will not disclose any Confidential Information received from the other to any third parties under any circumstances without the prior written consent of the other party unless such disclosure of Confidential Information is required by law, legal process or any order of any government, regulatory, statutory, judicial or quasi-judicial authority. Service Provider, in this connection, agrees to abide by the laws especially applicable to confidentiality of information relating to customers of SBOSS's and SBI's per-se, even when the disclosure is required under the law. In such event, the Party must notify the other Party that such disclosure has been made in accordance with law; legal process or order of a government, regulatory, statutory, judicial or quasi-judicial authority.

16.5 Each party, including its personnel, shall use the Confidential Information only for the purposes of achieving objectives set out in this Agreement. Use of the Confidential Information for any other purpose shall constitute breach of trust of the same.

16.6 Each party may disclose the Confidential Information to its personnel solely for the purpose of undertaking work directly related to the Agreement. The extent of Confidential Information disclosed shall be strictly limited to what is necessary for those particular personnel to perform his/her duties in connection with the Agreement. Further each Party shall ensure that each personnel representing the respective party agree to be bound by obligations of confidentiality no less restrictive than the terms of this Agreement.

16.7 The non-disclosure obligations herein contained shall not be applicable only under the following circumstances:

(i) Where Confidential Information comes into the public domain during or after the date of this Agreement otherwise than by disclosure by receiving party in breach of the terms hereof.

(ii) Where any Confidential Information was disclosed after receiving the written consent of disclosing party.

(iii) Where receiving party is requested or required by law or by any Court or governmental agency or authority to disclose any of the Confidential Information, then receiving party will provide the other Party with prompt notice of such request or requirement prior to such disclosure.

(iv) Where any Confidential Information was received by the receiving party from a third party which does not have any obligations of confidentiality to the other Party.

(v) Where Confidential Information is independently developed by receiving party without any reference to or use of disclosing party's Confidential Information.

16.8 Receiving party undertakes to promptly notify disclosing party in writing any breach of obligation of the Agreement by its employees or representatives including confidentiality obligations. 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.

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

16.10 Any document received from SBOSS shall remain the property of SBOSS and shall be returned (in all copies) to SBOSS on completion of Service Provider's performance under the Agreement.

16.11 Upon expiration or termination of the Agreement, all SBOSS's proprietary documents, customized programs partially or wholly completed and associated documentation, or SBOSS's materials which are directly related to any project under the Agreement shall be delivered to SBOSS or at SBOSS's written instruction destroyed, and no copies shall be retained by Service Provider without SBOSS's written consent.

16.12 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 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.

17. DATA PROTECTION

17.1 Service provider shall apply appropriate physical, technical and organizational measures to ensure a high level of security for Personal Data appropriate to the respective risk and the ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services as per the relevant laws of India.

17.2 If Personal Data of SBOSS is disclosed to the Service Provider, the service provider shall comply with all applicable data protection laws and regulations.

17.3 Service Provider agrees that it will Submit Third Party review by a CERT-IN Auditor for the SOC implementation and SBOSS IT Security Posture on an annual basis or as advised by the bank (SBI) and agrees to implement required mitigation related changes.

17.4 The Service Provider shall ensure that all data centers where the data of SBOSS is stored, processed, or backed up, must be guaranteed to reside within India only (Service provider has to provide an undertaking along with data center letter).

17.5 If the service provider becomes aware that data may have been accessed, disclosed, or acquired without proper authorization and contrary to the terms of this agreement or the contract, then the service provider shall use reasonable efforts to alert SBOSS of any data breach within 24 hrs or at earliest along with the nature and scope of the data breach. It shall immediately take such actions as may be necessary to preserve forensic evidence and eliminate the cause of data breach.

18. DATA MANAGEMENT:

18.1 The service provider shall manage data isolation in a multi-tenant environment.

18.2 The service provider shall ensure compliance to the SBOSS's backup and Retention policy.

18.3 The service provider shall transfer data backup in house either on demand or in case of contract or order termination for any reason.

