बड़ौदा ग्लोबल शेयर्ड सर्विसेज लिमिटेड
Baroda Global Shared Services Ltd.
(A wholly owned subsidiary of Bank of Baroda)

Request for Proposal [RFP] For

Selection of Managed Security Service Provider for implementing comprehensive C-SOC services.

RFP NO: BGSSL/RFP/IT/2024-25/03
Dated: 10th May, 2024

Registered office:
5TH Floor, Baroda Sun Tower,
C -34,G Block, BKC, Bandra East, Mumbai -400051

Corporate Office:
27th Floor, GIFT One Tower, Road - 5C,
Zone-5, GIFT CITY
Gandhi Nagar, Gujarat – 382355

Table of Contents

1. Introduction

1.1. Invitation for Tender offers

Baroda Global Shared Services Limited (herein after termed as BGSSL or Company), wholly owned subsidiary of Bank of Baroda, invites sealed tender offers (Eligibility, Technical bid and Commercial bid) from eligible, reputed entities for **RFP for Selection of Managed Security Service Provider for implementing comprehensive C-SOC services,** the term bidder/ prospective bidder refers to the primary bidder participating for delivering services/goods mentioned in the scope of works.

Complete set of tender documents may be downloaded by eligible bidder from the website of the Company. The Company reserves the right to reject any or all offers without assigning any reason.

Technical Specifications, Terms and Conditions and various formats and proforma for submitting the tender offer are described in this document, Annexures and Appendices.

1.2. About the Company

Established in the year 2017, Baroda Global Shared Services Ltd., a Company having its Regd. Office at 5th Floor, Baroda Sun Tower, C-34, G-Block, Bandra – Kurla Complex, Bandra (E), Mumbai 400051 , India and Corporate Office at 21st/27th Floor, Tower 1, GIFT City, Gandhinagar, Gujarat - 382355 (herein after referred to as a 'Company') is a wholly owned subsidiary of Bank of Baroda, a large public sector bank having global presence with its vast network of over 9,500+ branches.

1.3. Information Provided

This document contains statements derived from information believed to be reliable at the date obtained but does not purport to provide all the information that may be necessary or desirable to enable an intending contracting party to determine whether or not to enter into a contract or arrangement with the Company in relation to the **RFP for Selection of Managed Security Service Provider for implementing comprehensive C-SOC services**. Neither the Company nor any of its employees, agents, contractors, or advisers gives any representation or warranty, express or implied, as to the accuracy or completeness of any information or statement given or made in this document.

1.4. For Respondents Only

The document is intended solely for the information of the party to whom it is issued ("the Recipient" or "the Respondent").

1.5. Confidentiality

The Invitation document is confidential and is not to be disclosed, reproduced, transmitted, or made available by the Recipient to any other person. The Invitation document is provided to the Recipient on the basis of undertaking of confidentiality given by the Recipient to Company. Company may update or revise the document or any part of it. The Recipient acknowledges that any such revised or amended document shall be received subject to the same confidentiality undertaking. The Recipient will not disclose or discuss the contents of the document with any officer, employee, consultant, director, agent, or other person associated or affiliated in anyway with Company or any of its customers or suppliers without the prior written consent of Company.

This document is meant for the specific use by the Company/ bidder. This document in its entirety is subject to Copyright Laws. The Bidders or the Recipients or the Respondents, as the case may be, will be held responsible for any misuse of information contained in the document, and are liable to be prosecuted by the Company in the event that such a circumstance is brought to the notice of the Company. By downloading the document, the interested party is subject to the confidentiality clauses herein.

1.6. RFP disclaimer

This Request for Proposal containing Annexures and subsequent Addenda and Corrigenda (Herein after called as RFP or tender) has been prepared solely for the purpose of enabling the Company to select a Service Provider for **RFP for Selection of Managed Security Service Provider for implementing comprehensive C-SOC services**. As per specifications, terms and conditions and scope defined in this RFP (herein after referred as **RFP for Selection of Managed Security Service Provider for implementing comprehensive C-SOC services.**

The bidder will be required to be innovative, capable and would need to extend all their resources and services in order to meet the expectation of the Company towards providing the required services.

This RFP document is not a recommendation, offer or invitation to enter into a contract, agreement or other arrangement in respect of the supply and services as per the scope of this RFP.

In such instances wherein the BGSSL may need any further documents from respective Service Provider during the entire term of its Selection of bidders to render Services/goods, the Service Provider shall be under an obligation to provide the required documents as and when demanded by the Company.

1.7. Important Details (Schedule of Events, contact & communication details etc.)

1.	RFP No.	**BGSSL/RFP/IT/2024-25/03**
2.	Brief Description of the RFP	**RFP for Selection of Managed Security Service Provider (MSSP) for implementing comprehensive C-SOC services**
3.	Company's Address for Communication and submission of Tender	Online Submission of Tender Baroda Global Shared Services Ltd.
4.	Date of publishing the tender on Baroda Global Shared Services Ltd (BGSSL)'s website **www.bgss.in**	10th May, 2024
5.	Last date of submission of Queries for Pre-Bid Meeting	16th May, 2024 Before 6:00 pm
6.	Date & Venue of Pre-Bid Meeting	Pre- Bid meeting will be carried out on virtual basis with bidders who have submitted the queries to BGSSL E-mail ID **Vendormgmt@bgss.in** Query to be submitted Before due date of pre-bid query last date.
7.	Last date & time for submission of Bids	*30th May, 2024, Before 3:00 pm*
8.	Date and time of Opening of Eligibility andTechnical Bid	Since submission of bids are online, Technical & Eligibility documents will be opened by BGSSL and acknowledgment will be communicated to the participating bidders via email
9.	Date and time of Opening of CommercialBid	The commercial bids of only those vendors who qualify in both eligibility and technical evaluation will be opened. The date for opening of the commercial bid would be communicated separately to the technically eligible bidders.
10.	Bid document cost (non-refundable) Tender Fees	*Rs. 5,000/-*
11.	EMD	Rs. 7,50,000/-
12.	Contact Person for any clarification	Manager – IT & Procurement Baroda Global Shared Services Ltd. LL: 079-61800352 Mobile no. 84889 68633

<table>
<tr><td></td><td></td><td>Email ID: vendormgmt@bgss.in</td></tr>
<tr><td>13</td><td>Online Submission</td><td>Kindly submit documents online thru
https://eauction.auctiontiger.net/EPROC/
For any queries while submitting kindly connect with
<table>
<tr><th>Name</th><th>Phone Number</th><th>Email Id</th></tr>
<tr><td>Hiral Purohit</td><td>6352631968</td><td>hiral.purohit@eptl.in</td></tr>
<tr><td>Utkarsh</td><td>6352632098</td><td>utkarsh@eptl.in</td></tr>
<tr><td>Manish Pathak</td><td>9265562819</td><td>manish.p@eptl.in</td></tr>
<tr><td>Mubassera Mansuri</td><td>7859800621</td><td>mubassera@eptl.in</td></tr>
<tr><td>Fahad Khan</td><td>6352631766</td><td>fahad@eptl.in</td></tr>
</table>
Important Note :
If you are participating first time on AuctionTiger, Kindly register your profile on portal - https://eauction.auctiontiger.net/ & once profile has been registered kindly contact above mentioned support team for Profile approval and Bidder mapping in subjected event.</td></tr>
</table>

The above dates are tentative and subject to change without any prior notice or intimation. Bidders should check website www.bgss.in for any changes / addendums to the above dates and/or any other changes to this RFP. Bidders to confirm with Company the time & venue -1- day prior to any of the above scheduled events. All processes will be done electronically/online.

The services of selected vendor can automatically be availed by Bank of Baroda and all its subsidiaries, basis terms and conditions of the requirement and in line with the cost identified for the said RFP.

1.8. Costs to be borne by bidders

All costs and expenses incurred by Bidders in any way associated with the development, preparation, and submission of their responses to the RFP, including but not limited to attendance at meetings, discussions, presentations, demonstrations, etc. and providing any additional information required by the Company, will be borne entirely and exclusively by the Bidder and the Company shall not liable for any costs and/or expenses in relation to responses to the RFP and/or shall not entertain any requests / representations regarding bearing/sharing of costs and /or expenses. The Bidder acknowledges and agrees to bear all financial obligations incurred in connection with their participation in the RFP process.

1.9. Legal Relationship

No binding legal relationship will exist between any of the Bidders and the Company until execution of a definitive legal agreement.

1.10. Right to Reject Bids

BGSSL reserves the absolute and unconditional right to reject the response to this RFP if it is not in accordance with its requirements and no correspondence will be entertained by the BGSSL in the matter. The bid is liable to be rejected if:

a) It is not in conformity with the instructions mentioned in the RFP document.
b) It is not accompanied by the requisite Application Money and Earnest Money Deposit (EMD), if applicable.
c) It is not properly or duly signed by authorized signatories.
d) It is received after the expiry of the due date and time.
e) It is incomplete including non- furnishing the required documents. It is evasive or contains incorrect information.
f) There is canvassing/lobbying/influence/cartelization, etc. of any kind.
g) It is submitted anywhere other than the place mentioned in the RFP.

1.11. Technical Proposal Attention Items

i. This RFP is not a contract offer. Receipt of a proposal neither commits BGSSL to award a contract to any Bidder, nor limits BGSSL's rights to negotiate with any Bidders, suppliers or contractors in BGSSL's best interest. BGSSL reserves the right to contract with any Bidder, supplier or contractor at its own discretion.
ii. BGSSL reserves the right to request additional information necessary and pertinent to the project so as to assure the Bidder's ability and qualification to perform the contract.
iii. Failure to answer any questions within stipulated timeline at any stage of this RFP may be considered non-responsive and the proposal may be disqualified.
iv. For any ambiguity, omissions or unclear content in the RFP the Bidders should request BGSSL to clarify along with pre-bid queries within the time line mentioned in the "[A] Important Dates.
v. For all technical details and relevant standards and specifications of this RFP that may not be stated in detail; Bidders should ensure and provide quality and industrial standard products to BGSSL.
vi. In case of any difference in the standards between this RFP and the Bidders' proposal, the higher standards shall prevail and be applicable.
vii. Expenses incurred in the preparation of proposals in response to this RFP are the sole responsibility of the selected Bidders.
viii. BGSSL reserves the right to accept or reject any and all proposals, or any part of any proposal, without penalty. Any allowance for oversight, omission, error, or mistake by the selected Bidder made after receipt of the proposal will be at the sole discretion of BGSSL.

1.12. Disqualification

Any form of canvassing/lobbying/influence/cartelization, etc. by the Bidder may result in disqualification of such Bidder.

1.13. Information Confidentiality

All information contained in this RFP is strictly confidential. The Bidder shall not share this information with any other person/party not connected with responding to the RFP or even with other potential Bidders. The information contained in the RFP or subsequently provided to Bidder(s), whether verbally or in writing by or on behalf of Company shall be subject to the terms and conditions set out in the RFP and any other terms and conditions subject to which such information is provided.

1.14. Recipients' Obligation to Inform Itself

It is the Recipient's sole and whole responsibility to conduct all necessary investigation and analysis regarding any information contained in the document and the meaning and impact of that information. The Company shall not be held liable for any consequences arising from the Recipient's failure to diligently fulfill this obligation.

1.15. Evaluations of Offers

Each Recipient acknowledges and accepts that the Company may, in its sole and absolute discretion, apply whatever criteria it deems appropriate in the selection of organizations, not limited to those selection criteria set out in this document. The issuance of document is merely an invitation to offer and must not be construed as any agreement or work order or arrangement nor would it be construed as material for any investigation or review to be carried out by a Recipient. The Recipient unconditionally acknowledges by submitting its response to this document that it has not relied on any idea, information, statement, representation, or warranty given in this document.

1.16. Errors and Omissions

Each Recipient should notify the Company of any error, omission, or discrepancy found in this documents within 7 days from the date of issuance of this RFP. Every such notification should be communicated to the email address provided by the Company under Clause 1.7 i.e., Important Details (Schedule of Events, contact and communication details, etc.), of this RFP document.

1.17. Acceptance of Terms

The purpose of the RFP is to provide necessary information to the potential Bidders, who qualify and intend to submit their response to the RFP. Though the RFP has been prepared with sufficient care and diligence with an endeavor to provide all required information to the potential Bidders, Company acknowledges the fact that the potential Bidders may require more information than what has been provided in the RFP. Accordingly, in such cases, the potential Bidder(s) may seek additional information/clarification required from Company. Company reserves the right to provide such additional information/ clarification at its sole discretion. In order to respond to the RFP, if required, and with the prior permission of Company, each Bidder may conduct their own study and analysis, as may be necessary, at their own cost and expense ensuring they adhere to the timelines mentioned in the RFP. No additional time will be provided to Bidders to undertake any analysis or study.

Company makes no representation or warranty and shall incur no liability, whatsoever, under any law, statute, rules or regulations on any claim the potential Bidder may make in case of failure to understand the requirement and respond to the RFP.

Company may, in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information given in the RFP and specify additional user requirements or cancel the RFP at any time without assigning any reason thereof and without any notice.

While due care has been taken in the preparation of this document, Company will not be held responsible for any inaccuracy in the information provided herein. The recipient/potential bidders of the RFP must apply its judgment, care and conduct its own investigation and analysis regarding any information contained in the RFP document including but not limited to the scope of work, Deliverables and timelines, etc.

It is the Bidder's responsibility to:

A. Properly understand and examine the RFP;

B. Examine all other information available on reasonable inquiry relevant to the risks, contingencies and circumstances affecting its response;

C. Satisfy itself as to the completeness, correctness and sufficiency of its response;

The Bidder shall, by responding to the Company's RFP document, be deemed to have fully read, understood and accepted all the terms as stated in this RFP document.

1.18. Liabilities of the Company

The Company and its directors, officers, employees, contractors, representatives, agents, and advisors make no representations or warranty with regard to the - accuracy, reliability or completeness of this RFP Document. They disclaim all liability from any loss, claim, expense (including, without limitation, any legal fees, costs, charges, demands, actions, liabilities, expenses or disbursements incurred therein or incidental thereto) or damage, (whether foreseeable or not) ("Losses") suffered by any person acting on or refraining from acting because of any presumptions or information (whether oral or written and whether express or implied), including forecasts, statements, estimates, or projections contained in this RFP Document or conduct ancillary to it whether or not the losses arises in connection with any ignorance, negligence, inattention, casualness, disregard, omission, default, lack of care, immature information, falsification or misrepresentation on the part of the Company or any of its directors, officers, employees, contractors, representatives, agents, or advisors. The information contained in this RFP Document is selective and the Company may in its absolute discretion, but without being under any obligation to do so, update, modify, mend, or supplement or withdraw the information in this RFP Document.

This Invitation is not an offer by the Company, but an invitation for Bidders responses. No contractual obligation on behalf of the Company whatsoever shall arise from the invitation process unless and until a formal Purchase Order/Work Order is signed and executed by duly authorized officials of the Company and the selected/empanelled bidder (i.e., Vendor).

Willful misrepresentation of any fact within the Bid by the Bidders will lead to the cancellation of the definitive agreement, without prejudice to the other actions that the Company may take. All the submissions, including any accompanying documents, will become the exclusive property of Baroda Global Shared Services Ltd.

2. Requirements Summary

2.1. Intent

The Company is issuing this RFP document (hereinafter referred to as "the RFP" which expression shall include all attachments and annexures hereto as well as all amendments, addendums, modifications and alteration hereto) to prospective bidders, (hereinafter referred to as "the Bidder") to enable them to participate in the competitive bidding for **RFP for Selection of Managed Security Service Provider for implementing comprehensive C-SOC services**.

The bidder will be required to be innovative, capable and would need to extend all their resources and services/ goods in order to meet the expectation of the Company towards the desired results.
The Company at its discretion reserves the right to change the scope of the RFP considering the size and variety of the requirements and the changing business conditions.

2.2. Tenure

The appointment of the selected firm for providing Managed Security Services C-SOC shall be initially for a period of Three years & renewable thereafter for Two years on mutually agreed basis.

2.3. Language

The **RFP for Selection of Managed Security Service Provider for implementing comprehensive C-SOC services** should be in English. However it should have the capability to support certain communication templates in Hindi language. This capability shall be a part of standard offering of the **RFP for Selection of Managed Security Service Provider for implementing comprehensive C-SOC services** including report printing by the Company users. The data in the database will be stored in English language.

3. Scope of Work

The objective of the project for BGSSL (Baroda Global Shared Services Ltd) is to enhance and streamline the cyber security posture and operational efficiency of BGSSL's Cyber Security Operations Centre (C-SOC) by outsourcing the monitoring and management of various critical security solutions and services to a Managed Security Service Provider (MSSP). This strategic move aims to ensure round-the-clock monitoring and management of cybersecurity threats, vulnerabilities, and incidents, thereby significantly reducing the risk of cyber-attacks and data breaches.
The BGSSL, for this purpose, invites proposal from bidders for primarily undertaking inter-alia the activities mentioned under the section 3 – Project Scope; for the BGSSL in respect of implementing and maintaining the C-SOC (Cyber Security Operations Centre) using SIEM, EDR/XDR/MDR, Vulnerability scanners, Security Analytics Platform, Security Orchestration Automation and Response (SOAR) platforms and other tools or platforms: -
The proposed solution should be scalable so as to support legacy applications used by our Company.
Project Scope: The broad project scope includes having System Integrator (SI) for designing, setting up, implementing, and maintaining the proposed Managed C-SOC solution operations on 24x7x365 basis. The selected Bidder is expected to perform all activities pertaining to C-SOC operations as per global best practices.

The scope of work includes, but not limited to the following:

3.1. General Scope of work

1. The Proposed solution should be on standard platform, In case of Software platform, bidder should be responsible to provide the required Licenses.
2. The solution must automate internal health checks and notify the user in case of problems.
3. The Proposed solution should have capability to collect logs from most of the standard platforms like Microsoft Windows, Linux (All variants), MAC OS, AIX, Solaris, Firewalls, Network, other security devices or

solution, identified database servers, endpoint security management servers, web application firewalls, network firewalls, Active Directory servers, Web servers, Private cloud (VMware, Open Stack) & cloud services (AWS/Azure/GCP/Others), SAAS Solutions, O365, etc.

4. The Proposed SIEM solution should act as common data lake for Correlation, SOAR, NDR, UEBA and threat hunting.
5. The SIEM platform should have capability to provide automatic Notification to SOC teams (MSSP + BGSSL) as defined in playbooks based on Conditional decision & trigger Functions.
6. The Proposed solution should have inbuilt security mechanism for protecting itself from security attacks including encryption of Data in Transit and At Rest.
7. The proposed solution should have physical or logical separation of the collection module, logging module and analysis / correlation module with the ability for adding more devices, locations, applications, etc. (High Availability).
8. The proposed solution must support caching mode of transfer for data collection, so as to ensure data is being logged in the event loss of network connectivity, and resume sending of data upon network connection.
9. The proposed solution must be able to collect data from new devices added into the environment, without disruption to the ongoing data collection.
10. The proposed solution must provide for secure user access via HTTPS, SSH.
11. The proposed solution must have a user-friendly interface to convert statistical results to dashboards with a single click and should able to integrate with any 3rd party / Open source SIEM.
12. The proposed solution must be able to monitor and report user and privileged users access activities.
13. The Proposed solution must offer all of the below built-in threat detection techniques out of the box: (1) Detect Web Application Threats. (2) Detect advanced persistent threat (APT) Threats. (3) Integrate with leading Honeypot solutions. (4) Integrate with leading Network Behavior Anomaly Detection (NBAD), Network Detection and Response (NDR) tools. (5) Give visibility of endpoints also by integrating with Endpoint Detection and Response (EDR), Data Loss Prevention (DLP), Host Intrusion Prevention System (HIPS), and Antivirus etc. for endpoint analytics. (6) Integrate with Security Orchestration, Automation, and Response (SOAR) tools for automation. (7) Integrate with leading Threat Intelligence Platform (TIP) (8) User and Entity Behavior Analytics (UEBA).
14. The proposed solution must provide a query interface that allows users to search for data stored within the solution.
15. The solution shall be able to capture all details in raw log, events and alerts and normalize them into a standard format for easy comprehension and it should be able to parse and filter logs based on type, date, etc.
16. In addition to the advanced analytics capabilities like Managed detection and response (MDR), solution should have capabilities to define rules on event logs captured from various sources to detect suspicious activities Examples but not limited though: (1) Failed login attempts. (2) Login attempts from suspicious locations. (3) Authorization attempts outside of approved list. (4) Vendor logins from unauthorized subnets. (5) Vertical & Horizontal port scans. (6) Traffic from blacklisted IPs. (7) Login attempts at unusual timings.
17. The solution must have an incident and change management review framework for incident and change management. Review framework to facilitate tracking, investigation, pivoting and closure.
18. The proposed solution must be able to read data input from the following static log file formats: (a) Archived Log Files (Single line, Multi-line, and Complex XML and JSON Structure). (b) Windows Events Logs. (c) Standard Log Files from applications such as Web (HTTP) servers, FTP servers, Email (O365/Others), SMTP relay, DNS servers, DHCP servers, Active Directory servers, etc.
19. The solution must be able to provide the capability to fully customize alerts, reports and dashboards to the business requirements.
20. The solution must allow tracking of incidents from correlation rule through investigation of that event to closure.
21. The proposed solution must come with out-of-the-box integration and dashboards, reports, rules etc., to provide rapid insights and operational visibility into large-scale UNIX and Linux environments machine data: syslog, metrics and configuration files.

