STATE BANK OF INDIA

Expression of Interest (EOI)

Setting up Next Gen Global Security Operations Centre (Next Gen GSOC)

EOI No.: SBI/GITC/SOC/2018/2019/30
Dated: 08/10/2018

**Security Operations Centre,
Information Security Department,
State Bank Global IT Centre,
'A'- Wing, Ground Floor,
Sector 11, CBD Belapur,
Navi Mumbai 400614 (Maharashtra)
INDIA**

Table of Contents

1. EOI Schedule and Address

Sr	Event	Date and Time
1.	Issuance of Expression of Interest (EOI) Document	08/10/2018
2.	Last Date and Time for completed EOI document submission	29/10/2018** Time 03.00 p.m.
3.	Opening of EOI	29/10/2018 Time 04.00 p.m.
4.	Address for EOI submission and all communication on the subject (Bank Address)	Dy. General Manager (SOC), Information Security Department (ISD), ‘A’ Wing, Ground Floor, State Bank Global IT Centre, Sector 11, CBD Belapur, Navi Mumbai 400614 (Maharashtra) Email : dgm.soc@sbi.co.in ; Cc agm1.soc@sbi.co.in; dc.balani@sbi.co.in Tel : 022-27537328 & 022-27537329

** In case the designated day happens to be a holiday; the next working day will be deemed as the last date for submission of EOI.

2. Introduction

a. State Bank of India **(SBI)** is the largest Bank in India with a network of around 25000 branches spread across India. The Bank also has presence in 35 countries across the globe. The Bank offers wide range of products and services to both Corporate and Retail Customers. The Bank also has one of the largest ATM networks of more than 60000 ATMs spread across the geographical locations. Bank also provides services to its customers through alternate channels such as Internet Banking, YONO, Payment Gateways and Mobile Banking etc. To expand the reach further, Bank has also deployed the cutting-edge technologies and innovative new banking models. The Bank has well established IS Security Policies, Standards and Procedures.

b. The Bank has various IT Security technologies like Firewalls, IPS/IDS, Load Balancers, WAF, Active Directory, Anti-virus, NAC, DLP, PIMS, ITAM, ITSM, EDR from number of OEMs etc.

c. The Bank already has a captive Security Operations Centre (SOC) setup in the year 2013 for real time monitoring of events for alerts on 24X7x365. Currently, SOC technologies such as SIEM, DAM, VM, NBAD, Firewalls Risk Management and Incident Management are deployed in the existing SOC.

d. Keeping in view the regulatory requirements in India (RBI, CERT-In, NCIIPC etc.) and foreign geographies, increasing innovative cyber threats and malwares, threats emanating from emerging technologies like AI/ML, blockchain, cryptocurrencies, bots, darkwebs, social engineering, cloud etc., it has been decided to setup a 24x7x365 basis operating state-of-the-art Next Gen Global Security Operations Centre (GSOC) for proactive monitoring as also predicting cyber-attacks (internal and external) on the Bank’s information processing setup.

3. Background

a. Objective of Expression of Interest (EOI)

State Bank of India (Bank) intends to select leading, reputed and experienced Applicants / Bidders in the Security Operations Centre (SOC) domain to supply technologies, deploy and integrate them cohesively with the IT setup of the Bank and manage the proposed Next Gen Global Security Operation Centre (GSOC) at SBI for five years on 24x7x365 days basis.

b. Invitation

Expression of Interest (EOI) is invited in a sealed envelope superscripted with "Expression of Interest (EOI) – setting up of Next Gen Global Security Operations Centre (GSOC)"

i. From the applicants / bidders who meet the eligibility criteria as set out in Annexure – "A".
ii. Who have solution strictly in line with the Broad Scope of Work as set out in this EOI and
iii. Agree to abide by the terms and conditions contained in this document.

Please note that the EOI is not a qualification criterion. Bank will float an Open/Closed RFP at its own discretion.

By participating in this EOI process, applicant / bidder confirms that they are in complete agreement with the Bank as per all the Terms and Conditions of this EOI.