18.4 Manage data reminiscence throughout the data life cycle.

18.5 Service provider shall implement in case additional mechanisms need to be implemented, for handling data.

18.6 Services provider shall not delete any data at the end of the agreement (for a maximum of 90 days beyond the expiry of the agreement) without the explicit approval of the SBOSS.

18.7 When the SBOSS or service provider (with prior approval of the SBOSS) scales down the infrastructure services, Service provider is responsible for deleting or otherwise securing SBOSSs Content/data prior to VM deleting and in case deleted, shall ensure that the data cannot be forensically recovered.

18.8 Service provider shall ensure the protection of the SBOSSs data from any unauthorized access, modification. Copying/storing. violation of these shall be treated as copyright

infringement.

19. TRANSFER OF DATA:

19.1 In the event of expiry or termination of this Agreement Service Provider shall cease to use the SBOSS's Data and, at the request of the SBOSS, shall destroy all such copies of the SBOSS's Data then in its possession to the extent specified by the SBOSS.

19.2 Except where, pursuant to paragraph (a) above, the SBOSS has instructed Service Provider to destroy such SBOSS's Data as is held and controlled by Service Provider, 1 (one) month prior to expiry or within 1 (one) month of termination of this Agreement, Service Provider shall deliver to the SBOSS:

19.3 An inventory of the SBOSS's Data held and controlled by Service Provider, plus any other data required to support the Services; and/or draft plan for the transfer of the SBOSS's Data held and controlled by Service Provider and any other available data to be transferred.

20. SOURCE CODE AGREEMENT:

20.1 Service provider shall deposit the custom code, if any, built specifically for SBOSS in SBOSS's code repository (GitHub)

20.2 Service provider shall deposit the latest version of source code in escrow account at regular intervals as mentioned in source code escrow agreement.

20.3 The SBOSS shall have the right to get the source code released and will receive no opposition/hindrances from the escrow agent and Service provider under the following conditions:

i. In the event wherein Service provider files a voluntary petition in bankruptcy or insolvency or has been otherwise declared Insolvent/bankrupt, or

ii. In the event wherein Service provider has declared its expressed/written unwillingness to fulfil his contractual obligations under this Agreement, or

iii. Service Provider is wound up, or ordered wound up, or has a winding up petition ordered against it, or assigns all or a substantial part of its business or assets for the benefit of creditors, or permits the appointment of a receiver for the whole or substantial part of its business or assets, or otherwise ceases to conduct its business in the normal course, or

iv Service Provider discontinues business because of insolvency or bankruptcy, and no successor assumes Service Provider's Software maintenance obligations or obligations mentioned in the Agreement; or Service Provider dissolves or ceases to function as a going concern or to conduct its operation in the normal course of business or intends and conveys its intention to do so; or Any other release condition as specified in source code escrow agreement.

20.4 The escrow agreement shall ipso-facto would get terminated on delivery of source code to either of the parties upon the terms & conditions mentioned in source code escrow agreement.

21 SANCTIONS FOR VIOLATIONS

21.1 Any breach of the provisions laid under this agreement by the Service Provider or any one employed by it or acting on its behalf shall entitle the SBOSS to take all or any one of the following actions, wherever required.

21.2 To immediately terminate the contract without assigning any reason or without giving any compensation to the Service Provider or SBOSS can take any action as deemed appropriate.

22 TERMINATION

22.1 SBOSS 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 SBOSS;
(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 22.1 (i) to 22.1 (iii), SBOSS 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, SBOSS shall have right to initiate action in accordance with above clause.

22.2 SBOSS, by written notice of not less than 30 (Thirty) days, may terminate the Agreement, in whole or in part, for its convenience. In the event of termination of the Agreement for SBOSS's convenience, Service Provider shall be entitled for payment for the services rendered (delivered) up to the effective date of termination
In the event SBOSS terminates the Agreement in whole or in part for the breaches attributable to Service Provider, SBOSS may procure, upon such terms and in such manner, as it deems appropriate, software or services similar to those undelivered and subject to clause 26 Service Provider shall be liable to SBOSS for any excess costs for such similar software or services. However, Service Provider, in case of part termination, shall continue the performance of the Agreement to the extent not terminated.

