SBI SG Global Securities Private Limited invites bids for Comprehensive / End-to-End SOC Services

Sl. No.	Item	Timelines
1	RFP release date	10 March 2026
2	Last date for sending the queries on RFP	13 March 2026
3	Last date for submission of Technical and Commercial Proposals	16 March 2026 (Revised Timeline – 18-March-2026)
4	Date for opening of Technical and commercial Proposal	Will be announced

Revision History

Sr. No.	Summary of Change	Edited By	Approved By	Version No.	Effective Date
1	Changes Performed: 1. **SCHEDULE OF EVENTS & DETAILS** - Update in submission timeline 2. "Deployment Models and Service Delivery Methodology" section – **OEM Priority Update** (Change considering regulatory landscape)	CISO	CRO	1.0	16-03-2026

Table of Contents

Contents

1. Deployment Models and Service Delivery Methodology 5
2. Eligibility Criteria 7
3. Detailed Scope of Work: 9
4. High Level Deliverables 12
4.1 Technical Specifications: 14
5. Period of Contract 36
6. End of Support 36
7. Terms and Conditions 37
8. OPENING AND EVALUATION OF BIDS 47
8.1 Opening of Technical Bids by the Company 47
9. Instructions to Bidder(s): 49
10. Service Level Agreement 51
ANNEXURE - I: A. Details required from the Bidder. 55
B. Capabilities of the Services provided by the bidder: 57
Annexure II- Financial Details 58
Annexure III - Details of OEM 59
Annexure IV- Statement of Deviation 60
Annexure V- Proposed team profile 61
Annexure VI- Sample NDA 62
Annexure VII –Commercial Proposal 62
Annexure VIII- BID FORM 63
Annexure IX: Project Timelines 65

DISCLAIMER

The information contained in this Request for Proposal ("RFP") document or information provided subsequently to bidders or applicants whether verbally or in documentary form by or on behalf of SBI-SG Global Securities Services Pvt. Ltd, is provided to the bidder(s) on the terms and conditions set out in this RFP document and all other terms and conditions subject to which such information is provided. This RFP document is not an agreement and is not an offer or invitation by SBI-SG Global Securities Services Pvt. Ltd to any parties other than the applicants who are qualified to submit the bids (hereinafter individually and collectively referred to as "Bidder" or "Bidders" respectively). The purpose of this RFP is to provide the Bidders with information to assist the formulation of their proposals. This RFP does not claim to contain all the information each Bidder require. Each Bidder may conduct its own independent investigations and analysis and is free to check the accuracy, reliability and completeness of the information in this RFP. SBI-SG Global Securities Services Pvt. Ltd makes no representation or warranty and shall incur no liability under any law, statute, rules or regulations as to the accuracy, reliability or completeness of this RFP. The information contained in the RFP document is selective and is subject to updation, expansion, revision and amendment. It does not purport to contain all the information that a Bidder require. SBI-SG Global Securities Services Pvt. Ltd does not undertake to provide any Bidder with access to any additional information or to update the information in the RFP document or to correct any inaccuracies therein, which may become apparent.

SBI-SG Global Securities Services Pvt. Ltd (SBI-SG), reserves the right of discretion to change, modify, add to or alter any or all of the provisions of this RFP and/or the bidding process, without assigning any reasons whatsoever. Such change will be published on the Company's Website (https://www.sbisgcsl.co.in/) and it will become part and parcel of RFP.

SBI-SG Global Securities Services Pvt. Ltd in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFP. SBI-SG Global Securities Services Pvt. Ltd reserves the right to reject any or all the Request for Proposals received in response to this RFP document at any stage without assigning any reason whatsoever. The decision of SBI-SG Global Securities Services Pvt. Ltd shall be final, conclusive and binding on all the parties.

1. Deployment Models and Service Delivery Methodology

a) The Company want to engage new vendor for Comprehensive / End-to-End SOC Services in place of current vendor with the priority below:

- **Priority 1 - SENTINAL ONE EDR + Qylis (ESENTIRE) SIEM, SOAR, IDENTITY and CNAPP, only**
- **Priority 2 - SENTINAL ONE EDR, SIEM, SOAR, IDENTIFY and CNAPP, only**.
- **Priority 3 – ESENTIRE -EDR, SIEM, SOAR, IDENTIFY and CNAPP, only**.

Remote services shall be offered by the Bidder from their own Security Operations Centre (SOC).

b) Bidder to note that currently the Company operates in 2 locations Mumbai + GiftCity (IFSCA Branch) in a hybrid infrastructure environment with Data Centre hosted at Mumbai + DR Centre at Hyderabad and Oracle Cloud Mumbai & Hyderabad.

c) The vendor shall deliver the Security Monitoring Services by deploying a model in which the log collector is deployed at Company's premise and other components like log storage, correlation and monitoring happens at bidder's SOC. Log Storage and other components such as SIEM/ Rules and correlation engine, Advanced Detection, triggering and response platforms are at bidder's OEM. Bidder will have to provide a declaration that Company's log data are stored within India boundaries and under no circumstances shall leave country's jurisdiction.

d) The management of devices, platforms and 24x7 monitoring, incident analysis etc. shall be performed from vendor's SOC.

e) The log retention period on the cloud should be 365 days as hot storage + locally stored as required by applicable Indian Regulations.

f) Bidder to consider DR requirements in the proposed design since the monitoring service is required for devices installed at Company's DR site as well.

g) Bidders should clearly mention the type of technologies to be used for creating the SOC setup for the Company such as SIEM, EDR, SOAR and other related technologies/modules.

h) Any interfaces/custom connectors required for integration be developed by the bidder for successful implementation of the SOC should be at no extra cost to the Company.

i) Vendor to provide in-person support to the Company's team during POC & integration of the in-scope devices and identification of correct log baselines and configuration changes required for effective correlation and monitoring with no additional cost.

j) Selected Bidder should design and implement security orchestration model and define the workflow automation so that security devices/applications are integrated and manual intervention is minimal in detecting and blocking threats. All the use cases to be validated prior to implementation.

k) Overall scope to ensure full coverage of 24*7*365 log monitoring aspects of various security solutions, devices, software, applications like Routers, Firewalls, Application Servers, Authentication Servers, Web Servers, Database Servers, DNS Servers, IDS, IPS Servers, Antivirus Server, Windows Server, *NIX Server, Proxy Server, DLP, DAM, VPN, DMARC Analytics, NAC, WAF, etc. and critical network security devices at the Data Centres and DR Site identified by the Company. Scope involves on-boarding of such devices to the monitoring platform, transition to new devices, at no additional cost to the Company.

l) Development and implementation of processes for management and operation of the SOC including (but not limited to) the following processes:

i. Configuration and Change Management
ii. Incident triaging and Escalation management processes
iii. Daily standard operating procedures
iv. Training procedures and material
v. Reporting metrics and continuous improvement procedures
vi. Data retention and disposal procedures
vii. BCP and DR plan and procedures for SOC
viii. Business continuity
ix. Threat Intelligence Management & Integration
x. Threat Hunting & Proactive Detection
xi. Vulnerability & Patch Management (SOC assets)
xii. Access Management & Privileged Access (SOC team)
xiii. Knowledge Management & Documentation
xiv. Audit, Compliance & Regulatory Reporting
xv. Vendor/Third-Party Risk Management (if applicable)

m) The bidder shall be responsible for defining a DR/ BCP plan for the SOC operations and ensures that periodic tests are conducted as per the testing

calendar agreed or as per regulation with the Company to ensure that all deliverables /SLAs are met in case the SOC operations are switched to alternate site (DR-SOC). The Data centre as well as DR site should mandatorily be located in India.

n) Bidder should provide elaborate utilization details that may affect the day-to-day normal functionality of existing IT infrastructure.

o) Provide on-demand support for forensic services in case of any incident.

p) Design, implementation of detailed threat modelling, use cases and improving the same on continuous basis.

q) Provide proactive threat intelligence and threat hunting services across networks end-points and anomalous user behaviour to detect advanced attacks like lateral movement, malware beaconing, data exfiltration, watering hole, process anomalies, services anomalies, account takeovers, etc.

r) Bidder needs to ensure that SIEM solution can integrate with the IT and Security Solutions using standard methods/ protocols/ message formats without affecting the existing functionality of SBI-SG.

2. Eligibility Criteria

Bidders meeting the following criteria are eligible to submit their Bids along with supporting documents. If the Bid is not accompanied by all the required documents supporting eligibility criteria, the same would be rejected.

Sl. No.	Qualification Criteria	Marks	Compliance (Y/N)	Supporting Documents to be Provided
1	Bidder must be a Limited Company registered under the Companies Act and in existence for at least 3 years as on RFP date.	3	Y/N	Certificate of Incorporation
2	Average annual turnover of at least ₹10 Crore specifically from cybersecurity / SOC / managed security services in last 3 financial years, with positive net worth in all 3 years.	12	Y/N	Audited balance sheets + CA certificate (with UDIN) highlighting cybersecurity turnover, overall turnover, and net worth
3	OEM solution must be recognized in Gartner / Forrester for broad-based EDR, SIEM & SOAR capabilities (in the last 3 years)	8	Y/N	Copy of relevant Gartner / Forrester report excerpts or recognition proof
4	Bidder / OEM must operate its own / captive New Generation SOC setup in India for log	12	Y/N	Undertaking by Authorized Signatory with SOC

Sl. No.	Qualification Criteria	Marks	Compliance (Y/N)	Supporting Documents to be Provided
	monitoring, correlation, analysis, and incident management.			location + Work Orders confirming activity
5	The proposed SOC solution/services must ensure full data residency in India — all processing, storage, analytics, and threat intelligence of client logs, PII, and security-relevant data must occur within India boundaries. No unauthorized cross-border transfer of raw client data / PII is permitted. Global threat intelligence may be integrated securely without exporting sensitive logs or PII. The solution must fully comply with: • MeitY / CERT-In guidelines • SEBI Cybersecurity and Cyber Resilience Framework (CSCRF) • Digital Personal Data Protection Act 2023 and Rules • RBI outsourcing norms (applicable to BFSI entities) • NCIIPC directives (if critical infrastructure)	10	Y/N	- Undertaking / self-declaration by the authorized signatory confirming full India-based operations, no unauthorized cross-border transfer of logs/PII, and adherence to all listed regulations. - High-level architecture diagram illustrating the deployment model (e.g., on-prem log collectors at client premises, secure forwarding to India-based processing/storage, local retention, and no export of raw sensitive data).
6	SOC / EDR / SIEM processes must hold ISO 27001 and/or SOC 2 Type II certification and OEM AppSec Reports	10	Y/N	Copies of valid certificates + Latest VAPT Summary report
7	Bidder must have provided Managed SOC Services (SIEM/EDR/SOAR) to at least 5 clients in India in the last 3 years. + OEM must provide (SIEM/EDR/SOAR) services in India with at least 8 and out of which 5 SEBI Regulated Clients	10	Y/N	Bidder and OEM share separate Purchase Orders / Invoices
8	Experience managing SOC/SIEM/EDR/SOAR at scale of at least 10,000–50,000 EPS (or equivalent) in at least one project in India (preferably BFSI / Govt / PSU) in last 3–5 years.	10	Y/N	Work Orders / Client letters stating EPS/scale + completion / ongoing certificate
9	Bidder must have at least 20–50 permanent cybersecurity professionals with relevant certifications (CISSP, CISM, GIAC, CEH, GCIH, OSCP, etc.) dedicated to SOC operations.	10	Y/N	HR certificate / undertaking + sample certification copies of key personnel
10	Bidder must not be blacklisted / debarred by RBI, CERT-In, MeitY, NCIIPC, SEBI or any Government / PSU / Regulatory Authority, nor involved in major cybersecurity / data breach litigations.	5	Y/N	Self-declaration / affidavit by Authorized Signatory covering listed regulators
11	The Managed SOC **Service**s Provider must not Sub-contract SOC **Services** to a 4th Party. **(Mandatory Condition)**	n/a	Y/N	Self-declaration / affidavit by Authorized Signatory

3. Detailed Scope of Work:

The minimum specified scope of work to be undertaken by the bidder shall be for PROVIDING MANAGED SECURITY SERVICES TO RUN SECURITY OPERATION CENTRE (SOC) SERVICES WITH MANAGED, EXTENDED DETECTION AND RESPONSE (Managed EDR + SIEM + SOAR + CNAPP) CAPABILITIES DESCRIBED UNDER SCHEDULE OF REQUIREMENTS (READ WITH DEPLOYMENT MODELS AND SERVICE DELIVERY METHODOLOGY, OF THIS RFP DOCUMENT).

(Scope of Work is aligned with the Deployment Models and Service Delivery Methodology)

The project scope in terms of the indicative number of services /devices is as follows-:

- For inventory please write to ciso@sbisgcsl.co.in

*10% variance per year be considered on total number of units and additional devices shall be charged per unit at existing unit rate only.

1. All logs should be forwarded through relay server and direct internet connection shall be allowed. SOC/EDR agent should be auto upgraded through console wherever applicable.
2. The broader Scope of work shall include but not be limited to High Level Deliverables or Technical Specifications mentioned under Section 4. The bidders are required to go through the complete RFP document thoroughly. The obligation /responsibilities mentioned elsewhere in the document, if any, shall be an integral part of the scope.
3. Bidder should monitor logs to detect malicious or abnormal events and raise the alerts for any suspicious events that may lead to security incidents in SBI-SG environment.
4. Monitoring should be done on 24/7/365 basis.
5. Bidder platform should have capability to collect logs from most of the standard platforms like Windows, Linux, Firewall, Network, API gateway, Load balancer and other security devices or solution, etc.
6. Bidder should develop, update and maintain log baselines for all security related platforms at SBI-SG that are required to be monitored.
7. Bidder should be able to monitor and analyze both internal and external attacks. In addition to security attacks on IT infrastructure, Bidder should also monitor for security events on business applications, databases and also identify network behaviour anomalies including zero-day attacks.
8. Bidder should monitor, detect and coordinate with respective stake holders for all the security incidents.

9. Bidder should send alert with details of mitigation steps to designated personnel within SBI-SG.
10. Bidder should maintain a knowledge base of alerts, incidents and mitigation steps and this knowledge base should be updated with evolving security events within and outside of SBI-SG.
11. Bidder Team should send customized alerts, advisories about the latest CVEs and latest threats getting exploited in the cyber world, to SBI-SG. Bidder should also provide the latest threat advisories to SBI-SG on daily basis and auto-sweeping in SBI-SG environment
12. Evidence for any security incident should be maintained in tamper proof manner and should be made available for legal and regulatory purpose, as required.
13. Bidder should add/delete/modify rules, reports and dashboards etc. on SIEM based on SBI-SG requirements and changing security threat landscape. The solution should support wizard- based interface for rule creation.
14. Bidder should provide MIS reports to SBI-SG on daily, weekly and monthly basis. Quarterly report for executive management review. Reporting requirements will be finalized with the selected criteria. Bidder should also have the provision to provide reports on demand whenever required by SBI-SG.
15. All deliverables including reports should undergo quality assurance process and should have continuous improvements in the metrics displayed. Bidder team should define quality metrics, measurement frequency and reporting periodicity in consultation with SBI-SG.
16. Bidder has to create and maintain RCAs for high and critical incidents. RCAs has to be made available to the auditor whenever needed.
17. On quarterly basis, Bidder should conduct CTF (Capture The Flag) events within the team to enhance the knowledge levels of support team and SBI-SG resources.
18. Bidder should participate and contribute in cyber security drills, CTF (Capture The Flag) events of SBI-SG.
19. Bidder should perform quarterly SIEM rules and dashboards review and optimize the solution in consultation with SBI-SG.
20. Bidder shall monitor, detect, prevent and appropriately respond against any known and un-known security threats, outliers, bot identification etc.
21. Bidder shall Transfer the knowledge to the SBI-SG employees about day to day operations, system/backend level troubleshooting, dashboard, creation of basic and advanced rules & analytical models, creation and customization of reports & queries etc without any additional cost to the Company.
22. Bidder shall support digital forensic investigation on need basis with complete replay of attack including the ingress and egress of payload without any additional cost. Provide complete insight into threat vector and impact analysis with detailed RCA.
23. Bidder has to reduce the false positives on the security incidents/events. False positive rate of the incidents has to be less than 4%.

24. Bidder should create the trends on reoccurring incidents and has to provide the remedial actions/suggestions on the same to SBI-SG IT Team.
25. Bidder shall be responsible to develop and maintain Standard Operating Procedures (SOP) and Create / Update & maintain all playbooks with respect to proposed solution day to day operations including but not limited to threat management, alert/incident management, reports & dashboards, forensics infrastructure maintenance, rules creation & fine tuning, install/upgrades, updates, asset Integration, Business Continuity data & configuration backup, restoration, archival, knowledge management, segregation of duties, change management, patch & version management. Bidder should ensure to update the proposed solution with the latest stable version within 2 months of its release.
26. All SOPs have to be reviewed on quarterly basis.

27. The Bidder shall ensure full compliance with the RBI Cyber Security Framework, Master Direction on IT Outsourcing (including managed SOC/SIEM/MXDR controls), applicable NHB guidelines, SEBI Cybersecurity and Cyber Resilience Framework (CSCRF) as enforced/clarified (including ongoing consultations on data localization), and all relevant preceding, existing, and future RBI/NHB/SEBI circulars, notifications, and guidelines related to EDR, SIEM, SOAR, CNAPP managed SOC services, cybersecurity operations, and data protection — along with all functional and non-functional requirements specified by SBI-SG in this RFP

Schedule of Requirements

Through this Request for Proposal (RFP), the Company wants to identify competent Vendors for designing and implementing the cost effective and comprehensive IT security log monitoring service as per the below criteria:

Functional Principles: The intent for implementing a SOC at the Company is covered in the below functional principles:

- **Detection of Information Security Threat and Prevention of Impact/ Breach:** The SOC should be able to identify information security threats/ vectors targeting Company's environment and prevent impact or breach due to them through implementation of adequate security mechanisms.

- **Incident Management:** Reporting and logging of information security incidents through the use of appropriate ticketing tools. Track and monitor the closure of these information security incidents and Escalation of these incidents to appropriate teams/ individuals in the Company.

- **Continuous Improvement:** Continuously improve SOC operations.

The Company is envisaging a Managed Security Services model under which the prospective vendor shall provide 24x7x365 monitoring from vendor's SOC. The scope would involve monitoring of core infrastructure and security components at Company's Managed Data Centre, Mumbai and the Disaster Recovery Centre, Hyderabad + OCI Cloud Primary in Mumbai + DR in Hyderabad.

The bidder is required to integrate the core Routers, Firewalls, Application Servers, Authentication Servers, Web Servers, Database Servers, DNS Servers, IDS, IPS Servers, Antivirus Server, Windows Server, *NIX Server, Proxy Server etc. with the proposed SIEM solution. Logs received from all these devices have to be correlated, analyzed for detection of threats, unusual user behaviour and proactive incident analysis in real time manner.

Company is looking for a Security Service Player which shall provide a "second layer of eyes approach" on the existing internal Security Controls and Monitoring services and help in augmenting the existing internal capabilities by having advanced SOC capabilities focused on detection of advanced threats apart from the traditional rule based SIEM capabilities which can help Company to have a proactive approach in determining the known and unknown threats faced by the Company to reduce the risk of breach of data and systems, the advanced features/capabilities expected out of the vendor apart from rule based monitoring such as employing off the shelf SIEM solutions are as follows:

a) Security Analytics, Monitoring and Feeds services
b) Incident Analysis and Response
c) Detect Unknown attacks, blind spots and deep detection.
d) Augmentation of rule-based detection systems with new approaches such as machine learning and Artificial Intelligence to detect patterns, abnormalities.

4. High Level Deliverables

Areas	Activities	Deliverables
Security Monitoring	Log Monitoring; Server Monitoring; Security and Network Device monitoring	• 24*7*365 log monitoring • Detection of threats from integrated log sources and based on the use cases defined. • Event Analysis • Alerts as per defined escalation matrix

Areas	Activities	Deliverables
Incident Management	Incident Analysis, Identification of all components of the incident, root cause analysis and mitigation plans	• Provide logs and incident report for any identified security incident. • Coordinate with Company's Team and help to contain attack/incident. • Provide evidences for legal and regulatory purpose, within timelines defined by Cert-In for reporting purpose.
SOC Maturity Improvement		• Quarterly briefings on Analysis and insights from data: trends, high risks areas, roadmap for strategic improvements, security posture benchmarking. Briefings on global threat trends, regulatory trends and cyber technology trends.
Report Management	Periodic reports; Trend analysis; Customized reports	• Review multiple reports including top attackers, attacks, attack targets, trends. • Monthly MIS reports for monitored devices. • Recommendation for improvement of security posture and threat landscape.
Monthly Review	Conducting monthly review covering SLA, Status of operations, Integration status and reports.	• Recommendations basis the trends observed in the monthly report • Any new threats observed and actions need to be taken.
Global Intelligence Feeds	Continuous and regular global feeds from external known agencies.	• Threat and Vulnerability customised advisories with auto sweeping in our environment for any such detection. • Threat and Vulnerability customised advisories in form of E-mails. • Recommendations for security improvements. • Provide Historical, Operational, Analytical and predictive Analysis.

4.1 Technical Specifications:

S. No	Requirement	Comply (Full / Partial / No) and Reply/Comments
1	**Threat Intelligence and Analytic**	
1.1	The Service Provider shall maintain a Threat Intelligence and Analytics platform capable of detecting threats and integrating seamlessly with the SIEM solution.	
1.2	Service Provider shall anticipate likely threats from both external global intelligence sources and the Company's internal infrastructure.	
1.3	Service Provider 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 and false positives in threat intelligence feeds.	
1.4	Service Provider should apply threat intelligence received from different sources against the data received from different assets, network traffic, security events and users to determine likelihood of threats and impact and suggest preventive measures.	
1.5	Service provider should track status of assets against IoCs, Common Vulnerabilities and Exposures (CVEs) and support automated workflow for remediation.	
1.6	An up-to-date asset inventory mechanism shall be maintained and used to map threat intelligence and vulnerability data to applicable assets for proactive threat anticipation.	
2	**Artificial Intelligence & Machine Learning**	
2.1	Solution should have capabilities to detect any compromises by correlating alerts collected together over a period of time.	

S. No	Requirement	Comply (Full / Partial / No) and Reply/Comments
2.2	Solution should have capabilities to correlate alerts between sources and destination IPs to find similar or colluding threat signals / behaviours.	
2.3	Solution shall maintain a knowledge base of attacker tactics from global past breaches to build detection models (aligned with MITRE ATT&CK where applicable).	
2.4	Solution should use data science techniques to identify attack kill chains, including lateral movement (e.g., destination IP of one alert becoming source IP of another).	
2.5	Solution should have detection models to find out threats sources are linked to the same attacker by grouping alerts with common characteristics like time, day location, target asset profiles etc.	
3	**Rule Based Detection (Traditional SIEM Capabilities)**	
3.1	In addition to the advanced analytics capabilities like MDR, solution should have capabilities to define rules on event logs captured from various sources to detect suspicious activities Examples • Failed login attempts • Login attempts from suspicious locations • Authorization attempts outside of approved list • Vendor logins from unauthorized subnets • Vertical and Horizontal port scans • Traffic from blacklisted IPs • Login attempts at unusual timings • Change in behaviour pattern	
3.2	Rules shall support low-code/no-code creation, performance monitoring, suppression, and tuning to minimize false positives.	
4	**Incident Analysis**	

S. No	Requirement	Comply (Full / Partial / No) and Reply/Comments
4.1	Solution should support auto-triaging of alerts from a number of security products including Firewalls, PIM, DLP, IPS, WAF, Anti-APT, HIPS, AV etc.	
4.2	Solution should apply advanced techniques (including machine learning) considering context, historical behavior, and external threat intelligence to assign real-time criticality/risk scores to alerts (aligned to MITRE ATT&CK severity + asset criticality + business impact).	
5	**Incident Response**	
5.1	The Service Provider should provide automated incident analysis features/service for analysis of alerts received to answer the following: Impact on the assets. Attributes of an attacker. Determine other assets which may have been compromised. Determine how long the attack campaign was and where was first compromise. Preservation of artefacts and IOCs of an incident.	
5.2	Bidder to describe how it has a strong Incident Response Mechanism in providing Company a comprehensive information about a potential incident, assemble the appropriate context, investigate as make recommendations so that Company starts containment and remediation activities.	
5.3	Vendor to help Company's team in performing the post incident analysis and RCAs which shall help in improvising the Incident Management process and learning.	

S. No	Requirement	Comply (Full / Partial / No) and Reply/Comments
5.4	The Vendor should maintain an Incident Management Plan with at least the following-: Incident Management Plan and Governance. Incident Response plan and Governance Workflows for Incident Management and Response Communications and escalations Plan, Process and Metrics Incident Management and Response Case Management	
6	**Other requirements**	
6.1	The solution shall support event collection via industry-standard protocols and methods, including: Syslog (UDP/TCP), Syslog-NG, SDEE, SNMP v2/v3, ODBC, JDBC, FTP, SFTP, SCP, HTTP, HTTPS, WMI, OPSEC, NetFlow, Windows Event Logging, text/CSV/XML files.	
6.2	The proposed solution should be able to collect data from new devices added into the environment, without any disruption to the ongoing data collection.	
6.3	The proposed solution should have connectors to support listed devices/ applications, wherever required the vendor should develop customized connectors.	
6.4	All logs transferred to the SOC shall be authenticated (timestamped across time zones), encrypted in transit (strong encryption), and compressed (minimum 70–80% compression for optimization).	
6.5	Log collectors shall support load balancing across multiple instances and store both raw and normalized data for forensics.	

S. No	Requirement	Comply (Full / Partial / No) and Reply/Comments
6.6	The proposed solution should support log collection from all major operating systems and their versions but not limited to Windows, Linux, AIX, Solaris etc.	
6.7	The collectors should be able to store/retain both normalized and raw data for forensic purposes	
6.8	In case of the connectivity issues, the data collector should be able to store the data for a period of 4 hours at its own repository. The retention, deletion, synchronization with SIEM database should be automatic but it should be possible to control the same manually.	
6.9	The proposed solution should ensure that the overall load on the network bandwidth at DC, WAN level is minimal	
6.10	The proposed solution should have the capability to compress the logs by at least 70 % for storage optimization.	
6.11	The proposed solution should have capabilities to store the event data in its original format in the central log storage	
6.12	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.	
6.13	The proposed solution should support the following log collection protocols: Syslogover UDP / TCP, Syslog NG, SDEE, SNMP Version 2 and 3, ODBC, FTP, Windows Event Logging Protocol, Opsec, Netflow at a minimum.	
6.14	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.	

S. No	Requirement	Comply (Full / Partial / No) and Reply/Comments
6.15	The proposed solution should be able to perform the following correlations (but not limited to): Rule based, Vulnerability based, Statistical based, Historical based, Heuristics based, Behavioural based etc. across potentially disparate devices	
6.16	The dashboard provided to Company should be in the form of a unified portal that can show correlated alerts/ events from multiple disparate sources such as security devices, network devices, enterprise management systems, servers, applications, databases, etc.	
6.17	Events should be presented in a manner that is independent of device specific syntax and easy to understand for all users	
6.18	Any failures of the event collection infrastructure must be detected and operations personnel must be notified as per SLA.	
6.19	The proposed system should display all real time events. The proposed solution should have drill down functionality to view individual events from the dashboard.	
6.20	Dashboard should support reporting for consolidated relevant compliance across all major standards and regulatory requirements. This includes Cert-In, ISO 27001, SEBI regulations, RBI Regulations, GDPR Regulations, IT ACT, PCI DSS standards etc.	
6.21	The proposed solution should support creation of automated incident management workflows to track incident from creation to closure, provide reports on pending incidents. It should also permit upload of related evidences such as screenshots etc.	

S. No	Requirement	Comply (Full / Partial / No) and Reply/Comments
6.22	The proposed solution should support creation of automated Incident management workflows to track incident from creation to closure, provide reports on pending incidents. It should also permit upload of related evidences such as screenshots etc.	
6.23	Vendor to ensure logs are transmitted using strong encryption and no PII data is moved out of Company's Environment.	
6.24	The devices /log sources to be monitored shall be from Company's DC as well as DR. The solution should be able to collect logs from both DC-DR locations and the architecture proposed should clearly consider this requirement.	
6.25	The proposed solution should have high availability feature built in. There should be an automated switch over to secondary collector in case of failure on the primary collector. No performance degradation is permissible even in case of collector failure.	
6.26	Bidder's SOC should comply with relevant requirements specified for SOC in SEBI circulars: SEBI/HO/ITD-1/ITD_CSC_EXT/P/CIR/2025/119 dated August 28, 2025 — "Technical Clarifications to Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI Regulated Entities (REs)". SEBI/HO/ITD-1/ITD_CSC_EXT/P/CIR/2024/113 (August 20, 2024)	
7	**User and Entity Behavioural Analytics**	
7.1	The service should collect data through an endpoint agent and networking devices like SIEM, FW, Proxy, AD etc. That is capable of monitoring and collecting metadata for various types of behaviour. At a minimum, behaviour monitored should include:	

S. No	Requirement	Comply (Full / Partial / No) and Reply/Comments
	application usage, clipboard activity, email activity, file activity, log on and log off events, printer activity, process activity, web browsing, and desktop video capture, networking activity, etc.	
7.2	User and Entity Behaviour Analytics (UEBA) should use advanced algorithms (powered by machine learning) to baseline the activity of entities (e.g., users, devices, servers, applications, etc.) and calculate risk based on deviations From those baselines in order to identify security anomalies. These anomalies can be aligned to adversary behaviours such as lateral movement and malware command and control	
7.3	Bidder should configure following UEBA use cases but not limited to: • Account Compromise, Hijacking and Sharing • Privileged Access Abuse • Insider Threat Detection and Deterrence • Self-Audit and ID Theft Detection • Cyber Fraud Detection and Deterrence • Trusted Host and Entity Compromise • Stateful Session Tracking • Anomalous Behaviour and Watch Lists • SIEM and Risk Intelligence • Account lockout • Account creation • Account sharing • Service account classification • Dormant user accounts • Breach Forensic review • And support SBI-SG in identifying more use cases	
7.4	The service should be able to capture displayed text from any open application	

S. No	Requirement	Comply (Full / Partial / No) and Reply/Comments
	Policies shall allow selective deployment, filtering, keyword/pattern matching, exceptions, email notifications, and SIEM forwarding on violations.	
7.5	Should collect data from structured and unstructured data sources like voice, communication etc. for detecting anomalous behaviour	
7.6	Should collect data from structured and unstructured data sources like voice, communication etc. for detecting anomalous behaviour	
7.7	The service should be capable of capturing information about any processes started or stopped	
7.8	The service should be capable of capturing the rendered HTML from any websites visited.	
7.9	The service should provide a user interface for creating policies that can be selectively deployed to groups of endpoints or users. These policies should govern which data is collected and under what circumstances it is collected.	
7.10	Policies should allow for filtering and pre-filtering of data to determine the appropriate action. This includes searching any collected data for specific keywords or patterns matching regular expressions	
7.11	Policies should be able to define scenarios where data will not be collected despite the rules of other policies.	
7.12	The service should allow for policies to trigger an email notification.	
7.13	The service should allow for information to be automatically sent to a SIEM when certain policies are violated	

S. No	Requirement	Comply (Full / Partial / No) and Reply/Comments
7.14	The service should allow for searching and filtering of all collected data. If files or video have been collected, those items should also be made available for review	
7.15	The service should allow for various pieces of collected information to be grouped together into a case.	
8.	**Threat Hunting Requirements**	
8.1	Solution should have pre-built AI models to detect targeted attacks (unknown attacks from unknown threat actors). 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	
8.3	Solution should have analytical models to detect different stages of Cyber Kill chain.	
8.4	Solution should support all categories of hunting including Network Threat Hunting, User Behaviour Anomaly Hunting, Endpoint Threat Hunting.	
8.5	Network Threat Hunting should leverage existing network sources for better detection of advanced attacks. Network sources should include Net flow, Proxy, dynamic DNS, IPS, VPN, Firewall, AD/Windows, Email logs, target attacks	
8.6	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	
8.7	Solution should provide UBA dashboard based on various UBA models outcome.	

S. No	Requirement	Comply (Full / Partial / No) and Reply/Comments
	UBA Dashboard should highlight risky users based on objective scoring of users based on composite risk score comprising all behaviour anomalies of the user Organization should be able to define risk thresholds based on their risk appetite	
8.8	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.)	
8.9	Solution should support applying AI models on WAF events to detect targeted web application attacks.	
8.10	The tool should detect malware and botnets.	
8.11	The solution should detect activities related to Advanced Persistent Threats (APT) and Trojans using additional APT solution in future.	
8.12	The tool should be able to perform Network Traffic Pattern Analysis based on IP addresses, groups of.	
8.13	IP addresses, source/destination IP pairs and Bandwidth Analysis etc.	
8.14	The tool should be able to perform Real time monitoring of host behaviors and traffic analysis to identify threats.	
8.15	The tool should detect common events like DDoS / DoS, Scanning, Worms, Unexpected application services (e.g., tunnelled protocols, backdoors, use of forbidden application Protocols), Policy violations, etc.	
8.16	The tool should be able to identify from where the attack originated.	
8.17	The events generated by the system should be classified at various risk level like High, Medium, Low etc	

S. No	Requirement	Comply (Full / Partial / No) and Reply/Comments
8.18	Should be able to get regular feed from global threat intelligence for proactive monitoring and alerting.	
9	**Detection & Response (EDR + SIEM)**	
9.1	The solution should provide consolidated detection, investigation, and response capabilities across Endpoints. The solution should provide more context with mapping to the MITRE ATT&CK TTPs for faster detection and higher fidelity alerts.	
9.2	The solution should provide unified platform that enables security teams to view the entire chain of events across endpoints and Servers. The solution should provide unified platform that enables security teams to run a root cause analysis, investigate the execution profile of an attack, and identify the scope of impact across assets.	
9.3	The solution must be capable to map and corelate all assets within the environment such as endpoint, servers, O365, cloud etc. The solution should collect and correlate EDR activity data for one or more vectors—endpoints, servers.	
9.4	The solution should have Detection Models combining multiple rules, and filters using techniques such as machine learning and data stacking. The detection model may use one or more filters to detect suspicious behaviours or events based on associated MITRE techniques.	
9.5	The Solution should assign a score to the alert and should calculate the score based on the severity of the matched detection model and the impact scope of the incident (such as number of users, number of endpoints, servers, O365 email accounts, etc.).	

S. No	Requirement	Comply (Full / Partial / No) and Reply/Comments
9.6	The solution must be capable to integrate with SIEM Solution up to the level where SOC analyst is able to receive alerts on the incident/events.	
9.7	The solution should integrate up-to-the-minute intelligence reports from internal and external sources to help identify potential threats to our environment. The Solution should be able to manage the Suspicious Object List and Exception List to control the specific information for synchronization.	
9.8	The Solution should offer contextually aware response options for rapid action like Isolate devices, delete emails, terminate processes, and more from a single platform. The solution should be able to terminate an active malicious process on a target endpoint or on all affected endpoints.	
9.9	The solution should detect events matching with behaviours mapped into the MITRE ATT&CK framework. The solution should list the events that are mapped into the MITRE ATT&CK framework, the Administrator/Analyst can use these events as starting point to do further investigations.	
10	**CNAPP**	
10.1	The proposed solution shall provide a comprehensive Cloud-Native Application Protection Platform (CNAPP) that integrates CSPM, CWPP, CIEM, KSPM, DSPM, CDR, IaC scanning, vulnerability management, and attack path analysis into a unified platform for securing cloud-native applications, workloads, and infrastructure across build, deploy, and runtime phases in multicloud and hybrid environments.	
10.2	The solution should deliver unified visibility and centralized dashboards showing all cloud resources, workloads, identities, data stores, containers, serverless functions, and hybrid	

S. No	Requirement	Comply (Full / Partial / No) and Reply/Comments
	assets across OCI, VM, Kubernetes clusters, and on-premises environments.	
10.3	The solution should continuously discover and assess misconfigurations in cloud infrastructure (such as public storage buckets, overly permissive IAM roles, open security groups, unencrypted volumes) with contextual risk scoring based on exposure, exploitability, and business impact.	
10.4	The solution should scan Infrastructure as Code (IaC) files including Terraform, CloudFormation, Kubernetes manifests, identify insecure configurations, and support automated blocking or flagging of risky deployments.	
10.5	The solution should perform vulnerability scanning of container images, virtual machine images, software dependencies (via SBOM), and code artifacts to detect CVEs, malware, embedded secrets, and outdated libraries, with prioritization based on runtime context and exploit paths.	
10.6	The solution should audit and harden Kubernetes clusters by checking RBAC, pod security policies, network policies, and admission controllers, and detect runtime drift or anomalous container behaviour such as privilege escalation or cryptojacking.	
10.7	The solution should monitor runtime workloads (VMs, containers, serverless functions) for anomalous processes, file modifications, network command-and-control activity, ransomware behaviour, and zero-day or fileless attacks, with automated containment options such as quarantine or process termination.	
10.8	The solution should discover over-privileged IAM roles, unused permissions, toxic permission combinations, and identity drift, and provide	

S. No	Requirement	Comply (Full / Partial / No) and Reply/Comments
	recommendations or automated remediation for enforcing least-privilege access.	
10.9	The solution should correlate configuration, identity, workload, and network signals to detect active threats, visualize multi-stage attack paths, and map events to MITRE ATT&CK techniques for contextual alert enrichment.	
10.10	The solution should discover and classify sensitive data (PII, PHI, credentials) stored in cloud object storage, identify shadow data or exposure risks, and detect potential data exfiltration patterns.	
10.11	The solution should support agentless scanning methods wherever feasible to minimize performance impact and operational overhead, while allowing optional agent-based enhancements for deeper runtime visibility when required.	
10.12	The solution should provide automated remediation recommendations, policy-as-code enforcement in DevOps workflows, and integration with existing SIEM/SOAR systems for alert forwarding and orchestrated response.	
10.13	The solution should deliver consolidated compliance reporting and evidence aligned to ISO 27001, PCI DSS, RBI CSF, SEBI CSCRF 2025, DPDP Act 2023, and other relevant regulatory standards, with mapping to specific controls and continuous auditing support.	
12	**Identity Security**	
11.1	The proposed solution shall provide comprehensive identity security capabilities, including Identity Threat Detection and Response (ITDR), and continuous monitoring of identity risks across on-premises, cloud, SaaS applications, and hybrid environments.	

S. No	Requirement	Comply (Full / Partial / No) and Reply/Comments
11.2	The solution should automatically discover and inventory all human and non-human identities (service accounts, machine identities, API keys, OAuth tokens, workloads), detect shadow/rogue accounts, stale identities, and maintain an up-to-date identity asset register across all connected directories and systems.	
11.3	The solution should analyze identity permissions and entitlements to identify over-privileged accounts, unused permissions, toxic combinations (e.g., admin rights combined with sensitive resource access), and excessive privilege sprawl across cloud and on-premises environments.	
11.4	The solution should enforce least-privilege access by supporting just-in-time (JIT) access, just-enough-access (JEA), time-bound elevations, dynamic authorization, and automated policy tightening for privileged and high-risk identities.	
11.5	The solution should monitor and detect anomalous identity behaviors in real time, including impossible travel logins, unusual sign-in locations/times/devices, mass password resets, abnormal privilege escalations, account takeovers, and lateral movement via identity abuse.	
11.6	The solution should correlate identity events with endpoint, network, cloud workload, and application logs to detect identity-based attack paths (e.g., credential dumping → privilege escalation → persistence), and map them to MITRE ATT&CK techniques (TA0006, TA0008, etc.).	
11.7	The solution should provide automated response actions for high-risk identity incidents, such as temporary account suspension, session termination, MFA enforcement, password reset	

S. No	Requirement	Comply (Full / Partial / No) and Reply/Comments
	forcing, or access revocation, with integration to existing SOAR/SIEM for orchestrated playbooks.	
11.8	The solution should support privileged session monitoring, recording, and auditing for admin, root, service, and break-glass accounts, including command logging, keystroke capture (where compliant), and playback for forensic review.	
11.9	The solution should enable continuous access reviews and certification campaigns for high-risk entitlements, with automated workflows for approval/revocation and evidence collection to support compliance with RBI regulations, SEBI CSCRF 2025, DPDP Act 2023, and ISO 27001 Annex A.5.	
11.10	The solution should detect and prevent common identity attacks such as password spraying, brute force, credential stuffing, Golden SAML, Kerberoasting, Pass-the-Hash/Ticket, and token theft, using behavioral analytics and threat intelligence feeds.	
11.11	The solution should integrate with existing directory services (Active Directory, LDAP, Entra ID, Okta, etc.) and MFA providers to enforce strong authentication controls, risk-based adaptive authentication, and phishing-resistant methods (FIDO2/WebAuthn, certificate-based).	
11.12	The solution should provide centralized dashboards with identity risk scoring, top risky identities/users, entitlement heatmaps, anomalous activity timelines, and consolidated compliance reporting for identity-related controls.	
12	**Other Requirements**	
12.1	The proposed solution should support collection of events through customization of connectors or similar integration for the assets that are not	

S. No	Requirement	Comply (Full / Partial / No) and Reply/Comments
	natively supported. Solution should adhere to industry standards for event collection: syslog, OPSEC, WMI, SDEE, ODBC, JDBC, FTP, SFTP, SCP, HTTP(S), text file, CSV, XML file etc.	
12.2	The proposed solution should have connectors to support listed devices/ applications, wherever required the Bidder should develop customized connectors.	
12.3	All logs transferred to bidder's SOC should be Authenticated (timestamped across multiple time zones) encrypted and compressed before transmission.	
12.4	The proposed solution provides options to load balance incoming logs to multiple collector instances.	
12.5	The collectors should be able to store/retain both normalized & raw data for forensic purposes.	
12.6	In case of the connectivity issues, the data collector should be able to store the data for a period of 4 hours at its own repository. The retention, deletion, synchronization with SIEM database should be automatic but it should be possible to control the same manually.	
12.7	The proposed solution should ensure that the overall load on the network bandwidth at DC, WAN level is minimal.	
12.8	The proposed solution should have the capability to compress the logs by at least 85 % for storage optimization.	
12.9	The proposed solution should have capabilities to store the event data in its original format in the central log storage.	
12.10	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.	

S. No	Requirement	Comply (Full / Partial / No) and Reply/Comments
12.11	The proposed solution should support the following log collection protocols: Syslogover UDP / TCP, Syslog NG, SDEE, SNMP Version 2 & 3, ODBC, FTP, Windows Event Logging Protocol, Opsec, Netflow at a minimum.	
12.12	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.	
12.13	The dashboard provided to Company should be in the form of a unified portal that can show correlated alerts/ events from multiple disparate sources such as security devices, network devices, enterprise management systems, servers, applications, databases, etc.	
12.14	Any failures of the event collection (log stoppage) infrastructure must be detected and operations personnel must be notified as per SLA.	
12.15	Dashboard should support reporting for consolidated relevant compliance across all major standards and regulatory requirements. This includes ISO 27001, NIST, PCI DSS,HIPAA standards etc.	
12.16	Incident management workflows to track incident from creation to closure, provide reports on pending incidents. It should also permit upload of related evidences such as screenshots etc.	
12.17	Bidder to ensure logs are transmitted using strong encryption & no PII data is moved out of Company's Environment.	
12.18	Log storage & retention shall be for a period of 1 year	
12.19	The solution Should have Auto Remediation Features Solution should provide a central	

S. No	Requirement	Comply (Full / Partial / No) and Reply/Comments
	gateway level protection without the use of endpoint agents or any other tool.	
12.20	Solution should process security information for servers, routers, switches, firewalls, and endpoints - IoT devices, laptops, desktops, tablets, printers, phones and any other devices which connects to the organizations network.	
12.21	Solution should support multiple network segments including LAN, WAN, DMZ, WIFI Networks, MPLS Links simultaneously on a single instance.	
12.22	Solution should be able to identify the infection by considering suspicious network traffic, behaviour, source and destination analysis and not requiring to interact directly with the infected device(s) / hosts.	
12.23	Solution should automatically prioritize the risk on the basis infected devices (data transferred, AV Patching, Type of Malware, User importance to the organization and whether the communication was successful) Solution should be able to detect infection without the use of file analysis software.	
12.24	Solution should be able to view file download activity associated with infected endpoints for a required duration to qualify the attack on an endpoint Solution should provide machine intelligence and big data analytics capability to aggregate evidence and identify threat.	
12.25	Solution should have the capability to detect persistent threats, which are communicated through executable files, pdf files, flash files, RTF files amongst other file formats.	
12.26	Solution should provide risk rating capability basis, number of attempts made, data transferred, asset criticality, provide details on recorded threat, threat intent, researcher notes,	

S. No	Requirement	Comply (Full / Partial / No) and Reply/Comments
	crimeware used and local communication activity.	
12.27	SOAR Integration (New): The solution must integrate SOAR capabilities for automated orchestration, playbook execution, and response actions (e.g., isolate endpoint, block IP, quarantine file) triggered by high-fidelity alerts or analyst approval.	
12.28	Proactive Threat Hunting Services (New): Bidder to conduct proactive threat hunting with defined cadence (at least monthly documented hunts), including hypothesis-driven hunts mapped to MITRE ATT&CK and emerging BFSI threats. Provide hunt reports and findings.	
12.29	Vulnerability Management Integration (New): Solution must support vulnerability prioritization, integration with asset management, automated scanning correlation, risk-based patching recommendations, and tracking to closure (aligned with SEBI CSCRF vulnerability controls).	
12.30	Data Localization & Compliance (New): All data processing, storage, and analytics must ensure full data residency in India (no cross-border transfer of logs/PII) per DPDP Act 2023, RBI payment data norms, and SEBI CSCRF 2025. Provide architecture diagram and undertaking.	
12.31	Log Retention (New – Aligned Standard): Security-relevant logs (raw and normalized) shall be retained for a minimum of 365 days with audit trails.	
12.32	Purple Teaming / Threat Emulation (New): Bidder to conduct regular (at least half-yearly) purple teaming/threat emulation exercises to validate detection efficacy, with shared reports and tracked remediation.	

S. No	Requirement	Comply (Full / Partial / No) and Reply/Comments
12.33	Advanced Dashboard & Reporting (New): Dashboard and reporting shall include executive summaries, compliance heatmaps (SEBI CSCRF, RBI CSF, ISO 27001), and customizable KPIs (MTTD/MTTR, false positive rate, alert trends).	
12.36	SOC Security & Audits (New): Bidder to provide annual security audits/certifications of their SOC (ISO 27001, SOC 2 Type II, CERT-In empanelment) and commit to annual penetration testing/red teaming of the service.	

Scalability

a) All components of the SOC must support scalability to provide continuous growth to meet the requirements and demand coming in from various user departments.
b) Modular design of the SOC is an excellent strategy to address growth without major disruptions.
c) A scalable SOC shall easily be expanded or upgraded on demand. Scalability is important because new computing component is constantly being deployed, either to replace legacy component or to support new missions.

Availability

a) All components of the SOC must provide adequate redundancy to ensure high availability of the Governance applications and other SOC services.
b) Designing for availability assumes that systems will fail, and therefore the systems are configured to mask and recover from component or server failures with minimum application outage.
c) The bidder shall make the provision for high availability for all the services of the Data Centre.

Interoperability

a) The entire proposed system/ subsystem should be interoperable, in order to support information flow and integration.
b) Operating systems and storage technologies from several vendors must interact well with each other. These systems should also support the open architecture solutions where information/ data can be ported to any system, whenever desired.

5. Period of Contract

a) Bidder is required to provide the services for a period of 1 year which may be further extended up to 1 year as per mutual agreement provided the Bidder's performance is satisfactory to the Company. However, on extension of the term of service, the enhancement of rate shall not exceed 5% in Contract Value.

b) Post completion of the contract/ or in the event of early termination, the bidder is expected to provide support for transition of the services to the nominated members of SBI-SG (or) to a third party nominated by SBI-SG

c) The bidders are expected to provide technical and commercial proposals in accordance with the terms and conditions contained herein. Evaluation criteria, evaluation of the responses to the RFP and subsequent selection of the successful bidder shall be as per the process defined in this RFP. Their decision shall be final and no correspondence about the decision shall be entertained.

d) In case of termination of contract / end of contract period, bidder has to provide extended services, with the rates mentioned as of last year. This extension of services to be provided till procurement of next solution/ till 1 year, with same terms and conditions.

e) If any support is required after the contract w.r.t. to logs, the bidder has to provide the same.

f) Bidder shall provide transition support, which amongst other shall include provision of logs, rules, technical architecture of solution as deployed, detailed description of the processes, etc. as part of the transition to subsequent service provider or SBI-SG on completion or on termination of contract. The support will be for a period of Max 6 months.

6. End of Support

The components of the SOC Service proposed as part of this RFP response should not reach end of support during the period of contract (supporting document should be attached). None of the equipment proposed should be end of life or out of production by the OEM at the time of bidding or at the time of supply. The Bidder should provide Road map for components of the solution proposed. In case if any item reaches end of support during the period of contract, bidder has to

replace the same before end of support date with higher version/ upgraded model at no additional cost to the SBI-SG.

7. Terms and Conditions

7.1 Offer Validity Period

Bids shall remain valid for a period of 180 days after the date of opening of Commercial bids as mentioned in the 'RFP Notification' or as may be extended from time to time. SBI-SG holds the right to reject a bid valid for a period shorter than 180 days as non-responsive, without any correspondence.

7.2 Format and Signing the Proposals Submitted

The Bidder(s) shall prepare soft copy of entire Bid. In case of any discrepancy, Hard Copy of the bid would be considered as Final. Soft copy shall be password protected and password shall be disclosed post the bid-opening.

The original and all copies of bid proposal submitted by the Bidder(s) shall be typed or printed in a clear typeface. An accompanying letter is required as per Annexure VIII, signed by an authorized signatory of the Bidder(s), committing the Bidder(s) to the contents of the original response. All pages in the bid should be authenticated by a duly authorized signatory of the Bidder(s) under seal.

7.3 Rejection of Bid

The bid is liable to rejected if:

i. The document doesn't bear signature of authorized person
ii. It is received after expiry of the due date and time stipulated for Bid Submission

Incomplete / incorrect bids, including non – submission or non – furnishing of requisite documents

7.4 Modification and/or withdrawal of Proposal

Proposals once submitted will be treated as final and no further correspondence for modification shall be entertained. No proposal shall be modified after the deadline for submission of proposals. No proposal shall be allowed to be withdrawn after the last date of submission of the bid. The Bidder(s) will not be allowed to withdraw the proposals.

7.5 Completeness of the Proposals

The Bidder's proposal is subject to an evaluation process. Therefore, it is important that the Bidder(s) carefully prepares the proposal and answers questionnaire

completely. The quality of the Bidder(s) proposal will be viewed as an indicator of the Bidder(s) capability to provide the solution and Bidder(s) interest in the project. The Bidder(s) is required to respond to the RFP only in the prescribed format. Under no circumstances, should the format be changed, altered and modified. All pages including all supporting documents in the bid should be authenticated by a duly authorized signatory of the Bidder(s) under seal.

7.6 Right of Verification

SBI-SG reserves the right to verify any or all statements made by the Bidder(s) in the proposal documents and to inspect its facility or any other client site, if necessary, to establish about the Bidder(s) capabilities to undertake the required tasks. SBI-SG reserves the right to inspect/audit any of the Bidder(s) offices, locations, software, hardware etc. through its employees or nominated agencies. The Bidder(s) would have to co-operate and provide access to these units, systems, software, etc. The Bidder(s) will need to furnish the contact details of their existing clients.

7.7 Acceptance or Rejection of the Proposals

SBI-SG reserves the right not to accept any bid, or to accept or reject a particular bid at its sole discretion without assigning any reason whatsoever and the decision of SBI-SG will be treated as final. The RFP responses/bids/proposals not submitted in the prescribed format or incomplete in any sense are likely to be rejected. SBI-SG also has the right to re-issue the Tender without the Bidder having the right to object to such re-issue

To bid, the Bidding Document should be emailed to cro@sbisgcsl.co.in with on commercial part with password protected & other part separately and subject line as "Bid to RFP- Comprehensive / End-to-End SOC Services". The password for commercial part should not be shared on the email. On Bid opening day, the password shall be shared when called upon for password.

7.8 Commercial Price Bid

a. The Commercial Price Bid will give all relevant price information and the bidder will quote prices only in Indian Rupees.
b. The Price Bid should not contradict the Technical Bid in any manner with respect to terms and conditions mentioned in the RFP.
c. It is mandatory to submit the commercial Price Bid in the prescribed pro-forma (Annexure VII) duly filled in, along with the offer.

7.9 Price Composition

a. The Charges/fees quoted should be in Indian rupees only. The Charges/fees shall be on a fixed price basis and should not be linked to the Foreign exchange.

b. The Charges/fees should be quoted with breakup as per the Bill of material except taxes. The taxes would be payable at actual at the applicable rates.

7.10 No Price Variations

The commercial offer shall be on a fixed price basis. No upward revision in the price would be considered on account of subsequent increases in any government tax, etc. during the offer validity period. However, if there is any reduction on account of government levies, during the offer validity period, the same shall be passed on to SBI-SG.

7.11 Material Alterations and Ambiguous Information

The Bidder(s) should ensure that there are no cuttings, erasures or over-writing, illegible or undecipherable figures in the documents submitted. The proposals may be disqualified on this score alone. The decision of SBI-SG is final and binding.

7.12 Right to Alter Quantities / Repeat orders

SBI-SG reserves the right to alter the number of locations specified in the tender, and to delete/substitute items from the ones specified in tender. SBI-SG may also place order for various services which are only part of this RFP in addition to the quantities mentioned in this tender at the same rate terms and conditions including the cost agreed upon.

7.13 SOC Integration

Responsibility for integration of devices/solution would be vested on remote SOC team. The bidder shall factor the cost of integration in the unit cost of SOC services while proposing commercials. SBI-SG will not pay additional cost for integration.

Development of connector, if required, for integration of devices, servers, applications etc. shall be developed by the SOC service provider and cost for development of such connector should be factored in the unit cost of SOC services.

Device/solution would be considered integrated only after acceptance from SBI-SG information security team, post which the commercial charges of integrated devices would be applicable.

The integration of device/server/application/web server etc. completed and accepted by SBI-SG before 15th of the month will be considered for calculating billing for that month during the quarterly billing cycle.

7.14 Bidder Queries

a. All queries with regards to this bid, if any, must be sent to: **CISO@sbisgcsl.co.in +CRO@sbisgcsl.co.in**

b. SBI-SG is not obliged to divulge the nature and configuration of its IT/IT Security Infrastructure.

c. SBI-SG at its sole discretion, reserves the right whether or not to respond to queries raised by bidders or provide written clarifications. No oral responses to a clarification request shall be constructed as amending this RFP document. No extension of any deadline will be granted on the basis grounds that SBI-SG has not responded to any question or provided any clarification.

7.15 Proposal Ownership

The proposal and all supporting documentation submitted by the bidders shall become the property of SBI-SG unless it agrees to the bidders 'specific requests, in writing, the proposal and documentation to be returned or destroyed.

7.16 Bidder(s) Status

Each Bidder must indicate whether or not they have any actual or potential conflict of interest related to contracting services with SBI-SG.

7.17 Bidder(s) indication of Authorisation to Bid

Responses submitted by Bidder(s) to this RFP represent a firm offer to contract on the terms and conditions described in the Bidder(s) response. The proposal must be signed by an official authorized to commit the Bidder(s) to the terms and conditions of the proposal. The signatory should have the authority to sign the documents

7.18 Cost of the Proposal

All costs relating to preparation, submission of its proposal, attending the clarification sessions and bid opening as well as arranging for the Technical Presentation to SBI-SG will be borne by the Bidder and SBI-SG will not be responsible or liable, in any way, for any such costs, regardless of the conduct or outcome of the process.

7.19 Payment Terms

Payments will be released quarterly on submission of invoice at the end of each quarter. This will be derived on the basis of yearly cost submitted as part of the commercials vis-a-vis actual count of integrated devices/solutions (on a quarterly basis), deployment of resources and Compliance level to agreed SLA.

7.20 Award of Contract

Any award to be made pursuant to this RFP will be based upon the proposal with appropriate consideration given to technical methodologies, quality of resources employed Bidder deliverables and factsheet of past projects of similar nature with similar clients, cost proposed and SBI-SG's requirements.

The acceptance of a Bid for New Generation SOC will be communicated in writing at the address supplied by the Bidder(s) in the RFP response. Any change of address of the Bidder(s), should therefore be promptly notified in writing to SBI-SG.

7.21 RFP Ownership

The RFP and all supporting documentation/templates/annexure are the sole property of SBISG should NOT be redistributed without prior written consent of SBI-SG. Any violation of this will be a breach of trust and SBI-SG would be free to initiate any action deemed appropriate.

7.22 Proposal Ownership

The proposal and all supporting documentation submitted by the bidders shall become the property of SBI-SG unless it agrees to the bidders 'specific requests, in writing, the proposal and documentation to be returned or destroyed.

7.23 Bidder(s) indication of Authorisation to Bid

Responses submitted by Bidder(s) to this RFP represent a firm offer to contract on the terms and conditions described in the Bidder(s) response. The proposal must be signed by an official authorized to commit the Bidder(s) to the terms and conditions of the proposal. The signatory should have the authority to sign the documents.

7.24 Signing of Contract

The selected Bidder(s) shall be required to enter into a contract with SBI-SG, within thirty days of the award of the tender (i.e. issuance of a Letter of Intent by SBI-SG) or within such extended period, as may be specified by SBI-SG. At the time of execution of the contract a Memorandum of Understanding (MoU) containing the terms and conditions necessary for the due performance of the work in accordance with the bids and acceptance thereof will be signed. The contract will be based on this RFP, modification arising out of negotiation/clarification etc., the Bidder(s) offer document with all its enclosures and will include the following documents:

The Bidder(s) proposal in response – technical and commercial proposals separately Modification to the proposal, if any, after negotiation/clarification. Related Technical Specifications Copies of the licenses, certifications etc.

SBI-SG reserves the right to stipulate, at the time of finalization, any other document(s) to be enclosed as part of the final contract.

7.25 Order Cancellation

SBI-SG may at its discretion decide to cancel the complete order or partial order. SBI-SG may cancel the partial order by giving 3 months' notice period and complete order by giving 6 months' notice period in the event of one or more of the following conditions:

Delay in installation and commissioning beyond 2 weeks from project timelines.

Failure to meet the performance standards mentioned in this document

However, during the notice period, the bidder is expected to deliver the same level of services as prescribe in RFP and same payment terms will be applicable.

7.26 Confidentiality and Non-Disclosure

The Bidder(s) shall be under obligation and binding of the confidentiality-cum-non disclosure undertaking to be submitted along with response to this RFP. The draft of the same is attached **Annexure VI.** The Bidder(s) have to execute Non-Disclosure Agreement on Rs.100/-Non judicial stamp paper. The undertaking should be notarized and stamped.

7.27 Empanelment of the Bidder and Exit

SBI-SG reserves its right to empanel one or more than one Bidder(s) for one or both scope of activity/activities proposed. Deployment of services in terms of location and scope will be the sole prerogative of SBI-SG.

Upon empanelment, selected Bidder(s) shall be required to enter into Service Level Agreement (SLA). Such Service Level Agreement shall be initially for a period of Three (3) years extendable upto additional Two (2) years and may be extended thereafter at mutually agreed terms and conditions. Such decision shall be at the sole discretion of SBI-SG. **The service level agreement shall be on Principal to Principal basis. (**Refer SLA)

Empanelled Bidder(s) shall be required to put in place necessary security and all possible safeguards to maintain necessary confidentiality of data and/or information received in any form from SBI-SG. The empanelled Bidder(s) shall be required to submit the details of all safeguards in place at its facility before commencement of the proposed activity.

The empanelled Bidder shall have to abide by SBI-SG Information Security Policy for the activities that shall be carried out for SBI-SG. This policy and procedures is almost aligned to requirements of ISO 27001 standards (ISMS).

The SLA between SBI-SG and empanelled Bidder(s) will have these security controls and liabilities of the empanelled Bidder(s) for violation of SBI-SG IT and IS policy, standards and procedures.

7.28 No Commitment to Accept Lowest or Any Tender

SBISG shall be under no obligation to accept the lowest or any other offer received in response to this notice and shall be entitled to reject any or all offers without assigning any reason whatsoever.

7.29 Amendments to this RFP

Amendments to the RFP may be issued by SBI-SG during the RFP process as required. Amendments to RFP so made shall be deemed to form an integral part of the RFP.

7.30 Tender / RFP Cancellation

During the process of scrutiny, evaluation and comparison of offers, SBI-SG may, at its discretion, seek clarification from all or any of the bidders on the offer made by them. The request for such clarification and the bidder's response will necessarily be in writing and should be submitted within time stipulated by SBI-SG. In the event of any of the failure to submit the response for clarification sought within the stipulated time, their bill is liable to be rejected.

SBI-SG reserves the right to cancel the Tender/RFP at any time without assigning any reasons whatsoever.

7.31 Taxes and Duties:

a. Bidder will be entirely responsible for all applicable taxes, duties, levies, imposts, costs, charges, license fees, road permits etc., in connection with delivery of Hardware and Software at site including incidental services, Transportation, Installation and Commissioning. Payment of Sales Tax/VAT/GST, Service Tax, etc. if applicable, will be made at actual, on production of suitable evidence of payment by the Bidder.

b. The Bidder shall be liable to pay all applicable corporate taxes and income tax that shall be levied according to the laws and regulations applicable from time to time in India.

c. Wherever the laws and regulations require deduction of such taxes at the source of payment, Purchaser shall effect such deductions from the payment due to the Bidder. The remittance of amounts so deducted and issuance of certificate for such deductions shall be made by Purchaser as per the laws and regulations in force. Nothing in the Contract shall relieve the Bidder from his responsibility to pay any tax that may be levied in India on income and profits made by the Bidder in respect of this Contract

7.32 Indemnity

The Bidder(s) shall indemnify SBI-SG and keep indemnified against any loss or damage that SBI-SG may sustain on account of any violation(s)/breach/infringement of intellectual property, confidentiality, privacy, patents, trademarks, statutory/regulatory guidelines/instructions etc., by the Bidder(s).

The Bidder(s) shall, at its own cost and expenses, defend and indemnify SBI-SG against all third-party claims including, but not limited to, those of the infringement of Intellectual Property Rights, including patent, trademark, copyright, trade secret or industrial design rights, arising from use of the Products or any part thereof in India.

The Bidder(s) shall expeditiously meet any such claims and shall have full rights to defend itself there from. If SBI-SG is required to pay compensation to a third party resulting from such infringement, the Bidder(s) shall be fully responsible therefore, including all expenses and court and legal fees.

The Bidder(s) shall also be liable to indemnify SBI-SG, at its own cost and expenses, against all losses/damages, which SBI-SG may suffer on account of violation by the Bidder(s) of any or all national/international trade laws, norms, standards, procedures, etc.

Further, the Bidder(s) shall indemnify SBI-SG and keep indemnified against any loss or damage that SBI-SG may sustain on account of any violation of patents, trademark, license, etc., by the Bidder(s) in respect of hardware, hardware components, software, tools, etc. supplied as part of the New Generation SOC services.

7.32.1 Regulatory Change – Data Residency Compliance & Contingency

The Bidder / OEM represents, warrants and undertakes that:

A - It shall establish and make fully operational a dedicated data centre (or equivalent compliant infrastructure) physically located within the territory of India for all processing, storage, retention, analytics, threat intelligence enrichment, and any other handling of Client Data (including but not limited to logs, telemetry, PII, security events, configurations, dashboards, alerts, forensic artefacts, and all derived or processed data) no later than **30 November 2026**.

B - From the date of such operationalisation, all Client Data shall at all times remain exclusively within Indian territory and shall not be transferred, mirrored, processed, or made accessible from any location outside India, except as expressly permitted under applicable law or with the Client's prior written consent.

In the event that SEBI, CERT-In, MeitY, or any other Indian regulatory or statutory authority issues a binding direction, circular, guideline, notification, or order (a "**Strict Residency Mandate**") that:

- prohibits or materially restricts any transfer, processing, storage, or access to Client Data outside the territory of India, or

- imposes a mandatory requirement for 100% data localization / residency within India,

the following provisions shall immediately apply:

1. **Migration Obligation** The Provider shall, at its sole cost and expense, promptly and diligently migrate (or cause to be migrated) all Client Data, configurations, historical logs, dashboards, rulesets, playbooks, and related workloads to the India-based infrastructure (or to an alternative solution fully compliant with the Strict Residency Mandate and acceptable to the Client) within **30 calendar days** from the date the Strict Residency Mandate becomes effective or enforceable (whichever is earlier).
2. **Interim Business Continuity** During the migration period and until successful completion, the Provider shall ensure uninterrupted access to all Client Data, dashboards, alerting, reporting, and SOC services necessary for the Client's business continuity and regulatory compliance obligations.
3. **Right to Terminate for Cause** If the Provider fails to complete the migration within the stipulated 30-day period (or such extended period as may be mutually agreed in writing), the Client may, at its sole discretion and without incurring any liability:
    a. Terminate this Agreement **forthwith** by written notice;
    b. Suspend payments under the Agreement until compliance is achieved; or
    c. Engage an alternative provider and require the Provider to cooperate fully in transition at no additional cost to the Client.
4. **Transition & Exit Assistance** Upon termination under this clause or upon expiry of the Agreement, the Provider shall, at no additional cost to the Client:
    a. Provide full, secure, and complete migration / transition assistance for a period of **90 calendar days** (or longer if reasonably required) to the Client's nominated successor provider;
    b. Deliver all Client Data in industry-standard, machine-readable formats (e.g., CEF, JSON, CSV, Parquet) with integrity hashes;
    c. Issue a signed certificate of secure, irrecoverable deletion of all Client Data from the Provider's systems, backups, and third-party environments (in compliance with NIST SP 800-88 or equivalent);
    d. Provide chain-of-custody documentation for any forensic or evidentiary data.
5. **Indemnity** The Provider shall fully indemnify, defend and hold harmless the Client, its affiliates, directors, officers and employees against any and all losses, damages, costs, expenses (including legal fees), fines, penalties, regulatory sanctions, third-party claims or liabilities arising directly or indirectly from:
    a. Any failure to migrate or comply with the Strict Residency Mandate;
    b. Any unauthorized retention, access, transfer, exposure or leakage of Client Data during the transition or post-termination period;

c. Any regulatory non-compliance, enforcement action, or reporting obligation of the Client (including under SEBI CSCRF, RBI cybersecurity directions, DPDP Act 2023, or CERT-In directives) caused or contributed to by the Provider's delay or non-performance.

Liability under this indemnity shall be **unlimited** in cases of gross negligence, wilful misconduct, fraud, or material breach of data residency obligations.

6. **Survival** This clause shall survive termination or expiry of the Agreement for a period of **five (5) years** or such longer period as may be required under applicable law or regulatory direction.

7.33 Dispute Resolution

Any dispute or differences whatsoever arising between the parties out of or in relation to the construction, meaning, interpretation and operation or effect of these Proposal Documents or breach thereof shall be decided by SBI-SG. Such decision by SBI-SG shall be final and binding on the Bidder(s).

7.34 Disaster Recovery and Business Continuity Planning (BCP)

All the bidders participating in the tender should submit the BCP document, which is, accepted as best practice. Only the selected bidder will submit the final plan after studying the SBI-SG's environment, infrastructure and business operations.

7.35 Audit by Third Party

SBI-SG at its discretion may appoint third party for auditing the activities of ON-SITE Services and operations of entire services provided to SBI-SG.

7.36 Intellectual Property Rights

SBI-SG will own all intellectual property rights to all design, software and/or systems created specifically for implementation at SBI-SG under this contract. The Bidder(s) shall fully protect and indemnify SBISG from all legal actions, claims, or damages from third parties arising out of use of software, designs or processes supplied by the Bidder(s).

7.37 Solicitation of Employees

Bidder(s) will not hire employees of SBI-SG or solicit or accept solicitation (either directly, indirectly, or through a third party) from employees of SBI-SG directly involved in this contract during the period of the contract and one year thereafter, except as the parties may agree on a case-by-case basis.

7.38 Jurisdiction

Courts in Mumbai will have exclusive jurisdiction.

7.39 Condition of Acceptance

The selected Bidder(s) and SBI-SG will specify during contracting, the criterion for acceptance and milestones (both technical and functional). Failure, to meet the acceptance criterion may result in termination of the arrangement and/or contract. No payments will be made and SBI-SG may claim damages from the Bidder(s). In such an eventuality, SBI-SG will be free to engage any other Bidder(s).

At the discretion of SBI_SG, acceptance tests will be conducted by the bidder at the site in the presence of the officials of SBI-SG. The tests will check for trouble-free operation apart from physical verification and testing. There shall not be any additional charges payable by SBI-SG for carrying out this acceptance test. SBI-SG will take over the system on successful completion of the above acceptance test. An average uptime of 99.5% for duration of test period and no impact to IT infrastructure shall be considered as satisfactory.

The solution will not be accepted as complete if any service as required is not available or not up to the standards projected by the Bidder in their response and the requirement of this RFP.

The Company will accept the solution on satisfactory completion of the above inspection. The contract tenure for the service will commence after acceptance of the service by the Company.

In case of discrepancy in services provided, the Company reserves the right to cancel the contract.

8. OPENING AND EVALUATION OF BIDS

8.1 Opening of Technical Bids by the Company

The Bidders' names, Bid modifications or withdrawals and such other details as the Company, at its discretion, may consider appropriate, will be announced at the time of technical Bid opening.
Bids and modifications sent, if any, that are not opened at Bid Opening shall not be considered further for evaluation, irrespective of the circumstances. Withdrawn bids will be returned unopened to the Bidders.

8.2. Preliminary Evaluation

a. The Company will examine the Bids to determine whether they are complete, required formats have been furnished, the documents have been properly signed, and the Bids are generally in order.
b. Prior to the detailed evaluation, the Company will determine the responsiveness of each Bid to the Bidding Document. For purposes of these

Clauses, a responsive Bid is one, which conforms to all the terms and conditions of the Bidding Document without any deviations.

c. The Company's determination of a Bid's responsiveness will be based on the contents of the Bid itself, without recourse to extrinsic evidence.
d. If a Bid is not responsive; it will be rejected by the Company and may not subsequently be made responsive by the Bidder by correction of the non-conformity.

8.3. Technical Evaluation

a) Only those Bidders and Bids who have been found to be in conformity with the eligibility terms and conditions during the preliminary evaluation would be taken up by the Company for further detailed evaluation. Those Bids who do not qualify the eligibility criteria and all terms during preliminary examination will not be taken up for further evaluation.
b) During evaluation and comparison of bids, the Company 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.
c) Bidders scoring less than 90 marks (minimum cut-off score) out of 100 marks in the technical evaluation will not be considered for the selection process.
d) The evaluation of technical proposals, among other things, will be based on the following parameters and also given the percentage of marks:

i. Technical requirements as described in RFP
ii. Service capabilities of bidder
iii. Past experience of the bidder in similar lines of business
iv. Bidder Presentation
v. Project and Implementation Plan
vi. Project Governance Approach

This weightage shall be taken into consideration for arriving at the winner of the bidding process. The bidder getting highest score in the techno-commercial evaluation will be declared as winner bidder.

e) The winner bidder shall be required to facilitate POC (Proof of Concept) for one week for sample devices. Only after successful POC, next steps shall be taken. In case of POC failure for L1 bidder, next L2 and L3 bidder shall be approached for necessary POC. Accordingly, winning bidder shall be subject to successful result of POC of sample devices.

f) As part of technical bid, bidder will also submit their approach methodology covering each of the activities and the proposed implementation schedule. The Bidders shall be invited to deliver

a presentation about the services and activities that are proposed. The presentations would be rated by a competent panel chosen appropriately by SBI-SG and scores would be assigned to each of the presentations. The bidders are expected to submit the soft copy of the presentation to SBI-SG prior to the presentation.

g) Bidders will be evaluated based on the proposals submitted and initial evaluation of the technical proposals, Bidder(s) will be required to present to SBI-SG officials, the proposed solution, discuss related implementation approach and methodologies, and introduce the project team and governance structure in the form of a presentation. These presentations should cover details of the proposal described in this RFP document and its annexure as well as enclosures

8.4 Commercial Proposal

a. The Commercial Proposal must contain the charges for individual Services. The bidder may also submit different pricing for different approaches proposed for SBI-SG environment. SBI-SG may consider the approach and the respective commercial for approach as per its own discretion. The commercial proposal format is provided in the **Annexure VII** to this RFP.
b. The charges proposed by the Bidder(s) and agreed to by SBI-SG for the activities covered under scope of RFP shall remain frozen during the term of contract which is 3+2=5 years from the term date mentioned in Letter of Intent (LOI).
c. The cost should be quoted in Indian Rupees only and should be exclusive of the applicable Goods and Service taxes. Relative cost, cost as a percentage to some other factor is not acceptable in the commercial format. Tax Deduction at Source (TDS), as applicable, will be deducted by SBI-SG.
d. Bids in consortium are strictly prohibited.
e. The Commercial proposal is required to be submitted separately email marked to **ciso@sbisgcsl.co.in** + **cro@sbisgcsl.co.in** **subject line as "Bid to RFP-Comprehensive / End-to-End SOC Services"** and no other document should be submitted with the Commercial proposal. Only one (1) soft copy and hardcopy (original) of the commercial proposal needs to be provided.

9. Instructions to Bidder(s):

1. The bidders(s) should submit technical and commercial proposal in response to this RFP.

2. Company at its own discretion decide whether only one Scope shall be considered or Both However Commercials shall be shared in same sheet specified in Annexure VII.

3. The Technical proposal should contain information necessary to establish the credentials of the interested bidder(s). The information to be covered is indicated below. Necessary documentary evidences needs to be enclosed.

4. Brief Company overview with name and address and year of establishment.

5. Management details including ownership pattern, shareholding, whether a listed company etc.

6. Business performance during last four Financial Years along with brief summary of audited financial results as per Annexure-IV.

7. Details of SOC facilities with address, infrastructure details and contact person details.

8. Demonstrable New Generation SOC capabilities w.r.t. Artificial intelligence, Machine Learning, Data analytics, orchestration Name a few and other allied activities. Please provide the details and proposed process flow

9. Details of Backup/Business Continuity Plan in place.

10. Details of data security measures and certifications.

11. Details of contracts relating to SOC awarded like SOC Implementation and Services etc (if any).

12. Details of industry awards, recognitions, affiliations and certifications, if any.

13. List of existing clientele with information on New Generation SOC and quality check activities being handled for them and volumes scope wise handled during last four Financial Years

14. Letter from competent authority of Bidder(s) on name, designation, contact details of the authorized person for communication.

15. Lead time required for taking over the SOC activities.

16. Information with regard to your Company being blacklisted by State/Central Govt. undertakings/public sector units or whose contracts have been terminated because of this reason.

17. All pages of the proposal except un-amended printed literature shall be initialled by the person(s) signing the proposal.

18. The commercial proposal should only contain the charges offered for the proposed activity. The format of commercial proposal is provided in the **Annexure VII** to this RFP.

19. The cost should be quoted in Indian Rupees only and should be exclusive of applicable taxes. Relative cost, cost as a percentage to some other factor is not acceptable in the commercial format. Tax Deduction at Source (TDS) in India, as applicable, will be deducted by SBI-SG.

In case the technical or commercial proposal is incomplete in any respect, SBI-SG reserves the right to reject such proposals summarily.

10. Service Level Agreement

SLA as described below provides for minimum level of services required as per contractual obligations based on performance indicators and measurements thereof. The Vendor shall ensure provisioning of all required services while monitoring the performance of the same to effectively comply with the performance levels.

The services provided by the Vendor shall be reviewed by the SBI-SG GLOBAL SECURITIES SERVICES PVT. LTD on quarterly basis and SBI-SG GLOBAL SECURITIES SERVICES PVT. LTD shall:

- Check performance of the Vendor against this SLA over the review period of 3 month and consider any key issues of the past period's performance statistics including major incidents, service trends, etc.
- Discuss escalated problems, new issues and matters still outstanding for resolution.
- Review of statistics related to rectification of outstanding faults and agreed changes.
- Obtain suggestions for changes to improve the service levels.

In case, if desired, SBI-SG GLOBAL SECURITIES SERVICES PVT. LTD may initiate an interim review to check the performance and the obligations of the Agency. The Company will conduct quarterly review of the services rendered by the Service Provider at mutually agreed schedules, dates and representatives from both the Company and Service Provider should attend such performance review meetings. The SLA may be reviewed periodically i.e. quarterly and revised, if required.

The Company shall have the right to inspect / audit the SOC, Tools, Techniques and procedure adopted by the Service Provider in line with security activity outsourced by the Company, independently or through the outsourced experts and call for detailed report without compromising the Service Provider's Security.

The SLA takes into consideration the following aspects-

1. Equipment Availability Related Service Levels
2. Technical Support desk Services

3. Compliance and Reporting Procedures

The following measurements and targets shall be used to track and report performance on a regular basis. The targets shown in the following table are applicable for the duration of the contract.

10.1 Service Level Agreements

Sl. No.	Service Area	Service Level / Targets	Compliance Threshold (Monthly)	Penalty (as % of Monthly SOC Payment)
1	Monitoring and Incident Alerting / Notification	24×7 real-time monitoring of all in-scope devices / logs / endpoints. Incidents categorized as per severity (Critical, High, Medium, Low). **MTTA** (Mean Time to Acknowledge alert internally): 1. Critical: ≤ 5 minutes 2. High: ≤ 15 minutes 3. Medium: ≤ 30 minutes 4. Low: ≤ 60 minutes **MTTD** (Mean Time to Detect – from event occurrence to alert generation): 1. Critical: ≤ 10–15 minutes average 2. High: ≤ 30 minutes average **Notification SLA** (from MTTA to client notification): 1. Critical: within 15 minutes 2. High: within 30 minutes 3. Medium: within 60 minutes 4. Low: within 4 hours (informational / best-effort) False Positive Rate (Critical/High alerts): ≤ 20% monthly average	≥ 98% for MTTA + MTTD	≥ 98%: No penalty 95–97.99%: 2% 90–94.99%: 5% < 90%: 20–25% False Positive >25% (severe for systemic failure)
2	Incident Investigation / Initial Response & Containment	24×7 incident response capability. **MTTR – Initial Response & Containment Initiation** (from alert acknowledgment / event detection): 1. Critical: Containment initiation within 30 minutes (target ≤15 min best-effort) 2. High: within 60 minutes 3. Medium: within 120 minutes **Initial Investigation Report** (preliminary findings, IOCs, containment status, next steps):	≥ 97.5% adherence across all timelines (MTTR + reports)	≥ 97.5%: No penalty 95–97.49%: 2% 90–94.99%: 5% < 90%: 20% Repeated Critical/High breach RCA delay (>72 hrs without justification)

Sl. No.	Service Area	Service Level / Targets	Compliance Threshold (Monthly)	Penalty (as % of Monthly SOC Payment)
		1. Critical: within 60 minutes 2. High: within 90 minutes 3. Medium: within 180 minutes **Full Containment / Root-Cause Analysis (RCA) Report**: 1. Critical & High: Preliminary RCA + containment confirmation within 24 hours; Final RCA within 48–72 hours (extendable to 5 days for complex cases with daily updates) 2. Medium: Final RCA within 5–7 business days All reports delivered to designated client personnel via secure channel (encrypted email / portal).		
3	Reports & Dashboard	Daily: by 10:00 AM IST · Weekly: by 10:00 AM Monday · Monthly: by 5th working day Accurate, actionable dashboards with key metrics (e.g., MTTD/MTTR trends, top threats)	≥ 98%	< 98%: 3–5% (escalated for repeated misses)
4	SOC Service Uptime / Availability	Platform and monitoring service availability (excluding scheduled maintenance with prior notice)	99.99%	≥ 99.5%: No penalty 99.0–99.49%: 3% 98.0–98.99%: 5% 95.0–97.99%: 10% < 95%: 25–50% (or 100% in extreme cases, per financial sector norms)
5	Periodic Review Meeting	Monthly review meeting with SOC PM/delegate and client officials. Covers SLA status, operations, key/new threats, issues/challenges. Report issued post-meeting. Any missed meeting without prior written approval incurs penalty.	100% (every month)	Missed (without approval): 1–2% per occurrence
6	Breach Investigation & Forensic Support (as part of Incident Response)	SOC to provide breach/confirmed incident investigation support, including: • Evidence preservation & collection (logs, memory, disk images as feasible). • Timeline reconstruction, IOC identification, and scope assessment. • Root cause analysis (RCA) and mitigation recommendations. • Coordination with client/external forensics experts if mutually agreed	Adherence to agreed/above timelines for each qualified breach incident a	Delay beyond agreed timeline: 2–5% of monthly SOC payment per week of delay (or pro-rated investigation/IR fee if separately billed), capped at 20–25%. • Escalated for regulatory/reportable breaches: Additional remedies (e.g., credit or

Sl. No.	Service Area	Service Level / Targets	Compliance Threshold (Monthly)	Penalty (as % of Monthly SOC Payment)
		for advanced needs (e.g., litigation-grade). Timelines (from confirmation of breach / request for deeper investigation): 1. Initial findings/update & containment status: within 24–48 hours (prioritize containment to limit damage). 2. Preliminary investigation report (scope, IOCs, initial RCA): within 3–5 business days. 3. Final detailed RCA report + action plan/recommendations: within 10–21 calendar days (target 7–14 days for standard cases; extendable by mutual agreement for highly complex breaches, with progress updates every 7 days). Exclusions: Client-caused delays, third-party dependencies, or force majeure.		accelerated support) if delay impacts RBI/SEBI reporting obligations. • No penalty if extension is mutually approved in writing.
7	Exit Strategy & Data Portability	Upon termination / Data Migration within Cloud Services / Migration to different OEM / Migration to different MSSP : Secure data return/export (logs, configs, reports) within 30–60 days; secure deletion/purge. Transition assistance for handovers. (Evidence to be provided for 1. data transfer in standard formats, 2. integrity and erasure)	100% (per event)	Non-adherence: 10–25% + indemnities

ANNEXURE - I: A. Details required from the Bidder.

#	Details Required from the Bidder	Response
1	Bidder's experience in Information Security Services (maximum number of years for each) SOC Services EDR	
	SIEM	
	CNAPP	
	Managed SOC/ EDR	
2	Bidder's experience in providing SOC services to BFSI companies (count and names of BFSI clients)	
3	Bidder's experience in providing SOC services for count of assets/devices across its customer base (Total number of devices managed: clients wise count of devices managed and/or devices managed from bidder's own SOC)	
4	Certifications possessed by the Bidder in connection with the quality of processes and services delivered/methodology used in delivery (e.g., ISO 27001, 22301, etc.)	

5	Current strength of employees in the Bidder's organization (In India) with experience in services/solutions as per the scope of RFP	
6	Current strength of the employees in the Bidder's organization (In India) with experience in similar projects in BFSI environment	
7	Profile of team members with relevant roles, experience and security certifications held by them. Provide details on as many resources as possible. (Relevant experience means that the experience on either exactly the same service/ set of service being proposed or on similar projects) (Certifications Include but limited to: CEHv9, CISSP, GCIH, GIAC, GCFA, CCNA, CCNP and other product/service related certifications)	

Sr no.	Employee name and ID	Job Role And Designation	Years of Relevant experience	Total years of experience	Professional certifications held and educational qualifications
n..					

B. Capabilities of the Services provided by the bidder:

#	Service	Full	Partial	NA
1	Brand Abuse, Anti phishing and anti-rogue			
2	Malware containment and Anti-Malware			
3	Threat anticipation, assessment and hunting			
4	On demand forensic investigation			
5	User entity behavioural analytics (UEBA)			
6	Network behaviour anomaly detection			
	(NBAD)			
7	Log and Storage management			
8	eDiscovery and legal evidence collection			
9	Run book/playbook response			
10	Deep and Dark web monitoring			
11	Event and Incident Management			
12	Global security advisory			
13	Cloud Security Posture Management (CSPM)			
14	Cloud Workload Protection Platform (CWPP)			
15	Cloud-Native Application Protection Platform (CNAPP)			
16	Cloud Detection and Response (CDR)			
17	Cloud Infrastructure Entitlement Management (CIEM)			
18	Kubernetes/Container / VM Security Posture & Runtime (KSPM/Kubernetes Security)			
19	Multi-Cloud / Hybrid Visibility & Log Ingestion			
20	Cloud Threat Hunting & Proactive Assessment			

Annexure II- Financial Details

Sr. No.	Field	2022-23	2021-22	2020-21
1.	**Audited**			
2.	**Paid up Capital**			
3.	**Tangible Net Worth**			
4.	**Total Assets**			
5.	**Total Sales (net of excise)**			
6.	**PBDIT**			
7.	**Profit after Tax**			
8.	**Revenue from Information Security Services**			

Please fill all the above columns (do not leave any column blank) and attach audited

Balance Sheets and Profit and Loss statements for the last three years.
For item no 8 –

Provide copies of PO/ letter of engagement

Date:

Signature of Authorized Official with Seal

Annexure III - Details of OEM

The bidder must provide the following details for the original manufacturers of the products proposed to be provided:

Name of the Product with full specifications (please enclose Brochure if available)

1. Name of the Manufacturer
2. No. of years in business
3. Address of the Manufacturer
4. Contact details like phone, fax, and email
5. PAN number and Sales Tax number
6. List of manufacturing locations (worldwide)
7. Description of manufacturing locations
8. Description of production facilities
9. Description of inspection and testing facilities
10. Certifications possessed by the manufacturer (ISO etc.)
11. Any other information about the manufacturer
12. Industry Recognitions

Place:

Date:

Seal and signature of the bidder

Annexure IV- Statement of Deviation

We certify that except for the following deviations, we agree to abide by all other clauses, terms, conditions, and specifications mentioned in the RFP

Main RFP/ Annexure No.	Clause/ Sub Clause No.	Deviation	Specific Page no. of the response

Signature of Authorized signatory (With seal)

Date: Place:

Note: If there are no deviations the bidder has to give his response by writing 'NIL' in the statement

Annexure V- Proposed team profile

Sr. No	Name of Proposed Engagement Manager /Proposed Team Member	Date Of Joining	Prof. Qualifications	Age and total experience	Certifications/ Accreditations	Experience in Solution Implementation and operations	IT Security Expertise In terms of years and areas of expertise

Documentary proofs are to be enclosed to substantiate the claims made.

Place:

Date: Seal and signature of the Bidder

Annexure VI- Sample NDA

NDA Format.docx

Annexure VII –Commercial Proposal

Commercial format

Commercial Format for SOC.xlsx

Annexure VIII- BID FORM

Date:_____

To,

The Chief Risk Officer,

SBI-SG Global Securities Services Private Limited

Jeevan Sewa Annexe,

S.V. Road, Santacruz (West),

Mumbai 400 054

Dear Sir,

Ref: RFP No. SBISG-GSS/2025-26/12

We have examined the RFP, the receipt of which is hereby duly acknowledged and subsequent pre-bid clarifications/ modifications / revisions, if any, furnished by the Company and we agree to offer our SOC services as detailed in Annexures, as per the terms and conditions spelt out in the RFP.

While submitting this bid, we certify that:

- The undersigned is authorized to sign on behalf of the VENDOR and the necessary support document delegating this authority is enclosed to this letter.
- We declare that we are not in contravention of conflict of interest obligation mentioned in this RFP.
- Indicative prices submitted by us have been arrived at without agreement with any other Bidder of this RFP for the purpose of restricting competition.
- The indicative prices submitted by us have not been disclosed and will not be disclosed to any other Bidder responding to this RFP.
- We have not induced or attempted to induce any other Bidder to submit or not to submit a bid for restricting competition.
- The rate quoted in the indicative price bids for the scope of services are as per the RFP and subsequent pre-bid clarifications/ modifications/ revisions furnished by the Company, without any exception.

3. If our offer is accepted, we undertake to complete the desired activity within a period of 6 weeks from date of Purchase Order.
4. We agree to abide by the Bid and the rates quoted therein for the orders awarded by the Company up to the period prescribed in the Bid, which shall remain binding upon us.
5. 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.

6. 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 namely "Prevention of Corruption Act 1988".

7. We certify that we have not made any changes from the contents of the RFP/EOI document read with its amendments/clarifications provided by the Company submitted by us in our Bid document. It is further certified that the contents of our bid are factually correct. We also accept that in the event of any information / data / particulars proving to be incorrect, the Company will have the right to disqualify us from the bid.

8. We understand that you are not bound to accept the lowest or any Bid you may receive.

9. The vendor herby undertakes that its name does not appear in any "Caution" list of RBI / IBA or any other regulatory body for outsourcing activity.

Dated this ..... day of 2026

(Signature) (Name) (In Capacity of)

Duly authorized to sign Bid for and on behalf of

Annexure IX: Project Timelines

Bidders need to provide project time line for the below mentioned milestone

	W1	W2	W3	W4	W5
Description					
Project Plan					
Deployment of Resource					
Training					
Installation and Configuration					
Integration of various devices & security solutions					
UAT					
Final Signoffs					

********************End of RFP********************