A Sealed envelope containing complete set of signed hard copy of EOI document and a soft copy thereof (in a CD/DVD) should be submitted by post to or be delivered in person at the undernoted office (on any working day) on or before the date and time mentioned in "EoI Schedule and Address" section of this document.

4. Applicant's / Bidder's Eligibility Criteria

This EOI is open to all applicants / bidders who fulfil the eligibility criteria as set out in Annexure-'A' of this document and is in agreement with the Bank as per terms and conditions of this EOI document. The applicant should furnish documentary evidence supporting and information provided by them as per the EOI process.

Bidder could be System Integrator (SI) partnering with OEMs of SOC technologies and front ending for the project or OEM who is also a system integrator, partnering with other SOC technologies OEMs and front ending for the entire project.

The bidder needs to share the choice of OEM for each SOC technology proposed in response to this EOI. The bidder should restrict to only one OEM option for each SOC technology and describe relationship between bidder & respective OEM.

5. Broad Scope of Work

The bidder needs to highlight their ability to supply, deploy, integrate, migrate data & logs from existing SOC of the Bank and run very large and complex Next Gen Global SOC (GSOC), manage partnerships with the OEMs of SOC solutions. The broad scope of the work is as below.

The SI and OEMs are responsible for following –

1. System Integrator – Supply GSOC technologies, integrate GSOC with source IT systems, provide onsite L1 & L2 human resources for first 1 - 2 years and manage the project.
2. OEM – Deploy, install, integrate their own solution with every other solution / technology deployed in the GSOC setup, deploy L3 and L4 onsite resources, automation of L1 & L2 activities within first year, migration of data and logs from current SOC to new GSOC.

The bidder has to supply, deploy, integrate (within GSOC setup and logs source systems), operate and manage the GSOC in SBI premise for 5 years. The GSOC must be up and running in totality by 31st March 2019.

a. Supply of indicative Next Gen Global SOC (GSOC) solutions –

    1. Security Information and Event Management (SIEM)
    2. Big Data Lake exclusively for collating the logs received by SOC, performing analytics, normalization, threat analysis and retention of both raw and normalized logs for regulatory compliance purpose.
    3. User and Entity Behavior Analytics (UEBA)
    4. Security Orchestration, Automation and Response (SOAR)
    5. Cognitive AI & ML Based Incident detection and analysis (AI/ML)
    6. Database Activity Monitoring (DAM)
    7. Vulnerability Management (VM)
    8. Network Behavior Analysis (NBA)
    9. IT – Governance, Risk & Compliance (IT-GRC)
    10. Sandboxing and Malware reverse engineering tools
    11. Red and Blue teaming tools
    12. Threat Intelligence Platform

b. The GSOC should have following broad strong capabilities from day 1:

    1. Total compliance to RBI cyber security framework circular instructions dated 2nd June 2016 and all preceding circular and guidelines related to information security requirements in the Bank.
    2. Ability to sustain the size, complexity and geographic spread of Bank’s IT infrastructure and its growth YoY. Presently, 3 Lakh + desktops with various agents like AV, NAC and 60000+ IT systems including Servers, Network and Security systems, Cloud and 500+ applications etc. are deployed in the Bank. Please refer “Logs Source systems for GSOC” section below for log sources.
    3. Architecture should have multi-tier, distributed, high availability (DC and DR) deployment having flexibility to deploy on premise as well as on private cloud.
    4. Self-learning, proactive, predictive & cognitive by completely leveraging AI/ML and deep analytics.
    5. Robotic process automation (RPA) for all daily routine activities like L1 and L2 incident creation leveraging SOAR. False positive rate to be less than 2 % with a confidence level for each auto incident created to be more than 85% in the beginning to be achieved beyond 90% within first 6 months.
    6. Structured and unstructured data i.e. all the events to be stored in data lake like environment.
    7. Identify Known and unknowns threat, outliers, bots identification.

8. Malware analysis/re-engineering and Sandboxing capabilities.
9. Anti-phishing, Antimalware, anti-rogue mobile application, brand abuse across State Bank Group.
10. Continuous Red teaming, Blue teaming exercises with 100 % detection by GSOC for every security incident.
11. Digital forensic investigation with complete replay of attack including the ingress and egress of payload.
12. Continuous collaboration with global threat intelligence stakeholders.
13. Perform advanced threat hunting on real-time basis.
14. Proactive and predictive capabilities for identifying potential threats, threat campaign by adversaries along with heat map and confidence score of above 70% for predictive capabilities.
15. SIEM including Deep Packet Inspection capabilities, UEBA, IT-GRC, SOAR and Big Data Lake platform must be single point of collation / convergence of logs from GSOC technologies, Security, Operational and Emerging technologies for correlation, analytics and must provide 360 degree real-time analysis and incident reporting.
16. Logs collated by GSOC technologies from all log sources as enumerated below must be correlated on real-time basis within SIEM, UEBA, SOAR, IT-GRC for depicting conclusive complete kill chain of incident and report the same to stakeholders on real-time basis.
17. SOC must be able to detect attacks emanating from emerging technologies.
18. Configuration and Customization of the tools as per SBI requirements on ongoing basis.
19. Uptime of each component level at minimum 99.99% on quarterly basis.

c. <u>Logs source systems for GSOC:</u>

1. Security technologies such as Firewall, IPS/IDS, WAF, LB, SSL interceptor / inspection, AV, AD, EDR, APT, Honeypots, NAC, DLP, IAM, FIM, SSO, PIMS, ITAM, encryption/masking/hashing technologies are not considered as SOC technologies in SBI. These are feeder technologies / source system of logs provided to the GSOC.
2. Operational technologies include OS, databases (traditional and big data), webservers, applications, networking technologies, middleware, virtualization and cloud technologies (private/hybrid/public) i.e. entire IT infrastructure and business applications (like CBS, Internet Banking, Mobile Banking, YONO etc.) These are feeder technologies / source system of logs provided to the GSOC.
3. Emerging technologies include chatbots, voice bots, blockchain, cryptocurrency, augmented & virtual reality, IOT. These are feeder technologies / source system of logs provided to the GSOC.
4. We have technologies deployed from all major OEMs in each log sources technology type.
5. Bank is not intending to position the SOC for financial or non-financial transaction fraud risk management system.

Note : The technologies cited above as log source systems must not be proposed by bidder as a part of GSOC.

6. <u>Process before submission of EOI</u>

a. Modification in Request for EOI document:

At any time prior to the deadline for submission of EOI, SBI may modify any part of this document. Such change(s) if any may be in the form of an addendum /corrigendum and will be uploaded in Bank's website at https://bank.sbi

All such change(s) will automatically become part of this EOI and binding on all applicants. Interested applicants are advised to regularly refer the Bank's URL referred above.

b. Extension of date of submission of EOI:

Request for extension of date for submission of EOI will not be entertained. However, the Bank at its discretion may extend the deadline in order to allow prospective applicants / bidder a reasonable time to take the amendment / changes, if any into account**.**

7. <u>Format and Signing of EOI</u>

a. The applicant should prepare EOI strictly as desired in this Request for EOI Document.

1. EOI should be typed (*font: Arial; Size: 12)* and submitted on A4 size paper, spirally and securely bound and with all pages therein in serial order.
2. All pages of the EOI should be signed only by the authorized person(s) of the company/firm/bidder. Any interlineations, erases or overwriting shall be valid only if the person(s) signing the EOI authenticates them. The EOI should bear the rubber stamp of the applicant on each page except for the un-amendable printed literature.
3. The applicants / bidder should demonstrate that they meet eligibility criteria given in Annexure – 'A' of this EOI.
4. As a part of this EOI, the applicant has to submit detailed approach paper on how they propose setting up of Next Gen Global Security Operations Centre (GSOC) along with the requirements, Annexure-'B' and Annexure-'C' to setup the same.
5. Power of Attorney should be submitted to support the authorized signatory status. Contact detail of the authorized signatory and an authorized contact person on behalf of the applicant is to be provided as under: -

Particulars	Authorized Signatory for signing the EOI	Authorized contact person
Name		
Designation		
Email ID		
Landline		
Mobile No		
Fax No.		
Address		

6. EOI should comprise of

(i) Request for EOI document duly signed & stamped on each page

(ii) Your EOI in the proposed initiative along with documents / information / confirmation on the requirements as mentioned in this document with necessary supporting documents duly signed & stamped
(iii) Proposed solution document with suggested deployment architecture and related official supporting. It should include the requirements / sizing on deployment
(iv) Completed EOI Documents along with Annexure -'B' and Annexure – 'C' should be submitted in prescribed time line.

b. In case any discrepancy is observed between hard and soft copy, the hard copy will be considered as the base document.

8. **Process after submission of EOI**

a. All EOIs received by the designated date and time will be examined by the Bank to determine if they meet criteria/terms and conditions mentioned in this document including its subsequent amendment(s), if any, and whether EOI is are complete in all respects.
b. On scrutiny, the EOI is found NOT in desired format /illegible /incomplete /not containing clear information, in view of SBI, to permit thorough analysis or failing to fulfil the relevant requirement will be rejected for further evaluation process.
c. SBI reserves the right, at any time, to waive any of the requirements of this Request for EOI document if it is deemed in the interest of SBI.
d. If deemed necessary, the Bank may seek clarifications on any aspect of EOI from the applicant. If a written response is requested, it must be provided within 24 hours. Beyond the response received, if any, will not be considered. However, that would not entitle the applicant to change or cause any change in the substances of their EOI document already submitted. Bank may also make enquiries to establish the past performance of the applicants in respect of similar work. All information submitted in the application or obtained subsequently will be treated as confidential.
e. After examining the EOI, some or all eligible applicants may be asked to make presentation of the solution and demonstrate proof of concept.
f. SBI may shortlist the applicants who fulfil the eligibility criteria, have solution as per the requirement of the Bank and are agreeing to abide by the terms and conditions of the Bank. Bank's judgment in this regard will be final.
g. Bank may issue an Open/Closed Request for Proposal (RFP) to shortlisted applicants for inviting technical and indicative commercial bids for next process of procurement. However, please note that short listing of applicants should not be treated as a contract for the proposed work.
h. Applicants will be advised about shortlisting of their EOIs or otherwise. However, applicants will not be provided with information about comparative position of their EOIs with that of others.
i. Nothing contained in this EOI shall impair the Bank's Right to issue 'Open Tender' on the proposed solution.
j. The bidder, whose proposed solution is finally selected, shall have to provide the sizing of the solution implementable within the Bank and achieve the stated objectives.

9. Terms & Conditions:

i. Lodgement of an EOI is evidence of an applicant's consent to comply with the terms and condition of Request for EOI process and subsequent bidding process. If an applicant fails to comply with any of the terms, its EOI may be summarily rejected.
ii. Wilful misrepresentation of any fact in the EOI will lead to the disqualification of the applicant without prejudice to other actions that the Bank may take.
iii. The EOI and the accompanying documents will become property of SBI. The applicants shall be deemed to license, and grant all rights to SBI, to reproduce the whole or any portion of their product/solution for the purpose of evaluation, to disclose the contents of submission to other applicants and to disclose and/ or use the contents of submission as the basis for EOI process.
iv. SBI reserves the right to accept or reject any or all EOI s received without assigning any reason therefore whatsoever and the Bank's decision in this regard will be final.
v. No contractual obligation whatsoever shall arise from the EOI process.
vi. Any effort on the part of applicant to influence evaluation process may result in rejection of the EOI.
vii. SBI is not responsible for non-receipt of EOIs within the specified date and time due to any reason including postal delays or holidays in between.
viii. SBI reserves the right to verify the validity of information provided in the EOIs and to reject any bid where the contents appear to be incorrect, inaccurate or inappropriate at any time during the process of EOI or even after award of contract.
ix. Applicants shall be deemed to have:

a. examined the Request for EOI document and its subsequent changes, if any for the purpose of responding to it.
b. examined all circumstances and contingencies, having an effect on their EOI application and which is obtainable by the making of reasonable enquiries.
c. satisfied themselves as to the correctness and sufficiency of their EOI applications and if any discrepancy, error or omission is noticed in the EOI, the applicant shall notify the Bank in writing on or before the end date/time.

x. The applicant shall bear all costs associated with submission of EOI, presentation/POC desired by the Bank. Bank will not be responsible or liable for any cost thereof, regardless of the conduct or outcome of the process.
xi. Applicants must advise the Bank immediately in writing of any material change to the information contained in the EOI application, including any substantial change in their ownership or their financial or technical capacity. Copies of relevant documents must be submitted with their advices. For successful applicants, this requirement applies until a contract is awarded as a result of subsequent bidding process.
xii. Applicant shortlisted must not advertise or publish about the result of process / engagement with the Bank on the subject in any form without prior written permission from the SBI.
xiii. The detail scope of work will be included in the Request for Proposal (RFP document.
xiv. Subcontracting is not permitted.
xv. The Bank may review eligibility criteria, Terms & Conditions and other evaluation criteria as per requirements of the Bank at the time of publishing RFP for setting up of Next Gen Global Security Operations Centre (GSOC).
xvi. SBI shall have the right to cancel the EOI process itself at any time, without thereby incurring any liabilities to the affected Applicants. Reasons for cancellation, as determined by SBI in its sole discretion include but are not limited to, the following:

a. Services contemplated are no longer required.
b. Scope of work not adequately or clearly defined due to unforeseen circumstance and/or factors and/or new developments.
c. The project is not in the best interest of SBI.
d. Any other reason.

xvii. The Selected applicant / bidder have to get themselves annually audited by external empanelled Auditors appointed by the Bank/ inspecting official from the Reserve Bank of India or any regulatory authority, covering the risk parameters finalized by the Bank/ such auditors in the areas of products (IT hardware/ software) and services etc. provided to the Bank and the Applicants are required to submit such certification by such Auditors to the Bank. The Selected bidder and or his / their outsourced agents / sub – contractors (if allowed by the Bank) shall facilitate the same. The Bank can make its expert assessment on the efficiency and effectiveness of the security, control, risk management, governance system and process created by the Bidder. The Bidder shall, whenever required by the Auditors, furnish all relevant information, records/data to them. All costs for such audit shall be borne by the Bank.

Where any deficiency has been observed during audit of the Applicant on the risk parameters finalized by the Bank or in the certification submitted by the Auditors, the Applicant shall correct/ resolve the same at the earliest and shall provide all necessary documents related to resolution thereof and the auditor shall further certify in respect of resolution of the deficiencies. The resolution provided by the Applicant shall require to be certified by the Auditors covering the respective risk parameters against which such deficiencies have been observed.

Applicant shall, whenever required by the Bank, furnish all relevant information, records/data to such auditors and/or inspecting officials of the Bank/Reserve Bank of India and or any regulatory authority. The Bank reserves the right to call and/or retain for any relevant material information / reports including audit or review reports undertaken by the bidder (e.g., financial, internal control and security reviews) and findings made on Selected bidder in conjunction with the services provided to the Bank.

xviii. In the event of failure of the Bidder to render the Services or in the event of termination of agreement or expiry of term or otherwise, without prejudice to any other right, the Bank at its sole discretion may make alternate arrangement for getting the Services contracted with another Applicant. In such case, the Bank shall give prior notice to the existing Bidder. The existing Service Provider shall continue to provide services as per the terms of contract until a ‘New Service Provider’ completely takes over the work. During the transition phase, the existing Service Provider shall render all reasonable assistance to the new Service Provider within such period prescribed by the Bank, at no extra cost to the Bank, for ensuring smooth switch over and continuity of services.

10. <u>Disclaimer</u>

SBI is not committed either contractually or in any other way to the applicants whose applications are accepted. The issue of this Request for EOI does not commit or otherwise oblige the Bank to proceed with any part or steps of the process.

Subject to any law to the contrary, and to the maximum extent permitted by law, SBI and its directors/officers/employees/contractors/agents and advisors disclaim all liabilities (including liability by reason of negligence) from any loss or damage, cost or expense incurred or arising by reasons of any person using the information and whether caused by reasons of any error, omission or misrepresentation in the information contained in this document or suffered by any person acting or refraining from acting because of any information contained in this Request for EOI document or conduct ancillary to it whether or not the loss or damage arises in connection with any omission, default, lack of care or misrepresentation on the part of SBI or any of its officers, employees, contractors, agents or advisors.

Please Note:

Since this is not a Request for Proposal (RFP), commercials are not required to be submitted at this stage.

Annexure – “A”

Eligibility Criteria

Sr. No	Eligibility Criteria	Compliance (Yes / No)	Supporting Document to be submitted
1	The bidder should be a reputed global company registered in India under the Companies Act 1956. The bidder/ company /firm should be in existence for more than 3 years in India.		Copy of Certificate of Incorporation issued by Registrar of Companies and full address of the registered office.
2	The bidder should have average annual IT turnover of Rs.250 Crores and Rs.100 Crores of SOC projects, during last three Financial Years (2015-16, 2016-17, 2017-18)		Audited balance sheet and P&L statement of the bidder for the last three financial years: 2015-16, 2016-2017, 2017-18 and certificate from CA.
3	Bidder should be a net profit-making organization in each of the last three financial years (2015-16, 2016-17, 2017-18)		Audited balance sheet for the last three financial years should be enclosed.
4	The bidder should be OEM (Original Equipment Manufacturer) or their highest level partners in India for the solutions including but not limited to: SIEM, UEBA, Big Data Lake, SOAR, IT-GRC, VM, DAM, NBAD, Analytics, Threat Hunting platform, Malware reverse engineering and sandboxing Threat intelligence platform, AI & ML based threat detection solutions, Red & Blue teaming tools etc.		Letter from Authorised Signatory of OEM certifying the level of relationship with bidder.
5	OEM of each technology proposed for GSOC must be a reputed global company registered in India under the Companies Act 1956 and have strong client support centres in India.		Certificate of incorporation in India from each OEM
6	The bidder should have setup at least one captive SOC with one Lakh EPS at large organisation in last 3 years using the same OEMs and technologies as proposed.		Undertaking in this regard by the authorized signatory describing implanted solutions
7	The SIEM solution proposed to be offered to the Bank by		Undertaking in this regard by the authorized signatory.

	the bidder must be from the solutions figuring in the Gartner's Leader / Challengers Quadrant consistently for the three years i.e. year 2015, 2016 and 2017.		
8	The SIEM, UEBA & Security analytics proposed must have been deployed at one clients with at least 5,00,000 EPS globally in last 3 years.		Self-declaration by the bidder. Name of top two clients in terms of EPS.
9	The bidder or any of its group / sister concern company should not be any of the following – a. Network Integrator for the Bank b. Application related service provider for the Core Banking Solution for the Bank (Domestic & abroad) c. ISSPs empanelled with SBI.		Self-declaration signed by Authorized Signatory of the bidder.
10	The bidder or any of its group / sister concern company should not have been blacklisted by any Regulatory or Government Authority or Public-Sector Undertaking or any Law Enforcement Authority for breach of any Regulations or Laws as on date of submission of the tender, otherwise the bid will not be considered.		Self-declaration signed by Authorized Signatory of the bidder.

Annexure – “B”