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

(i) 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.

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

(iii) 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 SBOSS tantamount to fraud or prejudicial to the interest of SBOSS or its employees.

(iv) 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.

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

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

22.7 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 or before the date of termination or expiration; the obligation of indemnity; obligation of payment; confidentiality obligation; Governing Law clause; Dispute resolution clause; and any right which a Party may have under the applicable Law.

23 DISPUTE REDRESSAL MACHANISM & GOVERNING LAW

23.1 All disputes or differences whatsoever arising between the parties out of or in connection with this Agreement (including dispute concerning interpretation) or in discharge of any obligation arising out of the Agreement (whether during the progress of work or after completion of such work and whether before or after the termination of this Agreement, abandonment or breach of this Agreement), shall be settled amicably.

23.2 If the parties are not able to solve them amicably within 30 (thirty) days after dispute occurs as evidenced through the first written communication from any Party notifying the other regarding the disputes, either Party [SBOSS or Service Provider] shall give written notice to other party clearly setting out there in, specific dispute(s) and/or difference(s), and shall be referred to a sole arbitrator mutually agreed upon, and the award made in pursuance

thereof shall be binding on the Parties.

23.3 In the absence of consensus about the single arbitrator, the dispute may be referred to an arbitration panel; one to be nominated by each Party and the said arbitrators shall nominate a presiding arbitrator, before commencing the arbitration proceedings. The arbitration shall be settled in accordance with the applicable Indian Laws and the arbitration shall be conducted in accordance with the Arbitration and Conciliation Act, 1996.

23.4 Service Provider shall continue work under the Agreement during the arbitration proceedings, unless otherwise directed by SBOSS or unless the matter is such that the work cannot possibly be continued until the decision of the arbitrator is obtained.

23.5 The venue and seat of Arbitration proceeding shall be held at Delhi, India, and the language of the arbitration proceedings and that of all documents and communications between the parties shall be in English.

23.6 This Agreement shall be governed by laws in force in India. Subject to the arbitration clause above, all disputes arising out of or in relation to this Agreement, shall be subject to the exclusive jurisdiction of the courts at Delhi only.

23.7 In case of any change in applicable laws that has an effect on the terms of this Agreement, the Parties agree that the Agreement may be reviewed, and if deemed necessary by the Parties, make necessary amendments to the Agreement by mutual agreement in writing in good faith, in case of disagreement obligations mentioned in this clause shall be observed.

24. POWERS TO VARY OR OMIT WORK

24.1 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 SBOSS. SBOSS 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 SBOSS, thereof, in writing with reasons for holding such opinion and SBOSS 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 SBOSS 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 SBOSS 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.

24.2 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.

25. WAIVER OF RIGHTS

Each Party agrees that any delay or omission on the part of the other Party to exercise any right, power or remedy under this Agreement will not automatically operate as a waiver of such right, power or remedy or any other right, power or remedy and no waiver will be effective unless it is in writing and signed by the waiving Party. Further the waiver or the single or partial exercise of any right, power or remedy by either Party hereunder on one occasion will not be construed as a bar to a waiver of any successive or other right, power or remedy on any other occasion.

26. LIMITATION OF LIABILITY

26.1 The maximum aggregate liability of Service Provider, subject to clause 26.3, in respect of any claims, losses, costs or damages arising out of or in connection with this Agreement shall not exceed 50 (Five) % of the total Project Cost.

26.2 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.

26.3 The limitations set forth in Clause 26.1 shall not apply with respect to:

(i) claims that are the subject of indemnification pursuant to Clause 13 (infringement of third party Intellectual Property Right);
(ii) damage(s) occasioned by the Gross Negligence or Willful Misconduct of Service Provider;
(iii) damage(s) caused by Service Provider for breach of Confidentiality Obligations.
(iv) Regulatory or statutory fines imposed by a Government or Regulatory agency for non-compliance, due to Service Provider, of statutory or regulatory guidelines applicable to SBOSS, provided such guidelines were brought to the notice of Service Provider.