22. The solution must be able to provide the capability to annotate events, modify status, and build a chronological timeline for the incident before and after a triggered event.
23. The proposed solution must be able to run any search on a schedule and set alerting conditions based on thresholds and deltas in the number and distribution of events.
24. The solution should support integration with industry-leading threat intelligence sources and provide a mechanism to apply threat intelligence to logs and events for analysis.
25. The solution should be able to create and apply rules and policies that define appropriate action to be taken based on defined criteria.
26. The solution should provide a capability to manage and monitor security-related incidents and investigations from a centralized console.
27. The solution must support the use of machine learning algorithms for behavior analysis and anomaly detection.
28. The proposed solution must support secure transmission of logs over encrypted channels (e.g., TLS/SSL).
29. The offered solution must provide a central management interface for Components such as SIEM, SOAR, EDR/XDR/MDR, Threat Management, and Case Management. Further, the solution should have administrative functions from a web-based user interface for SIEM, SOAR, and all related modules in the current phase of implementation. The Management appliance/server of SIEM and SOAR along with all required software, and licenses shall be provided by the Bidder in the solution.
30. The Solution should provide End Point Protection (EPP) and Endpoint Detection and Response (EDR) capabilities for Windows, Linux, and Mac.
31. The Solution should provide the capability to Isolate or block various network components.
32. The Solution should provide the capability to do encryption to protect user data from unauthorized access.
33. The Solution should provide the capability to manage the personal firewall of endpoints.
34. The SOAR Solution must be in a single dashboard as of SIEM.
35. Threat Intelligence Feeds shall be included with the SIEM & SOAR solution.
36. The solution must readily support 500 + out of the box integration with different technologies solutions.
37. The proposed solution must be scalable and should not have any limitation on number of incidents as well as actions on integrated platforms.
38. SOAR solution must streamline app development with our intuitive drag-and-drop interface, designed for efficiency and ease of use.
39. The Solution should design complex workflows effortlessly with visual workflow designer, enabling seamless integration of processes and tasks.
40. The solution must carry out data enrichment based on endpoint triggers and automate the process by getting details from various sources deployed in organization.
41. The solution must provide automated response by quarantine, isolating host, capture memory dump etc. as part of endpoint actions.
42. The solution must securely store and manage files within the platform, providing easy access and organization for all your data needs.
43. The solution must safeguard sensitive authentication data with robust encryption, ensuring the highest levels of security and compliance.
44. The solution has a marketplace for a wide range of apps, integrations, and extensions, expanding the capabilities of SOAR solution.
45. SOAR can be utilized for daily status updates. SOAR can be used for updating the Tickets automatically of Vulnerabilities.
46. The Solution should provide layered endpoint protection with Fake Credentials to Trap, Malware identification, Intrusion prevention, Behavior analysis, End Point Deception, Automated remediation, Endpoint isolation and it should work on windows, Linux and Mac.
47. The proposed solution has the incident management/ticketing system workflow, and the solution shall support creating incidents automatically based on the rules defined and tracking them.
48. The Solution must provide threat intelligence feed (free and commercial) for identifying new global threats the globe as DDoS (Slowloris or LOIC etc.), Malicious IP Addresses, Domains, URLs, Filename, File hash, Email

address, Known C&C (Command and Control) hosts, Geolocation feeds like latitude and longitude, AS Number, ISP, Country, etc.

49. The Solution should Provide proactive threat intelligence and threat hunting services across network endpoints and anomalous user behavior to detect advanced attacks like lateral movement, malware beaconing, data exfiltration, watering hole, process anomalies, service anomalies, account takeovers, etc.
50. Assessment of threat intelligence feeds for their effectiveness and efficiency on a regular basis and changing threat intelligence feeds provider if required
51. The solution should proactively inform about potential security threats/vulnerabilities, and new global security threats/ zero-day attacks in circulation and suggest and implement suitable countermeasures to safeguard client assets and data against such evolving threats/attacks along with the analysis.
52. The solution should have advance capabilities to predicting attacks and able to gather low-false positive threat intelligence on adversary tactics, indicators etc.
53. The solution should be able to support early alerts and notify operations team without impacting the business-critical systems
54. The solution should implement real-time alert mechanisms to notify security operations teams of potential threats.
55. The solution should be able to assign multiple IP addresses across subnets to network decoys through static IP addressing.
56. The solution should automatically detect scanning and L2 attacks such as ARP flood and IP scan etc.
57. The solution should support synchronization of time with NTP servers and push the same on decoys
58. Any interfaces/custom connectors required for integration to be developed by the solution provider for successful SOC implementation at no extra cost to client
59. The solution should provide capabilities to centrally publish reports from various scanners and manual security testing
60. The solution should provide Vulnerability dash boarding based on the various assets
61. The solution should allow the creation of workflows to assign various vulnerabilities for remediation.
62. The solution should allow to remove the de-duplicates when assets are scanned using multiple scanners
63. The solution Should support attack simulation for testing the effectiveness of the security controls
64. The solution should support attack simulation scenarios for various operating systems such as windows, Linux and Mac.
65. The solution should provide the capability to define the control requirements inline to ISO 27001, RBI guidelines and other leading best practices.
66. The solution should support the creation of web-based policies and procedures required for security practices
67. The solution should support the various User awareness campaigns, emails, quizzes, wallpaper, videos, graphics etc.
68. The solution should provide the capabilities to perform and document table top exercises.
69. The Managed security service providers (MSSP) shall consolidate functions of incident monitoring, detection, response, coordination, and computer network defense tool engineering, operation, and maintenance.
70. The MSSP will be responsible for the comprehensive vulnerability assessment of the internal network and infrastructure, application, to maintain the integrity and security of BGSSL's IT ecosystem, that involves conducting regular Vulnerability Assessment and Penetration Testing (VAPT) to pinpoint weaknesses across networks, systems, and web applications; executing web application security assessments to identify security flaws in web-based applications; engaging in Red Team activities to simulate cyber-attack scenarios against BGSSL's digital assets, thereby testing the resilience of security measures and incident response protocols; and performing network security assessments to uncover vulnerabilities, misconfigurations, and security issues within the network infrastructure.
71. In the event of a security incident, the MSSP will be tasked with swift and thorough investigation and analysis. They must determine the nature, scope, and potential impact of each incident, enabling informed decision-making regarding response actions. Following predefined incident response procedures, the provider promptly initiates appropriate mitigation measures to contain and remediate the incident. Additionally, they

ensure that incidents are escalated to the appropriate personnel within the organization or external stakeholders as necessary, facilitating effective coordination and resolution.

72. To maintain the efficacy of their security operations, the MSSP should continuously fine-tune and optimize their monitoring and detection system. This includes refining SIEM rules, correlation logic, and alert thresholds to minimize false positives and maximize detection accuracy. Additionally, the provider optimizes the configurations of security tools based on evolving threats and organizational requirements, ensuring that resources are allocated effectively to address the most significant risks.
73. The MSSP will be committed to continuous improvement, regularly reviewing and assessing their SOC operations to identify areas for enhancement. By fostering a culture of continuous improvement, the provider helps the organization to stay ahead of evolving cyber threats and maintain a resilient security posture.
74. The MSSP should ensure that all security measures, tools, compliance, and services comply with industry best practices, regulatory requirements, and BGSSL's internal policies and standards, to maintain a strong and compliant security posture.
75. The MSSP should provide various levels of management reports to the BGSSL and implementing Escalation Matrix in order to handle Information Security Incidents efficiently.

3.2. Broader Scope of Work

The selected Bidder is expected to perform all activities pertaining to C-SOC operations as per global best practices including but not limited to:

3.2.1. Activity 1 – Event Review

The purpose of this activity is to provide you with on-going alert management for the SIEM System. SIEM monitoring will be performed by the SIEM Analyst.

1. Monitor alerts and policy exceptions (security events) generated by the SIEM System as per coverage agreed;
2. Identify critical events as notified by SIEM dashboard;
3. Fine-tune rules and reduce false-positives;
4. Enable/disable out of the box correlation rules as appropriate;
5. Provide remediation/countermeasure recommendations, if applicable;
6. Adjust alert prioritization options based on criticality;
7. Perform analysis of potentially critical security alerts; and
8. Perform updates to existing policy rules and define new rules as per the evolving threats;
9. Create, test and initial tuning of correlation/custom rules;
10. Test cases for custom rules and event monitoring;
11. Perform activities for reporting;
12. Send offense data to the Ticketing System for conversion into a ticket by the ticketing system that is owned and managed by the Service Provider.
13. Periodically review tickets generated in MSSP's ticket system and closure comments for any fine tuning of security policies/rules/correlation rules and submit a report on action need to be taken for further improvement of incident raising and its resolution.

3.2.2. Activity 2 – Reports Generation, Review, and Analysis

The follow activities for reporting requirements:

1. Generate reports as per pre-decided frequency and monthly MIS report;
2. Review and analyze reports;
3. Perform analysis of potentially harmful security alerts based on report data.
4. Upload log files and reports electronically and in their native formats to a central repository provided for audit purposes and manage report distribution.
5. Performing root cause analysis (RCA) and submission of RCA report for security incidents as per Bank's

requirement.

6. To submit Gap analysis report for deployed security solutions.

3.2.3. Activity 3 - Tool Management:

The purpose of this activity is to provide on-going management, tuning, report generation, and maintenance of currently deployed and solutions deployed as per the scope.

1. Manage user access including user and group permissions updates
2. Review system disk space usage and verify data collection
3. Roll-out of new agents / perform new configuration for deployed solutions as per BGSSL's requirement
4. Harden C-SOC systems, Server, Firewall, Network device and etc., as and when applicable
5. Update / upgrade systems and related security tool agents deployed in endpoints / servers.
6. Security tools optimization & fault management along with restoration test.
7. Provide inventory of the systems to asset management team
8. Monitoring of the deployed tools including utilization of storage, CPU, RAM, interfaces etc.
9. Modify approved changes (configuration / policies) as per change requests;
10. Provide timely updates on available patches / signature / versions from OEM for deployed security solutions.
11. To perform architecture review for deployed solutions and propose / execute required changes after obtaining required approvals from competent authority;
12. Preparation, Review and Management of C-SOC asset inventory;
13. To ensure uptime and round the clock availability for all deployed security solutions in C-SOC and Co-ordinate with OEM for support in case of any issue
14. To submit root cause analysis report for downtime (if any) for all security solutions deployed in C-SOC.
15. To conduct RCA and submit RCA report for high priority incidents identified through different solutions deployed in C-SOC.
16. To conduct Gap analysis for deployed security solutions;
17. Troubleshooting deployed solutions in case of any performance degradation / solution unavailability / solution downtime.
18. To conduct DC – DR Cut-over / Cut-back activity for deployed solutions as and when required.
19. To manage Storage Area Network (SAN) deployed for long term storage of logs pertaining to Security Solutions.
20. Ensure sufficient storage space availability on deployed SAN solution to ensure log retention as per BGSSL's requirement.
21. Management of Network switches / related infra deployed for connecting C-SOC solution to BGSSL's Network.
22. Health monitoring of C-SOC solutions.
23. Monitor the logs collected from different log sources for security threats.
24. Process reengineering for continual improvement of deployed solutions.
25. Perform research and investigation if any tool does not perform as expected.
26. Manage all the C-SOC infra including but not limited to all the hardware, software, appliances, Virtual infra, Storage infra, TOR switches etc., for smooth functioning of tools and C-SOC operations.
27. Indicative Security Solution Services and Frequency of Delivery is defined as follows:

C-SOC Security Solution Management	
Activity Detail	**Indicative Frequency of Delivery**
Systems, Servers, Firewalls, Network devices, Etc., Hardening	As and when required
Update/Upgrade/Patching	As and when required

Backup/Restore	As per the policy defined by BGSSL
Configuration Management	As and when required
Configuration Review & Performance Tuning	As and when required
Incident/Change Management	As and when required
Access Management	Continuous
Manual /SOP Preparation and Review	As per the policy defined by BGSSL
Device Problem Management	As and when required
DR Drill of Security Solution	As and when requested by client
Inventory Management	Continuous
Creation / modification of Custom policies	Continuous
Integration with IT / IS infrastructure (Existing/Future)	As and when required
Monitoring policies	Continuous
Custom Reports	As and when required

3.2.4. Activity 4 - Security Incident & Event Management (SIEM):

The purpose of this activity is to provide on-going management, tuning, report generation, and maintenance of the SIEM solution including but not limited to the following:

1. The solution should have a High Availability feature built in. There should be an automated switch over to secondary collectors/Agent server in case of failure on the primary collector/Agent Server.
2. The SIEM tool should be capable of sending automated email and SMS as other modes of communication for alerts related to critical incidents.
3. The solution provider should provide 24X7 monitoring & Security Analysis of the infrastructure through SIEM solution.
4. The solution provider should patch the SIEM systems and related components as and when required in case new updates are available and new vulnerabilities are identified.
5. Log should be retained for a period of 6 months online, 1 year offline and shall be available for querying.
6. Technologies proposed to be deployed by bidder and OEMs should leverage self-learning, analytics models powered by Artificial Intelligence / Machine Learning (AI/ML) and should be capable of handling extremely high IOPS without latency.
7. The SIEM tool can be either software based, or appliance based. In case of Software based SIEM solutions, bidder shall bundle necessary hardware. OEM must certify that the hardware proposed by the bidder is sufficient to cater to the RFP requirement. Hardware proposed in both cases should be rack mountable with dual power supply and should comply with Data Centre Standards.
8. In case if SIEM device does not support application / DB / device out of the box, in that case Bidder should include cost of development of parser and ensure that application / Database / device are integrated with SIEM solution. Further any new application / Database device should be able to integrate with SIEM.
9. Individual report should be provided for integrated servers, network & security devices, configured rules, application logs, incidents, alerts and other security reviewed systems/processes.
10. In case the BGSSL changes network architecture, SIEM should be able to integrate accordingly.
11. Integrate devices with SIEM solutions, create custom parsers, configure DSMs, and customize dashboards.
12. Proposed SIEM solution should act as common data lake for Correlation, SOAR, NDR, UEBA and threat

hunting.

13 Solution should able to integrate with any 3rd party / Open source SIEM.
14 Check suspicious IPs for risk scoring, recommend new security configurations, and utilize security intelligence data to prioritize incidents.
15 Conduct asset discovery, perform root cause analysis for security incidents, and submit RCA reports.
16 Maintain blacklist/whitelist IPs and approved whitelist URLs, assess suspicious IPs for risk scoring, and recommend new security configurations based on global best practices.
17 Utilize expertise and security intelligence data to correlate activity patterns, associate behavior with known attacks, and classify and prioritize incidents accordingly.
18 The SIEM solution must offer a web-based interface for viewing BGSSL Network security events, registering incidents across all event sources, and providing drill-down capabilities to analyze attack patterns comprehensively. Its dashboard should include filtering options for events based on criteria such as geographical location, device type, and attack type.
19 The purpose of this activity is to provide on-going management, tuning, report generation, and maintenance of the SIEM solution including but not limited to the following:
20 Manage user access including user and group permissions updates;
21 Review application performance, capacity, and availability make recommendations as appropriate;
22 Review and manage SIEM System capacity management, Verify log collection.
23 Regularly backup logs as per defined backup and archival frequency; and Restore logs as required or for the purpose of testing.
24 Provide problem determination / problem source identification for SIEM System for activities including but not limited to the following:
   a. Creating Tickets as required and tracking progress of open Tickets;
   b. Managing Incidents to resolution / closure, in accordance with established procedures and subsequently closing Ticket upon resolution;
   c. Providing escalation and exception handling for Incidents, consistent with established procedures as per defined matrix;
   d. Review SIEM OEM announcements & manage SIEM system update;
   e. Schedule and test application upgrades and install application patches and software updates in order to improve performance, or enable additional functionality;
25 Customize / create dashboard; Submission of RCA for security incident
26 Asset Discovery and maintenance of integrated asset inventory;
27 Performing root cause analysis (RCA) and submission of RCA report for security incident as per BGSSL's requirement.
28 Individual report should be provided for integrated servers, network & security devices, configured rules, application logs, incidents, alerts and other security reviewed systems/processes.
29 Maintaining blacklist/whitelist IPs and approved whitelist URLs.
30 Check suspicious IP's for risk scoring (1-10) before forwarding for blacklisting.
31 Recommend new security configurations based on the global best practices.
32 To utilize expertise and security intelligence data to correlate activity patterns with signature severity to associate their behavior with known attacks. The function leverages intelligence & attack analysis and source & target determination to classify and prioritize incidents.

3.2.5. Activity 5 – PCAP / Forensic Solution

The purpose of this activity is to provide on-going management, tuning, report generation, and maintenance of the PCAP / Forensic solution including but not limited to the following:

1 The purpose of this activity is to provide on-going management, tuning, report generation, and maintenance of the PCAP / Forensic solution including but not limited to the following:
1 To maintain the solution and conduct forensic analysis on as per BGSSL's requirement and help BGSSL to conduct forensic analysis activities.

2 To conduct the activity in a structured fashion using global best practices for conducting forensic analysis. Methodologies and deployed Forensic tool to be handled by the vendor for conducting the forensic analysis.
3 To follow defined process for the management of the evidences that are collected during the forensic analysis.
4 To submit detailed analysis reports (RCA), summary reports, evidences collected in scientific manner, etc. as required in forensic analysis activity in such a manner that it is producible on any legal / regulatory forum by BGSSL, with assurance of non-repudiation, audit trail evidences, required by forensic best practices. The forensic report should be admissible as per the domestic and foreign legal framework**.**

3.2.6. Activity 6 – Deception (Decoy) Solution

The purpose of this activity is to provide on-going management, tuning, report generation, and maintenance of the Deception (Decoy) solution including but not limited to the following:

1 Create social engineering profiles that will be used as the decoys;
2 Maintain deployed decoys placed on high-value target end-point / network etc.
3 Maintain deployed threat intelligence decoys as per internet facing landscape of BGSSL;
4 Configure and manage reports and alerts, as applicable;
5 Analysis of alerts generated in the solution console or in SIEM, investigate the hit on configured decoy and submit RCA as applicable.

3.2.7. Activity 7 – Data Leakage Prevention (DLP) and Data Classification Solution

The purpose of this activity is to provide on-going management, tuning, report generation, and maintenance of the Data Leakage Prevention (DLP) solution and Data Classification solution including but not limited to the following:

1. Review existing Data classification policies and suggest improvements.
2. Define the scope and risk associated with sensitive data.
3. Configure the policies as per the requirement.
4. Troubleshoot the policy and tool related issues.
5. Customize the policies to reduce false positives based on the input from client
6. Configure DLP violation alerts as per the requirement and technical feasibility.
7. Exception creation as per the requirement.
8. Prepare reports at periodic frequency.
9. Compliance to regulator guidelines issued from time to time with respect to information security and sensitive data handling including but not limited to masking of PII data.
10. Performing regular whitelisting as per approved process and release of quarantined messages.
11. To discover sensitive data (discovery scan) across an IP range.

3.2.8. Activity 8 – Web Application Firewall (WAF) Solutions

The purpose of this activity is to provide on-going management, tuning, report generation, and maintenance of the deployed Web Application Firewall (WAF) solutions including but not limited to the following:

1 On alerts generated in the WAF solutions console or in SIEM, investigate application access attempts that lead to the alerts;
2 Perform analysis on specific events generated in the solution to determine attempts to attack the applications as well as false positives received;
3 Perform policy changes for fine-tuning policies;
4 Update logs that are integrated with the SIEM;
5 Configure alerts as per the requirement and technical feasibility;
6 Prepare reports at periodic frequency;
7 On-boarding new application in WAF solution as per BGSSL's requirement & enabling blocking mode of security filters for managing HTTPS traffic.

8 Analyzing WAF console for irregular traffic / hits / attacks to block threats.
9 Configuration and Review of policies to cover all attacks including but not limited to top 10 OWASP attacks.
10 To perform testing to identify vulnerabilities that include OWASP top 10 attack
11 Keep track of renewal of SSL certificate expiry of on-boarded applications.

3.2.9. Activity 9 - SSL Off-loading Solution

The purpose of this activity is to provide on-going management, tuning, report generation, and maintenance of the SSL Off-loading solution including but not limited to the following:

1 Configure the policies as per BGSSL's requirement.
2 Review of configured policies, traffic forwarding issues and setup new policies and suggest improvements.
3 Keep track of renewal of SSL certificate expiry.
4 Exception creation as per the requirement.
5 Prepare reports at periodic frequency.

3.2.10. Activity 10 – Database Activity Monitoring (DAM) Solution

The purpose of this activity is to provide on-going management, tuning, report generation, and maintenance of the Database Activity monitoring (DAM) solution including but not limited to the following:

1 Configuration of policies / rules / agent deployment on Database servers / node addition in solution console for enforcing access control and proper rights management on databases.
2 Monitoring access to databases, database activities, alerting / blocking unauthorized access/activities.
3 Reporting of deviations to the policies defined in DAM solution.
4 Solution monitoring for detecting unusual Database activities including read, write, delete etc. and to review configured policies & suggest improvements.
5 Exception creation as per the requirement.
6 Prepare reports at periodic frequency.

3.2.11. Activity 11 - Security Monitoring:

The purpose of security monitoring is to continuously observe and analyze the network, systems, and applications of an organization to detect and respond to potential security threats and incidents effectively including but not limited to the following:

1 The proposed solution has the incident management/ticketing system workflow and the solution shall support creating incidents automatically based on the rules defined and tracking them
2 Service Provider should monitor, detect, and manage incidents for the following minimum set of IT infrastructure security events. Service Providers should indicate their event list in the proposal response. This is an indicative minimum list and is not a comprehensive/complete set of events
   a. Buffer overflow attacks
   b. Port & vulnerability scans
   c. Password cracking
   d. Worm/virus outbreak
   e. File access failures
   f. Unauthorized server/service restarts
   g. Unauthorized changes to firewall rules
   h. Unauthorized access to systems
   i. SQL injection
   j. Cross-site scripting

3.2.12. Activity 12 - Comprehensive Incident Management Solution:

The incident management solution should be designed to efficiently register and respond to security events, providing seamless trouble ticket generation and lifecycle management. Solution should include but not limited to the following:

1 Provide incident management services including identification, analysis, response, remediation, and reporting within the defined timelines for all identified incidents.
2 Support BGSS handling incidents that could involve containment/eradication/recovery/root cause analysis
3 Identify the origin of the threat, online root cause analysis, mitigation steps, and measures to prevent recurrence, utilizing network/host forensic techniques
4 Report the identified incidents to respective teams and ensure closure of identified incidents
5 The incidents shall be reported based on the SLAs defined in BGSS information security policies
6 Prepare reports and dashboards to present the incident monitoring activities status to top management
7 Reporting and logging of information security events and incidents using proposed ticketing tools. Track and monitor the closure of these information security events and incidents and Escalation of these events and incidents to appropriate teams/ individuals in the organization.
8 Service Providers 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 BGSS
9 To carry out 24x7 real-time monitoring, logging, and analysis of security events
10 To analyze and correlate the security logs for real-time alerts on violations, attack, or unusual behavior
11 To automatically detect incidents based on the rule-based alerts being generated by the SIEM tool.
12 To provision a dedicated incident dashboard, which shall provide a systematic view of the various tickets along with their criticalities.
13 To implement a suitable incident escalation matrix for handling Information Security Incidents effectively.
14 To provision a ticketing tool for monitoring the various information security incidents and assigning the same as per the escalation matrix. The ticketing tool shall have the functionality to ensure that the incident is assigned to appropriate personnel.
15 To monitor the closure of the information security incidents and escalation of these incidents with the concerned team. Service Provider shall build capability for automatic closure of incidents wherever possible.
16 To enable security orchestration across multiple stakeholders for effective remediation of security incidents
17 To enable automated remediation of security incidents wherever possible using a defined playbook on the SOAR platform.
18 To maintain an internal repository of the various cyber security incidents
19 To carry out user and network behavior analysis of incidents.
20 To provision analytics tools to apply data analytics techniques (AI & ML) for carrying out effective incident response.
21 To carry out basic forensic analysis & investigation and malware analysis for incidents requiring in-depth postmortem, attribution, or legal action.

3.2.13. Activity 13 - Network Insight Solution Management, Security Orchestration and Response Services:

The objective of this initiative is to ensure continuous oversight, optimization, reporting, and upkeep of the Network Insight solution, encompassing, but not restricted to, the subsequent tasks:

1 Investigate alerts triggered within the solution console or Security Information and Event Management (SIEM) platform, focusing on ongoing cyber-attacks.
2 Conduct thorough malware detection and analysis to identify and mitigate potential threats.
3 Identify and address insider threats, lateral movement, and network-based attacks in real-time.
4 Implement measures to detect and prevent data exfiltration attempts, safeguarding sensitive information.
5 Identify and track malware hashes traversing the network for proactive threat mitigation.
6 Review existing rules within the Network Insight solution and SIEM platform for efficacy and relevance.
7 Configure additional rules as per the specific requirements outlined by BGSSL (insert full form if available) to enhance threat detection capabilities.
8 Continuously refine rule sets based on evolving security landscape and organizational needs.
9 **Security Orchestration and Response Services:** the Service Provider shall administer and manage security

orchestration and response services for automating low-level security incidents. The Service Provider shall at a minimum carry out the following activities:

10 Define policies and rules for classifying incidents and automating responses to low-level security responses
   a. Define escalation policies for specific issues that require human intervention or require deeper analysis
   b. Manage low-level incidents and false alarms by automating responses and standard operations
   c. Provide monthly reports of all incidents managed and escalated through SOAR tools
   d. Half-yearly review of rules and policies.

3.2.14. Activity 14 - Anti-Advanced Persistent Threat (Anti-APT) Solution Management:

The primary objective of this role is to oversee the continuous management, optimization, reporting, and upkeep of the Anti-Advanced Persistent Threat (Anti-APT) solution. The responsibilities include but are not limited to:

1 Proactively monitor alerts generated within the Anti-APT solution or the Security Information and Event Management (SIEM) system.
2 Conduct thorough investigations into detected attacks in real-time.
3 Utilize event playback functionalities to analyze incidents and understand the scope and impact of potential threats.
4 Conduct comprehensive analysis of connection paths and associated activities to identify potential threats and vulnerabilities.
5 Document and report discovered attempts to connect to the Anti-APT solution, detailing the nature of the attacks and their potential implications.
6 Ensure timely and accurate updates to logs integrated with the SIEM system, maintaining a comprehensive record of security events and activities.
7 Configure alerts within the Anti-APT solution based on specific requirements and technical feasibility, ensuring that critical security events are promptly identified and addressed.
8 Collaborate with incident response teams to develop and execute effective mitigation strategies in response to identified security incidents, minimizing the impact and preventing recurrence.
9 Ensure adherence to relevant regulatory requirements, industry standards, and organizational policies governing the management of advanced persistent threats and related security measures.

3.2.15. Activity 15 - File Integrity Monitoring (FIM) Solution Management

This role is responsible for the ongoing management, optimization, report generation, and maintenance of the File Integrity Monitoring (FIM) solution. Key responsibilities include, but are not limited to, the following:

1 Configure policies within the FIM solution to control access to files and track all changes, including file movement, copying, or content modifications**.**
2 Troubleshoot policy issues and create exceptions as required by BGSSL's specifications to ensure smooth operation of the FIM solution.
3 Fine-tune and configure policies to align with regulatory compliance standards, particularly PCI-DSS, ensuring that file integrity monitoring meets industry regulations and requirements.
4 Employ a range of cryptographic generation algorithms to detect evasion tactics exploiting signature weaknesses.
5 Monitor the FIM solution console to detect changes and deviations from established baselines, facilitating the early detection of file alterations or unauthorized activities.
6 Integrate newly commissioned high-priority devices into the FIM solution, ensuring comprehensive coverage and monitoring capabilities across all critical endpoints and nodes.
7 Provide support for incident response activities by leveraging FIM data to investigate security incidents, identify root causes, and implement remediation measures.
8 Maintain comprehensive documentation of FIM configurations, policies, exceptions, and incident reports, and generate periodic reports to communicate security posture and compliance status.
9 Conduct training sessions and knowledge-sharing initiatives to enhance the skills and capabilities of SOC

personnel in effectively utilizing and managing the FIM solution.

10 Apply, modify, and add exceptions to policies on nodes and endpoints within the FIM solution, ensuring that security rules are effectively enforced while accommodating specific operational needs.
11 Capable of grouping servers based on service and applying uniform policies, even across different operating systems and applications.
12 Integrate with SIEM to track changes and provide detailed event logs, including the chain of events, user attribution, and timestamps.

3.2.16. Activity 16 - Threat Intelligence, Threat Hunting and Dark Web Monitoring Service:

This service should be designed to monitor Threat Intelligence Feed and Dark Web activities, encompassing the following:

1 Service Providers must provide threat intelligence feed (free and commercial) for identifying new global threats the globe as DDoS (Slowloris or LOIC etc.), Malicious IP Addresses, Domains, URLs, Filename, File hash, Email address, Known C&C (Command and Control) hosts, Geolocation feeds like latitude and longitude, AS Number, ISP, Country, etc.
2 Proactively inform about potential security threats/vulnerabilities, and new global security threats/ zero-day attacks in circulation and suggest and implement suitable countermeasures to safeguard BGSS assets and data against such evolving threats/attacks along with the analysis.
3 Ensure classifications of threats and attacks.
4 Unlimited static and dynamic malware analysis.
5 Provide proactive threat intelligence and threat hunting services across network endpoints and anomalous user behavior to detect advanced attacks like lateral movement, malware beaconing, data exfiltration, watering hole, process anomalies, service anomalies, account takeovers, etc.
6 Ensure monitoring of Malware Scanning / Protection / Presentation / Reporting
7 Ensure Anti-Phishing and Anti-APT services are available as part of the SOC services and must be monitored.
8 User behavior analytics should be a part of SOC services. User behavior analytics for detecting abnormal behavior of users on network and hosts
9 The Service Provider should have capabilities to perform advanced threat detection and threat hunting using artificial intelligence and machine learning models.
10 To aggregate threat feeds and prioritize Indicators of Compromise (IOCs) in a single threat management platform for accelerated triage, response, and remediation. The threat feeds shall be shared with BGSS & security devices of the Data Centre.
11 To analyze the incidents/logs from SIEM and analytics platform with pattern-based analysis and manual deductive approach to identify potential threats
12 To correlate, investigate, and suspect anomaly behaviors of attackers before a compromise turns into a full-on breach
13 To detect and identify advanced threats by using security analytics including analytics such as user behavior analytics & network behavior analytics.
14 To apply behavioral analysis to a large volume of data sets
15 To analyze the security logs to protect against known/unknown sources of threats
16 To integrate APIs with alerting systems, threat intelligence, SOAR platforms, ticketing systems, and log sources
17 Provisioning interactive visualizations to effectively analyze information
18 To maintain and share an analyst knowledge database across the team
19 The Service Provider shall build the capability to identify and detect new, emerging, and unknown threat vectors. This is in addition to identifying and detecting already known Threat Vectors (e.g. Vishing, Social Engineering, Anti-Phishing Services, Anti-APT, etc.). The intelligence that the Service Provider builds in the security analytics should be able to build an emerging threat pattern and help prevent it before it manifests into an attack.
20 The Service Provider shall conduct threat hunting exercises in the infrastructure of the BGSS. The Service

Provider shall ensure that the rules configured in the SIEM tool are updated to detect the latest threats

21 Threat Intelligence should deliver a comprehensive range of timely adversary and technical threat intelligence through a customizable portal or Dashboard
22 Threat Intelligence should provide data feeds and APIs for automated consumption by the SIEM Tool
23 Threat Intelligence provided must be relevant, context-rich, timely, and accurate
24 Threat Intelligence feeds should contain who, how, and why you are being targeted
25 Threat Intelligence to provide reputation data feeds for actionable intelligence on IP addresses and Domains/URLs exhibiting malicious activity such as malware distribution and botnet command and control server communication. The data feeds should be derived from activity on the Internet and a reputation score along with additional contextual attributes should be provided for each of the IP addresses and Domains/URLs.
26 The Service Provider shall provide integration with threat intelligence feeds (free and commercial) to provide the latest information on (indicative list): (a). Malicious IP addresses (b). Malicious Domains/URLs (c). Malware C2s (d). Banking Botnets related to IOCs (e). DDOS Botnet IOCs (f). Phishing (g). Ransomware
27 Latest Vulnerabilities a. Miners etc. b. Suspicious domains c. Malware signatures d. IP addresses and URLs associated with malicious activity
28 ML/AI analytics for threat investigations and adding more context to the security incidents.
29 Assessment of threat intelligence feeds for their effectiveness and efficiency on a regular basis and changing threat intelligence feeds provider if required.
30 Monitor and Respond to Threat Intelligence Inputs: Receive and act upon inputs from Threat Intelligence feed providers, leveraging available data to proactively identify, mitigate, and remediate security threats.
31 Derive Actionable Insights: Analyze threat feeds to derive actionable insights for preventing emerging threats to the IT infrastructure.
32 Customize Rules Based on Threat Intelligence: Tailor security rules based on insights gleaned from Threat Intelligence feeds, ensuring relevance and effectiveness.
33 Provide Customized Security Advisories: Regularly track global security threats and vulnerabilities, advising the BGSSL on potential upgrades or changes to its security infrastructure. Advisories should be customized to suit the BGSSL's specific security needs and environment.
34 Integrate with SIEM: Integrate threat intelligence feeds directly into the Security Information and Event Management (SIEM) system using APIs or other automated methods. Demonstrate alignment of threat intelligence with the banking scenario. The number of integrated threat intelligence feeds is tied to Service Level Agreements (SLAs).

3.2.17. Activity 17 - Network Access Control (NAC) Solution Management:

The SOC provider will be responsible for managing, optimizing, generating reports, and maintaining the Network Access Control (NAC) solution on an ongoing basis. This includes, but is not limited to, the following tasks:

1 Ensure that users and devices accessing BGSSL’s network are securely authenticated and authorized.
2 Monitor access attempts rigorously, permitting entry only to devices authorized by BGSSL's policies.
3 Assess configured protocols and policies to establish and enforce rules governing network access for devices and users.
4 Configure new policies within the NAC solution in accordance with BGSSL’s specific requirements. Modify existing policies as necessary to adapt to changing security needs.
5 Regularly review configured policies to identify areas for improvement and implement enhancements to bolster network security posture.
6 Address NAC policy exceptions as required by BGSSL, customizing policies to accommodate unique operational or security demands.
7 Deploy NAC configuration on switches as needed, ensuring seamless integration and consistent enforcement of access control measures.
8 Generate reports at predefined intervals, documenting NAC activities, policy adjustments, and compliance status for review and audit purposes.

3.2.18. Activity 18 - Vulnerability Management & Penetration Testing (PT/WASA):

The SOC provider is tasked with the ongoing management, vulnerability scanning, report generation, and maintenance of the Vulnerability Management (VM) solution. This includes, but is not limited to, the following:

1 To assess the vulnerability of internal assets / devices / Web Applications / Etc., by conducting vulnerability assessment at defined frequency / ad-hoc basis across internal IP network ranges. Vulnerability scan should include applicable network ranges, using deployed scanning tools to identify known vulnerabilities (for example, backdoors, security patch level, CGI-Bin, e-mail, Web, and file transfer protocol ("FTP").
2 To analyze and document scan findings and recommendations to be included in the Vulnerability Assessment Report;
3 To prepare and submit Vulnerability Assessment Report;
4 Reduce False positives;
5 Exclude accepted vulnerabilities for the defined period of time in the VA report.
6 To analyze multiple scans and prepare trend and ageing analysis of vulnerabilities.
7 To perform discovery scans.
8 The Penetration Testing must include Network PT of internet-facing devices/servers and Web Application Security Assessment (WASA) of websites hosted on the Internet. The network penetration testing should include but not be limited to activities like identification of all existing services running on the device/server, determination of open ports and the level of access on them, and listing of all vulnerabilities that are visible to the external world, as well as providing Vendors to fix those vulnerabilities. The bidder should also provide the list of CVEs applicable as per the BGSS environment.
9 The WASA should be carried out to check the security weaknesses including, but not limited to, the latest top 10 Open Web Application Security Project (OWASP) vulnerabilities. Web applications on Internet-facing web servers may be of different platforms (JSP, ASP, PHP, .NET, etc.) hosted on different types of web servers (Oracle, Apache HTTP/Tomcat, IIS, etc.) and running on different Operating systems (Windows, Linux etc.).
10 The IP addresses of the network devices may be either IPv4 or IPv4/IPv6 dual stack. The IP addresses of devices configured as IPv4/IPv6 dual stack has been considered as single IP address. The penetrating testing shall be conducted for both IPv4 and IPv6 address to identify any configuration security weaknesses in the network devices.
11 The PT/WASA shall be external to the network and will be performed remotely simulating non-destructive external hacking attacks to test the current security of the network and web applications. The bidder should ensure that there is continuity of services during the PT/WASA. In case of any disruption in data or services or business continuity is detected, the bidder shall share with BGSS, the details of test cases/payloads used.
12 The penetration testing shall be preferably conducted during off-hours/non-peak times and mutually agreed between the bidder and BGSS. The bidder shall give prior intimation to the BGSS team about the start and end time of the PT/WASA activity.
13 The bidder will perform the Remote PT/WASA from the public domain (Internet) to find out vulnerabilities in network devices and web applications hosted on the Internet.
14 IP addresses of devices for which penetration testing is to be conducted shall be provided to the successful bidder(s) at the time of conducting PT/WASA activity.
15 The method for Penetration test will be "Black Box, Non-Destructive & Non-privilege" mode.
16 Bidder may run a series of tests conducted like information gathering from the public domain, port scanning, system fingerprinting, service probing, vulnerability scanning, manual testing, password cracking, IDS/IPS testing, Router/Firewall testing, etc. The tools used for the testing shall be state-of-the-art latest versions of tools and techniques, which are used by hackers with an objective to unearth vulnerabilities and weaknesses of the IT infrastructure. These tools shall be run in such a way that it does not affect the availability of the running systems/services of BGSS
17 Web applications and websites hosted on the Internet shall be tested for security weaknesses like cross-site scripting, SQL injection, invalidated inputs, etc. The industry benchmark standards including, but not

limited to, the latest top 10 OWASP vulnerabilities must be followed to highlight vulnerabilities that exist in web applications

18 The vendor should be able to carry out a Penetration Test for IPv6 IP addresses also. The IPs mentioned by BGSS may be either IPv4 or IPv6 or both, depending upon the type of devices/services running and IPs assigned to it.
19 The vendor should be able to carry out Penetration test for all type of Operating Systems, Appliances, and Applications available in BGSS, which are exposed to the Internet
20 The vendor shall complete the PT/WASA activity for the IPs/Domains
21 The vendor shall provide Recommendations/Guidelines on types of corrective actions to plug the vulnerabilities.
22 In case of revalidation, the vendor shall conduct the revalidation testing and submit the report within 5 days from the date of the duly filled, signed, and sealed revalidation request.
23 After completion of the PT/WASA activity and revalidation (if requested) by the vendor the vendor shall obtain the duly filled, signed, and sealed completion certificate
24 BGSS will designate a single point of contact from their location to coordinate the penetration testing activities with the vendor and to handle any emergency situation. The contact person details shall be exchanged at the time of the Award of the Work Order.
25 Additionally, a demonstration of penetration (if possible) as a Proof of Concept (only to prove possibility and not to cause real damage) may be given.
26 After revalidation (if requested) by BGSS, the vendor will be required to recheck/revalidate the vulnerabilities and re-submit the final report within 5 days
27 To ensure timely payments, the vendor shall ensure all the required documents and deliverables are provided as per BGSS's schedule and requirement.

3.2.19. Activity 19 - Red Team Assessment and Social Engineering:

The SOC solution should provide robust capabilities for Red Team Assessment and Social Engineering exercises. It should support regular simulations of social engineering attacks to assess employee awareness and response readiness. The solution should enable scenario-based testing to mimic real-world threats and evaluate the effectiveness of security measures. It should also offer comprehensive reporting and recommendations for enhancing security posture based on assessment outcomes.

1 The vendor shall be responsible for delivering social engineering exercises every quarter for a year and should be able to capture statistics to measure the success of the exercise
2 Vendor and BGSS are required to determine a target list of BGSS's employees and the scenarios used for social engineering. The vendor should be able to develop scenarios based on BGSS's environment, newsworthy events, and previously successful attacks
3 Vendor should be able to perform email and phone based social engineering campaigns
4 Vendors using social engineering should be able to harvest BGSS's employees' credentials
5 The Vendor should support low and advanced level of phishing exercise not limited to just Email
6 The vendor should have the capability to personalize and gamified to make the learning process for efficient and engaging
7 The Vendor should provide multiple scenarios for creating phishing campaign not just limited to spear-phishing, ransomware, or CEO fraud
8 The Vendor should have support of more than 15 languages for creating phishing scenarios
9 The Vendor should have inbuilt templates for creating phishing campaigns and also have capability to run a wizard for the creation of phishing campaigns and templates
10 The Vendor should have the capability to schedule the campaign to run in the near future and use the smart campaigns option to address multi-level of awareness per employee automatically.
11 The Vendor should provide a dashboard for each phishing campaign.
12 The Vendor should provide customize report in CSV, PDF, etc. format
13 The Vendor should have the capability to install a plugin with Outlook or any other email client for reporting

any phishing incident

14 The vendor must use non-destructive methods necessary to accomplish a set of jointly agreed-upon mission objectives while simulating attacker behavior.
15 Assessment must be done in the Company's production environment against a realistic, "no-holds barred" attacker.
16 The scope of the assessment must cover the internal security team's ability to prevent, detect, and respond to incidents in a controlled and realistic environment.
17 The vendor must closely mimic a real attacker's active and stealthy attack methods by using Technic, Tactics, and procedure (TTP) seen on real, recent incident response engagements in order to assess the security team's ability to detect and respond to an active attacker scenario.
18 Vendors must adopt a fact-based risk analysis and recommendations approach.
19 Objective and Scope of Red Team operations must be mutually agreed upon between consultant and the company. The vendor should apply industry experience to identify objectives that represent primary risk to the company's core business functions
20 The engagement must follow the phase of the attack life cycle which minimally should consist of Initial Compromise, Establish Foothold, Lateral Movement, and Complete Mission
21 Vendors must leverage a combination of proprietary intelligence repositories as well as industry leading commercial threat intelligence tools and techniques throughout the engagement.
22 The scope of engagement should include testing of the company's detection and response capabilities.

3.2.20. Activity 20 - Audit, Mock-drill and Cyber drill, Cyber Crisis Management Plan (CCMP), BCP / DR Drills, Advisory and MITRE Attack Framework:

Ensuring audit compliance, conducting drills, managing crises, maintaining continuity, providing advisory services, aligning with frameworks, and facilitating continuous improvement. This includes, but is not limited to, the following:

1 **Audit and Compliance Oversight:** Conduct audits to ensure adherence to security standards and regulations, with prompt resolution of identified issues.
2 **Mock-Drills and Cyber Exercises:** Simulate cyber threats to assess response capabilities and identify vulnerabilities, followed by remediation actions.
3 **Cyber Crisis Management Plan (CCMP):** Develop and implement a comprehensive plan to effectively manage and mitigate cyber incidents, including communication and escalation protocols.
4 **Business Continuity Planning (BCP) and Disaster Recovery (DR) Drills:** Testing resilience against disruptions through scenario-based exercises, ensuring continuity of critical operations.
5 **Advisory Services and Threat Intelligence:** Staying informed about emerging threats and regulatory changes, with proactive guidance on security measures and compliance.
6 **MITRE Attack Framework Alignment:** Aligning security strategies with the MITRE Attack Framework to enhance threat detection and response capabilities.
7 **Continuous Improvement:** Regularly review and update security measures, processes, and protocols to adapt to evolving threats and maintain effectiveness.
8 **Asset Management and Documentation:** Maintain accurate inventory and documentation of security assets and resources for efficient management and compliance purposes.

3.2.21. Activity 21 - Governance, Risk & Control (GRC) Solution

The objective of this activity is to ensure the continuous management, tuning, report generation, and maintenance of the Governance, Risk & Control (GRC) solution. This encompasses various tasks, including but not limited to:

1 Leveraging the GRC solution for comprehensive governance purposes.
2 Implementing access and process controls, as well as managing risks through the GRC solution.
3 Continuously customizing and optimizing the GRC solution to ensure alignment with the BGSSL's compliance and regulatory needs.

3.2.22. Activity 22 – Antivirus Monitoring

1 Monitor and control the execution of applications to prevent unauthorized or malicious software from running.
2 Identifies and blocks attempts to exploit vulnerabilities in the system.
3 Monitors files and processes in real-time for any malicious activity.
4 Provides advanced monitoring and response capabilities to detect and respond to security incidents on endpoints.
5 Analyzes the behavior of applications and processes to identify and block suspicious activities.
6 Monitors web traffic in real time to block access to malicious websites and phishing attempts
7 Scans email attachments and content for malware and other threats.
8 Monitors network traffic and enforces firewall rules to prevent unauthorized access.
9 Monitors and controls the use of external devices such as USB drives to prevent the spread of malware.
10 Monitor the centralized console to manage security settings across the network.
11 Monitors critical system files for any unauthorized changes or tampering.
12 Monitors and controls the transfer of sensitive data to prevent data breaches.
13 Monitors and protects mobile devices against malware and other security threats.
14 Extends protection to cloud environments by monitoring and securing cloud-based resources.

3.2.23. Activity 23 - File server Auditing and Analysis

1 Monitor and audit file and folder access activities.
2 Track who accessed specific files or folders, when, and from where.
3 Keep track of user activities on the file server.
4 Monitor file and folder creations, modifications, deletions, and permission changes.
5 Audit changes in file and folder permissions.
6 Identify users who modify permissions and the changes made.
7 Identify and monitor sensitive data within files.
8 Receive alerts for activities involving sensitive information.
9 Set up real-time alerts for critical file server events.
10 Receive notifications for unauthorized access or changes.
11 Generate comprehensive reports on file server activities.
12 Access dashboards for visualizing trends and patterns in file access.
13 Track file versions and changes over time.
14 Retrieve historical data on file modifications.
15 Identify and monitor data owners for specific files and folders.
16 Track changes in ownership
17 Monitor changes to file content to ensure data integrity.
18 Detect unauthorized modifications to critical files.
19 Analyse and report on user access permissions.
20 Identify users with excessive or inappropriate access rights.
21 Generate reports to demonstrate compliance with data protection regulations.
22 Meet audit requirements by providing detailed file server activity logs.
23 Utilize behavioural analytics to identify unusual or suspicious user activities.
24 Detect potential security threats based on user behaviour patterns.
25 Archive and restore files for data recovery purposes.
26 Ensure data availability and integrity.
27 Integrate with Security Information and Event Management (SIEM) systems for centralized monitoring.
28 Correlate file server events with broader security intelligence.
29 Generate instant email notifications when there is a sudden spike in failed attempts to modify or delete business-critical files.
30 Stay aware of indicators of compromise, such as a file activity during non-business hours, and more.

3.2.24. Activity 24 - Active Directory Monitoring

1 Monitor user and account management (Create, modify, and delete)
2 Monitor Enabled, Disabled, and Locked user account status.
3 Monitor OUs and Create, modify, and delete OUs to organize and manage objects in AD.
4 Automate user provisioning and deprovisioning processes.
5 Perform bulk operations on user accounts.
6 Import user data from CSV files for mass changes.
7 Generate reports on user modifications, including changes to attributes.
8 Track changes to user accounts over time.
9 Monitor and report on permissions assigned to users and groups.
10 Identify users with elevated privileges.
11 Identify and manage inactive user accounts.
12 Generate reports on users who have not logged in for a specified period.
13 Generate reports on group memberships for users.
14 Identify users belonging to specific security or distribution groups.
15 Perform clean-up tasks to identify and remove stale objects.
16 Monitor, Manage, and maintain a clean and efficient AD environment.
17 Create and automate custom workflows for AD tasks
18 Implement approval mechanisms for critical changes.
19 Monitor GPO Policies and Link or unlink GPOs to OUs.
20 Delegate specific AD tasks to non-administrative users.
21 Define roles and permissions for delegated tasks.
22 Generate reports on user logon activities.
23 Monitor user logon patterns and locations.
24 Generate reports to demonstrate compliance with regulatory requirements.
25 Track changes and activities for audit purposes.
26 Enable users to reset their passwords securely and monitor the same.

3.2.25. Activity 25 - Network Monitoring

1 Create customized dashboards to visualize key performance metrics.
2 Monitor specific devices or performance parameters on a single screen.
3 Monitor and analyze event logs from servers and devices.
4 Identify and respond to critical events and security incidents.
5 Visualize the network topology with interactive maps.
6 Identify the relationships between devices and their connections.
7 Automatically discover devices on the network
8 Identify and add devices to the monitoring system.
9 Monitor the availability of network devices and servers.
10 Receive alerts for devices that are down or experiencing connectivity issues.
11 Analyze network traffic patterns using NetFlow or sFlow.
12 Identify sources and destinations of traffic for capacity planning.
13 Track the performance metrics of network devices.
14 Monitor CPU usage, memory utilization, and other performance indicators
15 Monitor network bandwidth usage in real time.
16 Identify bandwidth hogs and optimize network performance.
17 Receive real-time alerts for network faults and issues.
18 Diagnose and troubleshoot problems promptly.
19 Manage and track changes to device configurations.
20 Rollback configurations to a previous state if needed.
21 Set threshold values for performance metrics.
22 Receive alerts when metrics exceed predefined thresholds.
23 Monitor virtual environments, including VMware and Hyper-V.

24 Track the performance of virtual machines and hosts.
25 Monitor the performance of critical applications.
26 Identify bottlenecks affecting application responsiveness.
27 Define and monitor SLAs for network performance.
28 Ensure compliance with service level agreements.

3.2.26. Activity 26 - Syslog / Event log monitoring

1 Monitor logs generated by critical applications.
2 Track application-specific events for troubleshooting and security.
3 Monitor and audit user activities on critical systems.
4 Track user logon/logoff, file access, and other activities
5 Perform log forensics to investigate security incidents.
6 Analyse log data to trace the timeline of events.
7 Monitor changes to configurations and settings in critical systems.
8 Track changes to Active Directory, file servers, databases, etc.
9 Collect logs from various sources, including Windows and Linux servers, network devices, applications, and security appliances.
10 Correlate events in real time to identify patterns or security incidents.
11 Correlation helps in detecting advanced threats and security incidents.
12 Generate predefined reports for compliance with regulations such as PCI DSS, HIPAA, GDPR, and more.
13 Demonstrate adherence to industry-specific security standards.
14 Archive log data for historical analysis and compliance.
15 Retain logs based on regulatory requirements.
16 Search and query log data based on specific criteria
17 Perform ad-hoc searches to investigate security incidents.
18 Set up real-time alerts for specific events or security incidents
19 Receive notifications via email or SMS when critical events occur.
20 Create customizable dashboards to visualize log data.
21 Generate detailed reports on security events, compliance, and system activities.
22 Collect and analyse syslog messages and SNMP traps.
23 Correlate syslog events with other log data for a holistic view.
24 Analyse user behaviour to detect anomalies and insider threats
25 Identify deviations from normal behaviour patterns.

3.2.27. Activity 27– Shadow CISO

The purpose of Shadow CISO is to advise leadership on cybersecurity matters, challenging assumptions, supporting special projects, and mentoring staff.

1 Support in developing and updating the ISO 27001 policy, procedure, and process to align the latest version ISO27001:2022
2 Provide recommendations for improving security posture through technology, processes, and people
3 Help in the creation, review, and update of information security policies, standards, and guidelines
4 Ensure compliance with regulatory requirements and industry standards like ISO 27001
5 Conduct and assist in cybersecurity risk assessments.
6 Provide guidance on risk mitigation strategies and prioritization.
7 Support the Incident Response Team in planning, response, and recovery activities.
8 Offer insights for post-incident analysis to prevent future breaches
9 Advise on security considerations in vendor selection and management processes.
10 Assess third-party services and products for compliance with the organization's security policies.
11 Provide input on the design and implementation of security architectures.
12 Recommend security tools and technologies to enhance defense capabilities
13 Mentor internal security staff, enhancing their skills and knowledge.
14 Provide cybersecurity leadership and decision-making support across departments.

3.2.28. Activity 28 – Phishing Campaign & User Awareness

The purpose of a phishing campaign is typically to deceive individuals into divulging sensitive information such as passwords, credit card numbers, or other personal data. User awareness initiatives aim to educate individuals about the dangers of phishing and how to recognize and avoid phishing attempts. By raising awareness and providing training on best practices for identifying and responding to phishing attacks, organizations can empower employees and users to be more vigilant and resilient against such threats.

1. Launching monthly awareness campaign; measuring & communicating training feedback to management
2. Helping in creating knowledge repository & training records for Client
3. Training sessions on a Quarterly basis for all employees along with Quiz.
4. Create engaging and informative security awareness training content tailored to various roles within the organization
5. Update training materials regularly to reflect the latest threats and security practices.
6. Provide feedback and targeted training to individuals who fall victim to simulations.
7. Train employees on how to recognize and promptly report security incidents or suspicious activities.
8. Provide guidance on the initial steps to take in the event of a suspected breach
9. Educate staff on relevant regulatory requirements and the importance of compliance.
10. MSSP vendor will understand the BGSS environment
11. MSSP will run tool based phishing campaign on a monthly basis.

3.3. Licenses and Hardware

1. Bidder will be solely responsible to arrange all the required Hardware, Software or any other related components that are required to run C-SOC Services.
2. The Company will not be responsible or liable for any infringements or unauthorized use of the licensed products by the Bidder in performance of any activity/obligations undertaken by the Bidder in terms of this RFP. In the event of any claims against the Company for any license related issues, the selected Bidder will have to act upon the same and all liabilities and claims whatsoever will have to be settled by the selected Bidder.
3. Further if the selected Bidder has missed out providing any required licenses to the Company, then the Company will not bear any additional amount for procurement of such licenses at a later date.
4. The selected Bidder is required to consider the Technical Support of the Solution and related application / System for the period of contract from day one.

3.4. Implementation Methodology

The selected Bidder should follow a suitable methodology for delivering the requirements of the RFP for the entire contract period. Accordingly, the Bidder should factor for necessary effort and team deployment. The methodology should clearly lay out the overall steps from initiation to closure of this engagement.

3.5. Service Levels and Uptime Assurance:

The Bidder is responsible for completing assigned tasks within agreed timelines and service levels. Failure to meet these standards will result in penalties. The Bidder must adhere to the service level agreements outlined in the Terms and Conditions.

3.6. Terms & Conditions With The Successful Bidder :

3.7. Contract period:

The Contract with the selected Bidder will be valid for a period of 3 years with an option to extend the contract on yearly basis for maximum up to 2 years on the agreed upon price as specified in the commercial bid format as specified.

Bidder has to properly handover all operational activities along with relevant documentation to the BGSSL officials. The contract will be deemed completed only when all the items and services contracted by the BGSSL are provided as per requirement and accepted along with the associated documentation provided to BGSSL's employees; as per the requirements of the contract executed between the BGSSL and the Bidder.

3.8. Subcontracting

The selected service provider/bidder is prohibited from subcontracting or assigning any work, service, or performance under this project to anyone other than its personnel. If subcontracting for specialized services outlined in the scope of work is necessary, it must be explicitly stated in the proposal/response document, including all pertinent details. No work/services may be subcontracted without prior written permission from the BGSSL.

3.9. New Implementation of Tools and Services During Contract Period:

Throughout the contract duration, the BGSSL reserves the right to introduce new tools, technologies, or services. In such instances, the selected Bidder is obligated to furnish operational support for these additional services. The BGSSL will provide the successful Bidder with a three-month prior notice period to facilitate skill development necessary for supporting these new tools, technologies, or services.

3.10. SLA for SOC associated services

The selected Bidder shall establish service levels for the provision of IT services required to support and sustain the services listed below. These service levels aim to ensure that the necessary elements and commitments are in place to consistently deliver IT service support to the BGSSL.

The primary objectives of this Agreement are:

- Clearly defining service ownership, accountability, roles, and responsibilities.
- Providing a clear, concise, and measurable description of the services provided to the BGSSL.
- Aligning expectations of expected service provision with actual service support

Sr. No	Service Area	Accepted Service Level on monthly basis	Penalty	Remark
1	SOC solutions or any component there of (hardware, software, appliances, etc. operated by Service Provider). Impact on Production, demanding immediate attention. Leading to disruption of objective performed by said tools & services.	1) 99.95% and above 2) 99.95% to 97.92% 3) 97.91% to 95.83% 4) Less than 95.82%	NA 1% 5% 10%	The non-availability due to connectivity, power or any act of God shall be excluded.
2	Degradation of SOC solution - Slowing down the operations of any component or solution thereof resulting in delayed detection of incidents and alerts, responses, report generations, etc.	Detection within 15 minutes and Response within one hour after detection.	1% for mutually agreed time frame after the passage of response period. The cap will be 10%for that month.	
3	Downtime of standby / HA components	Alerts within 15 minutes. Response and resolution time of 48 hours	1% for every one hour after end of Resolution period of 48 hours with cap of 10% for that month.	

4	Incident Monitoring and Response till Resolution	24x7 monitoring of security Incidents generated by SOC solution for all in scope devices/systems. Categorization of events into Critical, High, Medium and Low priority shall be carried out in consultation with the selected Bidder.	All Critical, High and Medium priority offenses should be logged as incident tickets mutually agreed upon by MSSP and BGSSL and responded as per below SLAs: Events along with action plan/ mitigation steps should be alerted to designated team's, else penalty will be as per the below SLA: Critical Events: Critical events within 10 minutes of the event identification (email alert & Incident to be raised in ticketing solution). Update should be provided every 30 minutes or as desired by the BGSSL in discussion with the Service Provider till the closure of the incident. Penalty for missing will be as follows: 1-2 events: 2% 3-4 events: 5% 5-6 events: 7% 7 and above events: 10%	

			High Priority Events: High priority events within 30 minutes of the event identification (email alert & Incident to be raised in ticketing solution). Update should be provided every 1 hour or as desired by the BGSSL in discussion with bidder till the closure of the incident. Penalty will be as follows: 1-3 events: 2% 4-6 events: 5% 7 & Above events: 7% **Medium Priority** Medium priority events within 60 minutes of the event identification (email alert & Incident to be raised in ticketing solution). Update should be provided every 4 hours or as desired by the BGSSL in discussion with bidder till the closure of the incident. Penalty will be as follows: 1-3 events : 1% 4-6 events : 2% 7-10 events : 3% 11 and above events: 5% **Low Priority** / Operational Events need to be logged and maintained for reference. An incident ticket need not be raised for such incidents. However these need to be included in the daily reports.	

5	Report and Dashboard	Periodic reports to be provided to BGSSL as defined in the RFP	**Daily Reports:** Critical reports should be submitted as and when required. Timings will be mutually decided.Delay in reporting for daily report for more than 3 hour shall incur a penalty of 3% Weekly Reports: To be decided mutually. **Monthly Reports:** 4th of each month.Delay in reporting by more than 3 days for both weekly and monthly reports shall incur a penalty of 5% of monthly charges Scheduled Reports from Online storage (up to 3 months data) should be generated and displayed on the user screen/ console within 15 minutes else Penalty of 2%. Reports from Online storage (above 3 month data) should be generated and displayed on the user screen/ console within 1 hour else penalty of 2%.	

6	Vulnerability Assessment	The Bidder is expected to provide Vulnerability Assessment Reports with remediation steps. An incident needs to be logged for all vulnerabilities identified and the incident response SLA shall apply for these.	To be conducted for identified devices. Frequency of assessment and devices as per BGSSL requirements. Ad- hoc scan to be conducted as and when required by the BGSSL. Advance notice of 4 hours for VA will be given.Delay in performing VA scan beyond notice period of 4 hours will attract penalty of 2% every 4 hours.Reports for VA within 12 hours and any delay beyond that shall incur a penalty of 2% per 4 hours.Any vulnerability which was present in the plugin of the scanner and was not Selected/ overlooked will lead to penalty of 2% per vulnerabilities. All the above SLA will have cap of 10%.	
7	Governance	The Bidder is expected to conduct a regular review meeting resulting in a report covering details about current SOC SLAs, status of operations, key threats and new threats identified, issues and challenges etc.	Meeting as per Governance model for next Three years to be conducted during the operations phase. A delay of more than three days beyond mutually agreed scheduled meeting will incur a penalty of 1% and so on with cap of 10%	

8	SOC solution management – Version / Release/Upgrades / Patches	The bidder should notify the BGSSL team and guarantee that all layers of the SOC stack— including firmware, software, middleware, etc.—are updated with either the latest version or the previous one (n-1), as required.	A penalty of 2% will be applied for every fortnight of failure to notify the BGSSL of the latest versions/releases/upgrades /patches for the SOC solution upon their release. Additionally, there will be a penalty of 2% for every week of failure to inform the BGSSL of critical security patches for SOC components. Furthermore, a penalty of 2% will be imposed for every week of delay in the implementation process.	
9	Audit of SOC	Examinations of SOC upgrades, infrastructure releases, versions, etc., in accordance with BGSSL and/or policy standards (N-1).	Audit observations regarding updating/patching should be resolved within a mutually agreed timeframe. A penalty of 5% will be levied for every week of delay in implementing critical and important observations notified by the BGSSL. Additionally, a penalty of 1% will be applied for each recurring observation. The maximum penalty per audit cycle is capped at 10% of the monthly charges.	

10	Incident Escalation	Ensure that incidents are escalated according to the timelines outlined in the escalation matrix defined by the BGSSL. Penalties will be applied for delays in incident escalation beyond 30 minutes.	Penalty for missing critical incident escalations: 1-2 events: 2% 3-4 events: 5% 5-6 events: 7% 7 and above events: 10% Penalty for missing high-priority incident escalations: 1-3 events: 2% 4-6 events: 5% 7 and above events: 7% Additionally, penalties will be applied for delays beyond 2 hours in incident escalation. Penalty for missing medium-priority incident escalations: 1-3 events: 1% 4-6 events: 2% 7-10 events: 3% 11 and above events: 5%	
11	Closure of Incidents:	Upon closure of an incident in the ticketing solution, the Bidder team is responsible for analyzing the closure remarks and the provided resolution. The incident should then be marked as closed in the SIEM solution. If the closing remarks are deemed unacceptable, the ticket should be reopened in the ticketing solution.	Penalties will be applied for delays exceeding 1 hour in taking action on closed incidents in the ticketing solution.Penalty for missing critical incident escalations: 1-2 events: 2% 3-4 events: 5% 5-6 events: 7% 7 and above events: 10% Penalty for missing high-priority incident escalations: 1-3 events: 2% 4-6 events: 5% 7 and above events: 7% Additionally, penalties will be applied for delays exceeding 2 hours in taking action on closed incidents in the ticketing solution.Penalty for missing medium-priority incident escalations: 1-3 events: 1% 4-6 events: 2% 7-10 events: 3% 11 and above events: 5%	

12	Database Maintenance	Ensure availability of relevant logs online for the last 6 months. Arrange archived logs available for analysis. Ensure there is no loss of logs. Perform data backup and archiving of logs older than 6 months.	Any deviation from these maintenance tasks will result in a penalty of 1% of the quarterly billing cycle for each quarter until improvement is demonstrated, as indicated in the quarterly review report.	
13	Incidents Assigned to C-SOC Bin	Incidents should be attended on immediate basis as and when the same is assigned to C-SOC team.	Delay in attending as per defined SLA of BGSSL will attract penalty. Penalty for missing critical incident escalation will be as follows: 1-2 events: 2% 3-4 events: 5% 5-6 events: 7% 7 and above events: 10% Penalty for missing High priority incident escalation will be as follows: 1-3 events: 2% 4-6 events: 5% 7 & Above events: 7% Penalty for missing Medium priority incident escalation will be as follows: 1-3 events : 1% 4-6 events : 2% 7-10 events : 3% 11 and above events: 5%	
14	Maintain SOC Team / Staff Attrition	The bidder shall maintain a staff attrition rate of no more than 10% per month. Report immediately if it exceeds above the said limit.	N A	

4. RFP Response Instructions

4.1. Rules for responding to the RFP

All responses received after the due date/time would be considered late and would be rejected. Bidder must furnish requirements as per the formats provided in the RFP document.

4.2. Price

A. The Bidder is requested to quote in Indian Rupee (INR). Bids in currencies other than INR would not be considered. The date for opening of price bids would be communicated separately to the successful bidders post the completion of the technical evaluation

B. The prices and other terms offered by bidders must be firm for an acceptance period of 180 days from the opening of the commercial bid.

C. The prices quoted by the bidder shall be all inclusive, that is, inclusive of all taxes, duties; levies etc. except GST (wherever applicable) will be paid extra. Octroi /entry tax / GST will be paid on actual on production of original receipt. There will be no price escalation during the contract period and any extension thereof. Bid submitted with an adjustable price quotation will be treated as non-responsive and will be rejected.

D. In case of any variation (upward or down ward) in Government levies / taxes / cess / excise / custom duty etc. which has been included as part of the price will be borne by the Bidder. Variation would also include the introduction of any new tax / cess/ excise, etc. provided that the benefit or burden of other taxes quoted separately as part of the commercial bid like GST and any taxes introduced instead of Service tax, VAT and levies associated to Service Tax, VAT or any new taxes (other than excise, custom duties, other duties and associated government levies) introduced after the submission of bidder's proposal shall be passed on or adjusted to the Company. Local entry tax / GST and Octroi will be paid on actuals based on receipt provided. If the Bidder makes any conditional or vague offers, without conforming to these guidelines, the company will treat the prices quoted as in conformity with these guidelines and proceed accordingly. Local entry taxes / Octroi / GST whichever is applicable, if any, will be paid by BGSSL on production of relative invoices / payment receipts / documents. Necessary documentary evidence should be produced for having paid the customs / excise duty/ GST, sales tax, if applicable, and or other applicable levies

E. If any Tax authorities of any state, including, Local authorities like Corporation, Municipality etc. or any Government authority or Statutory or autonomous or such other authority imposes any tax, charge or levy or any cess / charge other than VAT or GST & entry tax or Octroi and if the Company has to pay the same for any of the items or supplies made here under by the Bidder, for any reason including the delay or failure or inability of the Bidder to make payment for the same, the company has to be reimbursed such amounts paid, on being intimated to the Bidder along with the documentary evidence. If the Bidder does not reimburse the amount within a fortnight, the Company shall adjust the amount out of the payments due to the Bidder from the Company along with the interest calculated at commercial rate

F. Terms of payment as indicated in the Purchase Contract that will be issued by the company on the selected Bidder will be final and binding on the bidder and no interest will be payable by the Company on outstanding amounts under any circumstances. If there are any clauses in the Invoice contrary to the terms of the Purchase Contract, the bidder should give a declaration on the face of the Invoice or by a separate letter explicitly stating as follows "Clauses, if any contained in the Invoice which are contrary to the terms contained in the Purchase Contract will not hold good against the Company and that the Invoice would be governed by the terms contained in the Contract concluded between the Company and the bidder".

The Company will consider the Total Cost of Ownership (TCO) over a [Three year period]. –

1. **The bidder will be required to submit commercial bids as part of the bid submission**. The Company would open commercial bids of technically qualified bidders in front of these bidders' representatives after the technical evaluation is completed.

2. **Normalization of bids:** The Company will go through a process of technical evaluation and normalization of the bids to the extent possible and feasible to ensure that bidders are more or less on the same technical

ground. After the normalization process, if the Company feels that any of the bids needs to be normalized and that such normalization has a bearing on the price bids; the Company may at its discretion ask all the technically short- listed bidders to resubmit the technical bids once again for scrutiny. The Company can repeat this normalization process at every stage of technical and commercial submission or till the Company is satisfied. The bidders agree that they have no reservation or objection to the normalization process and all the technically short listed bidders will, by responding to this RFP, agree to participate in the normalization process and extend their co- operation to the Company during this process. The bidders, by submitting the response to this RFP, agree to the process and conditions of the normalization process.

3. **The Price offer shall be on a fixed price basis.** Bid submitted with an adjustable price quotation will be treated as non-responsive and will be liable to be rejected. The rate quoted by the bidder should necessarily include the following:
   I. The terms and conditions of the RFP and subsequent contract.
   II. The Bidder must provide and quote for the product and services as desired by the Company as mentioned in this RFP. Any products / services not proposed to be provided by the Bidder will result in the proposal being incomplete, which may lead to disqualification of the Bidder.

4.3. Bid Security and Performance Guarantee

I. Tender Fees

Tender fees (Bid Document Cost) is non-refundable as per mentioned in RFP clause no. 1.7.
Bidders are requested to submit tender fees of **Rs. 5,000/- (Rupees Five Thousand Only)** by way of RTGS/NEFT in the following bank account.

Account Name	Baroda Global Shared Services Ltd.
Account Number	29040200000658
Branch Name	Vidhan Sabha Branch ,Sector-11, Gandhinagar, Gujarat -382011
IFSC Code	BARB0VIDHAN (fifth character "ZERO")

Separate mail should be sent to vendormgmt@bgss.in with UTR no. as acknowledgment and UTR No. to upload on online portal.
Offers made without the Tender fees deposit will be rejected.

II. Bid Security

A. Bidders are required to submit an Earnest Money Deposit (EMD) for **Rs. 7,50,000/- (Rupees Seven Lakhs Fifty Thousand Only)** by way of RTGS/NEFT favoring BGSSL Bank's account.

Account Name	Baroda Global Shared Services Ltd.
Account Number	29040200000658
Branch Name	Vidhan Sabha Branch ,Sector-11, Gandhinagar, Gujarat -382011
IFSC Code	BARB0VIDHAN (fifth character "ZERO")

B. Separate mail should be sent to vendormgmt@bgss.in with UTR no. and UTR No to upload on online portal.
C. Offers made without the Earnest Money Deposit will be rejected.
D. The amount of Earnest Money Deposit would be forfeited in the following scenarios:
   1. In case the Bidder withdraws the bid prior to validity period of the bid and after last date of submission of the bid for any reason whatsoever.
   2. In case the successful Bidder refuses to accept and sign contract within 1 month of issuance of contract order/letter of intent for any reason whatsoever; or

3. In case the successful Bidder fails to provide the performance guarantee of 5% of contract value within 45 days from the date of issuance of Purchase Order by Company or signing of the contract, whichever is earlier, for any reason whatsoever, the EMD will be fortified.
4. EMD UTR no. needs to share separately in auction tiger portal.

Note: Exemption from submission of Application Money/Tender fees and Bid Security shall be given to bidders, who are Micro, Small Enterprises (MSE) / Startups. The bidders who are MSE have to submit necessary document issued by Ministry of MSME Government of India and the bidders who are startups have to be recognized by Department of Industrial Policy & Promotion (DIPP) to avail the exemption. To qualify for Bid Security and tender cost exemption, firms should necessarily enclose a valid copy of registration certificate issued by Ministry of MSME Government of India / DIPP which are valid on last date of submission of the tender documents along with "Bid Security Declaration" accepting that if they withdraw or modify their bids during period of validity etc., they will be suspended for the time specified in the tender document. MSE/Startup firms which are in the process of obtaining MSME / DIPP certificate will not be considered for Application Money and Bid Security exemption.

III. Performance Guarantee

A. The successful bidder shall provide a Performance Guarantee within 30 days from the date of receipt of the order or signing of the contract whichever is earlier in the specified format as provided by BGSSL to the extent of 5% of the total contract value of for the entire period of the Three year contract plus 6 months and such other extended period as the Company may decide for due performance of the project obligations. The guarantee should be of that of a Scheduled Commercial Bank only.

B. In the event of non-performance of obligation or failure to meet the terms of this RFP the Companyshall be entitled to invoke the performance guarantee without notice or right of demur to the bidder. Any amount pending for payment due to non-achieving of milestone/s set under the agreement or any other reason solely attributable to the bidder should be included in the remaining amount of the contract value.

C. The Company reserves the right to recover any dues payable by the selected bidder from any amount outstanding to the credit of the selected bidder, including the pending bills and/or invoking Performance Guarantee, if any, under this contract.

D. If the Performance guarantee is not submitted within the stipulated time, the Company reserves the right to cancel the order / contract and the earnest money deposit taken from the bidder, will be forfeited.

E. In such cases wherein the Bidder fails to perform its Services or provide Goods in accordance to the terms defined under the Agreement, the BGSSL shall have discretionary and absolute right to invoke the Performance Bank Guarantee towards any penalty or losses occurred to the BGSSL. The project will be deemed complete only when all the solutions and items contracted for by Company are delivered in good condition, installed, commissioned, implemented, tested and accepted along with the associated certification, documentation and training provided to Company's employees in compliance with the terms of this RFP and as per the requirements of the contract executed between Company and the selected bidder and the acceptance criteria defined in this document is met.

F. The bid security (EMD) would be returned to the successful Bidder after the submission of the performance guarantee.

4.4. Others

A. Responses to this RFP by the Bidders shall not constitute an obligation on the part of the Company to award a contract for any services or combination of services. Failure of the Company to select a Bidder shall not result in any claim whatsoever against the Company and the Company reserves the right to reject any or all bids in part or in full, without assigning any reason whatsoever.

B. By submitting a proposal, the Bidder agrees to promptly contract with Company for any work awarded to

the Bidder, if any. Failure on the part of the selected Bidder to execute a valid contract with Company within 45 days from the date of Purchase order herein will relieve Company of any obligation to the Bidder, and a different Bidder may be selected based on the selection process of Company.

C. The terms and conditions as specified in the RFP, addenda and corrigenda issued by the Company thereafter are final and binding on the Bidders. In the event the Bidder is not willing to accept the terms and conditions of Company, the Bidder may, in sole discretion of Company, be disqualified.

D. The Bidder must strictly adhere to the delivery dates or lead times identified in their proposal including the project timeline. Failure to meet these delivery dates, unless it is due to reasons entirely attributable to the Company, may constitute a material breach of the selected Bidder's performance. In the event that the Company is forced to cancel an awarded contract (related to this RFP) due to the Bidder's inability to meet the established delivery dates that Bidder will be responsible for any re-procurement costs suffered by the Company. The liability of re-procurement costs in such an event could be limited to the amount actually spent by Company for procuring similar deliverables and services. The re-procurement cost would be established post a reasonable due – diligence of the re-procurement cost to be incurred.

E. By submitting the bid, the Bidder represents and acknowledges to the Company that it possesses necessary experience, expertise and ability to undertake and fulfill its obligations, under all phases involved in the performance of the provisions of this RFP. The Bidder represents that all services supplied in response to this RFP shall meet the proposed **RFP for Selection of Managed Security Service Provider for implementing comprehensive C-SOC services** requirements of the Company. The Bidder shall be required to independently arrive at a Solution, which is suitable for the Company, after taking into consideration the effort estimated for implementation of the same. If any services, functions or responsibilities not specifically described in this RFP are an inherent, necessary or customary part of the deliverables or services and are required for proper performance or provision of the deliverables or services in accordance with this RFP, they shall be deemed to be included within the scope of the deliverables or services, as if such services, functions or responsibilities were specifically required and described in this RFP and shall be provided by the Bidder at no additional cost to Company. The Bidder also acknowledges that Company relies on this statement of fact, therefore neither accepting responsibility for, nor relieving the Bidder of responsibility for the performance of all provisions and terms and conditions of this RFP, Company expects the Bidder to fulfill all the terms and conditions of this RFP. The modifications, which are accepted by the Company in writing, shall form a part of the final contract.

F. The Bidder shall represent that the proposed **RFP for Selection of Managed Security Service Provider for implementing comprehensive C-SOC services** and its documentation and/or use of the same by Company shall not violate or infringe the rights of any third party or the laws or regulations under any governmental or judicial authority. The Bidder represents and agrees to obtain and maintain validity throughout the Contract, of all appropriate registrations, permissions and approvals, which are statutorily required to be obtained by the selected Bidder for performance of the obligations of the selected Bidder. The Bidder further agrees to inform and assist the Company for procuring any registrations, permissions or approvals, which may at any time during the contract period be statutorily required to be obtained by the Company for availing services from the selected Bidder.

G. All terms and conditions, payments schedules, time frame for implementation, expected service levels as per this RFP will remain unchanged unless explicitly communicated by Company in writing to the Bidders. The Bidder shall at no point be entitled to excuse themselves from any claims by Company whatsoever for their deviations in conforming to the terms and conditions, payments schedules, expected service levels, time frame for implementation etc. as mentioned in this RFP.

H. The Bidder covenants and represents to Company, the following:

i. It is duly incorporated, validly existing and in good standing under as per the laws of the jurisdiction of its incorporation.

ii. It has the corporate power, necessary licenses and permission and authority to perform its obligations hereunder and to execute appropriate contracts in terms of this RFP. The performance of terms and conditions under the RFP by it and the performance of its obligations hereunder are duly authorized and approved by all necessary action.

iii. The execution, delivery and performance under an Agreement by such Party:
- Will not violate or contravene any provision of its documents of incorporation.
- Will not violate or contravene any law, statute, rule, regulation, licensing requirement, order, writ, injunction or decree of any court, governmental instrumentality or other regulatory, governmental or public body, agency or authority by which it is bound or by which any of its properties or assets are bound.

iv. Except to the extent that the same have been duly and properly completed or obtained, will not require any filing with, or permit, consent or approval of or license from, or the giving of any notice to, any court, governmental instrumentality or other regulatory, governmental or public body, agency or authority, joint venture party, or any other entity or person whatsoever.

v. To the best of its knowledge, after reasonable investigation, no representation or warranty by such party in this tender and subsequent agreement, and no document furnished or to be furnished to the other party to this RFP and subsequent agreement, or in connection herewith or with the transactions contemplated hereby, contains or will contain any untrue or misleading statement or omits or will omit any fact necessary to make the statements contained herein or therein, in light of the circumstances under which made, not misleading. There have been no events or transactions, or facts or information which has come to, or upon reasonable diligence, should have come to the attention of such party and which have not been disclosed herein or in a schedule hereto, having a direct impact on the transactions contemplated hereunder.

vi. The selected Bidder shall undertake to provide appropriate manpower as well as other resources required, to execute the various tasks assigned as part of the project, from time to time. The Company has the right to interview any and all of the resources deputed by the selected bidder and only upon satisfaction will allow the resource to work on the project.

vii. All RFP response documents would become the property of the Company and the Company also would not return the bid documents to the Bidders.

viii. Company will not bear any costs incurred by the Bidder for any discussion, presentation, demonstrations etc. on proposals or proposed contract or for any work performed in connection therewith.

ix. Company reserves the right to reject a proposal for award if it determines that the Bidder recommended for award has engaged in corrupt or fraudulent practices in competing for the contract in question.

4.5. Other RFP Requirements

1. Company reserves the right to cancel this RFP any time or at any stage without any reason / notice to the bidder or change/add/modify any terms and conditions of the RFP by issuing addenda/corrigenda and putting it on Company's website.
2. Company reserves the right to extend the dates for submission of any and all responses to this document.
3. Bidders shall have the opportunity to get their doubts clarified pertaining to the RFP in order to clarify any issues they may have, prior to finalizing their responses. All questions are to be submitted to the contact officer, not later than the query submission date noted in RFP and as indicated by Company from time to time. Responses to inquiries and any other corrections and amendments will be distributed to all Bidders by fax or in electronic mail format.
4. If there are conflicting points in the RFP, the Company reserves the right to take a position on the conflicting issue which will be binding on the selected Bidder any time during the period of contract. No appeal will be entertained.
5. Preliminary Scrutiny – Company will scrutinize the offers to determine whether they are complete, whether any errors have been made in the offer, whether required technical documentation has been furnished, whether the documents have been properly signed, and whether items are quoted as per the schedule. Company may, at its discretion, waive any minor non- conformity or any minor deficiency in an offer. This shall be binding on all Bidders and Company reserves the right for such waivers and Company's decision in the matter will be final.
6. Clarification of Offers – To assist in the scrutiny, evaluation and comparison of offers, Company may, at its discretion, ask some or all Bidders for clarification of their offer. Company has the right to disqualify the Bidder whose clarification is found not suitable to the project requirements.

7. No Commitment to Accept Lowest bid or any bid – Company shall be under no obligation to accept the lowest price bid or any other offer received in response to this RFP. Company will not be obliged to meet and have discussions with any Bidder, and / or to listen to any representations in respect of the rejection.
8. Erasures or Alterations – The offers containing erasures or alterations will not be considered. There should be no hand-written material, corrections or alterations in the offer. Technical details must be completely filled up. Correct technical information of the product being offered must be filled in. Filling up of the information using terms such as "OK", "accepted", "noted", "as given in brochure / manual" is not acceptable. Company may treat the offers not adhering to these guidelines as unacceptable. The proposals should be in the template that is recommended and provided in this RFP. Bids with eraser/over writing/cutting are liable to be rejected.
9. Right to Alter requirements – Company reserves the right to alter the requirements specified in the RFP. Company also reserves the right to delete one or more items from the list of items specified in the RFP. Company will inform all Bidders about changes, if any. The Bidder agrees that Company has no limit on the additions or deletions on the items for the period of the contract. Further the Bidder agrees that the prices quoted by the Bidder would be proportionately adjusted with such additions or deletions in quantities. The Company will have the right to increase or decrease any quantities in the bid and the unit/pro-rata rates would be applicable for such alterations in quantities till the period of the contract.
10. Since some of the payment terms warrant monthly payouts from Company vis-à-vis SLA monitoring, it is to be noted that any such monthly payments will be released and penalties if any, as defined by SLAs, shall be adjusted in the payment for the last month. Balance penalties, if any shall be levied in the payment for the subsequent months.
11. The Bidder shall perform its obligations under this RFP as an independent contractor and may engage subcontractors (with requisite prior permission from Company applicable, if any) to perform any of the deliverables or services. Neither this RFP nor the Bidder's performance of obligations under this RFP shall create an association, partnership, joint venture, or relationship of principal and agent, master and servant, or employer and employee, between Company and the Bidder or its employees, subcontractor; and the Bidder shall not have the right, power or authority (whether expressed or implied) to enter into or assume any duty or obligation on behalf of Company.
12. Details of Sub-contracts, as applicable: If required by Company, selected Bidder should provide complete details of any subcontractor/s used for the purpose of this engagement. It is clarified that the selected bidder will not subcontract primary functions stipulated in this RFP and notwithstanding the use of subcontractors by the selected Bidder for purposes other than main functions, the selected Bidder shall be solely responsible for performance of all obligations under the RFP irrespective of the failure or inability of the subcontractor chosen by the selected Bidder to perform its obligations. The selected Bidder shall also have the responsibility for payment of all dues and contributions, as applicable, towards statutory benefits for its employees and sub- contractors.
13. The Bidder has to submit the escalation matrix up to the highest management authority of the Bidder the along with necessary contact details.
14. However, the selected Bidder shall install and commission the solution, in terms of this RFP, at locations designated by Company or at such Centers as Company may deem fit and the changes, if any, in the locations will be intimated to the Bidder.
15. The selected Bidder is responsible for managing the activities of its personnel or the personnel of its subcontractors/franchisees, if any, and will be accountable for both. The Bidder shall be vicariously liable for any acts, deeds or things done by their employees, agents, contractors, subcontractors, and their employees and agents, etc. which is outside the scope of power vested or instructions issued by Company. Bidder shall be the principal employer of the employees, agents, contractors, subcontractors etc. engaged by Bidder and shall be vicariously liable for all the acts, deeds or things, whether the same is within the scope of power or outside the scope of power, vested under the Contract to be issued for this RFP. No right of any employment shall accrue or arise, by virtue of engagement of employees, agents, contractors, subcontractors etc. by the selected bidder, for any assignment under the contract to be issued for this RFP. All remuneration, claims, wages, dues etc. of such employees, agents, contractors, subcontractors etc. of

the selected bidder shall be paid by selected bidder alone and Company shall not have any direct or indirect liability or obligation, to pay any charges, claims or wages of any of selected bidder's employee, agents, contractors, and subcontractors, etc. The selected bidder shall hold Company, its successors, assignees and administrators and its directors and officials, fully indemnified and harmless against loss or liability, claims, actions or proceedings, if any, that may arise from whatsoever nature caused to Company through the action of selected bidder 's employees, agents, contractors, subcontractors etc. However, the selected bidder would be given an opportunity to be heard by Company prior to making of a decision in respect of such loss or damage.

16. Company shall inform the selected bidder of all known breaches and claims of indemnification and the selected bidder shall be required at their expense to remedy the breaches, defend, manage, negotiate or settle such claims. The written demand by Company as to the loss / damages mentioned above shall be final, conclusive and binding on the selected bidder and selected bidder shall be liable to pay on demand the actual amount of such loss / damages caused to Company including but not limited and all costs and expenses, including, without limitation, reasonable attorneys' fees and court costs. In respect of demands levied by Company on the Bidder towards breaches, claims, etc. Company shall provide the selected bidder with details of such demand levied by Company. For the purposes of this section, the indemnity may include but not limited to the areas mentioned, i.e., "claims arising out of employment, non-payment of remuneration and non-provision of statutory benefits by the selected bidder to its employees, its agents, contractors and sub-contractors." However, there are other indemnities such as indemnity for IPR violation, confidentiality breach, etc., that the Bidder is expected to provide as per the RFP. The selected bidder's representative will be the point of contact for Company. The delivery, installation, configuration status of the project should be reported on a weekly basis.
17. In case of software supplied with the solution the selected bidder should ensure that the same is licensed and legally obtained with valid documentation made available to Company.
18. Technical inspection and performance evaluation – Company may choose to carry out a technical inspection/audit and performance evaluation of solution offered by the Bidders. The Bidder would permit Company or any person/persons appointed by Company to observe the technical and performance evaluation / benchmarks carried out by the Bidder. Any expenses (travel, stay, etc.) incurred for the same would be borne by the Company with prior approval of BGSSL.
19. The Bidder shall ensure that the solution provided and sized by the Bidder is capable of meeting Company's current and terminal year transaction and business volumes.

5. Additional Information

1. Selected bidder and/or its authorized service providers should have their own employees for execution of projects. However, selected bidder will be fully responsible for the service for the service providers. Company will not make any reference to them. In case of any deficiency in service, penalties will be to the selected Bidder's account.
2. The selected bidder shall solely be responsible for all payments (including any statutory payments) to its employees and / or subcontractors and shall ensure that at no time shall its employees, personnel or agents hold themselves out as employees or agents of Company, nor seek to be treated as employees of Company for any purpose, including claims of entitlement to fringe benefits provided by Company, or for any kind of income or benefits. The selected bidder alone shall file all applicable tax returns for all of its personnel assigned hereunder in a manner consistent with its status as an independent contractor of services; and the selected bidder will make all required payments and deposits of taxes in a timely manner.

5.1. Numbering of Pages

All pages of the bid including brochures are to be numbered as Page --- (current page) of --- (total pages) in a seriatim along with proper index. The numbering shall be done separately for Eligibility Bid, Technical Bid and Commercial Bid, and not section-wise.

5.2. Authorized Signatory

The Bidder shall submit the bid authenticated by an authorized person from any of their offices in India. The Bidder's authorized signatory shall authenticate by sign and seal, each page of the bid in original and photocopies including brochures/ pamphlets/ write–up etc.

The selected Bidder shall indicate the authorized signatories who can discuss and correspond with BGSSL, with regard to the obligations under the contract. The selected Bidder shall submit at the time of signing the contract, a certified copy of the resolution of their Board, authenticated by Company Secretary/Director, authorizing an official or officials of the company or a Power of Attorney copy to discuss, sign agreements/contracts with BGSSL. The Bidder shall furnish proof of signature identification for above purposes as required by BGSSL.

5.3. Cost of Preparing the Bids

The cost of preparing the response to this RFP will be the responsibility of the Bidder and Company will not be liable for any cost incurred by the Bidder.

5.4. Clarification on RFP Document

A. The Bidder shall carefully examine and understand the specifications /conditions of RFP, intent of the RFP and seek clarifications, if required, to ensure that they have understood all specifications/conditions/intent of RFP for implementing the Origination Systems Solution in total.
B. The Bidder in all such cases must seek clarification in writing in the same serial order of that of RFP by mentioning relevant page number and clause number of RFP. Such clarifications should be sought, by submitting a list of queries as per **Appendix 07 – Pre Bid Query Format** in writing to Company on or before the timeline prescribed in this RFP under "Schedule of activities and events"
C. All clarifications/queries on the bid are to be in writing and are to be addressed to:

Vendormgmt@bgss.in

Pre-bid queries can be submitted in the format provided in Appendix 07 - Pre Bid query format on the following email-ids:

Vendormgmt@bgss.in

5.5. Normalization of bids:

Company may go through a process of technical evaluation and normalization of the bids to the extent possible and feasible to ensure that Bidders are more or less on the same technical ground. After the normalization process, if Company feels that any of the bids needs to be normalized and that such normalization has a bearing on the price bids; Company may at its discretion ask all the technically Shortlisted Bidders to resubmit the technical and commercial bids once again for scrutiny.

The re-submissions can be requested by Company in the following two manners

- Incremental bid submissions in part of the requested clarifications by Company, OR
- Revised submissions of the entire bid in the whole

Company can repeat this normalization process at every stage of bid submission till Company is satisfied. The Bidders agree that they have no reservation or objection to the normalization process and all the Bidders will, by responding to this RFP, agree to participate in the normalization process and extend their co-operation to Company during this process. The Bidders, by submitting the response to this RFP, agree to the process and conditions of the normalization process.

5.6. Validity of Bids

The bids shall remain valid for a period of 180 days from the last date of submission of bids. All responses including commercial and technical bids would be deemed to be irrevocable offers/proposals from the Bidders and shall, if accepted by Company, form part of the final contract between Company and the selected Bidder. Company may seek further extensions of the bid validity, if required.

5.7. Bidder's Quote/Offer

I. Bidders are requested to attach a letter from an authorized signatory attesting the veracity of information provided in the responses. Unsigned responses would be treated as incomplete and are liable to be rejected.
II. The Bidder must furnish requirements as per the formats provided in the RFP document.
III. While submitting the bid, the Bidder is required to comply with inter alia the following CVC guidelines detailed in Circular No. 03/01/12 (No. 12-02-6 CTE /SPI (I) 2 / 161730 dated 13.01.2012)

Commission has decided that in all cases of procurement, the following guidelines may be followed:

- In a tender, either the Indian agent on behalf of the Principal/OEM or Principal/OEM itself can bid but both cannot bid simultaneously for the same item/product in the same tender.
- If an agent submits bid on behalf of the Principal/OEM, the same agent shall not submit a bid on behalf of another Principal/OEM in the same tender for the same item/product.

The Bidder is required to comply with inter alia the GFR guidelines against rule no. 144 - Fundamental principles of public buying (for all procurements including procurement of works).

The decision of the Company shall be final and binding in this regard.
Related Parties -

- In the following circumstances company will have discretion to reject the Proposal/ response or accept the Proposal/ response with some conditions stipulated by 'the Bank'.
- Proposal/Response submitted by holding company and its subsidiary
- Proposal/Responses submitted by companies having common director/s
- Proposal/ Responses submitted by partnership firms / LLPs having common partners
- Proposal/Responses submitted by companies having the same group of promoters/ management
- Any other proposal/ response in the sole discretion of the company is in the nature of multiple bids.

5.8. Integrity Pact

All bidder will be required to enter into an integrity pact on minimum Rs 300 Stamp paper with the Company or on a stamp paper of such other higher amount as may be prevalent in the state from where the bidder is executing the integrity pact as per the CVC guidelines in Appendix 05.

5.9. Submission of Bids

1. Bids must be submitted online through Procure Tiger https://eauction.auctiontiger.net/EPROC
   No Submission shall be submitted in Hard copy.
2. The response should be submitted by the authorized person on or before the last date & time of submission mentioned in section 1.7. If the last date of submission of RFP response is declared as a holiday for any reason, then the last date for submission of RFP response will fall on the next working day of the Company. The bids which are received after the scheduled date and time will be rejected by the Company.
3. The responses should not be submitted by post or by courier.
4. For all eligibility, technical and commercial bid, authorization letter as specified in **Appendix 03** and other mandatory documents, appendix, annexure as per mentioned in RFP, the Bidders are required to submit online only.
5. The bid should constitute three separate parts. The response should be organized and submitted in the online portal as required mandatory documents required in RFP.
6. All the submitted page/documents duly signed and stamp by Authorized person.
7. Online Bid submission related query you may contact as per mentioned details in RFP section 1.7 serial no.12 and 13.

Part I – Eligibility Bid & Technical Bid:

I. The Eligibility Bid containing the response to eligibility requirements for services is to be uploaded in a separate section on online portal as mentioned in **Annexure A (with all necessary supporting)**.
II. Covering letter certifying eligibility criteria compliance (eligibility criteria as defined in **Annexure A)**

III. Letter with details of authorized signatories/Power of Attorney's in the name of the authorized signatories who can represent the Bidder/s with regard to the obligations under the RFP or contract.
IV. Softcopy of duly filled up **Annexure A** – Eligibility criteria compliance including supporting credential letters/testimonials from relevant organizations or copies of documentation from clients or purchase order copies certifying compliance.
V. The Bidder should also include the masked (without prices) commercial bid in the technical bid. The masked Indicative Commercial Bid which would be submitted as part of the Technical bid should contain "XX" instead of actual commercial value for ALL the corresponding commercial values. The Bidder must note that the masked commercial bid should be actual copy of the commercial bid submitted with prices masked and not the Pro-forma/format of the **Appendix 02 – Commercial Bid** in the RFP.
VI. The soft copy of the technical proposal should be bound in such a way that the sections of the proposal can be segregated. Signed copy of the RFP, all annexure and appendices fully filled up need to be uploaded.

The Bidders have to note that the Eligibility & Technical Proposal must contain the following:

a. Duly filled and signed Annexure – A by the authorized signatory with all respective relevant mandatory supporting documents.
b. Masked copy of the Bidder's **Appendix 02 – Commercial Bid** duly masking the price details
c. Duly signed authorizations letter as per **Appendix 03** (enclose POA, Board resolution, etc.)
d. Duly signed covering letter by the authorized signatory as per **Appendix 04 – Bid undertaking letter**
e. Integrity Pack on Rs. 300 Stamp as per **Appendix 05.**
f. Conformity letter as per **Appendix 06.**
g. SOC MSSP experience details as per **Appendix 08.**
h. Bid Security declaration in case of MSE bidders applying as per **Appendix 09.**
i. Detailed presentation on following :
    - Company profile
    - Past Performance & Credentials.
    - Proposed Managed Security Services C-SOC for BGSSL and sample presentation with action plan.
    - Timeline for Implementation.
    - Strategic Thinking Innovations executed, If any need to specify with details
    - Awards & Recognitions.
    - Recommending tools/Processes for implementing Comprehensive C-SOC.
    - Showcase selected bidders' experience and deploying such system/applications/tools.
    - Resource management and planning.
j. All Annexure and Appendix and its supporting as per mentioned in RFP.

Part II – Commercial Bid

I. The bidder will be required to submit commercial bids as a part of the bid submission.
II. The placement of soft copy of commercial bid in eligibility bid or technical bid envelopes/sections will make the bid liable for rejection. All the placement of relevant documents to be against their respective criteria.
III. Post the commercial evaluation process the H1 bidder would be required to submit their final commercial as per **Appendix 02 – Commercial Bid** and other terms and conditions of the RFP on prices. In a nutshell, the commercial Bid details will need to be provided for all requirements of the Company to arrive at TCO of the solution.
IV. It is the bidder's obligation to supply all the items within the ultimate sum that the company and the chosen bidder have agreed upon.

Notes -

1. GST will be paid extra on actual basis.
2. Billing will done on quarterly basis
3. TCO will be considered only for calculation purpose, Payment will be made on actual Active devices basis.
4. BGSSL does not make any commitment for fixed qty. It may vary month on month.
5. All applicable Taxes / Duties/levies and license charges should be included in the Bid.
6. Applicable taxes (TDS) would be deducted at source, if any, as per prevailing rates.

5.10. Overall Bid

1. The segregated envelopes containing Eligibility Bid, Technical Bid and Commercial Bid for the **RFP for Selection of Managed Security Service Provider for implementing comprehensive C-SOC services** shall be submitted in online portal as mentioned in **RFP section no. 1.7.**
2. The Bidder shall take care to submit the Bid properly online so that the documents are clearly visible. The Bidder shall submit the bid in suitable capacity of the file such that the documents do not jumble up and Mix-up during scrutiny. The Bids, which are not uploaded in proper manner are also liable to be rejected.
3. The price schedule shall be submitted in commercial Bid only and not in technical or eligibility criteria or with any consolidated documents or otherwise.
4. The Bidder while furnishing the cost under the above heads must furnish the split up cost particulars of all major components/line items under each head and no extra cost would be allowed
5. Further, the Bidder has to quote for all the components, while the components kept blank will be considered as zero cost.
6. Bids with Incorrect information are liable to be rejected.

5.11. Compliance Statement

The Bidder shall certify the compliance or deviation of all clauses, terms conditions.

5.12. Opening of Bids

1. Opening of Eligibility and Technical Bids

A. Opening of eligibility and technical bids: - Since submission of bids are online, Technical & Eligibility documents will be opened by BGSSL and acknowledgment will be communicated to the participating bidders via email as mentioned in **section 1.7 – Important Details.**

B. The rejection or acceptance of the bid will be done only after evaluation at the discretion of Company.

C. During evaluation of the eligibility and technical bids, Company may seek from the Bidder clarifications on the bid submitted by the Bidder. The request for such clarification and the response from the Bidder shall be in writing as and when requested by the company.

D. After the evaluation of the eligibility bids Company will finalize the list of eligible bidders whose technical bid will be considered for the technical evaluation stage. The eligible bids will undergo a detailed technical evaluation as per the terms and conditions of this RFP.

E. Company will announce the list of bidders who qualify technical evaluation and whose commercial bid will be considered for the commercial evaluation stage.

F. The Bidders may note that no further notice will be given in this regard. Further, in case Company does not function on the aforesaid date due to unforeseen circumstances or holiday then the bid will be accepted on the next working day of the Company and bids will be opened at the same venue on the same day.

G. Company however reserves the right to change the date & time of opening of Eligibility and Technical bid without assigning any reason whatsoever. In case there is a change in the schedule the same will be intimated to the Bidders by publishing on the Company's website for enabling them to be present during the Bid opening.

2. **Opening of Commercial bid**
   A. In case the Company decides to go for Open bid process for commercial evaluation, the commercial bids will be opened in front of the bidders after the technical evaluation is complete. The date of opening of commercial bids will be intimated to the Bidders who have been evaluated for Technical Bid.
   B. The evaluation of the Commercial Bids as per the RFP guidelines would be done subsequently.
   C. Post the completion of the detailed commercial evaluation the final ranking of the bidders would be announced According to the evaluation methodology mentioned in point No. 6. The selected bidder would not necessarily be lowest One.

5.13. Examination of Bids

1. Company will do preliminary examination of bids to know whether they are complete in all respects, whether any computational errors have been made, whether the documents have been properly signed and whether the bids are generally in order. The Bidders have to note that
   A. If there is any discrepancy between words and figures, the amounts in words will prevail.
   B. If there is discrepancy between percentage and amount, the amount calculated on percentage basis will prevail.
   C. If there is discrepancy between unit price and total price that is obtained by multiplying the unit price and quantity, the unit price will prevail and the total price shall be corrected by Company.
   D. If there is discrepancy in the total arrived at Commercial Bid, correct total will be arrived at by Company and the same will prevail over the total furnished in the Commercial Bid.
2. In the event the Bidder has omitted to quote for any line item in the commercial bid, Company would take the highest price quoted by any of the participating Bidders as the cost, for such for arriving at the TCO for the purpose of evaluation of the defaulting/deviating Bidders. However, the same shall be provided by the defaulting/deviating Bidder, in case selected at no cost to Company for the period of the contract.
3. Company ascertains and concludes that everything as mentioned in the RFP documents circulated to the Bidders and responded by the Bidders have been quoted for by the Bidders, and there will be no extra cost associated with the same other than the cost quoted by the Bidder.
4. In the event Company has not asked for any quotes for alternative prices, and the Bidder furnishes the alternative price in the Bidder's commercial bid, the higher of the prices will be taken for calculating and arriving at the TCO. However, payment by Company will be made at the lower price.
5. The **Appendix 02 – Commercial Bid** is an indicative list of items used for the purpose of Bidder evaluation through TCO. The availment quoted by the Bidders in the **Appendix 02 – Commercial Bid** will be decided by Company based on the requirements from time to time during the period of the contract. The Bidder cannot compel Company to avail any or all the items quoted by them in **Appendix 02 – Commercial Bid.** However for the purpose of calculating of TCO, bid will be considered as fixed priced bid.
6. Company would like to expressly state that any assumptions, terms, conditions, deviations etc. which the Bidder includes in any part of the Bidder's response to this RFP, will not be taken into account either for the purpose of evaluation or at a later stage, unless such assumptions, terms, conditions, deviations etc. have been accepted by Company and communicated to the Bidder in writing. The Bidder at a later date cannot make any plea of having specified any assumptions, terms, conditions, deviations etc. in the Bidder's response to this RFP.
7. During the preliminary examination, Company will also verify whether the Bidder has responded in full to the RFP or whether it is partial or conditional. The bids that are incomplete or conditional are liable to be rejected.

6. Evaluation Methodology

A two stage process is adopted for selection of the bidder:

Stage1: Eligibility cum Technical Bid

Stage 2: Evaluation methodology for eligible bidder

- Technical Bid Evaluation
- Commercial Bid Evaluation
- Weighted evaluation

During evaluation of the Tenders, the Company, at its discretion, may ask the Bidder for clarification in respect of its tender. The request for clarification and the response shall be in writing, and no change in the substance of the tender shall be sought, offered, or permitted. The Company reserves the right to accept or reject any tender in whole or in parts without assigning any reason thereof. BGSSL reserves the absolute and unconditional right to reject the response to this RFP if it is not in accordance with its requirements and no correspondence will be entertained by BGSSL in the matter. The bid is liable to be rejected if it is not in conformity with the instructions mentioned in the RFP document. The decision of the Company shall be final and binding on all the bidders to this document and Company will not entertain any correspondence in this regard.

6.1. Eligibility Bid

Eligibility criterion for the Bidder to qualify this stage is clearly mentioned in Annexure A – Eligibility Criterion Compliance to this document. The bidder would need to provide supporting documents as part of the eligibility proof.

6.2. Evaluation Methodology for Eligible Bidder

After qualifying the eligibility criteria, the evaluation will be a three stage process. The stages are:

- Technical Bid Evaluation
- Commercial Bid Evaluation
- Weighted evaluation

The technical evaluation and the commercial evaluation shall have the weightage of 70% and 30% respectively and this weightage shall be considered for arriving at the successful bidder. The evaluation methodology vis-à-vis the weight- ages are as under:

Technical Bid Evaluation

The bidder needs to achieve a cut – off score of 70 marks in this evaluation stage to be qualified for commercial bid opening. Only those bidders who achieve the specified cut – off scores would be short-listed for Commercial Bid Evaluation. The Technical Proposal will be evaluated for technical suitability and the criteria for evaluation of technical bids are mentioned in Appendix 01.

In case there is only one Bidder having technical score of 70 or more, BGSSL may, at its sole discretion, also consider the next highest technical score of greater than 60 and qualify such Bidder. In case, none of the participating Bidders achieve greater than 60 score, BGSSL, at its sole discretion, may qualify two Bidders on the basis of the top 2 scores. However, BGSSL at its discretion may reject the proposal of the Bidder or will not consider Bidder below cut-off marks by relaxing as mentioned above, if in BGSSL's opinion the Bidder could not present or demonstrate the proposed services as described in the proposal or in case the responses received from the customer contacts / site visited are negative or the proposed solution does not meet BGSSL's requirement.

Commercial Bid Evaluation

The bidder who achieves the required cut – off technical score as part of technical evaluation shall be qualified for commercial bid opening. The commercial bid would be evaluated based on a "Total Cost of Ownership" ('TCO') basis. The key considerations of the TCO would be the total payouts for entire project through the

contract period of 3 years.

Weighted Evaluation:

On the basis of the combined weighted score for technical and commercial evaluation, the bidders shall be ranked in terms of the total score obtained. The proposal obtaining the highest total combined score in evaluation of quality and cost will be ranked as H-1 followed by the proposals securing lesser marks as H-2, H-3 etc. The proposal securing the highest combined marks and ranked H-1 shall be recommended for award of contract.

As an example, the following procedure can be followed:

A score (S) will be calculated for all qualified bidders using the following formula: Clow/C X100 +T (1-X)

C stands for discounted rate arrived basis of commercial evaluation; Clow stands for the lowest rate arrived basis of commercial evaluation. T stands for technical evaluation score and X is equal to 0.30.

#	Bidder	Technical Evaluation Marks (T)	Discounte dRate I	T * 0.70 (A)	[(Clow / C)x 100] x 0.30 (B)	Score (S = A +B)
1	AAA	75	120	52.5	25	77.5
2	BBB	80	100	56	30	86
3	CCC	90	110	63	27.3	90.3

In the above example, Clow is 100.

In the above example, CCC, with the highest score becomes the successful bidder (H1).

In case of more than one bidder with equal highest score (S) up to three decimal, then number of decimal will be increased.

The Company may in its absolute discretion engage in discussion or negotiation with H1 bidder. The decision of the Company shall be final and binding on all the bidders to this document. The Company reserves the right to accept or reject an offer without assigning any reason whatsoever.

7. Payment Terms

The bidder must accept the payment terms proposed by the Company. The commercial bid submitted by the bidder must be in conformity with the payment terms proposed by the Company. Any deviation from the proposed payment terms would not be accepted. The Company shall have the right to withhold or deduct (in event of SLA breach) any payment due to the selected bidder, in case of delays or defaults on the part of the selected bidder. Such withholding of payment shall not amount to a default on the part of the Company. If any of the items / activities as mentioned in the price bid is not taken up by the Company during the course of the assignment, the Company will not pay the professional fees quoted by the bidder in the price bid against such activity / item.

Successful Bidder shall be paid quarterly at the end of each quarter against receipt of satisfactory report of support and operations by bidder resources of previous quarter from BGSSL's IT Head.

There shall be no escalation in the prices once the prices are fixed and agreed to by the Company and the selected bidder. Payment will be released by the Company as per above payment terms on submission of relevant documents.

The Company will pay invoices within a period of 30 days from the date of receipt of undisputed monthly invoices. Any dispute regarding the invoice will be communicated to the selected bidder within 15 days from the date of receipt of the invoice. After the dispute is resolved, Company shall make payment within 15 days from the date the dispute stands resolved.

8. Terms & Conditions

8.1. General

- The Company expects the bidder to adhere to the terms of this RFP document and would not accept any deviations to the same.
- The company expects that the bidder appointed under this RFP Document shall have the single point responsibility for fulfilling all obligations and providing all deliverables and services required by Company.
- Unless agreed to specifically by the Company in writing for any changes to the RFP document issued the bidder responses would not be incorporated automatically in the RFP document.
- Unless expressly overridden by the specific agreement to be entered into between the Company and the bidder, the RFP document shall be the governing document for arrangement between the Company and the selected bidder.

8.2. Indemnity

(a) The Vendor shall indemnify the Company, and shall always keep indemnified and hold the Company, its employees, personnel, officers, directors, (hereinafter collectively referred to as "Personnel") harmless from and against any and all losses, liabilities, claims, actions, costs and expenses (including attorneys' fees) relating to, resulting directly or indirectly from or in any way arising out of any claim, suit or proceeding brought against the Company as a result of:

i. Company's authorized / bona fide use of the Deliverables and /or the Services provided by Vendor under the Agreement; and/or
ii. any act of commission or omission, fraud, negligence, breach on the part the Vendor and/or its employees, agents, sub-contractors in performance of the obligations under the Agreement; and/or any act of omission of statutory requirement and/or
iii. claims made by employees or subcontractors or subcontractors' employees, who are deployed by the Vendor, against the company; and/or
iv. claims arising out of employment, non-payment of remuneration and non-provision of statutory benefits by the Vendor to its employees, its agents, contractors and sub-contractors, if any.
v. breach of any of the term of the Agreement or subsequent purchase order or breach of any representation or false representation or inaccurate statement or assurance or covenant or warranty of the Vendor under the Agreement and subsequent purchase order; and/or
vi. any or all deliverables or services infringing any patent, trademarks, copyrights or such other Intellectual Property Rights; and/or
vii. breach of confidentiality obligations of the Vendor contained in the Agreement; and/or
viii. The acts, errors, representations, misrepresentations, willful misconduct or Negligence or gross misconduct attributable to the Vendor or its employees or sub-contractors under the Agreement.
ix. Loss of data due to Vendor provided Goods; and/or
x. Any deficiency in the services of the Vendor.
xi. Any transaction contemplated under the Agreement.
xii. The provisions of this Clause shall survive the termination of the Agreement.

(b) The Vendor shall at its own cost and expenses defend or settle at all point of time any claim against the Company that the deliverables and services delivered or goods supplied or provided under the Agreement infringe a patent, utility model, industrial design, copyright, trade secret, mask work or trade mark in the country where the deliverables, Goods supplied and services are used, sold or received, provided the Company notifies the Vendor in writing as soon as practicable when the Company becomes aware of the claim; and Cooperates with the Vendor in the defense and settlement of the claims.

(c) However, (i) the Vendor shall take sole control of the defense and all related settlement negotiations (ii) the Company will provide the Vendor with the assistance, information and authority reasonably necessary to perform the above and (iii) the Company does not make any statements or comments or representations about the claim without the prior written consent of the Vendor, except where the Company is required by any authority/regulator to make a comment/statement/representation.

(d) If use of deliverables is prevented by injunction or court order because of any such claim or deliverables is likely to become subject of any such claim then the Vendor, after due inspection and testing and at no additional cost to the Company, shall forthwith either 1) replace or modify the software / equipment with software / equipment which is functionally equivalent and without affecting the functionality in any manner so as to avoid the infringement; or 2) obtain a license for the Company to continue the use of the software / equipment, as required by the Company as per the terms and conditions of the Agreement and to meet the service levels; or 3) refund to the Company the amount paid for the infringing software / equipment and bear the incremental costs of procuring a functionally equivalent software / equipment from a third party, provided the option under the sub clause (3) shall be exercised by the Company in the event of the failure of the Vendor to provide effective remedy under options (1) to (2) within a reasonable period which would not affect the normal functioning of the Company.

(e) The indemnities under this clause are in addition to and without prejudice to the indemnities given elsewhere in this RFP.

8.3. No liability

- All employees engaged by the Service Provider shall be in sole employment of the Service Provider and the Service Provider shall be solely responsible for their salaries, wages, statutory payments etc. That under no circumstances shall company be liable for any payment or claim or compensation (including but not limited to compensation on account of injury/death/termination) of any nature to the employees and personnel of the Service Provider. Bidder shall be solely be responsible for hiring of its Employees by way of following procedure of its own choice which may include but shall not be limited to conducting direct personal interviews, issuing job descriptions considering its needs, etc.; Bidder shall be responsible for compliance of all laws, rules, regulations and ordinances applicable in respect of its Employees, sub-contractors and agents, including but not limited to Minimum Wages Act 1948, provident fund laws, Workmen's Compensation Act 1923, and shall establish and maintain all proper records including, but not limited to, accounting records required by any law, code, practice or corporate policy applicable to it from time to time, including records and returns as applicable under labour legislations;
- Company shall not be held liable for and is absolved of any responsibility or claim/litigation arising out of the use of any third party software or modules supplied by the Service Provider as part of this Agreement.
- Under no circumstances Company shall be liable to the Service Provider for direct, indirect, incidental, consequential, special or exemplary damages arising from termination of this project , even if Company has been advised of the possibility of such damages, such as, but not limited to, loss of revenue or anticipated profits or lost business
- The Parties hereto expressly agrees that the liability of the Company shall be limited to the extent of timely payment of undisputed invoices for the Services rendered by the Bidder.
- The Selected Empanelled Bidder's total liability under the said agreement shall be at actual loss and damage to reputation suffered by the Company.
- However, Selected Empanelled Bidder's liability in case of claims against the Company resulting from Willful Misconduct or Gross Negligence of Bidder, its employees and Subcontractors or from infringement of patents, trademarks, copyrights or such other Intellectual Property Rights or breach of confidentiality obligations shall be unlimited Subject to any law to the contrary, and to the maximum extent permitted by law neither parties shall be liable to other for any consequential/ incidental, or indirect damages arising out of this agreement.

8.4. Extension of Contract Post Expiry

- The Company desires to appoint the vendor for a total period specified in the RFP, considering the effort and investments required in the arrangement. However, understanding the complexities of the entire arrangement, Company would like to safe guard the interests of all the entities involved in the arrangement. Therefore, the Company would like to have options to revisit the arrangements and terms

of contract as well as to re-price the same (rates similar or less than existing arrangement) after the contract expiry, if necessary.

- The Company expects the benefits from any unanticipated decrease in technology infrastructure costs, over the term of the contract due to reduction of prices, efficient use of IT infrastructure/reduction of statutory charges, etc. and operations management methods that yield more efficient operations, to be passed on through re-negotiation. No conflict between the Selected Bidder and the Company will cause cessation of services.

8.5. Termination of Contract

In an event the Vendor is committing breach of any of the Clauses of the current RFP of any subsequent Agreement or making default, the Company shall be entitled, subject to other rights, measures and remedies available to it under this RFP or subsequent agreement and under the applicable laws from time to time, to terminate the Agreement and impose suitable penalty immediately without notice and without assigning any reason.

Notwithstanding the above, the Company shall have a right to terminate any subsequent Agreement, including for termination for convenience, by giving one month's notice in writing to the Bidder during the period of the Agreement without assigning any reason for such termination, whatsoever.

In such circumstances wherein the Vendor breaches this RFP or any subsequent Agreement or stops rendering its Services or render the Services in a manner not satisfactory to the Company, the Company may at its sole discretion terminate the Agreement and assign the Services to some other vendor of its choice and any expenses that the Company may incur, for assigning the Services to the new vendor and such other expenses to make it enable to render Services in a manner that the Company may not suffer losses due to the aforementioned acts of the Vendor, shall be paid by the Vendor to the Company on demand made by the Company in writing.

BGSSL shall have option to terminate / cancel this RFP at any stage without any prior notice. In following events BGSSL shall terminate this assignment or cancel any particular order if the Bidder:

- Breaches any of its obligations set forth in this assignment or any subsequent agreement and such breach is not cured within thirty (30) Working Days after BGSSL gives written notice; or
- Failure by the empanelled Bidder to provide BGSSL, within thirty (30) Working Days, with a reasonable plan to cure such breach, which is acceptable to BGSSL. or
- The progress regarding execution of the contract/ services/goods rendered by the Bidder is not as per the prescribed time line, and found to be unsatisfactory; or
- Supply of substandard materials/ services/goods; or
- Delay in delivery / installation / commissioning of services/goods; or

BGSSL may terminate this RFP or subsequent agreement on happening of following events:

- The vender unable to pay its debt as they fall due or otherwise enters into any composition or arrangement with or for the benefit of its creditors or any class thereof;
- A liquidator or a receiver is appointed over all or a substantial part of the undertaking, assets or revenues of the vender and such appointment continues for a period of twenty one (21) days;
- The vender is subject of an effective resolution for its winding up other than a voluntary winding up for the purpose of reconstruction or amalgamation.
- Failure of the Bidder make good the situation within the remedy period
- The selected Bidder commits a breach of any of the terms and conditions of the RFP/ contract.
- The selected Bidder becomes insolvent or goes into liquidation voluntarily or otherwise
- Discrepancy in the quality of services/goods / security expected during the implementation, rollout and subsequent maintenance process.
- The vender becomes the subject of a court order for its winding up.

Notwithstanding above, in case of change of policy or any unavoidable circumstances BGSSL reserve the right to terminate this assignment or any subsequent agreement and / or any particular order, in whole or in part by giving The empaneled Bidder at least 30 days prior notice in writing.

8.6. Other Rights or Remedies

Termination of the contract in whole or part is without prejudice to any other rights or remedies that either Party may have under the contract including the invocation of the performance guarantee by the Company, and does not affect any accrued rights or liabilities of either Party at the date of termination.

8.7. Effects of Termination

Notwithstanding termination of the contract in whole or in respect of any part of the Services for any reason, the contract continues in force to the extent necessary to give effect to those of its provisions which expressly or implicitly have effect after termination; and

Where Company terminates any Part of the Project, the parties shall continue to perform their respective obligations under the contract in connection with that portion of the Project in respect of which there has been no termination.

If BGSSL terminates or cancels the assignment on the default mentioned in the termination clause, in such case BGSSL reserves the right to get the balance contract executed by another party of its choice. In this event, the Bidder shall be bound to make good the additional expenditure, which BGSSL may have to incur to carry out bidding process for the selection of a new service provider and for execution of the balance of the contract.

Immediately upon the date of expiration or termination of the Tender and subsequent Agreement, BGSSL shall have no further obligation to pay any fees for any periods commencing on or after such date.

Without prejudice to the rights of the Parties, upon termination or expiry of this Tender and subsequent Agreement, BGSSL shall pay to Bidder, within thirty (30) days of such termination or expiry, of the following:

a) All the undisputed fees outstanding till the date of termination;

b) The rights granted to Bidder shall immediately terminate;

c) Upon BGSSL's request, with respect to (i) any agreements for maintenance, disaster recovery services/goods or other third-party services/goods, and any Deliverables not owned by the Bidder, being used by Bidder to provide the Services/goods and (ii) the assignable agreements, Bidder shall, use its reasonable commercial endeavors to transfer or assign such agreements and Bidder Equipment to BGSSL and its designee(s) on commercially reasonable terms mutually acceptable to both Parties.

d) Upon BGSSL's request in writing, Bidder shall be under an obligation to transfer to BGSSL or its designee(s) the Deliverables being used by Bidder to perform the Services free and clear of all liens, security interests, or other encumbrances at a value calculated as stated.

8.8. Consequence of Termination

If Company terminates the contract in whole or in respect of any part of the Project in accordance with its terms, it will incur no liability to the selected bidder as a result of such termination, other than:

- The charges or any other amounts due to selected bidder up to the date of termination;
- Amounts payable for any Services already performed at the date of the termination;
- Amounts payable for Services yet to be performed but which the parties agree not to terminate after performance of those services; and

The selected bidder understands the scale, tenure and criticality of this Project and that it would require tremendous commitment of financial and technical resources for the same from the selected bidder for the tenure of this tender and subsequent Agreement/Contract. The parties therefore agree and undertake that an exit at any point in time resulting due to expiry or termination of RFP and subsequent Agreement/Contract for any reason whatsoever would be a slow process over a period of six (6) months, after the completion of the

notice period, if any, and only after completion of the selected bidder's obligations under a reverse transition mechanism. During this period of Reverse Transition, the selected bidder shall continue to provide the Deliverables and the Services in accordance with this RFP and subsequent Agreement/Contract and shall maintain the agreed Service levels.

Upon Company's request, with respect to (i) any agreements for maintenance, disaster recovery services or other third-party applications/solutions, and any Deliverables not owned by the selected Bidder, being used by the selected Bidder to provide the Services and (ii) the assignable agreements, selected Bidder shall, use its reasonable commercial endeavors to transfer or assign such agreements and selected Bidder's equipment to Company and its designee(s) on commercially reasonable terms mutually acceptable to both parties.

Upon Company's request in writing, selected bidder shall be under an obligation to transfer to Company or its designee(s) the Deliverables being used by the selected bidder to perform the Services free and clear of all liens, security interests, or other encumbrances at a value calculated as stated.

As part of the reverse transition services, Company shall have the right, and selected bidder shall not object to or interfere with such right, to contract directly with any selected bidder's subcontractor.

Procedure for transition and migrating to the new appointed Bidder is as follows:

- Time frame for parallel run
- Skill transfer mechanism and in specific cases, the Loan management requirement
- Reverse Transition Plan
- Support for successful transition of resource to the new empanelled Bidder.

Reverse Transition Services are the services provided by selected bidder to Company during the reverse transition period which will start after completion of the three (3) months' notice period to facilitate an orderly transfer of the Services to Company or to an alternative third partly service provider nominated by Company. Where Company elects to transfer responsibility for service delivery to multiple Bidders, Company will nominate a services provider who will be responsible for all dealings with such Bidders regarding the delivery of Reverse Transition Services.

8.9. Warranties

- All the warranties held by or in the name of the selected bidder shall be assigned or transferred "As Is" in the name of the Company. The selected bidder shall execute any and all such documents as may be necessary in this regard.
- The parties shall return confidential information and will sign-off and acknowledge the return of such confidential information.
- Selected bidder shall provide all other services as may be agreed to by the parties in connection with the reverse transition services. However, in case any other services, in addition to the above are needed, the same shall be scoped and reasonably priced. Reverse transition services shall be charged based on selected bidder's then current time and materials rates.
- The selected bidder recognizes that considering the enormity of the assignment, the transition services listed herein are only indicative in nature and the selected bidder agrees to provide all assistance and services required for fully and effectively transitioning the services provided by the selected bidder under this tender and subsequent agreement, upon termination or expiration thereof, for any reason whatsoever.
- Further, the Bidder represents and warrants the Company that:

a) It is an authorized business establishment and holds all the requisite permissions, licenses, authorities, approvals and sanctions to conduct its business and to enter into the present agreement with the Company so as to render the Services/goods as agreed in this Agreement and the Bidder shall keep all such necessary permissions, licenses, approvals, etc. alive and active during the Term of this Agreement.

b) It has requisite skills, manpower, resources, infrastructure and other necessary means and resources to enable the Bidder to render Services/goods to the Company in a manner satisfactory to the Company and it shall keep requisite skills, manpower, resources, infrastructure and other necessary means and resources available during the Term of this Agreement.

c) It shall be the Bidder's sole responsibility to ensure compliance with every applicable existing and/or future laws of the Republic of India that may require any kind of compliance.
d) The Bidders shall be solely responsible for the quality, quantity, merchantability, guarantee, and warranties in respect of the Services/goods rendered to the Company.
e) The Bidder shall ensure that the Services/goods delivered are as per the satisfaction of the Company.
f) The Bidder warrants and represents that it has adequate rights under relevant laws including but not limited to various Intellectual Property Legislation(s) to enter into this Agreement with the Company and perform the obligations contained herein and that it has not violated/ infringed any intellectual property rights of any third party.
g) The Bidder shall ensure not to carry out such act which may result into unlawful, illegal, objectionable, obscene, vulgar, opposed to public policy, prohibited or is in violation of intellectual property rights including but not limited to Trademark and copyright of any third party. Any such act of the Bidder may lead to termination of this Agreement and suspension of Services/goods with no prior notice to the Bidder.
h) It is an authorized business establishment and holds all the requisite permissions, authorities, approvals and sanctions to conduct its business and to enter into the present agreement with the Company.
i) It is the Bidder's sole responsibility to ensure compliance with every applicable existing and/or future laws of the Republic of India that may require any kind of compliance.
j) It has adequate rights under relevant laws including but not limited to various Intellectual Property Legislation(s) to enter into this Agreement with the Company and perform the obligations contained herein and that it has not violated/ infringed any intellectual property rights of any third party.
k) The Bidder shall maintain absolute integrity, follow a decent standard of business ethics.
l) The Bidder shall adhere to the timelines, prescribed by either the Company or any other competent authorities or any third party for the performance of Services/goods under this Agreement, within which the Services/goods are to be rendered failing which the Company shall be entitled to penalize the Bidder in accordance to the terms of this Agreement.
m) There are no known pending actions, suits or proceeding, existing, threatened, anticipated or pending against Bidder which may prejudicially affect the due performance or enforceability of this Agreement or any obligation, act, omission or transactions contemplated hereunder, respectively.

8.10. Compliance with Laws

1. Compliance with all applicable laws: The Bidder shall undertake to observe, adhere to, abide by, comply with and notify the Company about all laws in force or as are or as made applicable in future, pertaining to or applicable to them, their business, their employees or their obligations towards them and all purposes of this tender and shall indemnify, keep indemnified, hold harmless, defend and protect the Company and its employees/officers/staff/personnel/representatives/agents from any failure or omission on its part to do so and against all claims or demands of liability and all consequences that may occur or arise for any default or failure on its part to conform or comply with the above and all other statutory obligations arising there from.
2. Compliance in obtaining approvals/permissions/licenses: The Bidder shall promptly and timely obtain all such consents, permissions, approvals, licenses, etc., as may be necessary or required for any of the purposes of this project or for the conduct of their own business under any applicable Law, Government Regulation/Guidelines and shall keep the same valid and in force during the term of the project, and in the event of any failure or omission to do so, shall indemnify, keep indemnified, hold harmless, defend, protect and fully compensate the Company and its employees/officers/staff/personnel/ representatives/agents from and against all claims or demands of liability and all consequences that may occur or arise for any default or failure on its part to conform or comply with the above and all other statutory obligations arising there from and the Company will give notice of any such claim or demand of liability within reasonable time to the Bidder.
3. The Bidder is not absolved from its responsibility of complying with the statutory obligations as specified

above. Indemnity would cover damages, loss or liabilities suffered by the Company arising out of claims made by its customers and/or regulatory authorities.

8.11. Assignment

1. The selected bidder agrees that the selected bidder shall not be entitled to assign any or all of its rights and/or obligations under this tender and subsequent agreement to any entity including selected Bidder's affiliate without the prior written consent of the Company.
2. If the Company undergoes a merger, amalgamation, takeover, consolidation, reconstruction, change of ownership, etc., this RFP/contract shall be considered to be assigned to the new entity and such an act shall not affect the rights of the Company and the Bidder under this RFP.

8.12. Insurance

Any losses or damages caused by the bidder or any of their representative on site/client premise, bidder will be liable to pay. To prevent this will appreciate an insurance policy to be in place, which will be discussed with final shortlisted bidder.

8.13. Inspection of Records and Audit

All records of Vendor with respect to any matters covered under this Agreement shall be made available to the Company or its designees at any time during normal business hours, as often as the Company deems necessary, to audit, examine, and make excerpts or transcripts of all relevant data. Said records are subject to examination. Company would execute confidentiality agreement with the Bidder, provided that the Vendors would be permitted to submit their findings to the Company, which would be used by the Company. The scope of such audit would be limited to Service being covered under this Agreement, and financial information would be excluded from such inspection, which will be subject to the requirements of statutory and regulatory authorities. BGSS and its parent organization-Bank of Baroda (BOB) also reserve the right to conduct an audit regarding the services provided by the Vendor. The Vendor should allow the Reserve Bank of India (RBI) or Bank of Baroda (BOB) or persons authorized by it to access BGSS - Vendor transaction related documents, records or transaction or any other information given to, stored or processed by the Vendor within a reasonable time failing which the Vendor will be liable to pay any charges/ penalty levied by RBI. BGSSL reserves right to ascertain information from the Banks and other institutions to which the bidders have rendered their services for execution of similar projects.

8.14. Publicity

The Bidder shall not make any press releases or statements of any kind including advertising using the name or any service marks or trademarks of the Company regarding the contract or the transactions contemplated hereunder without the explicit written permission of the Company. The Bidder shall not, use the Company's name as a reference, without the express written permission of the Company first being obtained, and then only strictly in accordance with any limitations imposed in connection with providing such consent. The Company agrees not to use the Bidder's trade or service marks without the Bidder's prior written consent.

8.15. Solicitation of Employees

During the term of the Contract and for a period of two years after any expiration of the contract period/termination or cancellation of the Contract, both the parties agree not to hire, solicit, or accept solicitation (either directly, indirectly, or through a third party) for their employees directly involved in this contract during the period of the contract and two year thereafter, except as the parties may agree on a case-by-case basis. The parties agree that for the period of the contract and two year thereafter, neither party will cause nor permit any of its directors or employees who have knowledge of the agreement to directly or indirectly solicit for employment the key personnel working on the project contemplated in this proposal except with the written consent of the other party.

The above restriction would not apply to either party for hiring such key personnel who

1. Initiate discussions regarding such employment without any direct or indirect solicitation by the other

party; or
2. Respond to any public advertisement placed by either party or its affiliates in a publication of general circulation

8.16. Visitorial Rights

The Company and its authorized representatives, including Reserve Bank of India (RBI) or Bank of Baroda (BOB) any other regulator shall have the right to visit any of the empaneled Bidder's premises without prior Request for Proposal – Selection of notice to ensure that data provided by the Company is not misused. The selected bidder shall cooperate with the authorized representative/s of the Company and shall provide all information/ documents required by the Company.

8.17. Monitoring and Audit

Compliance with security best practices may be subject to Monitoring and Audit or Inspection of Records by various periodic security audits performed by or on behalf of authorized representatives of BGSSL or Bank of Baroda (BOB) or Reserve Bank of India (RBI) or any governing authority. The periodicity of these audits will be decided at the discretion of the Company. These audits may include, but are not limited to, a review of: access and authorization procedures, physical security controls, backup and recovery procedures, security controls and program change controls. To the extent that the Company deems it necessary to carry out a program of inspection and audit to safeguard against threats and hazards to the confidentiality, integrity, and availability of data, the selected bidder shall afford the Company's representatives access to the selected bidder's facilities, installations, technical resources, operations, documentation, records, databases and personnel. The selected bidder must provide the Company access to various monitoring and performance measurement systems (both manual and automated). The Company has the right to get the monitoring and performance measurement systems (both manual and automated) audited without prior approval/notice to the selected bidder.

8.18. Guarantees

1. Bidder shall guarantee that the Services/software/solution and allied components used to service the Company are licensed and legal.
2. The Bidder also undertakes to keep all the licenses in force till the expiry of the contract period by renewing them as and when necessary.

8.19. Force Majeure

1. The Selected Bidder shall not be liable for forfeiture of its performance security, liquidated damages or termination for default, if any to the extent that its delay in performance or other failure to perform its obligations under the contract is the result of an event of Force Majeure. Each party shall within a week inform the other of the existence of a Force Majeure Event and shall consult together to find a mutually acceptable solution.
2. For purposes of this Clause, "Force Majeure" means an event explicitly beyond the reasonable control of the Selected Bidder and not involving the Selected Bidder's fault or negligence and not foreseeable. Such events may be due to or as a result of or caused by act of God, wars, insurrections, riots, earth quake and fire, revolutions, civil commotion, floods, epidemics, quarantine restrictions, trade embargos, declared general strikes in relevant industries, satellite failure, act of Govt. of India, events not foreseeable but does not include any fault or negligence or carelessness on the part of the parties, resulting in such a situation. In the event of any such intervening Force Majeure, either party shall notify the other in writing of such circumstances or the cause thereof immediately within five calendar days.
3. Unless otherwise directed by the Company in writing, the Selected Bidder shall continue to perform its obligations under the Contract as far as is reasonably practical, and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event.
4. In such a case the time for performance shall be extended by a period(s) not less than duration of such delay. If the duration of delay continues beyond a period of three months, the Company and the Selected Bidder shall hold consultations in an endeavor to find a solution to the problem.
5. Notwithstanding above, the decision of the Company shall be final and binding on the Selected Bidder.

8.20. Resolution of Disputes

1. The Company and the selected bidder shall make every effort to resolve amicably, by direct informal negotiation between the respective project managers of the Company and the selected bidder, any disagreement or dispute arising between them under or in connection with the contract.
2. If the Company project manager and Empanelled bidder's project manager are unable to resolve the dispute after thirty days from the commencement of such informal negotiations, they shall immediately escalate the dispute to the senior authorized personnel designated by the selected bidder and Company respectively.
3. If after thirty days from the commencement of such negotiations between the senior authorized personnel designated by the selected bidder and Company, the Company and the selected bidder have been unable to resolve amicably a contract dispute; either party may require that the dispute be referred for resolution through formal arbitration.

8.21. Arbitration:-

1. Any dispute, controversy or claims arising out of or relating to this RFP, its validity, breach or termination thereof, shall be settled by arbitration in accordance with the provisions of the Indian Arbitration and Conciliation Act, 1996.
2. All questions, claims, disputes or differences arising under and out of, or in connection with the RFP/ subsequent contract or carrying out of the work whether during the progress of the work or after the completion and whether before or after the determination, abandonment or breach of the RFP/ subsequent contract shall be referred to arbitration by a sole Arbitrator to be appointed by the Parties.
3. The place of arbitration shall be at Gandhinagar.
4. The arbitral procedure shall be conducted in the English and any award or awards shall be rendered in English. The procedural law of the arbitration shall be the Indian law.
5. The award of the arbitrator shall be final and conclusive and binding upon the Parties, and the Parties shall be entitled (but not obliged) to enter judgment thereon in any one or more of the highest courts having jurisdiction. The Parties further agree that such enforcement shall be subject to the provisions of the Indian Arbitration and Conciliation Act, 1996 and neither Party shall seek to resist the enforcement of any award in India on the basis that award is not subject to such provisions.
6. The rights and obligations of the Parties under or pursuant to this Clause, including the arbitration clause in this RFP, shall be under the exclusive jurisdiction of the courts located at Gandhinagar only.
7. If a notice has to be sent to either of the parties following the signing of the contract, it has to be in writing and shall be first transmitted by facsimile transmission by postage prepaid registered post with acknowledgement due or by a reputed courier service, in the manner as elected by the Party giving such notice. All notices shall be deemed to have been validly given on (i) the business date immediately after the date of transmission with confirmed answer back, if transmitted by facsimile transmission, or (ii) the expiry of five days after posting if sent by registered post with A.D., or (iii) the business date of receipt, if sent by courier.

8.22. Governing Law and Jurisdiction

This RFP and subsequent agreement with the Selected Bidders shall be governed and construed in accordance with the laws of India and courts in Gandhinagar, Gujarat will have the exclusive jurisdiction to determine the issues arising out of this RFP.

8.23. Corrupt and Fraudulent practice

1. As per Central Vigilance Commission (CVC) directives, it is required that Bidders observe the highest standard of ethics during the procurement and execution of such contracts in pursuance of this policy.
2. "Corrupt Practice" means the offering, giving, receiving or soliciting of anything of value to influence the action of an official in the procurement process or in contract execution.
3. "Fraudulent Practice" means a misrepresentation of facts in order to influence a procurement process or the execution of contract to the detriment of the Company and includes collusive practice among

Bidders (prior to or after bid submission) designed to establish bid prices at artificial non-competitive levels and to deprive the Company of the benefits of free and open competition.

4. The Company reserves the right to reject a proposal for award if it determines that the Bidder recommended for award has engaged in corrupt or fraudulent practices in competing for the contract in question.
5. The Company reserves the right to declare a Bidder ineligible, either indefinitely or for a stated period of time, to be awarded a contract if at any time it determines that the firm has engaged in corrupt or fraudulent practices in competing for or in executing the contract.
6. The successful bidder will be required to enter into an integrity pact with the Company as per the CVC guidelines. The integrity pact is available on the CVC website.

8.24. Waiver

No failure or delay on the part of either party relating to the exercise of any right, power, privilege or remedy provided under this RFP or subsequent agreement/contract with the other party shall operate as a waiver of such right, power, privilege or remedy or as a waiver of any preceding or succeeding breach by the other party nor shall any single or partial exercise of any right, power, privilege or remedy preclude any other or further exercise of such or any other right, power, privilege or remedy provided in this RFP all of which are several and cumulative and are not exclusive of each other or of any other rights or remedies otherwise available to either party at law or in equity.

8.25. Non-Exclusive

It is expressly understood and agreed by the Parties that the agreement will be a non-exclusive agreement. Nothing in the Agreement or RFP will be construed as creating any exclusive arrangement with the Bidder or as prohibit the Company from either acquiring similar, equal, or like goods and/or Services or from executing additional agreements with other entities or sources.

8.26. Violation of Terms

The Company clarifies that the Company shall be entitled to an injunction, restraining order, right for recovery, specific performance or such other equitable relief as a court of competent jurisdiction may deem necessary or appropriate to restrain the bidders from committing any violation or enforce the performance of the covenants, obligations and representations contained in this RFP. These injunctive remedies are cumulative and are in addition to any other rights and remedies the Company may have at law or in equity, including without limitation a right for recovery of any amounts and related costs and a right for damages.

8.27. Addition/Deletion of Qualified Offerings

1. Both parties agree that the intent of this RFP is to establish an initial set of service offerings. The Company recognizes that, as the use of these services expands, it is possible that additional services and/or service categories will be needed... Company may request a change order in the event of actual or anticipated change(s) to the agreed scope of work, services, deliverables and schedules. The selected bidder shall prepare a change order reflecting the actual or anticipated change(s) including the impact on deliverables schedule. The selected bidder shall carry out such services as required by the Company. The terms of the contract would apply to such incremental deliverables and services.
2. The selected bidder shall agree that the price for incremental offering cannot exceed the original proposed cost and the Company reserves the right to re-negotiate the price. At the unit rates provided for TCO calculations, the Company has the right to order as much as it wants at those rates. However, this excludes the hardware to be provided by the Bidder at their cost due to under sizing.
3. The Company is under no obligation to honor such requests to add service categories or amend this contract.
4. As a method for reviewing selected bidder's services and Company requirements, the Company will sponsor regular reviews to allow an exchange of requirements and opportunities.
5. All quantities mentioned in this RFP are indicative. The quantities of components to be procured as part of this RFP can be varied by the Company. This also includes the right to modify the number of source

systems, targets, reports & statements, dash boards, score cards, concurrent users etc.

8.28. Service Level Agreement and Non-Disclosure Agreement

The selected vendor shall execute:

a) **Service Level Agreement (SLA),** which must include all the services and terms and conditions of the services to be extended as detailed herein, and as may be prescribed or recommended by the Company.

b) **Non-Disclosure Agreement (NDA),** the selected vendor shall execute the SLA and NDA within two months the date of acceptance of letter of appointment or as intimated by the Company.

The stamp duty or any other associated charges to execute the above mentioned document shall be borne by the successful bidder.

8.29. Liquidated Damages and Penalty

1. Except in cases where the circumstances are beyond the control of the Bidder, the BGSSL may levy a penalty in case of errors, as a result of fraud or otherwise, by the Bidder or its personnel. The same will be based on defect definitions, defect charge criteria and associated charges as may be mutually agreed upon in writing from time to time.
2. The empaneled Bidder will be liable to pay a penalty of 1% of one month's charges paid to the empaneled Bidder or charges as may be mentioned in the Schedule to the agreement (whichever is higher) under the Agreement if the Bidder fails to render the services/ goods in accordance to the provisions of the Agreement signed between the empanelled Bidder and the BGSS.
3. The penalties and liquidated damages may be waived of in case the delay is for reasons attributable to BGSSL and Force Majeure. However, it shall be the responsibility of the Bidder to prove that the delay is attributed to BGSSL and Force Majeure. The Company may deduct the amount of penalty out of the payment to be made to the Bidder's fee.
4. If the Service Provider fails to perform its obligations as per the Agreement, then BGSSL reserves the right to get the balance work executed by another service provider as per the choice of BGSSL.
5. Since some of the payment terms warrant monthly/quarterly payouts from Company vis-à-vis SLA monitoring, it is to be noted that any such monthly/quarterly payments will be released and penalties if any, as defined by SLAs, shall be adjusted in the payment for the last month. Balance penalties, if any shall be levied in the payment for the subsequent months.

8.30. Set Off

Without prejudice to other rights and remedies available to the company it shall be entitled to earmark, set- off or adjust any amounts due to the company, under any clause of the RFP, from the selected bidder Provider against payments due and payable by the company to the selected bidder/Service Provider for the services rendered.

The provisions of this Clause shall override all other clauses and shall survive the termination of this Agreement. The selected Bidder/Service Provider shall not have the right to contest or dispute the Company's decision to exercise set-off, and such decision shall be final and binding.

8.31. Information Ownership

All information processed, stored, or transmitted by equipment belongs to the Company. By having the responsibility to maintain the equipment, the Bidder does not acquire implicit access rights to the information or rights to redistribute the information or any kind of ownership over the information. The Bidder understands that civil, criminal, or administrative penalties may apply for failure to protect information appropriately.

8.32. Sensitive Information

Any information considered sensitive must be protected by the selected bidder from unauthorized disclosure, modification or access. In the event of any security incidents, the selected bidder shall promptly notify the Company, provide a detailed incident report, and take immediate corrective actions to rectify and prevent

further breaches. Additionally, the selected bidder shall indemnify the Company against any losses, liabilities, or damages arising from the mishandling, unauthorized disclosure, or improper access to sensitive information by the Bidder or its representatives.

Types of sensitive information that will be found on Company's systems the selected bidder may support or have access to include, but are not limited to: Information subject to special statutory protection, legal actions, disciplinary actions, complaints, IT security, pending cases, civil and criminal investigations, etc.

8.33. Privacy and Security Safeguards

1. The selected bidder shall not publish or disclose in any manner, without the Company's prior written consent, the details of any security safeguards designed, developed, or implemented by the selected bidder under this contract or existing at any Company location. The selected bidder shall develop procedures and implementation plans to ensure that IT resources leaving the control of the assigned user (such as being reassigned, removed for repair, replaced, or upgraded) are cleared of all Company data and sensitive application software & data. The selected bidder shall also ensure that all sub-contractors who are involved in providing such security safeguards or part of it shall not publish or disclose in any manner, without the Company's prior written consent, the details of any security safeguards designed, developed, or implemented by the selected bidder under this contract or existing at any Company location.
2. The Bidder shall ensure that it remain compliant with Data Protection Laws of India as may be amended from time to time and shall keep and retain all the data including but not limited to Confidential Information on the servers located within the territory of India.
3. In such circumstances wherein the bidder becomes non-compliant at to the Data Protection Laws as agreed under sub-clause (b) hereinabove, the bidder shall be liable with the penalties as set forth in the applicable laws from time to time.
4. Any breach of this confidentiality obligation shall be considered a material breach of contract, and the company reserves the right to terminate the agreement with the selected bidder. Additionally, the selected bidder shall be liable for any damages, losses, or legal consequences arising from such unauthorized disclosures.

8.34. Confidentiality

A. "Confidential Information" means any and all information that is or has been received by the selected bidder ("Receiving Party") from the Company ("Disclosing Party") and that relates to the Disclosing Party; and is designated by the Disclosing Party as being confidential or is disclosed in circumstances where the Receiving Party would reasonably understand that the disclosed information would be confidential or is prepared or performed by or on behalf of the Disclosing Party by its employees, officers, directors, agents, representatives or consultants.

B. The Parties acknowledge that the existence and the terms of this Agreement and any oral or written information exchanged between the Parties in connection with the preparation and performance of this Agreement are regarded as "Confidential Information". Each Party shall maintain confidentiality of all such information and without obtaining the written consent of the other Party, it shall not disclose any relevant Confidential Information to any third parties, except for the information that:

C. Is or will be in the public domain (other than through the receiving Party's unauthorized disclosure); or

D. Is under the obligation to be disclosed pursuant to the applicable laws or regulations, rules of any stock exchange, or orders of the Court or other government authorities; or

E. Is required to be disclosed by any Party to its shareholders, investors, legal counsels or financial advisors regarding the Services contemplated hereunder, provided that such shareholders, investors, legal counsels or financial advisors shall be bound by the staff members or agencies hired by any Party shall be deemed disclosure of such Confidential Information by such Party, which Party shall be held liable for breach of this Agreement. This Section shall survive the termination of this Agreement for any reason. Without limiting the generality of the foregoing, Confidential Information shall mean and include any information, data, analysis, compilations, notes, extracts, materials, reports, drawings,

designs, specifications, graphs, layouts, plans, charts, studies, memoranda or other documents, or materials relating to the licensed software, the modules, the program documentation, the source codes, the object codes and all enhancements and updates, services/goods, systems processes, ideas, concepts, formulas, methods, know how, trade secrets, designs, research, inventions , techniques, processes, algorithms, schematics, testing procedures, software design and architecture, computer code, internal documentation, design and function specifications, product requirements, problem reports, analysis and performance information, business affairs, projects, technology, finances (including revenue projections, cost summaries, pricing formula), clientele, markets, marketing and sales programs, client and customer data, appraisal mechanisms, planning processes, etc. or any existing or future plans, forecasts or strategies in respect thereof.

F. "Confidential Materials" shall mean all tangible materials containing Confidential Information, including, without limitation, written or printed documents and computer disks or tapes, whether machine or user readable. Information disclosed pursuant to this clause will be subject to confidentiality forever.

G. Nothing contained in this clause shall limit the selected bidder from providing similar services/goods to any third parties or reusing the skills, know-how and experience gained by the employees in providing the services/goods contemplated under this clause, provided further that the selected bidder shall at no point use the Company's confidential information or Intellectual property.

H. The Receiving Party shall, at all times regard, preserve, maintain and keep as secret and confidential all Confidential Information and Confidential Materials of the Disclosing Party howsoever obtained and agrees that it shall not use the Company's confidential information or IPR, without obtaining the written consent of the Company.

8.35. Disclosing Party

A. The Disclosing Party shall disclose, transmit, reproduce or make available any such Confidential Information and materials to any person, firm, company or any other entity other than its directors, partners, advisers, agents or employees, sub-contractors and contractors who need to know the same for the purposes of maintaining and supporting the solution provided as a part of the RFP/ Contract. The Receiving Party shall be responsible for ensuring that the usage and confidentiality by its directors, partners, advisers, agents or employees, sub-contractors and contractors is in accordance with the terms and conditions and requirements of this RFP; or

B. Unless otherwise agreed herein, use of any such Confidential Information and materials for its own benefit or the benefit of others or do anything prejudicial to the interests of the Disclosing Party or its customers or their projects.

C. In maintaining confidentiality hereunder, the Receiving Party on receiving the Confidential Information and materials agrees and warrants that it shall:

   i. Take at least the same degree of care in safeguarding such Confidential Information and materials as it takes for its own confidential information of like importance and such degree of care shall be at least, that which is reasonably calculated to prevent such inadvertent disclosure

   ii. Keep the Confidential Information and Confidential Materials and any copies thereof secure and in such a way so as to prevent unauthorized access by any third party

   iii. Limit access to such Confidential Information and materials to those of its directors, partners, advisers, agents or employees, sub-contractors and contractors who are directly involved in the consideration/evaluation of the Confidential Information and bind each of its directors, partners, advisers, agents or employees, sub-contractors and contractors so involved to protect the Confidential Information and materials in the manner prescribed in this document

   iv. Upon discovery of any unauthorized disclosure or suspected unauthorized disclosure of Confidential Information, promptly inform the Disclosing Party of such disclosure in writing and immediately return to the Disclosing Party all such information and materials, in whatsoever form, including any and all copies thereof

D. The Receiving Party who receives the Confidential Information and Materials agrees that on receipt of

a written demand from the Disclosing Party, immediately return all written Confidential Information, Confidential Materials and all copies thereof provided to, or produced by it or its advisers, as the case may be, which is in Receiving Party's possession or under its custody and control

E. To the extent practicable, immediately destroy all analyses, compilations, notes, studies, memoranda or other documents prepared by it or its advisers to the extent that the same contain, reflect or derive from Confidential Information relating to the Disclosing Party
F. So far as it is practicable to do so, immediately expunge any Confidential Information relating to the Disclosing Party or its projects from any computer, word processor or other device in its possession or under its custody and control
G. To the extent practicable, immediately furnish a certificate signed by its director or other responsible representative confirming that to the best of his/her knowledge, information and belief, having made all proper enquiries, the requirements of this paragraph have been fully complied with
H. The rights in and to the data/information residing at the Company's premises, even in the event of disputes shall at all times solely vest with the Company
I. The Bidder represents and agrees that during the term of this RFP and subsequent contract, the Company shall not be responsible for any loss/damage (including malfunctioning or non-functioning of Deliverables) caused to the Deliverables for any reason, unless such loss/damage (including malfunctioning or non-functioning of Deliverables) is caused due to the willful act or gross willful misconduct of the Company or any of its personnel as certified jointly by the Company and Selected bidder. In such an event, the selected bidder shall promptly repair and/or replace the non- performing Deliverable with a suitable replacement, if required, without affecting the service level standards in this RFP.
J. The restrictions in the preceding clause shall not apply to:
    i. Any information that is publicly available at the time of its disclosure or becomes publicly available following disclosure (other than as a result of disclosure by the Disclosing Party contrary to the terms of this document); or any information which is independently developed by the Receiving Party or acquired from a third party to the extent it is acquired with the valid right to disclose the same
    ii. Any disclosure required by law or by any court of competent jurisdiction, the rules and regulations of any recognized stock exchange or any enquiry or investigation by any governmental, statutory or regulatory body which is lawfully entitled to require any such disclosure provided that, so far as it is lawful and practical to do so prior to such disclosure, the Receiving Party shall promptly notify the Disclosing Party of such requirement with a view to providing the Disclosing Party an opportunity to obtain a protective order or to contest the disclosure or otherwise agree to the timing and content of such disclosure.
K. The Confidential Information and Materials and all copies thereof, in whatsoever form shall at all times remain the property of the Disclosing Party and its disclosure hereunder shall not confer on the Receiving Party any rights whatsoever beyond those contained in this document or subsequent agreement
L. Confidential Information is any and all proprietary information disclosed by one party to the other. Confidential Information does not include information that is or becomes available to the recipient prior to the party providing such information or is public information in accordance with the applicable laws. Software in human-readable form (e.g. source code) and the Company's data values stored in computers will be considered Confidential Information whether or not marked as such.
M. The selected bidder shall also undertake to keep confidential all information (written or oral) concerning all facts of the business of the Company, which has been obtained or understood during the course of the assignment.

The confidentiality obligations shall survive the expiry or termination of the agreement/contract between the Selected Bidder and the Company.

8.36. Advancements

The selected bidder shall take reasonable and suitable action, considering economic circumstances, at mutually agreed increase/decrease in charges, and the Service Levels, to provide the Services/goods to the Company at a level that will enable the Company to take advantage of advancement in the industry from time to time.

8.37. Intellectual Property Rights

1. The Bidder claims and represents that it has obtained appropriate rights to provide the Deliverables upon the terms and conditions contained in this RFP.
2. The Bidder and the Company each acknowledge that performance of this Agreement, may result in the discovery, creation or development of inventions, methods, techniques, improvements, software designs, computer programs, strategies, data and other original works of authorship (collectively, the "Work Results").
3. Title to all Work Results and discoveries made by the Bidder resulting from the Work performed as per this Agreement shall reside in the Bidder.
4. Title to all Work Results made jointly by the Company and the Bidder, on the basis of the joint efforts recorded in writing from the work performed or Services rendered under this Agreement whether at the request of the Company or not shall reside jointly in the Company and the Bidder.
5. The Bidder shall in no manner shall use the Intellectual Property Rights i.e., Trademarks, Copyrights, name of the Company, etc. of the Company in any advertisement or other promotional activities without prior written confirmation from the Company. Such failure on the part of Bidder shall be deemed to be a Default made by the Bidder and be treated in accordance to the terms of this Agreement.
6. The Intellectual Property Rights shall be determined in accordance with Indian Laws.

8.38. Grievance Redressal

Any vendor who claims to have a grievance against a decision or action with regards to the provisions of this RFP may file a request at cs@bgss.in it may please be noted that the grievance can be filed by only that vendor who has participated in Procurement proceedings in accordance with the provisions of this RFP.

---------- End of the Document ----------

Annexures & Appendices

Annexure A	Eligibility Criteria

Appendix 01	Technical Bid
Appendix 02	Commercial Bid
Appendix 03	Authorization letter format for bid opening
Appendix 04	Bid undertaking letter
Appendix 05	Pre- Integrity Pact
Appendix 06	Conformity letter
Appendix 07	Pre Bid query format
Appendix 08	C-SOC MSSP experience details
Appendix 09	Bid Declaration Certificate (for MSME / Startup registered Bidders)