Contents of Technical Submission by the Bidder

Name of the Bidder: M/s

Sr.no	Contents of the EoI Response (w.r.t. SBI GSOC proposed setup)
1	Detailed unified technology GSOC architecture for size, complexity and geographic spread and growth of SBI vetted by all OEMs together.
2	Estimated EPS and per day data size in TB of the GSOC. Explain the rational how it is arrived at. Sizing guidelines for next five years.
3	Detailed unified reference functional GSOC architecture with data flow diagrams vetted by all OEMs together. (e.g. how IT-GRC will get inputs from SIEM, SOAR, VM and other non-SOC tools, how SIEM and analytics engine will get logs from DAM, VM, NBA for end to end correlation).
4	Share out of the box support of GSOC tools with each log source as per “Logs Source systems for GSOC” section.
5	Share out of the box integration support / compatibility of GSOC tools with each other (e.g. name the SIEM OEM with compatible DAM, IT-GRC, VM OEMs and vice-a-versa for each tool proposed)
6	Data and logs integration from source systems as per “Logs Source systems for GSOC” strategy cited above
7	Data, logs, rules, policies etc. migration strategy from current SOC to GSOC.
8	Provide resource deployment model (L1/L2/L3/L4) for Run operations. Clear description needs to be provided on how many resources (SI and OEM) per support level along with the experience, certifications and skills of the resources.
9	Confirmation on OEM of GSOC technologies must be ready to deploy their personnel resources onsite at SBI for 24x7x365 days operations.
10	Technical and Operational support mechanism with SI and OEMs available in India with location and number of resources for each OEM.
11	Availability of Certified resources of the proposed GSOC tools in India (give appx number certified trained resources technology wise)
12	System Integrator relationship with OEM (i.e. platinum, gold etc). Bidder to submit certificate obtained from each GSOC technology OEM on kind of relationship with them.
13	Plan to deploy the technologies and bring down the dependency on L1 & L2 resources by providing automation and reducing man power in less than two years’ timeframe.
14	Each OEM’s technology, innovation and functionality roadmap of their product for first 2 years and subsequent 3 years.
15	Clients wherein SI has implemented proposed GSOC technologies. Please provide technology-wise client list in the last 3 years.
16	Global clients wherein proposed GSOC technologies are operational by OEM or their partners. Please provide technology-wise client list in the last 3 years.
17.	The project plan with high level description of project phases and estimated duration.
18.	What is not deliverable in GSOC by SI & OEMs.

19. Bidder should provide complete solution stack to be presented in a tabular form:

Sr	Name of GSOC Solution	Product Name proposed	OEM partnership (if yes, type)
1	<SIEM>		
2			
3			

Annexure – “C”

PROFILE OF THE BIDDER

Sr. No.	Particulars	Response
01.	Name of the bidder	
02.	Country of HQ (if other than India) and Date of Incorporation	
03.	Head Quarters Address	
04.	Address in India & Date of Incorporation in India	
05.	Communication Details of Contact Official(s) – Name, Designation, Phone & Fax Number (with STD code), Mobile No. & E-mail Address.	
06.	Ownership structure (e.g. Company, Partnership)	
07.	Details of Partners / Directors	
08.	In case of limited companies, names of major shareholders with percentage holding.	
09.	Total number of offices worldwide and list thereof	
10.	Experience in Security Operations Centre setup & management (no of years with details of significant work done including volumes, capacities etc.)	
11.	Experience in implementing Security products (no. of years with details of products and implementation locations)	
12.	a. Total Number of Employees.	
	b. Total Number of Technical employees	
	c. Number of employees having Qualifications / Certifications (GSOC technologies proposed, CISSP, CEH, ISACA CRISC, CVA, CCNA, CCNE, CCSP, CCIE-Network, CCIE- Security etc.). (breakup of each to be given)	
13.	a. Tangible Net Worth, Total turnover, Sales & Profit for the last 3 Financial Years	
	b. Turnover relating to Security Operations Centre for the last three financial years.	
14.	Name of Primary Bankers/Financers & their address	
15.	Furnish information relating to the Clients where security operations have been undertaken.	

Sr. No.	Particulars	Response
16.	Furnish details of pending/past litigations within the last 3 years, if any.	
17.	Independent analyst (Gartner, IDC etc) report about your firm / company (if any) related to products / services in the information security domain	
18	Brief Bio-data of the key personnel to be associated with the proposed project	
19	Activities proposed to be covered under GSOC along with names of products / appliances/ solutions proposed for each activity, name & details of Partner companies / Applicants (please attach details of the arrangements). As per table given in Annexure-B	
20.	Names of proprietary products, technologies for Security Operations Centre, used by you.	
21	Details of empanelment / tie-ups / assignments with Government units and industry bodies	
22	Details of the proposed GSOC framework / approach, architecture, Technical approach	

Note – The bidder must attach appropriate document attested by their Authorized Signatory in support of their claim in compliance of the above particulars.

---End---