For the purpose of clause 26.3 (ii) "Gross Negligence" means any act or failure to act by 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.

"Willful 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.

27. FORCE MAJEURE

27.1 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.

27.2 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 Service Provider 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.

27.3 If Force Majeure situation arises, the non-performing Party shall promptly notify to the other Party in writing of such conditions and the cause(s) thereof. Unless otherwise agreed in writing, the non-performing Party shall continue to perform its obligations under the Agreement as far as is reasonably practical and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event.

27.4 If the Force Majeure situation continues beyond 30 (thirty) days, either Party shall have the right to terminate the Agreement by giving a written 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.

28. NOTICES

28.1 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, e-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, e-mail, telegram or facsimile)

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

28.3 The addresses for Communications to the Parties are as under.

(a) IN THE CASE OF SBOSS:

2nd Floor, NBCC Place,
East Wing, Bhisham Pitamah Marg,
Pragati Vihar, Lodhi Road, New Delhi, India, 110003

(b) IN CASE OF SERVICE PROVIDER:

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

29. GENERALTERMS & CONDITIONS

29.1 TRAINING: Service Provider shall train designated SBOSS officials on the configuration, operation/ functionalities, maintenance, support & administration for Software, application architecture and components, installation, troubleshooting processes of the proposed Services as mentioned in this Agreement wherever required.

29.2 PUBLICITY: Service Provider may make a reference of the Services rendered to SBOSS covered under this Agreement on Service Provider's Web Site or in their sales presentations, promotional materials, business plans or news releases etc., only after prior written approval from SBOSS.

29.3 SUCCESSORS AND ASSIGNS: This Agreement shall bind and inure to the benefit of the Parties, and their respective successors and permitted assigns.

29.4 NON-HIRE AND NON-SOLICITATION: During the term of this Agreement and for a period of one year thereafter, neither Party shall (either directly or indirectly through a third party) employ, solicit to employ, cause to be solicited for the purpose of employment or offer employment to any employee(s) of the other Party, or aid any third person to do so, without the specific written consent of the other Party. However, nothing in this clause shall affect SBOSS's regular recruitments as per its recruitment policy and not targeted to the employees of Service Provider.

29.5 SEVERABILITY: The invalidity or unenforceability of any provision of this Agreement shall not in any way effect, impair or render unenforceable this Agreement or any other provision contained herein, which shall remain in full force and effect.

29.6 MODIFICATION: This Agreement may not be modified or amended except in writing signed by duly authorized representatives of each Party with express mention thereto of this Agreement.

29.7 ENTIRE AGREEMENT: 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:
(i) This Agreement ;
(ii) Annexure of Agreement;
(iii) RFP No. : ----------dated ----------

29.8 PRIVITY: 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.

29.9 DUE AUTHORISATION: Each of the undersigned hereby represents to the other that she/ he is authorized to enter into this Agreement and bind the respective parties to this Agreement.

29.10 COUNTERPART: This Agreement may be executed in duplicate and each copy is treated as original for all legal purposes.

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.

STATE BANK OPERATIONS SUPPORT SERVICES PRIVATE LTD	**NAME OF SEVRICE PROVIDER/BIDDER/VEDOR**
By: Name:	By: Name:
Designation:	Designation:
Date	Date

WITNESS:

1. 1.

2. 2.

11 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					

12. Annexure G : Commercial Bid

Sr No	Particulars	Rate (in INR) (i)	Frequency (ii)	Total (in INR) (iii) = (i) * (ii)
1	(A) One-time Implementation Phase Cost		1	
	Particulars	**Monthly Rate (in INR)(i)**	**Frequency (ii)**	**Total (in INR) (iii) = (i) * (ii)**
2	(B) Operations Cost for Year 1*		12	
3	(C) Operations Cost for Year 2*		12	
4	(D) Operations Cost for Year 3*		12	
	Particulars			**Amount (in INR)**
5	**Total Cost of Project (E)= (A+B+C+D)**			

13. Annexure H : Reverse Auction – Overall Package Price

To arrive at L-1 bidder, Revers Auction will be conducted for the overall package price as shown below:

Total Price (in INR) excluding taxes		
S. No.	**Description**	**Amount** (in INR) (excl. taxes)
Overall package price (Yearly)		

*This Price shall remain valid during the entire contract period of three years.

ANNEXURE – J

Non-Disclosure Agreement (NDA)

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

THIS RECIPROCAL NON-DISCLOSURE AGREEMENT (the 'Agreement') is made at (Place _____) on _____ between:

State Bank Operations Support Services Pvt Ltd. (SBOSS), constituted under the Company's Act 2013, having its Regd Office at New Delhi (hereinafter referred to as 'Company', which expression includes its successors and assigns) of the ONE PART;

and

_____ a Private/Public Limited Company/LLP/Firm <*strike off whichever is not applicable*> incorporated under the provisions of the Companies Act, 1956/2013/ Limited Liability Partnership Act, 2008/Indian Partnership Act, 1932 <*strike off whichever is not applicable*>, having its Registered Office at _____ (hereinafter referred to as '_____', 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. SBOSS is carrying on business of providing operational support to its clients, has agreed to hire manpower resources for various positions (on-roll and off-roll) for deployment at its offices or SBOSS Client's branches.

2. For purposes of advancing their business relationship, the parties would need to disclose certain valuable confidential information to each other (the Party receiving the information 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 any confidentiality obligations 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, whether machine or user readable.

2. **Restrictions**

a. Each party shall treat as confidential the Contract and any and all information ('confidential information') obtained from the other 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 Sub-Contractor subject to such Sub-Contractor giving the SBOSS an undertaking on 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 construed as a breach of this Agreement by Receiving Party.

b. Receiving Party may disclose Confidential Information in accordance with judicial or other Government 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 either party, and

   ii. Government or Regulatory Authorities regulating the affairs of the parties and inspectors and supervisory bodies thereof

c. Confidential Information and Confidential Material may be disclosed, reproduced, summarized or distributed only in pursuance of Receiving Party's business relationship with Disclosing Party, and only as otherwise provided hereunder. Receiving Party agrees to segregate all such Confidential Material from the confidential material of others in order to prevent mixing.

3. **Rights and Remedies**

(a) Receiving Party shall notify Disclosing Party immediately upon discovery of any unauthorized use or 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.

4. **Miscellaneous**

(a) All Confidential Information and Confidential Materials are and shall remain the sole property 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 Willful 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 evaluating or advancing a business relationship between the parties, or any license rights whatsoever in any patent, copyright or other intellectual property rights pertaining to the Confidential Information.

(d) The terms of Confidentiality under this Agreement shall not be construed to limit either party's right to independently develop or acquire product without use of the other party's Confidential Information. Further, either party shall be free to use for any purpose the residuals resulting from access to or work with such Confidential Information, provided that such party shall maintain the confidentiality of the Confidential Information as provided herein. The term 'residuals' means information in non-tangible form, which may be retained by person who has had access to the Confidential Information, including ideas, concepts, know-how or techniques contained therein. Neither party shall have any obligation to limit or restrict the assignment of such persons or to pay royalties for any work resulting from the use of residuals. However, the foregoing shall not be deemed to grant to either party a license under the other party's copyrights or patents.

(e) 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 the 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) This Agreement shall be governed by and be construed in accordance with the laws of Republic of India. The parties agree to submit to the exclusive jurisdiction of appropriate Court in Delhi in connection with any dispute between the parties under the Agreement.

(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 36 months 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.

5. **Suggestions and Feedback**

Either Party from time to time may provide suggestions, comments or other feedback to the Other Party with respect to Confidential Information provided originally by the Other Party (hereinafter 'feedback'). Both Parties agree that all feedback is and shall be entirely voluntary and shall not in the absence of a separate agreement, create any confidentially obligation for the Receiving Party. However, the Receiving Party shall not disclose the source of any feedback without the Providing Party's consent. Feedback shall be clearly designated as such and, except as otherwise provided herein, each Party shall be free to disclose and use such feedback as it sees fit, entirely without obligation of any kind to other Party. The foregoing shall not, however, affect either Party's obligations hereunder with respect to Confidential Information of other party.

Dated this _____ day of _____ (Month) 2023__ at _____(place)

For and on behalf of _____

Name		
Designation		
Place		
Signature		

For and on behalf of _____

Name		
Designation		
Place		
Signature		

ANNEXURE – K

Commercial Bid Form

(Bidder's Letter Head)

(To be included in Commercial Bid Envelop)

To
State Bank Operations Support Services Pvt Ltd.
2 Floor, NBCC Place, South Wing, Bhisham, Pitamah Marg,
Pragati Vihar, Lodhi Road,
New Delhi, India, 110003

Dear Sirs,

Re: RFP No ----------

Having examined the Bidding Documents placed along with RFP, we, the undersigned, offer to provide the required infrastructure in conformity with the said Bidding documents for the sum of Rs (Rupees) (exclusive of taxes) or such other sums as may be ascertained in accordance with the Schedule of Prices attached herewith and made part of this Bid.

We undertake, if our Bid is accepted, to provide Managed SOC services within the stipulated time schedule. We agree to abide by the Bid and the rates quoted therein for the orders awarded by SBOSS up to the period prescribed in the Bid which shall remain binding upon us. Until a formal contract is prepared and executed, this Bid, together with your written acceptance thereof and your notification of award, shall constitute a binding Contract between us.

We undertake that, in competing for (and, if the award is made to us, in executing) the above contract, we will strictly observe the laws against fraud and corruption in force in India.

We have complied with all the terms and conditions of the RFP. We understand that you are not bound to accept the lowest or any Bid you may receive.

Dated this…… Day of 2024

(Signature)

(Name) (In the capacity of)

Duly authorized to sign Bid for and on behalf of

ANNEXURE L

Declaration for Acceptance of Scope of Work
(On Bidder's Letter Head)

To
State Bank Operation Support Services Pvt Ltd
New Delhi

Sir,

I have carefully gone through the scope of work (including the scope of work mentioned in responses to pre-bid queries/Corrigendum/Corrigenda) contained in the RFP ---------- dated ---------- for Managed SOC service provider. I declare that all the provisions of this RFP / Tender Document are acceptable to my company. I further certify that I am an authorized signatory of my company and am, therefore, competent to make this declaration.

Yours faithfully,

(Signature of the Bidder)
Printed Name
Designation
Seal
Date:
Business Address:

ANNEXURE M

Declaration for Acceptance of RFP Terms and Conditions
(On Bidder's Letter Head)

To
State Bank Operation Support Services Pvt Ltd
New Delhi

Dear Sir,

I have carefully gone through the terms & conditions contained in the RFP ----------dated ---------- for "Managed SOC Service partner. I declare that all the provisions of this RFP/Tender Document are acceptable to my company. I further certify that I am an authorized signatory of my company and am, therefore, competent to make this declaration.

Yours faithfully,

(Signature of the Bidder)
Printed Name
Designation
Seal
Date:
Business Address:

ANNEXURE – N

DETAILS OF KEY PERSONNE / CORE PROJECT TEAM

(On Bidder's Letter Head)

Bidder shall provide a detailed description of the proposed Core Project Team to be deployed for the project. The description should include details about the Project Team Hierarchy and a detailed explanation of the role to be played by each individual that would be part of the project. It is mandatory that Bidder to provide details of project handled, brief of the assignment, period for each of the resource proposed relevant to scope of the tender. Each resource deployed shall provide self- certificate indicating relevant experience of tender scope. Bidder shall have to ensure that background verification of each deployed person is done.

1) Proposed Position [only one candidate shall be nominated for each position Expert]:
2) Resource Name:
3) Nationality:
4) Date of Birth:
5) Educational Qualifications:
[Indicate college/university and other specialized education of staff member, giving names of institutions,
degrees obtained, and dates of obtainment]:
6) Certifications completed:
7) No. of years‟ of experience
8) Total No. of years with the firm

(Signature of the Bidder)
Printed Name
Designation
Seal
Date:
Business Address: