



Central Bank of India

Department of Information Technology

Tender No. GEM/2025/B/6180729

Request for Proposal (Bid) Document

For

**Supply, Implementation & Management of Next-
Generation Security Operation Centre (NG-SOC)
Solutions**



TABLE OF CONTENTS

| | | |
|------|---|----|
| 1. | Invitation for Tender Offers | 7 |
| 2. | Eligibility Criteria | 10 |
| 3. | EMD / Bid Security | 13 |
| 4. | Performance Bank Guarantee | 13 |
| 5. | Cost of Bidding | 14 |
| 6. | Manufacturer's Authorization Form | 14 |
| 7. | Scope of Work | 15 |
| 7.1 | Setting up NG-SOC | 16 |
| 7.2 | Transition from existing SOC to NG-SOC: | 21 |
| 7.3 | Scope Of Work For Proposed Solutions | 22 |
| 7.4 | Services | 28 |
| 7.5 | Security Dashboards | 30 |
| 7.6 | Oem's Responsibilities Engaged By The Bidder | 32 |
| 7.7 | NG-SOC Operations, Facility Management, Amc & Ats | 33 |
| 7.8 | Manpower Requirement & Desired Skillset | 39 |
| 7.9 | Training To Bank Employees | 48 |
| 8. | General Responsibility Of The Bidder | 48 |
| 9. | Project Timelines | 51 |
| 10. | Staggered Delivery Of The Equipment's | 51 |
| 11. | Contract Renewal | 51 |
| 12. | SLA Compliance | 51 |
| 12.1 | Service Level Agreements (SLA) | 51 |
| 12.2 | Service Levels During Implementation Phase | 51 |
| 12.3 | Service Levels Post Acceptance Of Solutions By The Bank | 52 |
| 13. | Responsibility Matrix | 57 |
| 14. | Liquidated damage | 57 |
| 15. | Land Border Sharing Clause | 58 |
| 16. | Monitoring & Audit | 59 |
| 17. | Bid Submission | 59 |
| 18. | Integrity Pact | 61 |
| 19. | Commercial Offers | 62 |
| 20. | Evaluation & Acceptance | 62 |
| 21. | Evaluation Process | 63 |



| | |
|---|----|
| 21.1 Eligibility Criteria Evaluation | 63 |
| 21.2 Technical Evaluation Criteria..... | 63 |
| 21.3 Commercial Evaluation Criteria | 68 |
| 22. Payment Terms | 69 |
| 22.1 Procedure For Claiming Payments..... | 69 |
| 22.2 AMC/ATS Payment Terms..... | 70 |
| 22.3 AMC & ATS And Warranty Costs..... | 70 |
| 23. Order Cancellation | 73 |
| 24. Indemnity | 73 |
| 25. Confidentiality & Non-Disclosure | 76 |
| 26. Force Majeure..... | 77 |
| 27. Resolution Of Disputes | 77 |
| 28. Independent Contractor | 78 |
| 29. Assignment | 79 |
| 30. Execution Of Contract, SLA & NDA | 79 |
| 31. Successful Bidder's Liability | 79 |
| 32. Information Ownership | 80 |
| 33. Inspection, Audit, Review, Monitoring & Visitations | 80 |
| 34. Information Security..... | 82 |
| 35. Intellectual Property Rights..... | 82 |
| 36. Termination | 83 |
| 37. Privacy & Security Safeguards..... | 85 |
| 38. Governing Law And Jurisdiction | 86 |
| 39. Compliance With Laws..... | 86 |
| 40. Violation Of Terms | 86 |
| 41. Corrupt & Fraudulent Practices | 87 |
| 42. Publicity | 87 |
| 43. Applicability Of Preference To Make In India, Order 2017 (PPP-MII Order)..... | 87 |
| 44. Compliance To Rbi Master Direction On Outsourcing Of It Services (RBI Circular Dated April 2023)..... | 87 |
| 45. Sustainable Sourcing..... | 90 |
| 46. Entire Agreement; Amendments | 91 |
| 47. Survival And Severability | 91 |
| 48. Amendments To Bidding Documents | 91 |
| 49. Period Of Validity | 91 |
| 50. Ownership, Grant And Delivery..... | 91 |



| | | |
|-----|--|-----|
| 51. | Last Date And Time For Submission Of Bids | 92 |
| 52. | Late Bids | 92 |
| 53. | Modifications and/or Withdrawal of Bids | 92 |
| 54. | Signing of Contract | 92 |
| 55. | Checklist for Submission | 93 |
| 56. | Annexure 1: Bill of Material | 95 |
| 57. | Annexure 2: Minimum Technical Specifications..... | 100 |
| 58. | Annexure 3: Conformity Letter..... | 128 |
| 59. | Annexure 4: Bidder's Information | 129 |
| 60. | Annexure 5: Letter for Conformity of Product as per RFP | 130 |
| 61. | Annexure 6: Undertaking for Acceptance of Terms of RFP | 131 |
| 62. | Annexure 7: Manufacturer's Authorization Form | 132 |
| 63. | Annexure 8: Integrity Pact | 133 |
| 64. | Annexure 9: Non-Disclosure Agreement | 139 |
| 65. | Annexure 10: Performance Bank Guarantee | 143 |
| 66. | Annexure 11: Bid Security (Earnest Money Deposit) | 146 |
| 67. | Annexure 12: Bidder's Particulars | 148 |
| 68. | Annexure 13: NPA Undertaking | 149 |
| 69. | Annexure 14: Undertaking letter (Land Border Sharing) | 150 |
| 70. | Annexure 15: Cover Letter | 153 |
| 71. | Annexure 16: Pre-bid Query Format | 154 |
| 72. | Annexure 17: Eligibility Criteria Compliance..... | 155 |
| 73. | Annexure 18 – Self declaration for compliance to RBI master direction on outsourcing of it services 158 | |
| 74. | Annexure 19: GOI Guidelines for preference to Make in India | 159 |
| 75. | Annexure 20: Guidelines on banning of business dealing | 162 |



Definitions and Acronyms

Following terms are used in the document interchangeably to mean:

| Acronym | Definition |
|---------------|--|
| AAA | Authentication, Authorization and Accounting framework in Networking |
| AD | Active Directory |
| AMC | Annual Maintenance Contract |
| API | Application Programming Interface |
| ASM | Attack Surface Management |
| ATS | Annual Technical Support |
| Bank/CBoI | Central Bank of India |
| BAS | Breach and Attack Simulation |
| “Bidder” | Single point of contact appointed by the Bank for procurement and supply of the equipment based on the Bill of Materials shared by the Bank. |
| “CBS” | Core Banking Solution |
| “CO” | Central Office |
| CVC | Central Vigilance Commission |
| DAM | Database Activity Monitoring |
| DC | Data Centre of the Bank which is located at Central Office, Belapur, Mumbai |
| DMZ | Demilitarized Zone |
| DNS | Domain Name Server |
| DRC | Disaster Recovery Centre which is located in Hyderabad |
| EMD | Earnest Money Deposit |
| EMS | Enterprise Management System |
| FPS | Flows Per Second |
| GbE/GigE/Gbps | Gigabit Per Second |
| GoI | Government of India |
| HA | High Availability |
| HDD | Hard Disk Drive |
| HO | Head Office |
| INR | Indian National Rupee |
| IP | Internet Protocol |
| IPS | Intrusion Prevention System |
| IT | Information Technology |
| LAN | Local Area Network |
| Mbps | Megabits Per Second |
| MPLS | Multi-Protocol Label Switching |
| MTBF | Mean Time before Failure |
| NDA | Non-Disclosure Agreement |
| NOC | Network Operations Centre |
| NMS | Network Management System |
| OEM | Original Equipment Manufacturer |
| PO | Purchase Order |
| RFP | Request for Proposal |



सेंट्रल बैंक ऑफ़ इंडिया
Central Bank of India

1911 से आपके लिए "सेंट्रल" "CENTRAL" TO YOU SINCE 1911

RFP for Supply, Implementation & Management of Next-Generation Security Operations Centre (NG-SOC) Solutions
Central Bank of India – Tender No – GEM/2025/B/6180729

| | |
|------|--|
| RMA | Return Material Authorization |
| RO | Regional Office |
| RPO | Recovery Point Objective |
| RTO | Recovery Time Objective |
| SIEM | Security Information and event Management |
| SSD | Solid State Drive |
| SMTP | Simple Mail Transfer Protocol |
| SOAR | Security Orchestration Automation and Response |
| SoW | Scope of Work |
| SLA | Service Level Agreement |
| SPOC | Single Point of Contact |
| SSL | Secure Sockets Layer |
| T&C | Terms & Conditions |
| Tbps | Terabits per second |
| TCO | Total Cost of Ownership |
| TCP | Transmission Control Protocol |
| TOR | Top of Rack |
| UAT | User Acceptance Test |
| VPN | Virtual Private Network |
| WAN | Wide Area Network |
| WAF | Web Application Firewall |
| ZO | Zonal Office |



1. INVITATION FOR TENDER OFFERS

Central Bank of India, The Bank, a body corporate constituted under the Banking Companies (Acquisition and Transfer of Undertaking) Act 1970 having its Central Office at Chandermukhi, Nariman Point, Mumbai-400021 hereinafter called "Bank" and having 90 Regional Offices (RO), 13 Zonal Offices (ZO) and 4617 plus branches spread across India, intends for select a bidder for Supply, Implementation and Management of Next Generation Security Operations Centre (NG-SOC) Solutions at Bank's Data Centre & Disaster Recovery Centre.

Bank invites unconditional online tender offers (Technical offer and Commercial offer) from eligible, reputed manufacturers and/or their authorized dealers for Supply, Implementation & Management of Next Generation (NG-SOC) solutions at DC & DRC.

The details are given below:

| | |
|--|--|
| Date of RFP Issue | 29/04/2025 |
| Bid Security (EMD) | An amount of Rs. 1,80,00,000/- (Rupees One Crore Eighty Lakhs Only) in the form of Bank Guarantee issued by a scheduled bank other than Central Bank of India for the entire period of Bid validity plus 3 months or by means of banker's cheque/ Account Payee Demand Draft /RTGS/NEFT in the account no.- 3287810289 of Central Bank of India (IFSC Code – CBIN0283154) with narration Tender ref no in favour of "Central Bank Of India" and payable at Mumbai/Navi Mumbai. |
| e-mail IDs for sending queries and Last Date for submission of queries | smitcsoc@centralbank.co.in, smitpurchase@centralbank.co.in, cminfosec@centralbank.co.in, smitlinfosec@centralbank.co.in latest by 07/05/2025 up to 16:00 hrs. Queries to be submitted with Proof of remittance of document/Tender cost |
| Date and time for Pre-Bid Meeting, | 08/05/2025 at 15:00hrs. |
| Last Date and Time submission of Bids Mode of bid submission & online | 04/06/2025 up to 15:00 hrs. |
| Time & Date of Opening of technical bids | 04/06/2025 at 15:30 hrs. |
| Mode of Submission | Government e Marketplace (GeM) |
| Response Types | 1.Technical Bid plus Document Cost plus Bid Security/EMD 2.Commercial Bid |
| Address for Communication | General Manager-IT Central Bank Of India Department Of IT (DIT), Plot no-26, Sector-11, CBD Belapur, Navi Mumbai- 400614 |



सेंट्रल बैंक ऑफ़ इंडिया
Central Bank of India

1911 से आपके लिए "केन्द्रित" "CENTRAL" TO YOU SINCE 1911

**RFP for Supply, Implementation & Management of Next-Generation Security Operations Centre (NG-SOC) Solutions
Central Bank of India – Tender No – GEM/2025/B/6180729**

| | |
|---------------------------|--|
| | Mail address: smitcsoc@centralbank.co.in, smitpurchase@centralbank.co.in, cminfosec@centralbank.co.in, smit1infosec@centralbank.co.in |
| Contact Telephone Numbers | 022- 67123669, 27582437, 67123583 |

For any clarification with respect to this RFP, the bidder may send their queries/suggestions, valuable inputs and proof of remittance of document cost or exemption certificate of MSE by email to the Bank. It may be noted that all queries, clarifications, questions etc., relating to this RFP, technical or otherwise, must be in writing only and should be sent to designated email ID within stipulated time as per Annexure 20.

In accordance with Government of India guidelines, Micro and Small Enterprises are eligible to get tender documents free of cost and also exempted from payment of earnest money deposit upon submission of valid MSE certificate copy.

Start-ups (which are not MSEs) are exempted only from Bid security amount.

Earnest Money Deposit mentioned above must accompany all tender offers (Technical Bid) as specified in this tender document.

Tender offers will normally be opened half an hour after the closing time. Any tender received without Earnest Money Deposit (EMD)/Document/Tender Cost etc will be disqualified.

Technical Specifications, Terms and Conditions and various format and Performa for submitting the tender offer are described in the tender document and its Annexures.

Extant guidelines of GeM shall be applicable.

General Manager-IT
Central Bank of India, DIT,
CBD Belapur, Navi Mumbai-400614

DISCLAIMER The information contained in this Request for Proposal (RFP) document or information conveyed subsequently to bidder(s) or applicants whether verbally or in documentary form by or on behalf of Central Bank of India (Bank), is provided to the bidder(s) on the terms and conditions set out in this RFP document and all other terms and conditions subject to which such information is provided.

This RFP is neither an agreement nor an offer and is only an invitation by Bank to the interested parties for submission of unconditional bids. The purpose of this RFP is to provide the bidder(s) with information to assist the formulation of their proposals. This RFP does not claim to contain all the information each bidder may require. Each bidder should conduct its own investigations and analysis and should check the accuracy, reliability and completeness of the information in this RFP and where necessary obtain independent advice. Bank makes no representation or

warranty and shall incur no liability under any law, statute, rules or regulations as to the accuracy, reliability or completeness of this RFP. Bank may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFP.



2. ELIGIBILITY CRITERIA

The Bidder must fulfil following eligibility criteria:

| # | Eligibility of the Bidder | Documents to be submitted | Compliance (Y/N) |
|----|--|--|------------------|
| 1. | Bidder should be a Registered company under Indian Companies Act. 1956/2013 or LLP/Partnership firm and should have been in existence for a minimum period of 5 years in India, as on date of submission of RFP. | Copy of the Certificate of Incorporation issued by Registrar of Companies/Registrar of firms and full address of the registered office of the bidder | |
| 2. | Bidder should be registered under G.S.T and/or tax registration in state where bidder has a registered office. | Proof of registration with GSTIN | |
| 3. | The bidder must have minimum annual turnover in India of Rs. 300 crores per annum in the last three financial years (i.e., 2021-22, 2022-23, 2023-24) of individual company and not as group of companies. | Copy of Audited Balance Sheet and Copy of Certificate of the Chartered Accountant for the last three financial years (i.e., 2021-22, 2022-23, 2023-24) | |
| 4. | The bidder should have made operating profits in at least two financial years out of last three financial years (i.e., 2021-22, 2022-23, 2023-24). | Copy of Audited Balance Sheet and Copy of Certificate of the Chartered Accountant for the last three financial years (i.e., 2021-22, 2022-23, 2023-24) | |
| 5. | The bidder should have a positive net worth in last three financial years (i.e., 2021-22, 2022-23, 2023-24) | Copy of Audited Balance Sheet and Copy of Certificate of the Chartered Accountant for the last three financial years (i.e., 2021-22, 2022-23, 2023-24) | |
| 6. | At the time of bidding, the Bidder should not have been blacklisted/debarred/ by any Govt. / IBA/RBI/PSU /PSE/ or Banks, Financial institutes for any reason including non-implementation/delivery of the order. Self- | Submit the undertaking on Company's letter head | |



| # | Eligibility of the Bidder | Documents to be submitted | Compliance (Y/N) |
|----|---|--|------------------|
| | declaration to that effect should be submitted along with the technical bid. | | |
| 7. | At the time of bidding, there should not have been any pending litigation or any legal dispute in the last five years, before any court of law between the Bidder or OEM and the Bank regarding supply of goods/services. | Submit the undertaking self-declaration on Company's letter head | |
| 8. | Bidder/OEM should not have <ul style="list-style-type: none"> NPA with any Bank /financial institutions in India Any case pending or otherwise, with any organization across the globe which affects the credibility of the Bidder in the opinion of Central Bank of India to service the needs of the Bank | Submit self-declaration on Company's letter head. | |
| 9. | Bidder should have service/support centre or should have arrangement for providing support in Mumbai and Hyderabad. | Submit the undertaking self-declaration on Bidder's letter head | |
| 10 | If the bidder is from a country which shares a land border with India, the bidder should be registered with the Competent Authority. | Certified copy of the registration certificate | |
| 11 | The Bidder should have implemented and managed SOC with on-premises SIEM solution with minimum 30000 Events Per Second (EPS) or 1TB / Day in at least one BFSI*/RBI/NPCI/BSE/NSE/SEBI/Govt./PSU in India. (*BFSI must be an organization having minimum of 1000 branches/ offices in India) | Letter of acceptance (LoA)/ purchase order/ work order/ contract/ completion certificate Deployment Certificate issued by client to the bidder/Particulars confirming relevant experience. | |
| 12 | The bidder shall have minimum 100 skilled resources on the payroll in India in the following areas (Subject Matter Expert): <ul style="list-style-type: none"> a. Network Security b. Data Security c. Application Security d. Cloud Security | List of resources with following details to be provided on company letter head: Name Designation Years of experience | |



| # | Eligibility of the Bidder | Documents to be submitted | Compliance (Y/N) |
|----|--|---|------------------|
| | e. Vulnerability Management f. Infrastructure Management | | |
| 13 | The proposed OEM's SIEM solution must have been implemented with minimum 60,000 Events Per Second (EPS) or 2 TB/Day in at least two BFSI*/RBI/NPCI/BSE/NSE/SEBI/ Govt./PSU in India during the last seven years. (*BFSI must be an organization having minimum of 1000 branches/ offices in India) | Copies of Completion Certificate/ reference letter/E-Mail from client /copy of purchase order /contract agreement /work order /engagement letter. | |
| 14 | The proposed OEM's UEBA solution must have been implemented in at least One BFSI*/RBI/NPCI/BSE/NSE/SEBI/Govt./ PSU in India) during the last seven years. (*BFSI must be an organization having minimum of 1000 branches/ offices in India) | Copies of Completion Certificate/ reference letter/E-Mail from client /copy of purchase order /contract agreement /work order /engagement letter. | |

***Note:** If case of unaudited Balance Sheet for FY 2023-24, Bidder needs to submit Provisional Balance Sheet along with copy of CA Certificate for FY 2023-24.

The bidder must submit only such document as evidence of any fact as required herein. The Bank, if required, may call for additional documents during the evaluation process and the bidder will be bound to provide the same.

Bank reserves the right to verify references provided by the Bidder independently. Any decision of bank in this regard shall be final, conclusive, and binding up on the bidder. Bank may accept or reject an offer without assigning any reason whatsoever.

1. Bidders need to ensure compliance to all the eligibility criteria points.
2. In-case of corporate restructuring the earlier entity's incorporation certificate, financial statements, Credentials, etc. may be considered.
3. In case of business transfer where Bidder has acquired a Business from an entity ("Seller"), work experience credentials of the Seller in relation to the acquired business may be considered.
4. Scheduled Commercial Bank does not include Payments Bank, Cooperative Banks or RRBs.
5. 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 RFP, either the Indian agent on behalf of the Bidder/OEM or Bidder/OEM itself can bid but both cannot bid simultaneously for the same item/product in the same RFP. The reference of 'item/product' in the CVC guidelines refer to 'the final solution that bidders will deliver to the customer.*
- *If an agent submits bid on behalf of the Bidder /OEM, the same agent shall not submit a bid on behalf of another Bidder /OEM in the same RFP for the same item/product.*

3. EMD / BID SECURITY

An amount of ₹ 1,80,00,000/- (Rupees One Crore Eighty Lakhs Only) in the form of Bank Guarantee issued by a scheduled bank other than Central Bank of India for the entire period of Bid validity plus 3 months or by means of Account Payee Demand Draft / banker's cheque /RTGS/NEFT in the account no.-3287810289 of Central Bank of India (IFSC Code – CBIN0283154) with narration Tender ref no in favour of “Central Bank Of India” and payable at Mumbai/Navi Mumbai.

The EMD / Bid Security shall be liable to be forfeited:

- a) if a Bidder withdraws its tender during the period of tender validity specified by the Bidder; or
- b) if the Bidder does not accept the correction of its Tender Price; or
- c) if the successful Bidder fails within the specified time to:
 - i. Sign the Contract; or
 - ii. Furnish the required security deposit.

The EMD / Bid Security of a Joint Venture (JV) must be in the name of the JV that submits the tender. If the JV has not been legally constituted at the time of bidding, the EMD / Bid Security shall be in the names of all future partners as named in the letter of intent.

The EMD / Bid Security will be refunded to The Successful Bidder, only after furnishing an unconditional and irrevocable Performance Bank Guarantee (PBG) as per Sr no.4

The EMD / Bid Security of unsuccessful Bidders shall be returned as promptly as possible after completion of bidding process.

4. PERFORMANCE BANK GUARANTEE

- i. As mentioned above, the Successful Bidder will furnish an unconditional and irrevocable Performance Bank Guarantee (PBG) from scheduled commercial Bank other than Central Bank of India, in the format given by the Bank in Annexure 11, for 5% of the total project cost valid for 66 months, (5 years for total project period plus 6 months for claim period) validity of PBG starting from its date of issuance. The PBG shall be submitted within 21 days of the PO acceptance by the Bidder.

- ii. The PBG so applicable must be duly accompanied by a forwarding letter issued by the issuing bank on the letterhead of the issuing bank. Such forwarding letter shall state that the PBG has been signed by the lawfully constituted authority legally competent to sign and execute such legal instruments. The executor (BG issuing Bank Authorities) is required to mention the Power of Attorney number and date of execution in his / her favour with authorization to sign the documents.
- iii. Each page of the PBG must bear the signature and seal of the PBG issuing Bank and PBG number.
- iv. In the event of the Successful Bidder being unable to service the contract for whatever reason, Bank may provide a cure period of 30 days and thereafter invoke the PBG, if the bidder is unable to service the contract for whatever reason.
- v. In the event of delays by Successful Bidder in AMC support, service beyond the schedules given in the RFP, the Bank may provide a cure period of 30 days and thereafter invoke the PBG, if required.
- vi. Notwithstanding and without prejudice to any rights whatsoever of the Bank under the contract in the matter, the proceeds of the PBG shall be payable to Bank as compensation by the Successful Bidder for its failure to complete its obligations under the contract, indicating the contractual obligation(s) for which the Successful Bidder is in default.
- vii. The Bank shall also be entitled to make recoveries from the Successful Bidder's bills or any other amount due to him, the equivalent value of any payment made to him by the bank due to inadvertence, error, collusion, misconstruction or misstatement.
- viii. The PBG may be discharged / returned by Bank upon being satisfied that there has been due performance of the obligations of the Successful Bidder under the contract. However, no interest shall be payable on the PBG.

5. COST OF BIDDING

The bidder shall bear all the costs associated with the preparation and submission of bid and Bank will in no case be responsible or liable for these costs regardless of the conduct or outcome of the bidding process.

6. MANUFACTURER'S AUTHORIZATION FORM

Bidders must submit a letter of authority from their manufacturers in Annexure 7 that they have been authorized to quote OEM Product.



7. SCOPE OF WORK

Central Bank of India intends to implement Next Generation Security Operations Centre (NG-SOC) solutions for protecting information assets at Primary Data Centre at Navi Mumbai and Disaster Recovery Site at Hyderabad. Bank expects Bidder to provide full-fledged services including but not limited to design, supply, implementation, configuration, customization, integration, migration, monitor, manage, backup, documentation, training, warranty support, post warranty maintenance support, arrangement with OEM and any other activities related to or connected to the NG-SOC solutions, devices, applications & technologies together at the Bank during the entire contract period of 5 years.

1. The Bank has envisaged the procurement of Next-Generation Security Operation Centre (NG-SOC) and associated hardware, software and tools, etc. required for operationalization of NG-SOC as per the requirement specified in this RFP.
2. Procurement of (NG-SOC) and associated infrastructure(s) mentioned in the RFP will be at Bank's discretion and Bank may not procure all the items mentioned in the RFP. Also, Bank may ask for staggered delivery of some of the component and associated infra. The details of the same will be shared with the successful bidder during implementation phase.
3. Design, validate & review the NG-SOC architecture along with in scope solutions at least once in year from OEM review of the implemented NG-SOC solutions with concurrence of the Bank.
4. Supply all required infrastructure and manpower for operations of NG-SOC solutions as per the detailed scope mentioned in this RFP.
5. Deploy qualified personnel in Bank's premises at Mumbai/Navi Mumbai and Hyderabad for configuration, monitoring and management of in scope NG-SOC solutions.
6. Inventory management of all assets (Hardware and Software etc.) supplied as part of the RFP.
7. Bidder to do proactive Security Threat Hunting across Bank's environment and implement adequate information security controls to protect Bank IT assets from breach.
8. Ensure all the commissioning, Integration, migration, relocation, updates, Upgrades, Patching, de-commissioning, Enhancements, Troubleshooting, Analysis, Health Checks, Backups, Audits, Documentation, SOP's, Creation of Knowledge Articles at Onsite for proposed NG-SOC solutions.
9. Supporting the Risk Management Process of the Bank by mitigating the risks for the assets under the scope of NG-SOC solutions.
10. Managing reporting and logging of security alerts /incidents through ticketing tool and closing the same as per the agreed SLA. Inbuilt / integrated incident management and



ticketing tool to generate automated tickets for the alert events generated by the SIEM/SOAR/UEBA.

11. Deliver and implement the solutions & services to the Bank in compliance with International Standards such as ISO, PCI-DSS, etc. and advisories issued from regulatory authorities and statutory directions.
12. Ensure that the supplied NG-SOC solutions and services top-of-the-line in terms of specifications, support, compatibility with other products. Also, they should be up to date in terms of product releases, version upgrades, patches, and other service packs.
13. The service delivery (SLA Management) and periodic reporting should be done through automated dashboards.
14. Provide immediate forensic support in case of any security / cyber incident.
15. Ensure continual improvement of NG-SOC operations, incorporating industry best practices, closure of audit observations and regulatory guidelines.
16. Ensure graceful transition from existing CSOC of the Bank to new NG-SOC along with migration activities.
17. The proposed solutions implemented by the Bidder should adopt evolving threats and technological advancements, including quantum computing, AI based threats.
18. All the tools/ application/ OS supplied as part of the project should be latest and supplied with Enterprise-wide Licenses and all the licenses should be in the name of **Central Bank of India**. Bank will have the right to use the tools for the functions provided by the tools in any manner and for any number of branches, offices, subsidiary units, joint ventures, or RRBs or in any future proposed Mergers, irrespective of the number of users, geographical location of the devices being monitored. Bank will also have a right to relocate any one or all the tools to different locations without any extra cost to the bank.
19. Online Access/Remote Access will not be provided by the Bank during implementation or for troubleshooting purpose. Onsite Resources should be deployed for implementations and for troubleshooting purpose.

7.1 SETTING UP NG-SOC

1. Supply, install, integrate, operate, maintain and manage all NG-SOC technologies together at Central Bank of India premises for Contract period for currently deployed entire IT & Security Infrastructure which will get added, upgraded etc. at the Bank during the Contract period.
2. Successful Bidder to study existing environment at bank, identify data sources required for integration, compliance, threat detection etc. and propose the solution architecture



to the bank. The bidder needs to create a detailed reference architecture of the solution in consultation with Bank team. The architecture should include identification and placement of log collection/forwarding hardware, network connections, log routing mechanisms, data replication methodology natively by the proposed application, data retention based on different retention periods across bank, etc.

3. Technologies proposed to be deployed in the NG-SOC 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.
4. As part of Proposed Next-Gen SIEM solution, SOAR should be part of the NG-SOC solution suite with 10 Security Analysts equivalent license plus 2 view only user licenses, SOAR must enable the orchestration and automation of security workflows, eliminating manual intervention to reduce mundane tasks. Successful bidder has to factor the underline hardware and software components for orchestration and automation of security workflows, etc.
5. Proposed Next-Gen SIEM solution should provide automated remediation of threats on IT infrastructure (OS, DB, networking techs, applications etc.), security implementation / threat prevention / mitigation technologies in real-time basis and update its conclusive action taken status back into security monitoring technologies immediately.
6. The intention should be to free up the personnel resources/ NG-SOC analysts/ IT teams from routine job and encourage them to invest their time more into threat hunting and advanced threat detection & prevention efforts.
7. The successful bidder should guarantee that the solution allows for the inclusion of manual changes within automated workflows within timeframe defined by Bank.
8. There should be feature to import the logs of any endpoint/server/device(s) into the system for analysis based on various parameters/inputs and processed data and findings should be available on screen and for download & export to various entities.
9. Bidder should study the entire bank environment, identify data required for User & Entity Behavioral Analytics (UEBA) to build baselines for users and entities, pull the required data from common data repository/data lake, deploy use cases and do anomaly detection.



10. Bidder should size the UEBA solution based on the no. of users, which is 40,000. Further, successful bidder has to factor for increase in no of users up to 45,000 during the contract period and has to size hardware, etc. accordingly.
11. The bidder shall ensure that the proposed solution should not create multiple data lakes/ data repository for UEBA, Next-Gen SIEM & for automation of security work flows. It should create a single data lake/data repository which Next-Gen SIEM, SOAR & UEBA should use.
12. The proposed solution must be containerized solution to provide the ease of adding functionalities such as UEBA, Threat hunting, Automation & Orchestration etc. Solution should not use traditional DB approach to avoid performance degradation during threat hunting.
13. Solution must provide unified GUI platform to manage and monitor the solution sought under NG-SOC solutions e.g. SIEM, UEBA, SOAR and should also support for Threat Hunting etc.
14. The real-time view of events with relevant severity score.
15. Storage of logs should be encrypted by using highest level encryption such as AES256 or equivalent or above.
16. Compression of event logs should be minimum of 1:8 or more.
17. Threat hunting should be deployed on top of the existing real time/historical events for arresting of incidents. Log extraction should be seamless.
18. The bidder must propose NG-SOC solutions i.e. SIEM, UEBA and SOAR from single OEM only. Further, there should be single & common dashboard/console/Database of all mentioned NG-SOC technologies in the RFP.
19. The bidder must ensure that logs should be collected from each datacentre with the help of connectors and should be sent to respective data repository/data lake layer in the datacentre. Proposed solution should replicate received data from connectors across DC & DR at the application layer natively without dual forwarding it from source device or from the connector.
20. Every technology deployed in the NG-SOC should transform itself from a purely rule based system to analytics & AI/ML based correlation system for logs, vulnerabilities & threat intelligence together for accurate risks prediction.



21. NG-SOC shall support curated knowledge base and model for cyber adversary behaviour, reflecting the various phases of an adversary's attack lifecycle and the platforms they are known to target like MITRE ATT&CK framework.
22. The NG-SOC should have following major technologies and related services with deep learning, analytics, automation of routine SOC activities to improve threat detection and response capabilities leveraging AI/ML –
- Next-Gen Security Information and Event Management (SIEM) compatible with NG-SOC features.
 - Common Data Repository/ Security Big Data Lake (SBDL)
 - User and Entity Behavior Analytics (UEBA)
 - Security Orchestration, Automation & Response (SOAR)
 - Integration with Existing and future tools/applications/solutions in Bank.
 - i. Security Technologies such as Firewall, IPS/IDS WAF, DAM, ADC (LB & SSL Off loader), Antivirus, ADDM, Endpoint & Network APT, Deception, NAC, DLP, SSO, PIM, ITSM etc.
 - ii. Operational technologies include OS, databases (traditional and big data), web servers, 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 etc.) These are feeder technologies / source system of logs provided to the SOC.
 - iii. The emerging technologies including but not limited to LinuxONE, Openshift, x86S390, Chat-bots, voice-bots, block chain, cryptocurrency, augmented & virtual reality, zero trust, IOT. These are feeder technologies / source system of logs provided to the SOC.
19. Delivery of all Technical & Functional Requirements as per RFP.
20. SIEM Sustained EPS / Volume 60,000 EPS or equivalent TB data/day. In case of Data volume ingestion, raw log size of event to be factored as 500 bytes and enriched logs of events (Raw + CEF) to be factored as 630 bytes for storage & licensing purpose. While the solution (Including hardware) should be scalable to support 1 lakh EPS or equivalent TB data/day whichever is higher in DC & DR separately during contract period without any additional Hardware, software and storage except EPS licenses.



21. Bidder has to implement the similar setup at both DC (Mumbai/Navi Mumbai) and DR (Hyderabad) locations.
22. UEBA Sustained EPS/Volume/No of User 40,000 EPS or equivalent TB per Day or 40,000 users.
23. UEBA & SOAR Should leverage only on SIEM or Common Data Repository storage as per architecture proposed by the bidder & OEMs.
24. Data Retentions Requirements:
Backup including infrastructure and software - Automated backup of all data / logs / Configuration for NG-SOC DC/DR setup. Bidder has to plan for back up of all logs as archival for the contract period.
25. OEMs should mandatorily ensure to collaborate with all necessary third parties' other OEMs. Any customization, removal of false positives, enhancement and other device/solution administration related activity required in solution to deliver seamless, fully functional integration, custom and native parsers, connectors, incidents management and related workflows, native and custom playbooks, alerts fine tuning, notifications, dashboards, reporting, customization of default templates, additional remediation efforts etc. without any extra charges to the Bank during the entire Contract period.
26. All the licenses and infrastructure provided as part of BoM should strictly adhere to requirements of the RFP. If during the Contract period, it is observed by the Bank that provided licenses are not adhering to the RFP requirements then all the additional hardware/software/licenses should be provided and configured without any additional cost to the Bank.
27. Bank may deploy the resources at both DC- Mumbai/Navi Mumbai and DR Hyderabad site as per Bank's requirement.
28. Minimum number of manpower to available in NG-SOC as per the shift, bidder has to factor adequate resources considering management of shift. Bank may increase/decrease the manpower as per requirement of the bank.
29. Bank at its sole discretion may place purchase order of any component of additional requirement during the contract period with the discovered pro-rata basis price. The rate contract will be valid for entire contract period.



30. The hardware/appliances that is going to be deployed at DC and DR locations should be identical and each component should be in High availability mode.
31. All the Hardware devices should be with latest processor and releases date should not be earlier than one year from the date of RFP.
32. All the hardware should be supplied as per EPS requirement asked by the Bank.
33. System should be capable for external and Internal disk space monitoring and alerting in case the (configurable) 70% threshold is reached. In case the performance is adversely affected or the thresholds exceeds the mentioned threshold as above, more than 3 times in a quarter, the vendor is required to upgrade the infrastructure and solution (as applicable), within one month without any additional cost to the Bank.
34. Storage should attach Backup device which also encrypt the data stored in the external back up media.

7.2 TRANSITION FROM EXISTING SOC TO NG-SOC:

Manage day to day operations of currently running SOC setup & the responsibilities of the vendor with respect to existing operational SOC include but not limited to

- Running existing SOC in parallel with NG-SOC until all existing log sources are integrated with NG-SOC.
- Maintain steady state of SOC ensuring health monitoring, uptime, collation of logs in real-time, correlation. Contract of existing SOC is valid upto Jan'26 and successful bidder is required to maintain the same for the minimum period of 1 Year after the expiry of existing contract.
- Raise the incidents / alerts in NG-SOC or existing SOC till next gen. SOC is implemented.
- All the data/logs of existing SIEM to be recorded and planned for the retention upto 10 years, the required infrastructure shall be provisioned by the bidder.
- The bidder shall be responsible to manage and monitor the existing SIEM (RSA Netwitness) as per the existing data available.
- The bidder shall be responsible for extraction of data/logs from the available data/logs at existing SIEM/SOC as and when required by investigating agency, regulators etc.
- Ensure security and other required patches are applied from time to time by obtaining same from respective OEMs.



- Maintain rules, configuration and other settings and change them as per Bank's requirements / security requirements.
- Once all the log sources integrated with existing SOC are migrated to NG-SOC, ensure the existing SOC is up & running in steady state with security patches by obtaining same from respective OEMs. Ensure that the reports are extracted from online / warehouse storage etc. Restore the logs from backup, is required to extract old logs for forensic investigation, as & when required.
- Bidder must ensure that the existing data remain usable for necessary searching, link analytics, threat hunting, regulatory requirements, forensic investigation etc.
- Bank has existing SOC setup with solutions like SIEM, SOAR. Bidder shall be required to meticulously plan for the complete transition of the existing Bank's SOC architecture, corresponding IT Infrastructure, Applications, Policies, Processes etc.
- Bidder must submit the project plan & transition timelines from current SOC to NG-SOC as a part of the RFP response without deviating from the requirements and timelines defined in this RFP.

7.3 SCOPE OF WORK FOR PROPOSED SOLUTIONS

Bidder shall deploy and manage the below-mentioned NG-SOC solutions i.e. Next-Gen SIEM, UEBA, Common Data Repository and SOAR (As part of NG-SOC) in Bank's premises to improve the security posture of Bank.

I. Next-Gen Security Information & Event Management (SIEM)

- The SIEM solution must enable Bank to collect, correlate, analyze, and derive a logical conclusion from logs, events, and information received by it from heterogeneous systems including Networking and Security systems, OS, Web servers, Applications, Databases, all security solutions, other infrastructure etc. on 24x7x365 basis.
- Bidder shall offer a complete solution that shall include hardware, software, all licenses, upgrades, updates, and subscriptions required for meeting the requirement for correlating and analysis of events.
- The Bidder should offer the SIEM device with all requisite modules for the collection of logs, monitoring, and displaying of events on individual device or on a correlation basis, to facilitate administrators to take proactive actions for the prevention of security threats that might occur on network access devices.



- The offered solution shall include toolkits/modules/utilities for integrating all required devices supported by the SIEM equipment without any additional cost implication to Bank.
- The offered solution shall provide storage and correlation of logs from various devices in Bank's network.
- The Bank intends to implement SIEM with a centralized dashboard to monitor various IT Security threats originating across the organization. The solution should provide a single dashboard with the correlation of threats originating in the form of events across various networks, security, and system devices in the organization.
- Deploy the SIEM for the in-scope infrastructure and security tools.
- Integration of log sources from various devices/servers/network devices/ security devices/applications/APIs with SIEM as part of the implementation
- Bidder should discuss and develop use cases with Bank & Implement in the project phase.
- The bidder should assess, configure/ migrate the use-cases deployed in the current SIEM to the newly procured SIEM.
- Bidder should carry out fine-tuning of use cases based on the evolving requirement in the ongoing operations phase.
- In case the systems are not able to send the logs to SIEM, the SIEM should be capable to fetch the logs from the point of failure.
- In case of separate logger and collector, If connectivity between log collection agents and logger is down, then the Log collector agents should retain the logs until connectivity is restored and send them once connectivity is re-established.
- Bidder will be responsible to store logs in an industry standard format, preferably in non-proprietary formats.
- Bidder should develop parsers for all log sources without any cost to the Bank.
- Bidder should develop parsers for non-standard logs in the ongoing operations phase, Bidder team deputed onsite will be expected to develop parsers for non-standard logs required during the ongoing operations phase without any cost to the Bank.
- The Bidder has to Identify and document all the data sources that need to be integrated with the SIEM, such as firewalls, intrusion detection/prevention systems, antivirus solutions, servers, and applications.
- The Bidder will be responsible for performing the testing of the SIEM solutions which are as:
 - Functional Testing: Validate that the SIEM system functions as expected, including data collection, correlation, alerting, and reporting.
 - Performance Testing: Ensure the SIEM solution performs efficiently under load, especially during peak events. In this regard, performance certificate is to be provided from the OEM as and when asked by the Bank.
- The Bidder has to document RCA for applicable incidents e.g. Critical, High priorities incidents ensuring accurate and detailed records are maintained. Document lessons



learned and integrated them into SOC processes, training, and threat detection strategies.

- The Bidder must provide regular reports (Daily/Weekly/Monthly/Quarterly) on security trends, alert volumes, and SOC activities. The reports should include but not limited to the following details:
 - Total alerts triggered
 - Open/Closure status of alerts
 - SLA status
 - Root Cause Analysis (RCA) wherever applicable
 - False positive ratio
 - Improvements/Suggestions
 - Rules Triggered
 - Pending Activities
 - SIEM/PIM Servers Onboarding status
- The Bidder has to track the following Metrics and share the details with Bank:
 - Mean Time to Detect (MTTD)- The average time taken to detect a security incident after it occurs.
 - Mean Time to Respond (MTTR)- The average time taken from the detection of an incident to its resolution.
- Bidder should generate various report as per requirement and create a customized dashboard to provide an overview of the security landscape of the organization. Further, dashboard should be provided with MITRE framework & other frameworks as per requirement of the Bank
- Bidders should offer incident management/case management tool with the proposed SIEM solution for automated ticket generation and it should be able to integrate with Bank's existing ITSM tool (Motadata).
- The OEM has to perform half yearly/yearly health check-up of the solution and provide the comprehensive report with suggestions/feedback, if any, to Bank.
- SIEM solution should be patched as and when required or in case new updates are available.
- The solution shall provide the following functionality:
 - Log Collection
 - Log Storage
 - Event Co-relation
 - Alerting
 - Dashboarding and Reporting
- SIEM tool and related components
 - The Bidder must provide monitoring & security analysis of the infrastructure through SIEM solution on 24x7 basis.
 - Monitor all security incidents using SIEM solution deployed at DC and DR and integrated with various infrastructure devices and security solutions of bank. The solution should integrate with Network devices / Security solutions / Servers / Applications / Database of Bank.
 - Provide continuous threat hunting to strengthen cyber security posture.



- Log collection
 - Logs from all devices / appliances / servers / applications / databases located at the geographically dispersed location should be collected. Bidder should develop the baseline for the level of logs to be enabled from different components of IT infrastructure assets.
 - The log baseline should be in line with global best practices. In case the systems/applications are writing logs to the local hard disks, solution should be capable to pull the logs from these devices through secure transfer.
 - Server logs collection to be monitored and alert to be raised, if logs not received after a threshold time, dashboard to be provided for the same. System should automatically initiate SMS/Email to respective stakeholders in case of non-reporting logs.
 - Only in the case where remote log collection is not feasible, Bidder should install agent on the servers and applications for collection of logs. Raw logs should be made available in case of legal requirement.
 - Bidder shall develop a framework to detect log stoppage issue based on the criticality of the log sources.
 - Bidder to troubleshoot log stoppage issue along with the system owners.
- Log aggregation and normalization
 - Logs collected from all the devices should be aggregated as per configured parameters.
 - Logs from multiple disparate sources should be normalized in a common format for event analysis and correlation.
 - Log collected on SIEM solution should be forwarded orchestration / analytical solution.
- Log archival.
 - Logs collected from all the devices should be stored in a tamper proof format on the archival device in the compressed and encrypted form. Collection of Logs and storage should comply with the Regulatory requirement and should maintain a chain of custody to provide the same in the court of law in case the need arises.
 - For correlation and report generation purpose, The solution will be able to retain six months logs online and 1 year in warm node (Six months + 12 months) and beyond that in Archival node . The online storage shall be stored in SAN and NAS can be considered for Archival.
 - Retrieval of archived logs should not require any proprietary tools/protocol and should be retrievable using open standards/protocols or else the retrieval tool should be provided to the Bank without any additional cost.
- Log correlation
 - Collected logs should be correlated according to various predefined criteria for generation of alert and identification of the incident. Correlation rules should be customized by the vendor / System Integrator on a regular basis to reduce false positives. In any case false negatives will not be permitted. In case of detection

of any such incident, correlation rules must be customized immediately to capture such incidents.

- Alert generation
 - Solution should be capable to generate alerts, register and send the same through message formats like SMTP, SMS, Syslog, SNMP as per user configurable parameters.
- Event viewer / dashboard / reports / incident management
 - SIEM Solution should provide web-based facilities to view security events and security posture of the Bank's Network and register incidents.
 - Solution should have drill down capability to view deep inside the attack and analyze the attack pattern. Dashboard should have filtering capability to view events based on various criteria like geographical location, Device type, attack type etc.
 - Dashboard should have Role based as well as Discretionary access control facility to restrict access to incidents based on user security clearance level.
 - Solution should provide various reports based on user configurable parameters and standard compliance reports like ISO 27001:2013/2022, ISO 31000:2018, ISO 27017:2019, ISO 27701:2019, ISO 22301:2019, PCI-DSS etc., and from regulatory and statutory authorities.
 - The Bidder will customize incident management / dashboard / reports for the Bank and will modify them as per the changing requirement of the Bank.
- Integration with in-scope monitored devices and interoperability.
 - The Bidder is responsible for integrating SIEM solution with the hardware items & security solutions. As the system integrator the Bidder will also be responsible for integrating all in scope security solutions/devices with the SIEM solution for log monitoring, correlation.
 - The SIEM solution should support integration of all windows, Linux, LinuxONE, RHCoS, HP-Tandem, UNIX flavoured Operating systems and OEM should develop the connectors wherever applicable without any extra cost to the Bank.
- Development of connectors/parsers for customized applications/devices
 - While it is expected that connectors for all the standard applications, APIs and devices will be readily available in the collector and Log management devices, connectors not available for devices will need to be developed. It is the responsibility of the Bidder to develop connector applications for all devices.
 - The solution shall support the various Use Cases to provide log collection, event correlation, alert generation, and escalation.
- SIEM Use case Management
 - The bidder shall ensure all the current SIEM assessed and use cases are transferred to the Next Gen SIEM solutions with/without optimization.
 - Bidder to develop new use cases as per the Bank's requirement.
 - Bidder to perform quarterly rule review which should include the following but not limited to,

- Total number of rules triggered alerts
- False positive vs True Positive
- MITRE ATT&CK Coverage
- Number of rules with no events
- Bidder to fine-tune to the rules based on the feedback received from Bank or SOC team
- Bidder to incorporate change management process in rule management
- Bidder to enhance the MITRE ATT&CK coverage and share the progress report
- Bidder to ensure up-to-date reference sets/Watchlist leveraged in SIEM use case
- Perform quarterly review of watchlist and remove stale indicators
- Bidder to fix the gaps identified by OEM or Auditor as part of the assessment
- Bidder to manage access provisioning and de-provisioning to the platform.
- Bidder to perform monthly access reconciliation and share the report with the Bank.

II. User and Entity Behavior Analytics (UEBA)

- UEBA as a part of analytical engine of NG-SOC shall deeply compliment SIEM.
- It should profile and analyze the activities of users and IT infrastructure objects from their digital footprint standpoint, to identify outliers who are (users) or which are (entities) inadvertently or deliberately performing unexpected activities thereby showing signs of behavior different than their peers in same team, group, business / IT unit or function, region, zone, delegated powers / authority etc.
- Solution should provide early warning or prediction must be done at very early stage by utilizing inbuilt deep analytics powered by AI/ML.
- UEBA should provide complete case management with quick, accurate, efficient, and complete replay of attack / kill chain life cycle on the console and reports right from reconnaissance, external penetration, gaining a foothold, deliver payload, appropriating privileges, lateral movement, internal reconnaissance, data collection, maintain presence & exfiltration of data, information, logs, self-destruct, wipe out forensic proof etc.
- Integrate with existing and proposed security solutions.
- Identify and integrate respective log sources such as Active Directory, Network Traffic etc.
- Define normal behavior baseline for user and entities.
- Use historical data collected in SIEM to train the UEBA models.
- Create alert thresholds based on the risk level of detected anomalies.
- Implement automated response actions for high fidelity alerts.
- Regularly update the UEBA model to address evolving threats.
- Fine-tune models to reduce false positives and provide high fidelity alerts.
- Create custom dashboards and reports as per Bank's requirements.
- Develop SOPs and How to Document for managing the operations.

III. Security Orchestration, Automation & Response (SOAR)

- Bank intends to use SOAR as orchestration, automation and remediation engine which should automate incident triage by leveraging artificial intelligence, Machine learning and self-learning capabilities to provide measurable reduction in time gaps between incident detection, analysis, and closure by continuous optimization of workflows, playbooks to lessen the dependency on NG-SOC Admins and NG-SOC Engineers.
- The solution should ensure that time between MTTD and MTTR should be improved gradually. Further, the vulnerability window should be within the tolerable time limit of the Bank.
- Having hundreds of inbuilt playbooks for threat detection & prevention technologies/ applications, IT infrastructure, their makes, models & versions, the SOAR should analyze incident and prioritize & perform triage leveraging joint efforts by personnel resources and technologies, create / update playbooks and thus standardize response to security incidents.
- SOAR should endeavour to build & customize playbooks leveraging its analytical abilities powered by AI/ML. Thus, the SOAR should support push and pull mechanism – push instruction into systems and pull data, information, logs from IT infrastructure using APIs, light weight / simple scripts etc. and pull mechanism is to extract relevant info, logs, data, emails, information, alerts from NG-SOC technologies, IT Infra, emails (to read IOCs etc.).
- SOAR licenses should be strictly based on number of active users/ analysts as defined in the scope of work. There should be no limitation / restriction in SOAR licenses based on the number of events coming to the SOAR or the number of playbooks or actions performed by the SOAR.
- The bidder shall develop custom integration as necessary within the defined timeline.
- Bidder shall develop custom playbooks as per the requirements. There should not be any limitation on the number of playbook bidder should develop during the tenure of the contract.
- Bidder to has to maintain separate UAT environment instance of SOAR.
- Bidder to perform periodic backup and store in a secure storage.
- Bidder to fix the gaps identified by OEM or Auditor as part of the assessment
- Bidder to build incident and alert layout.
- Bidder to troubleshoot playbook related errors.
- Bidder to manage access provisioning and de-provisioning to the platform.
- Bidder to perform monthly access reconciliation and share the report with the Bank.
-

7.4 SERVICES

- All professional services necessary to successfully implement the proposed Software Solution will be part of the RFP/Contract



- Bidder should ensure that key personnel with relevant skill sets are available to the Bank at the designated locations for installation and commissioning of the Solution/product.
- Bidder should ensure that the quality of methodologies for delivering the services, adhere to quality standards/timelines stipulated therefore.
- Bidder will transfer skills to relevant personnel from the Bank, by means of onsite / offsite training and documentation.
- Bidder shall provide and implement patches/ upgrades/ updates for hardware/ software/ Operating System / Middleware etc. as and when released by Service Provider/ OEM or as per requirements of the Bank. Bidder should bring to notice of the Bank all releases/ version changes.
- Bidder shall ensure to integrate all the identified and asked applications/solutions/Network devices with NG-SOC solutions.
- Bank will not pay any cost for custom integration of any applications/ Devices/ solutions. Bidder have to bear the cost with OEM, if any.
- Successful Bidder shall obtain the consent from the Bank before applying any of the patches/ upgrades/ updates. Solution must support older versions of the hardware/ software/ Operating System /Middleware etc. in case the Bank chooses not to upgrade to latest version.
- Successful Bidder shall provide maintenance support for Hardware/ Software/ Operating System/ Middleware over the entire period of Contract.
- All product updates, upgrades & patches shall be provided and implemented by the Bidder/ Service Provider free of cost during the entire contract and support period including Warranty, AMC and ATS tenure.
- Bidder shall provide legally valid Software/ hardware/ firmware Solution. The detailed information on license count and type of license shall also be provided to the Bank.
- The Bidder shall keep the Bank explicitly informed the end of support dates on related products/hardware/firmware and should ensure support during warranty and AMC, ATS and S&S. If any Software/hardware will become end of support during contract period bidder have to upgrade all the required equipment's/software's during contract period without any extra cost.
- Below services should be offered as part of NG-SOC Offering:

- i. Security Intelligence Feeds and Services
- ii. Threat Hunting Services:
 1. The bidder must conduct threat hunting exercise locally on the infrastructure
 2. The threat hunting exercise must be conducted regularly.
 3. The vendor must provide only experienced threat hunters (minimum 8yrs in cyber security) for the threat hunting exercise
 4. The threat hunting team must provide the threat hunting plan before every threat hunting exercise
 5. The threat hunting team must ensure the rules used by the SIEM are updated to detect the latest threats
 6. They should share the list of IOC provider's intelligence feeds.

7.5 SECURITY DASHBOARDS

As a part of deliverables, successful bidder must supply and install hardware-based video wall-based dashboard having minimum 16 HDMI based inputs with 4 outputs(4K resolution) with minimum screen to screen bezel (less than 1 mm) for viewing real-time incidents/events, alerts, status of action taken etc. The dashboard should be an easy-to-use Web User Interface with search function, create reports, as well as access cases and applications, with just a few clicks. The bidder should implement an integrated online security dashboard for the entire solution deployed as part of this RFP. The same is required to be implemented onsite at Bank's premises meeting the following requirements:

- The dashboard should be based on secure web based architecture and accessible to users only after verifying identity with Multi Factor Authentication mechanism. It should be made available as online portal and accessible through devices such as Desktop, Laptop, Mobile, Tablet and iPad. This should have the automated facility of sending e-mails and SMS and the dashboard should be available through mobile app, if feasible.
- The dashboard should be provided as integrated view by integrating with the following tools.
 - i. Risk baseline
 - ii. Asset database
 - iii. Security event/log monitoring tool
 - iv. Incident management process
 - v. Security Analysis, Mitigation and reporting
 - vi. Other security solutions/tools of Information Security Department.

vii. Other security solutions, Technologies and devices as required by Central Bank of India.

- Dashboard should display asset list and capture details including name, location, owner, branch, IP address, platform details etc.
- Dashboard should display risk baseline corresponding to multiple categories for IT infrastructure, applications and processes.
- There should be features to identify unique alerts between a particular period
- There should be feature for sending unique alert between a particular period to the identified stake holder official for further necessary action and this should be configurable and customizable.
- The summary should be available capturing the present status of Events/Incidents whether it is Open/Closed/In progress/Pending/Outstanding etc. between different periods.
- There should be option to generate reports like disk space utilization, peak memory utilization and other critical parameters.
- The dashboard should display the security status of IT infrastructure assets of Banks. Dashboard should have graphical display of asset security status based on locations, business units, Value, Platform, owner, Branch etc.
- Dashboard should capture risks in each asset. Dashboard should have the provision to click on the asset and track mitigation status corresponding to risks.
- There should be a graphical representation of risks across business units/locations. Dashboard should support drill down graphs to move to the level of individual assets and should support wide array of analytics and intelligence capabilities.
- Bank should be able to benchmark and track mitigation for new global threats and vulnerabilities using the dashboard. The applicability of new threats to Bank's assets should also be displayed. A drill down of assets affected by new threats, vulnerabilities and status of mitigation should also be supported.
- SLA data should be captured in the dashboard with compliance details.
- SLA reports as agreed upon by Bank should be generated on daily/monthly/quarterly frequency.



- Exclusive dashboard for uptime / down time of IT Assets, No of Log generated / Analyzed/recommendation etc.
- The Dashboard should be context oriented like Security, Business, Control & Risk etc.
- Dashboard should be available for following:
 - i. Top Management (Company View)
 - ii. Department Heads (View to the data associated with their function group / business line)
 - iii. CISO & CIO (complete and detailed dashboard of Security posture of the organization set-up being monitored through this SOC -NOC)
 - iv. System Administrator (for the systems associated with this administrator).
 - v. Network / Security Administrator (for devices / equipment for which he is administrator)
 - vi. Application Administrator
 - vii. Auditor (Internal Auditors, IT Auditor, ISO Certification Auditor or any other authorized official of the organization)

7.6 OEM'S RESPONSIBILITIES ENGAGED BY THE BIDDER

The bidder will provide the services of OEM to the success of the project during actual implementation by being involved in Solution design of the project till its completion. The OEM should be involved in the overall design, architecture, implementation, post implementation review, yearly review etc. for each of the proposed solution by the bidder as per the scope of work defined in RFP. Implementation should be done by the OEM.

Bidder will provide the certificate from OEM to Bank post implementation, confirming the implementation of their products with best industry practices and the standards and no vulnerability or malware in the installed device or appliance.

The following are the tentative expectations with respect to OEM involvement during the contract period, however Bank reserves the right to change the scope:

- Review of Business Requirements Specification (BRS) document, considering all quantitative and qualitative aspects related to configuration of the solution from an industry leading practices perspective and in tune with regulatory guidelines.



- Review of solution architecture to assess the extent to which same will support business requirements and review gaps/ customizations, if any
- Review of test strategy, scenarios and test cases developed for supporting the configuration for conducting UAT of the solution configured.
- OEM should perform:
 - Validation of solution design and architecture.
 - OEM vetting / go ahead would be necessary after implementation of its products.
- OEM should release the parsers immediately after upgradation/change in version of any application/Operating system etc.
- OEM shall release updated integration guides within 30 days of upgradation of any supported/unsupported applications/databases/devices.
- Bidder is responsible to arranging/conducting yearly review from respective OEM's without any additional cost to the Bank.

7.7 NG-SOC OPERATIONS, FACILITY MANAGEMENT, AMC & ATS

Bidder is responsible for below operational matters during the Contract period.

1. The bidder should manage, monitor, maintain and upgrade all NG-SOC solutions on ongoing basis encompassing all deployed hardware / firmware / middleware / software components by performing timely backups, continuous health monitoring, on-site and offsite support, troubleshooting, critical functional and performance bug fixes, all major product/feature enhancements within the warranty and AMC/ATS charges and as per the SLA defined by the Bank for Contract period.
2. All onsite resources should ensure to deliver the services leveraging NG-SOC technologies as mentioned in the technology details, architecture and Terms & conditions in the RFP, addendums, corrigendum, clarifications etc. issued by the Bank.
3. Bidder must seek consent for onboarding of any resources for the onsite support. Bank reserves the right to conduct interviews before onboarding of any such



resource(s). Any such resource will be onboarded only after getting approval from Bank.

4. The onsite resources must be provided with adequate guidance, assistance & support by competent offsite subject matter experts (SME) of the bidder & OEMs.
5. There should be considerable reduction in MTTD (Mean Time to Detect) and (Mean Time to Remediate) MTTR for security incidents by leveraging technology's own capabilities. All feasible daily routine and standard activities of L1 and L2 to be fully automated in phased manner by the end of first year of operationalizing NG-SOC setup. False positive rate to be less than 5%.
6. Bidder shall be responsible to develop and maintain Standard Operating Procedures (SOP) and base line documents with respect to NG-SOC day to day operations including but not limited to threat management, alert/incident management, reports & dashboards, rules creation & fine tuning, install/upgrades, updates, asset Integration, Business Continuity data & configuration backup, restoration, archival, knowledge management, segregation of duties, change management, patch & version management, KPI and KRI to measure NG-SOC performance etc. as per policies of the Bank. Bidder to create and modify SOP as per the requirement of the Bank periodically and from time to time, as applicable. All SOP will be reviewed by the Bank on quarterly basis.
7. All onsite personnel resources of the bidder should ensure to deliver the services leveraging NG-SOC technologies as mentioned in the technology details, architecture and Terms & conditions in the bid, RFP, annexure, addendums, clarifications etc. issued by the Bank.
8. Starting from Go-Live date of the NG-SOC, it is the responsibility of the Project Manager/L3 deployed by the bidder to furnish a Mandatory undertaking certifying the below at the end of first week of every month:
“To the best of our knowledge and on the basis of logs, data, information collected, analyzed and organized by the NG-SOC in the various systems and further analysis thereof by us using NG-SOC tools/solutions in line with the best practices, we hereby confirm that no major information / cyber security incident has happened during the last month. The logs, data, information etc. correlated by us confirm that there is no data and information have been compromised, exfiltrated and any of the systems have not been compromised or hacked. We also confirm that all the



NG-SOC solutions and services are in good health, optimally configured and running at highest capacity & capabilities to be fully effective in line with the best practices.”

9. Bidder to ensure efficient utilization and monitoring of EPS, optimizing capacity utilization, ensuring quality of data and system performance is maintained optimal, there are no security events omission, misfiring rules, heavy rules and reports etc.
10. L3 onsite personnel resources are expected to work act as Project Manager and to provide guidance to L1 & L2 resources.
11. Participate and contribute in every DR drill, cyber security drill, table-top exercises by the Bank, regulators or any third party.
12. Conduct DR drill of the NG-SOC on quarterly interval or as and when required by the Bank. The capacity of DR should be equivalent to 100% of current load and should be scalable as per annual growth.
13. Develop custom plug-ins, parsers, connectors, agents, adopters for all the systems in the Bank or related to the Bank periodically or as and when needed without any extra cost to bank during the contract period.
14. Develop the baseline for the level of logs to be enabled across the different components of IT including infrastructure, databases, business applications and devices etc. The log baselines should be in line with global best practices including NIST, SANS etc. followed by govt., regulatory compliances, Cybersecurity framework and ISO 27001:2022.
15. Perform fortnightly & monthly gap analysis of current levels of logs enabled in OS, databases, web servers, business applications and devices and entire IT infrastructure & recommend and implement remedial actions.
16. For log collection, wherever remote log collection is not feasible, bidder & respective OEM should work with the IT team to deploy the agent on the servers and applications.
17. Periodically assess the business requirements and configure the required rules, AI/ML based analytics models, self-learning models & processes and generate alerts as per the global best practices and Bank’s requirements.
18. The bidder should provide the on-site support for 24/7 around the year (365 days) for the period of warranty, AMC and ATS. L3/Project Manager executive should be available during Bank’s business hours and also whenever required by the Bank



during any activity. The support should cover the equipment management, software management, customization, policy installation, maintenance, support, consultation, trouble shooting, forensic analysis etc. As per the bank guidelines, to ensure the effectiveness of business continuity procedure.

19. Creating new reports and customize existing reports, dashboards, rules, queries, user interface in all forms to meet the dynamic requirements of the Bank.
20. Define formats for MIS reporting that includes daily, weekly and monthly or any periodical or ad-hoc reports, dashboards as per the Bank's requirements.
21. There should be alert generated and sent to concerned Application owner(s) for every Potential Security Threat and Incident identified based on the configured rules, and comprehensive AI/ML based modelling on the logs received from the respective Application(s). This mechanism should be based on OWASP foundation and other leading threat modelling Parameters based on the best practices. The required use cases should be developed and implemented for each business application as per requirements of the Bank during the contract period.
22. Transfer the knowledge to the Bank's SOC employees and/or Banks' InfoSec team about day to day operations, system / backend level troubleshooting, dashboarding, creating basic and advanced rules & analytical models, creation and customization of reports & queries etc.
23. End-to-End system level frontend and backend management & maintenance related knowledge need to be transferred to the Bank's staff by the bidder's onsite L1 & L2 resources.
24. There should not be any disruption or degradation in the Bank's network bandwidth utilization and availability due to excessive log transmission.
25. Bidder to conduct periodic health check of the NG-SOC systems/solutions by respective OEMs at least once in a year and share the report with the Bank. If any gap found or any recommendation in the report should be rectify or update to the solution by onsite resources of respective OEM within a week's time. OEMs to ensure that their respective systems/solutions operate efficiently, cohesively without any adverse impact on processing, correlation, alerting, dashboarding etc. as per expectations of the Bank, stipulated in the RFP.



26. Secure configuration baseline should be benchmarked and updated on a periodic basis with standards including SANS, NIST, CIS etc. followed by Bank's policies, CERT-IN, IDRBT, RBI,NCIIPC guidelines as updated from time to time.
27. The bidder should provide incident management/case management tool and should integrate with Bank's ITSM (Motadata) for ticketing system, tracking, incident management etc. Such entries in the ticketing tool should be able to provide activities/jobs completed, pending, pending at which/whose end etc. The performance & turnaround time/efficiency of onsite personnel resource would also be evaluated from the MIS generated from this tool/system.
28. All deliverables including reports, incidents/alerts, their closure, vulnerabilities reported and closed, dashboards, query optimization, indexing, automation based on AI/ML, backup & recovery activities etc. should undergo Quality Assurance process by the onsite resources on ongoing basis. Project Manager/L3 of the bidder should define quality metrics, measurement frequency and reporting periodicity in consultation with the Bank.
29. Bidder to ensure security of NG-SOC setup from cyber-attacks & malwares etc. Any suspicious activity, behaviour of the NG-SOC setup must be immediately taken into consideration and acted upon at the top priority.
30. For the security of the NG-SOC setup, bidder should integrate the complete NG-SOC setup with all the currently deployed tools and those procured from time to time by the bank. At present deployed tools include but not limited to AV, ATP, AD, PIM, Firewalls, NIPS, ITAM, ITSM, DLP, NAC, DAM, NBAD, PCAP etc.
31. The NG-SOC setup must be complete in all the respect with different solution components like SIEM, UEBA, Common Data Repository/Data Lake, SOAR etc. are fully integrated to deliver the functionality as one comprehensive solution to ensure logs are captured and the process is automated to perform the desired processes in real-time basis 24x7x365. The system should also be automated to raise the alert to the designated official(s) of the Bank, if there is no log received for a period of 15 minutes. This duration of 15 minutes would be reviewed and reduced depending on the future requirements of the Bank.
32. Review onsite & offsite users as per Segregation of Duties (SoD) like their roles & responsibilities, access level / rights in the NG-SOC technologies and other



- related onsite / offsite systems etc. on periodic basis and deactivate / modify user access etc. as per requirement with prior approval from the Bank.
33. The bidder should perform the advanced threat hunting on continuous basis. They should perform activities and incorporate changes based on global threat intelligence.
34. Successful bidder is required to support the Bank or it's appointed vendor during the digital forensic investigation process as and when required during the contract period
35. Bidder should engage the Subject Matter Expert(SME) as and when required for analytics, statistical models, configuring the systems for supervised & unsupervised learning leveraging AI&ML to take over the activities of L1 & L2 resources by systems, minimizing the false positives to below 5% within first year of by the end of first year of operationalizing NG-SOC setup.
36. Monitor, detect, prevent and appropriately respond against any known and unknowns security threat, risk, bots identification etc.
37. Bidder must provide the brief summary & presentation before going for any major hardware/firmware/middleware/software version upgrade to cover all new functionalities, features and bug fixes that are coming with new version/upgrade.
38. During the entire Contract period at any point of time, if the performance of any system of NG-SOC setup is found to be not satisfactory as per RFP requirement then the Bidder shall be responsible to upgrade the hardware, software, applications etc. to meet the RFP terms at no extra cost to the Bank.
39. Bidder to ensure that the NG-SOC technologies/solutions, services are capable & configurable to send logs, data, network traffic, security alerts etc. on demand to regulators like CERT-in, NCIIPC, RBI etc.
40. If any hardware, software, application, services has got additional component, feature, functionality, load bearing capability, domestic & foreign compliance requirements, security arrangement etc. the same can be activated or provided to the NG-SOC setup just by activating licenses and without procuring any hardware, then the same should be activated and provided in the NG-SOC setup of the Bank without any extra cost to the bank.



41. All proposed engineer, ought to be work at Bank's site, shall be on the company payroll and no subcontracting resources will be allowed to work on NG-SOC project.
42. Email and Telephonic Support should also be provided by the back end experts to the On-site support team.
43. The warranty period for the hardware & software will be three years from the date of Go-live followed by 2 years AMC/ATS as applicable.
44. Post the completion of warranty period, the successful bidder should provide comprehensive AMC & ATS for proposed solution, including other software, associated modules, hardware and services required to meet the requirements in the RFP.
45. Bidder needs to ensure that none of the solution component is declared as EOSL (End of Service Life) for minimum 7 years from the date of PO. If any component is declared as EOSL during the above period, the bidder shall replace the same with an equivalent or higher component meeting the RFP and solution requirements.
46. The AMC/ATS support for the complete solution should include the following:
 - i. All minor and major version upgrades during the period of contract at no extra cost
 - ii. Program updates, patches, fixes and critical security alerts as required.
 - iii. Documentation updates.
 - iv. 24*7*365 support for all the security application related malfunctions and ability to log requests online.
 - v. The Bidder should have back to back agreement with the OEMs for ATS and AMC support.

7.8 MANPOWER REQUIREMENT & DESIRED SKILLSET

This is the minimum manpower requirement per shift. Bidder shall factor the total resource required to meet the below requirement. However, Bank reserves right to increase/decrease the number of resources during the contract period and same will be notified to bidder in advance.

| Threat & Incident Management | | | | |
|------------------------------|---------|---------|-----------|-------|
| Analyst Type | Morning | General | Afternoon | Night |
| L1 | 4 | 0 | 4 | 3 |



| | | | | |
|--|----------------|----------------|------------------|--------------|
| L2 | 1 | 1 | 1 | 1 |
| L3 | 0 | 1 | 0 | 0 |
| SIEM, SOAR & UEBA Engineer/ Use case Engineering & Automation | | | | |
| Analyst Type | Morning | General | Afternoon | Night |
| L1 | 0 | 0 | 0 | 0 |
| L2 | 0 | 1 | 0 | 0 |
| L3 | 0 | 0 | 0 | 0 |
| Infrastructure Management | | | | |
| Analyst Type | Morning | General | Afternoon | Night |
| L1 | 0 | 0 | 0 | 0 |
| L2 | 0 | 1 | 0 | 0 |
| L3 | 0 | 0 | 0 | 0 |
| | | | | |

L3 Resource shall have the responsibilities of Project Manager also.

Desired skill set for Onsite resources:

| Resources Requirement | | |
|---|--|---|
| Threat & Incident Management L1 Triage Analyst | | |
| S.No | Role & Responsibilities | Resources/Shift |
| 1 | 24*7*365 monitoring of security alerts and events generated by SIEM and other in scope security solutions (both on-prem and SaaS solution) | 4 resources per shift for Morning and Afternoon and 3 resources in night shift. SOC Location: The resources may be deployed at both Primary and DR SOC situated in Mumbai/Navi Mumbai and |
| 2 | Triage potential security incidents and assigned severity based on the defined criteria | |
| 3 | Perform preliminary analysis to validate whether an alert represents a true security incident | |
| 4 | Investigate basic indicators of compromise (IOCs) and determine the scope and impact of the incident | |
| 5 | Escalate confirmed incidents to SOC L2 analysts with all relevant information | |
| 6 | Accurately document all findings, actions taken, and evidence collected during the triage process | |
| 7 | Maintain detailed logs of incident activities for further analysis and reporting | |



| | | |
|-------------------------|--|------------------------|
| 8 | Follow established incident response playbooks and standard operating procedures | Hyderabad respectively |
| 9 | Execute predefined use cases and scripts to gather additional information about alerts | |
| 10 | Monitor the health and performance of security monitoring tools and systems | |
| 11 | Report any issues or anomalies with the security tools to ensure continuous monitoring | |
| 12 | Participate in training and development programs to enhance cybersecurity skills | |
| Skills Required: | | |
| 1 | Understanding of networking and security concepts. | |
| 2 | Familiarity with common cyber threats and attack vectors. | |
| 3 | Proficiency in using proposed security monitoring tools and SIEM platforms. | |
| 4 | Analytical skills to assess and validate security alerts. | |
| 5 | Good communication and documentation skills. | |
| 6 | Ability to follow established procedures and protocols. | |
| 7 | The triage analyst shall have minimum 1 years of experience in Monitoring and responding to cyber threats, preferably possess at least one of the following certifications, a)Security+ b)CEH c) ECSA d) OEM Certification | |

| L2 Incident Responder | | |
|------------------------------|--|--|
| S. No | Role & Responsibilities | Resources/Shift |
| 1 | 24*7 analysis of the alerts escalated by the L1 Team | 1 Resource per shift (Morning, General, Afternoon & Night) |
| 2 | Lead and coordinate response activities for High and medium security incidents | |
| 3 | Perform root cause analysis to determine the origin and impact of incidents | |
| 4 | Develop and implement containment, eradication, and recovery strategies | |
| 5 | Correlate data from multiple sources to identify and respond to security events | |
| 6 | Develop and maintain incident response playbooks and runbooks | |
| 7 | Ensure standard operating procedures (SOPs) are followed and updated as needed | |
| 8 | Escalate critical incidents to SOC L3 or other senior incident responders when necessary | |



| | |
|-------------------------|---|
| 9 | Review all the alerts handled by SOC L1 Triage team and provide suggestions to improve triaging of the alerts |
| 10 | Document all actions taken during incident investigations and response |
| 11 | Prepare detailed incident reports and post-incident reviews |
| 12 | Communicate findings and recommendations to management and relevant stakeholders |
| 13 | Participate in security audits and assessments |
| 14 | Conduct regular reviews of incident response processes to identify areas for improvement |
| 15 | Provide SIEM finetuning recommendations to reduce the false positive alerts |
| 16 | Suggest new SIEM use cases to improve threat detection coverage |
| 17 | Provide mentorship and guidance to L1 analysts |
| Skills Required: | |
| 1 | Strong understanding of networking and security fundamentals. |
| 2 | Proficiency in analysing logs and network traffic. |
| 3 | Experience with malware analysis and reverse engineering. |
| 4 | Knowledge of scripting and automation (e.g., Python, PowerShell). |
| 5 | Excellent problem-solving and analytical skills. |
| 6 | Strong communication and documentation skills. |
| 7 | The L2 Incident responder shall have minimum 3-5 years of experience in Incident response, preferably possess at least one of the following certifications, a)Security+ b)ECSA c)GCFA d) GCFE e) CISSP f) OEM Certification |

| L3 /Project Manager | | |
|----------------------------|---|------------------------------|
| S.No | Role & Responsibilities | Resources/Shift |
| 1 | 08*6 analysis of the alerts escalated by the L2 or L1 Team and call support for critical issues | 1 Resource in General shifts |
| 2 | Lead the response to critical security incidents. | |
| 3 | Coordinate with other teams to contain, mitigate, and remediate incidents. | |
| 4 | Develop and execute advanced incident response strategies and playbooks. | |



| | |
|----|---|
| 5 | Gather and analyze evidence from compromised systems. |
| 6 | Conduct malware analysis to understand the behavior and impact of malicious code. |
| 7 | Analyze logs, network traffic, and other data sources to trace the origins of attacks. |
| 8 | Proactively hunt for threats within the network and endpoints. |
| 9 | Utilize threat intelligence to identify emerging threats and vulnerabilities. |
| 10 | Develop and refine threat detection use cases and signatures. |
| 11 | Perform in-depth root cause analysis to understand how incidents occurred and their impact. |
| 12 | Identify security gaps and weaknesses exploited by attackers. |
| 13 | Provide recommendations for improving security controls and preventing future incidents. |
| 14 | Work closely with other IT and security teams to coordinate response efforts. |
| 15 | Provide guidance and mentorship to L1 and L2 analysts. |
| 16 | Document all actions taken during incident response in detail. |
| 17 | Prepare comprehensive incident reports and post-incident reviews. |
| 18 | Communicate findings, impact, and recommendations to senior management and stakeholders. |
| 19 | Evaluate and recommend new security tools and technologies to enhance incident response capabilities. |
| 20 | Continuously improve incident response processes and playbooks. |
| 21 | Develop automation scripts to streamline incident response tasks. |
| 22 | Conduct training sessions for SOC staff to improve their incident response skills. |
| 23 | Stay current with the latest threats, attack techniques, and security best practices. |
| 24 | Participate in industry conferences, workshops, and training programs. |
| 25 | Lead and manage the Security Operations Centre (SOC) team to ensure effective monitoring, detection, and response to security incidents |
| 26 | Oversee the incident response process, ensuring timely and effective resolution of security incidents |
| 27 | Train, and develop SOC team members to maintain a high level of expertise and performance |



| | |
|-------------------------|---|
| 28 | Develop and implement SOC strategies, policies, and procedures to enhance security operations. |
| 29 | Detailed Responsibilities |
| 30 | Provide leadership and direction to the SOC team, ensuring alignment with Bank's goals and objectives |
| 31 | Manage the day-to-day operations of the SOC, including staffing, scheduling, and performance management |
| 32 | Oversee the incident response process, ensuring incidents are identified, investigated, and resolved promptly |
| 33 | Coordinate with other teams and stakeholders during incident response to ensure effective communication and resolution |
| 34 | Conduct post-incident reviews to identify lessons learned and improve future response efforts |
| 35 | Develop and implement SOC policies, procedures, and playbooks to guide security operations and incident response |
| 36 | Ensure policies and procedures are regularly reviewed and updated to reflect changes in the threat landscape and organizational needs |
| 37 | Conduct regular performance reviews and provide feedback to team members |
| 38 | Develop and implement long-term strategies to enhance the effectiveness and efficiency of the SOC |
| 39 | Identify areas for improvement and implement initiatives to enhance SOC capabilities and performance |
| 40 | Collaborate with other security teams, IT departments, and business units to ensure a coordinated approach to security |
| 41 | Communicate security incidents and risks to senior management and other stakeholders |
| 42 | Ensure accurate and timely documentation of security incidents, investigations, and actions taken |
| 43 | Represent the SOC in meetings, presentations, and discussions with internal and external stakeholders |
| 44 | Generate regular reports on SOC activities, incident trends, and key performance indicators (KPIs). |
| 45 | Adhere to SOC SLA and share monthly trend report |
| 46 | Provide management with insights and recommendations based on SOC analysis and findings |
| 47 | Oversee the implementation, and management of security tools and technologies used by the SOC |
| 48 | Ensure tools and technologies are properly configured, maintained, and optimized for performance |
| Skills Required: | |



| | | |
|-------------------------------------|--|------------------------|
| 1 | Minimum 6-8 Years of experience in Security operation centre and have 3 years as SOC Manager | |
| 2 | Knowledge of incident response frameworks (e.g., NIST, SANS). | |
| 3 | Proficiency in using and managing SIEM, SOAR and UEBA | |
| 4 | Knowledge of relevant security standards and regulations (e.g., ISO 27001, GDPR, HIPAA). | |
| 5 | Deep understanding of networking, operating systems, and security principles. | |
| 6 | Expertise in digital forensics, malware analysis, and reverse engineering. | |
| 7 | Strong analytical and problem-solving skills. | |
| 8 | Proficiency in using advanced security tools and technologies. | |
| 9 | Excellent communication and documentation skills. | |
| 10 | Ability to handle high-pressure situations and make critical decisions. | |
| 11 | Continuous learning mindset to stay updated with the evolving threat landscape. | |
| 12 | <p>Preferably shall have any two certifications from the mentioned list,</p> <p>Cyber Security - Any One</p> <p>1) CISSP (Certified Information Systems Security Professional)</p> <p>2) CISM</p> <p>3) CISA</p> <p>4) CEH</p> <p>Incident and Program Management - Any One</p> <p>5) ITIL (Information Technology Infrastructure Library)</p> <p>6) PMP (Project Management Professional)</p> | |
| L2 Infrastructure Management | | |
| S.No | Role & Responsibilities | Resources/Shift |
| 1 | 08*6 general shift and provide on call support for critical issues | |
| 2 | Log Source Management, Ensure timely integration of log sources | |
| 3 | SIEM Rule Management - Ensure rules are up to date to reduce false positives | |
| 4 | Performance Tuning: Optimize Solution hardware/other appliances performance to ensure efficient processing and alerting. | |
| 5 | Compliance and Reporting: Generate reports for compliance and audit requirements. | |



| | | | |
|---|---|---|--|
| 6 | Provide insights and context to support security investigations. | | |
| 7 | Platform Management: The installation, configuration, maintenance, update, upgrade of SIEM, UEBA & SOAR and any other in scope solutions. | | |
| 8 | Provide training and support to security analysts on the use and capabilities of these platforms. | | |
| 9 | Ensure that the platforms meet regulatory and compliance requirements. | | |
| 10 | Perform health check-up daily and share the reports with the stakeholders | | |
| 11 | Perform major and minor upgrades of the platform | | |
| 12 | Ensure all the components are patched up to (n-1) | | |
| 13 | Monitor the availability of all the deployed components | | |
| Skills Required: | | | |
| 1 | Deep understanding of networking, operating systems, and security principles. | | |
| 2 | Strong analytical and problem-solving skills. | | |
| 3 | Proficiency in using advanced security tools and technologies. | | |
| 4 | Excellent communication and documentation skills. | | |
| 5 | Ability to handle high-pressure situations and make critical decisions. | | |
| 6 | Continuous learning mindset to stay updated with the evolving threat landscape. | | |
| 7 | The platform engineer shall have minimum 2-3 years of experience in managing the similar solutions with OEM certification. | | |
| | | | |
| SIEM Use case and SOAR Automation Specialist | | | |
| S.No | Role & Responsibilities | Resources/Shift | |
| 1 | 08*6 general shift and provide on call support for critical issues | 1 resource in General shift On call support whenever required to handle High and Critical issues | |
| 2 | Platform management for SIEM, SOAR & UEBA any other in scope solutions. | | |
| | Integrate UEBA solutions with existing security infrastructure. | | |
| 3 | Model Development: Develop and fine-tune machine learning models to detect abnormal activities. | | |
| 4 | Reduce false positives by fine-tuning alerting mechanisms. | | |
| 5 | Create automated workflows to streamline security operations. | | |



| | |
|----|---|
| 6 | Implement and manage incident response playbooks. |
| 7 | Integrate SOAR platforms with various security tools and systems. |
| 8 | Enhance the efficiency of security operations through orchestration and automation. |
| 9 | Track and report on the effectiveness of automation and response efforts. |
| 10 | Work with security teams to understand their requirements and translate them into SIEM use cases |
| 11 | Design, implement, and test SIEM use cases to detect specific types of security threats |
| 12 | Continuously optimize use cases to improve detection accuracy and reduce false positives |
| 13 | Develop and implement SIEM rules and correlation logic to detect security incidents |
| 14 | Tune alerts to minimize false positives and ensure they are actionable |
| 15 | Create and maintaining parsers/connectors in SIEM and SOAR |
| 16 | Set appropriate thresholds for alerts based on analysis and threat intelligence |
| 17 | Ensure data is normalized and enriched for effective correlation and analysis |
| 18 | Develop and maintain log parsing rules to accurately ingest and process data |
| 19 | Maintain detailed documentation of SIEM use cases, including design, implementation, and tuning procedures |
| 20 | Generate reports on the performance and effectiveness of SIEM use cases |
| 21 | Work closely with stakeholders, including SOC analysts, incident responders, and IT teams, to ensure use cases meet their needs |
| 22 | Collaborate with OEM to troubleshoot issues and implement new features |
| 23 | Innovate and experiment with new use case ideas to enhance the SIEM's detection capabilities |
| 24 | Design and develop automated workflows to address common security operations tasks and incidents |
| 25 | Write and maintain scripts (e.g., Python, PowerShell) to support automation tasks |
| 26 | Create and implement playbooks that automate the response to security incidents. |
| 27 | Develop use cases for automation based on common incident scenarios and threat patterns |



| | |
|-------------------------|--|
| 28 | Automate the enrichment of security alerts with contextual information to improve decision-making |
| 29 | Integrate various security tools (e.g., SIEM, EDR, ITSM, firewalls, Threat intelligence platforms) with the SOAR platform. |
| 30 | Continuously optimize automated workflows to reduce false positives and enhance detection accuracy. |
| 31 | Tune the performance of automated workflows to ensure they operate efficiently and effectively. |
| 32 | Establish a feedback loop with security teams to gather input on automation performance and make necessary adjustments. |
| 33 | Monitor the performance and health of the SOAR platform and automated workflows |
| 34 | Maintain detailed documentation of automated workflows, playbooks, and scripts. |
| Skills Required: | |
| 1 | Proficiency with proposed SOAR and SIEM solutions |
| 2 | Experience in configuring, managing, and optimizing SOAR and SIEM platforms |
| 3 | Strong skills in scripting languages (e.g., Python, PowerShell, JavaScript) for developing automation scripts |
| 4 | Experience in writing and maintaining scripts to automate security tasks and processes |
| 5 | Experience in utilizing RESTful APIs to enable communication between different security tools |
| 6 | Experience in converting MITRE TTPs to Misuse cases for better detection and response |
| 7 | Shall have 3-4 Years of experience and proposed OEM certifications |

7.9 TRAINING TO BANK EMPLOYEES

Bidder(s) must mandatorily provide training to the Bank's Core team (Technical & Administrative). This training must be provided by OEM either at bidder's/OEM premises and with virtual/practical Lab with hands on experience on proposed suite of solutions. It is also the responsibility of the bidder to provide training manuals/SOP to each participant. All training material should be in English and should include Specific architecture and layout done for Bank. The bidder should arrange yearly training with minimum 5 days period of atleast 5 participants during the contract period. All out of pocket expenses related to training shall be borne by the selected bidder. Bidder shall have to "certificate of participation" to the trainees identified by Bank.

8. GENERAL RESPONSIBILITY OF THE BIDDER

- For the NG-SOC solution mentioned in the Bill of Material in Annexure-1, Bank has provided the minimum technical specification in Annexure 2.



- Bidders need to ensure that the solutions proposed are comply with these minimum technical requirements. The Bidder shall provide the sizing of the solution based on the information provided by the Bank in this RFP and Annexure 2 - of Minimum Technical Requirements. The Bidder shall provide the details of each individual solutions proposed along with the Hardware & software proposed, in Annexure-1 – Bill of Materials.
- Any components required for the successful implementation of the project should be the responsibility of the bidder.
- Bank is having EULA arrangement for Oracle. Accordingly, if the database proposed by the vendor is Oracle, no cost is to be mentioned. However, the license requirement should be clearly mentioned separately in the technical offer/document. If the proposed database is other than Oracle, the cost (original cost as well as ATS) should be mentioned and will be included in TCO.
- The Bidder shall provide the details of each individual solutions proposed along with the Hardware & software proposed in the RFP.
- Bidder should ensure dual power supply for all proposed solutions.
- Required racks, Network cables, data cabling and other component required for the successful implementation of the project should be the responsibility of the bidder. Bidder to provide the requirement at the time of bid submission.
- 42U Rack with dual PDU and perforated doors (600x800)
- All the equipment should be Rack Mountable and should have dual Power supply units.
- LTO-9 or above Library based backup solution should be provided with backup software and necessary licenses. Online backup feature should be available.
- In case the bidder proposes any alternate solution in place of backup solution as mentioned above, they should be able to provide back up in removable device (tapes) to enable the bank for offsite storage of backup.
- The Bidder should take adequate care to avoid quoting any equipment that will become end of sale within 2 years of supply to the Bank and end of support within 7 years from the date of the submission of offer. In case any hardware / component reaches end of support during the contract period, bidder has to replace the same with new one, including successful installation and migration of data at no additional cost to the Bank. Failure to replace the product well in time by the actual end of support date will be treated as violation of SLA. Bank will procure new solution in such case and cost will be deducted from payables / payments as penalty or by invoking PBG.
- The Bidder is required to procure, supply, install and provide subsequent comprehensive on-site warranty/AMC/ATS of the NG-SOC solution's equipment/appliance based on the Bill of Materials shared by the Bank and the solutions (Hardware, software, etc.) proposed and included in the Bill of Material by the Bidder for the solution.
- The delivery plan must be synchronized with the project delivery timelines of the Bank. Bidder is required to make available required resources that may be required for the successful completion of the entire assignment within the quoted cost to the Bank.



Delivery, Installation and Maintenance

- As a part of implementation of NG-SOC Solutions and associated hardware, the Bank expects the successful Bidder to provide power, space requirements for the equipment to be hosted at DC and DRC. However, the hosting environment requirement shall be provided by the Bank at Bank's DC and DRC.
- Bidder should coordinate with the SPOC (DC/DR) for all the assignments relating to this RFP.
- Bidder is responsible for delivery, transportation, transit insurance – including insurance till installation acceptance by the Bank, unpack, racking and stacking, installation, and configuration of NG-SOC solutions and associated hardware at DC, DRC and Central Office and other locations.
- The Bidder to do Power on self-test, basic configurations, migration, and installation of the equipment.
- Installation of the solutions is to be performed by OEM / OEM authorised partner for each solution.
- Any delay in installation of the NG-SOC Solution and associated hardware for whatsoever reasons should not entail in expiry of insurance and the same should be continued and extended up to the date of installation and acceptance of the delivered NG-SOC Solution and its associated licenses by the Bank.
- Bidder shall ensure compatibility of the supplied NG-SOC Solutions, hardware and licenses with the hardware and software systems being used in the Bank. In case of any compatibility issue arises between the proposed solution/appliance in existing setup during implementation or within 3 months of installation signoff, then the successful bidder is required to replace such solution/appliance, with the compatible one, at no additional cost to the bank within 4 weeks of the issue is identified by Bank or Bank's existing SI.
- Bidder should adhere to the service levels including delivery timelines specified in the RFP for the installation of NG-SOC Solutions and associated hardware supplied by them.
- In case of Hardware based Solutions, bidder shall provide replacement component from the same OEM, if any component is required to be taken out of the premises for repairs.
- Bidder must ensure that on call OEM support can be made available within one hour during the tenure of the contract.
- Bidder should ensure Knowledge Transfer to the Bank throughout delivery of the service, which should include detailed overview of the implementation and configuration parameters and features and functionality of the proposed Solutions under NG-SOC.
- Bidder is required to provide acceptance of Purchase Order, within 7 days of issuance of PO to the successful bidder by the Bank.
- All the components of this RFP should be covered under 24x7x365 direct OEM support for the tenure of the contract; that is the replacement of the defective components should be delivered within four hours from the time call is logged.

9. PROJECT TIMELINES

The successful Bidder is expected to adhere to the following timelines concerning the implementation of the NG-SOC Solutions and associated hardware at Bank's DC and DRC:

| # | Activity | Time for Delivery | Time for Installation | Time for Go Live |
|---|--|---|---|---|
| 1 | Delivery, Installation and Go Live of NG-SOC solutions | 10 Weeks from the acceptance of Purchase Order. | 16 Weeks from the date of acceptance of purchase order. | 8 months from the date of acceptance of purchase order. |

The Bank, at its discretion, shall have the right to alter the delivery schedule and quantities based on the implementation plan. This will be communicated formally to the Bidder during the implementation, if need arises.

Bank can also prioritize the implementation of the offered solutions part of the RFP and the priority of the same will be informed to the successful bidder during the implementation. In such case, project timelines will start from the date of intimation by the Bank.

10. STAGGERED DELIVERY OF THE EQUIPMENT'S.

Bank may ask for staggered delivery of some of the NG-SOC Solutions and associated hardware mentioned in the RFP. Details of the same would be shared with the successful Bidder at a later stage, if required.

11. CONTRACT RENEWAL

Bank, at its discretion, can opt to renew the contract for additional period of time on mutually agreed terms with the Bidder. However, any of the component should not be EOS for mutually agreed period. Bidder has to give confirmation on this score, before entering into agreement for additional period.

12. SLA COMPLIANCE

Bidder should ensure compliance with SLAs as defined in the RFP.

12.1 SERVICE LEVEL AGREEMENTS (SLA)

Bidder should monitor and maintain the stated service levels to provide quality customer service to the Bank.

12.2 SERVICE LEVELS DURING IMPLEMENTATION PHASE

- The Bidder is expected to complete the responsibilities that have been assigned as per the implementation timelines mentioned in Section 9 Project timelines.



Penalty would be levied for delivery, installation, and implementation delays for each solution and shall be a maximum of 10% of the total cost of that solution from the finalized Bidder for the Bank. The Bidder is required to adhere to the Service Level Agreements as mentioned below for the operations phase.

12.3 SERVICE LEVELS POST ACCEPTANCE OF SOLUTIONS BY THE BANK

12.3.1 UPTIME AND UPTIME PENALTY

- The selected bidder shall guarantee a 24x7x365 availability with monthly uptime of 99.90% for the solution as per Scope of Work and Technical and Functional requirements mentioned in the RFP, during contract period, which shall be calculated on monthly basis.
- The "Uptime" is, for calculation purposes, equals to the total contracted minutes in a month less Downtime. The "Downtime" is the time between the Time of Failure and Time of Restoration within the contracted minutes. "Failure" is the condition that renders the Bank unable to perform any of the defined functions on the Solution. "Restoration" is the condition when the selected bidder demonstrates that the solution is in working order and the Bank acknowledges the same.
- The selected bidder should consider high-availability (active-passive) at DC & DR.
- If the selected bidder is not able to attend the troubleshooting calls on solution working due to closure of the office/non-availability of access to the solution, the response time/uptime will be taken from the opening of the office for the purpose of uptime calculation. The selected bidder shall provide the Monthly uptime reports during the warranty period and ATS period, if contracted.
- The downtime calculated shall not include any failure due to bank, and Force Majeure.
- The percentage uptime is calculated on monthly basis as follows:

$$\frac{(\text{Total contracted minutes in a month} - \text{Downtime minutes within contracted minutes})}{\text{Total contracted minutes in a month}} * 100$$

- Contracted minutes of a month = No. of days in that month X 24 X 60.
- Uptime Penalty: Bidder shall ensure that a minimum 99.90% uptime of the solution is maintained monthly (Calculated on a monthly basis, which includes all the components of the solutions as a whole). Components hosted by the bidder in Data Centres such as appliances, solutions, Dashboard and the services offered by the bidder should have high uptime and penalties will be calculated for any unscheduled downtime as mentioned below:

| Sl. No | Service Level Category | Expected Service Level | Penalty | |
|--------|---|--|--|------------|
| 1 | NG-SOC Solutions Uptime (Individual systems at DC/ DR) | Bidder shall ensure that a minimum 99.90% uptime of the solution is maintained monthly (which includes all the components of the solutions as a whole). Components hosted by the bidder in Data Centers such as appliances, solutions, | Uptime % | |
| | | | calculated on monthly basis for each solution. | |
| | | | Uptime 99.90% | No Penalty |



**RFP for Supply, Implementation & Management of Next-Generation Security Operations Centre (NG-SOC) Solutions
Central Bank of India – Tender No – GEM/2025/B/6180729**

| | | | | |
|--|--|--|--|--|
| | | Dashboard and the services offered by the bidder should have high uptime and penalties will be calculated for any unscheduled downtime as mentioned below: | and above | |
| | | | Uptime 98.00% and above but below 99.90% | 1% of monthly NG-SOC operations charges |
| | | | Uptime 96.00% and above but below 98.00% | 2% of monthly NG-SOC operations charges |
| | | | Uptime 90.00% and above but below 96.00% | 5% of monthly NG-SOC operations charges |
| | | | Uptime Below 90.00% | 10% of monthly NG-SOC operations charges |

NG-SOC Operations Charges: AMC+ Resource costs for SOC monitoring and maintenance.

Note: Penalty will not be applicable, if the down time is caused due to any Bank dependency or planned and approved downtime. However, the bidder shall work in tandem with Bank and its existing System Integrator (SI) to resolve such issues and make the solution up & running.

Downtime: subject to the SLA, the accumulated time during which the System is not available to the Bank's users or customers due to system or infrastructure failure. It is measured from the time the Bank reports the incident through mail and /or log a call with the Bidder of the failure or the failure is known to the Bidder observed from the monitoring tools and availability measurement tools to the time when the System operations are restored.

12.3.2 PENALTIES FOR DELAY IN REPLACEMENT OF DEVICES:

Bidder should replace failed hardware and restore the services within 12 hours from reporting time. Otherwise, penalty will be levied on bidder as follows:

| Sl. No | Service Level Category | Expected Service Level | Penalty |
|--------|------------------------|------------------------|---------|
|--------|------------------------|------------------------|---------|



| | | | |
|----|--|---|--|
| 1. | Penalty for Delay in replacement of Devices hardware/software/tool/solution or any other components) | Bidder should replace failed hardware and restore the services within 12 hours from reporting time. Otherwise, penalty will be levied on bidder as follows. | Up to 12 hours: No Penalty |
| | | | 12 hours to 18 hours: 1% of cost of Hardware/ Appliance |
| | | | 18 hours to 24 hours: 2% of cost of Hardware/ Appliance |
| | | | More than one day (24 hours): 5% of cost of Hardware / Appliance |

12.3.3 PENALTY ON SERVICE LEVELS DURING OPERATIONS PHASE

| # | Service Area | Expected Service Level | Penalty |
|----|---|---|---|
| 1. | Security log monitoring(includes infrastructure assets) and Event Notification 24x7 monitoring of all in-scope devices | Notify critical events within 15 minutes of the event identification. 99.9 % and above | NA |
| | | 98% to 99.9 | 2% of monthly NG-SOC operations charges |
| | | 95% to 97.99% | 3% of monthly NG-SOC operations charges |
| | | 90% to 94.99% | 5% of monthly NG-SOC operations charges |
| | | Notify High priority events within 30 minutes of the event identification. 99.9 % and above | NA |
| | | 98% to 99.9 | 2% of monthly NG-SOC operations charges |
| | | 95% to 97.99% | 3% of monthly NG-SOC operations charges |
| | | 90% to 94.99% | 5% of monthly payment |
| | | Notify Medium priority events within 60 minutes of the event identification. 99.9 % and above | NA |
| | | 98% to 99.9 | 2% of monthly NG-SOC operations |



RFP for Supply, Implementation & Management of Next-Generation Security Operations Centre (NG-SOC) Solutions
Central Bank of India – Tender No – GEM/2025/B/6180729

| | | | | | | | | | | | | | | | |
|-----------------|---------------------------------------|---|---|---------------------------------------|-----------------|--|----------|---------|------|-------|--------|-------|-----|-------|---|
| | | | charges | | | | | | | | | | | | |
| | | 95% to 97.99% | 3% of monthly NG-SOC operations charges | | | | | | | | | | | | |
| | | 90% to 94.99% | 5% of monthly NG-SOC operations charges | | | | | | | | | | | | |
| | | Notify Low priority events within 90 minutes of the event identification. 99.9 % and above | NA | | | | | | | | | | | | |
| | | 98% to 99.9 | 2% of monthly NG-SOC operations charges | | | | | | | | | | | | |
| | | 95% to 97.99% | 3% of monthly NG-SOC operations charges | | | | | | | | | | | | |
| | | 90% to 94.99% | 5% of monthly NG-SOC operations charges | | | | | | | | | | | | |
| 2. | Incident response | <p>Response of the incidents is depicted as per the Bank’s SLA defined below:</p> <table><tr><td></td><td>Response Turnaround Time (TAT)</td></tr><tr><td>Severity</td><td></td></tr><tr><td>Critical</td><td>30 mins</td></tr><tr><td>High</td><td>1 Hrs</td></tr><tr><td>Medium</td><td>4 Hrs</td></tr><tr><td>Low</td><td>8 Hrs</td></tr></table> <p>Any violation in meeting the Turnaround time requirements will lead to penalty (Refer below mentioned formula).</p> <p>Percentage of incidents not meeting the Turnaround time monthly basis = (Total number of incidents not meeting TAT /Total number of incidents)*100</p> | | Response Turnaround Time (TAT) | Severity | | Critical | 30 mins | High | 1 Hrs | Medium | 4 Hrs | Low | 8 Hrs | <p>Any violation in meeting the Turnaround time requirements will be calculated on monthly basis.</p> <p>Bank shall impose a penalty of the overall monthly operation charges as mentioned below:</p> <p>Percentage of incidents not meeting the TAT</p> <p>5%< - Penalty of 10 percentage of the overall NG-SOC monthly operation charges</p> <p>2% <=5% - penalty of 5 percentage of the overall NG-SOC monthly operation charges</p> |
| | Response Turnaround Time (TAT) | | | | | | | | | | | | | | |
| Severity | | | | | | | | | | | | | | | |
| Critical | 30 mins | | | | | | | | | | | | | | |
| High | 1 Hrs | | | | | | | | | | | | | | |
| Medium | 4 Hrs | | | | | | | | | | | | | | |
| Low | 8 Hrs | | | | | | | | | | | | | | |



| | | | |
|----|---|--|--|
| 4. | Security Intelligence Advisories within 24 hours of vulnerability disclosure/global threat detection for each security device/solution/product as per asset inventory | Failed to take action on 5 intelligence feed/advisory | NA |
| | | Failed to take action on 10 intelligence feed/advisory | 2% of monthly NG-SOC operations charges |
| | | Failed to take action on 15 intelligence feed/advisory | 3% of monthly NG-SOC operations charges |
| | | Failed to take action on 20 intelligence feed/advisory | 5% of monthly NG-SOC operations charges |
| 2. | NG-SOC and other security solution management – Version/ Release/ Upgrades/ patches | Bidder to inform Bank and ensure that entire stack of NG-SOC – firmware, software, database, middleware, etc. are updated with latest stable firmware, patches, upgrades, release, version, etc. as per the Bank policy(N-1) (or) as per RFP i.e., N-1 release to be applied within 90 days in production. | Penalty of 2% of monthly NG-SOC operations cost per week of delayed updating/patching for any component of NG-SOC once notified by the Bank. |
| 3. | Audit/ VAPT of NG-SOC solutions | Compliance to be submitted within 21 working days for all Critical /High Risk Observations. For all other observations, compliance to be submitted within 1 month. | Penalty of 2% of monthly NG-SOC operations charges for critical and high observations. |
| | | Audit observations to be closed as per Bank's TAT (turnaround time). | |
| 5. | End of sale/ end of support/ end of life of any component | The bidder will have to replace/upgrade the component/software within 3 months from the date of declaration of End of Sale, End of Support/ End of Life. | Penalty of 1% of the cost of the component/ software (as per bill of material submitted by the bidder) after 3 months from date of declaration, per week thereafter from billing cycle payment, till the replacement of the component/ software. |
| 5. | Availability of minimum manpower as per this RFP and add | 99.9 % and above | NA |
| | | 98% to 99.9 | 2% of monthly NG-SOC FMS charges |

| | | | |
|--|----------------------------------|---------------|----------------------------------|
| | changes agreed from time to time | 95% to 97.99% | 3% of monthly NG-SOC FMS charges |
| | | 90% to 94.99% | 5% of monthly NG-SOC FMS charges |

13. RESPONSIBILITY MATRIX

The following table describes the responsibilities of the Bidder, Bank and original equipment manufacturer for problem management and issue resolution related to the applications and tools hosted on the hardware and software proposed by the Bidder.

| Sr. No | Activity | Bank | Bidder | OEM |
|--------|---|------|--------|---------|
| 1 | Solution Designing | S | P | V & M |
| 2 | Installation of the proposed hardware and software including configuration as per the solution design | S | P | P,V & M |
| 3 | Acceptance of the solution | S | P | - |
| 4 | SLA Reports | S | P | - |
| 5 | Incident Management | S | P | P |
| | S – Signed Off (Responsible for providing the go-ahead) P – Performed (Primary responsibility for executing the activity) V – Validated (Responsible for Validating the activity) M – Monitoring (Responsible for continuous monitoring of activity) | | | |

14. LIQUIDATED DAMAGE

The successful bidder must strictly adhere to the schedules for completing the assignments. Failure to meet these Implementation schedule, unless it is due to reasons entirely attributable to the bank, may constitute a material breach of the successful bidder's performance. In the event that the Bank is forced to cancel an awarded contract (relative to this RFP) due to the successful bidder's inability to meet the established delivery dates, and also the bank may take suitable penal actions as deemed fit.

Penalty: The successful bidder shall agree to the penalties structure in accordance with the following:

The Liquidated Damages (LD) shall be 0.5 % of the respective component, which have been delayed for each week or part thereof for delay until actual delivery or performance. However, the total amount of Liquidated Damages deducted will be pegged at 10% of the total contract value. Once the maximum is reached, the Bank may consider termination of the contract and other penal measure will be taken like forfeiture of EMD, Foreclosure of BG etc.

In this context Bank may exercise both the rights simultaneously and severally. In case the Bank exercises its right to invoke the Bank guarantee and not to terminate the contract, the

Bank may instruct to concerned bidder to submit fresh Bank guarantee for the same amount in this regard.

In case delay is attributable to Bank, proper evidence should be produced by Bidder.

15. LAND BORDER SHARING CLAUSE

The Bidder must comply with the requirements contained in O.M. No. 6/18/2019-PPD, dated 23.07.2020 Order (Public Procurement No. 1), Order (Public Procurement No. 2) dated 23.07.2020 and Order (Public Procurement No. 3) dated 24.07.2020. Bidder should submit the undertaking in Annexure 18 in this regard and also provide copy of registration certificate issued by competent authority wherever applicable.

Para 1 of Order (Public Procurement No. 1) dated 23-7-2020 and other relevant provisions are as follows:

- i. Any bidder from a country which shares a land border with India will be eligible to bid in this tender only if the bidder is registered with Competent Authority.
- ii. “Bidder” (including the term ‘tenderer’, ‘consultant’ or ‘service provider’ in certain contexts) means any person or firm or company, including any member of a consortium or joint venture (that is an association of several persons, or firms or companies), every artificial juridical person not falling in any of the descriptions of bidders stated hereinbefore, including any agency branch or office controlled by such persons, participating in a procurement process.
- iii. “Bidder from a country which shares a land border with India” for the purpose of this Order means:
 - a. An entity incorporated, established, or registered in such a country; or
 - b. A subsidiary of an entity incorporated, established or registered in such a country; or
 - c. An entity substantially controlled through entities incorporated, established or registered in such a country; or
 - d. An entity whose beneficial owner is situated in such a country; or
 - e. An Indian (or other) agent of such an entity; or
 - f. A natural person who is a citizen of such a country; or
 - g. A consortium or joint venture where any member of the consortium or joint venture falls under any of the above.

The beneficial owner for the purpose of (iii) above will be as under.

1. In case of a company or limited liability partnership, the beneficial owner is the natural person(s). who, whether acting alone or together, or through one or more judicial person, has a controlling ownership interest or who exercises control through other means.

Explanation

- a. “Controlling ownership interests” means ownership of or entitlement to more than twenty five per-cent of shares or capital or profits of the company.



- b. “Control” shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholder’s agreements or voting agreements.
2. In case of partnership firm, the beneficial owner is the natural person(s), who, whether acting alone or together or through one or more judicial person, has ownership of entitlement to more than fifteen per-cent of capital or profits of the partnership.
3. In case of an unincorporated association or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together or through one or more judicial person, has ownership of or entitlement to more than fifteen per-cent of the property or capital or profits of such association or body of individuals.
4. Where no natural person is identified under (1) or (2) or (3) above, the beneficial owner is the relevant natural person(s), who hold the position of senior managing official.
5. In case of trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with fifteen per-cent or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.
- iv. An agent is a person employed to do any act for another, or to represent another in dealings with third persons.

16. MONITORING & AUDIT

Compliance with security best practices may be monitored by periodic computer security audits / Information Security Audits/Statutory and Regulatory audit performed by or on behalf of the Bank. The periodicity of these audits will be decided at the discretion of the Bank. These audits may include, but are not limited to, a review of: access and authorization procedures, backup and recovery procedures, network security controls and program change controls. The successful bidder must provide the Bank access to various monitoring and performance measurement systems. The successful bidder has to remedy all discrepancies observed by the auditors at no additional cost to the bank. The monthly uptime (previous month) report needs to be submitted by the successful bidder before 5th of Every month to Bank at no additional cost to the Bank.

17. BID SUBMISSION

- All responses received after the due date/time be considered late and would be liable to be rejected. GeM portal will not allow lodgement of RFP response after the deadline. It should be clearly noted that the Bank has no obligation to accept or act on any reason for a late submitted response to RFP. The Bank has no liability to any Respondent who lodges a late RFP response for any reason whatsoever, including RFP responses taken to be late only because of another condition while responding.

Instructions to Bidders: e-tendering

E-tendering will be done through GEM portal. Bidders are required to get registered in GEM portal well in time.



Preparation & Submission of Bids

The Bids (Eligibility Cum Technical as well as Commercial) shall have to be prepared and subsequently submitted online only. Bids not submitted “ON LINE” shall be summarily rejected. No other form of submission shall be permitted.

The bidder has to submit their response in GeM portal before the bid end date & time mentioned in the GeM bid document. The physical documents (viz., EMD, Integrity Pact etc.,) should be submitted to the below mentioned officials before the bid end date & time at the Venue specified in the Bid Schedule.

Senior Manager
Security Operation Centre
Information Security Department
4th Floor, Central Bank of India
Plot No -26, Sector-11
CBD Belapur, Navi Mumbai, Maharashtra – 400614
Phone -022-67123571/022-27582437

The Name and address of the Bidder, RFP No. and Due Date of the RFP are to be specifically mentioned on the Top of the envelope containing physical documents.

Do's and Do not's for Bidder

- Registration process for new Bidder's should be completed at the earliest
- Bidder has to prepare for submission of their bid documents online well in advance as the upload process of soft copy of the bid documents may require encryption (large files take longer time to encrypt) and upload of these files to GeM portal depends upon bidder's infrastructure and connectivity.
- To avoid last minute rush for upload bidder is required to start the upload for all the documents required for online submission of bid one week in advance
- Bidder to initiate few documents uploads during the start of the RFP submission and help required for uploading the documents / understanding the system should be taken up with GeM portal support well in advance.
- Bidder should not raise request for offline submission or late submission since only online submission is accepted on GeM portal.
- Part submission of bids by the Bidder's will not be processed and will be rejected.

Terms & Conditions of Online Submission

1. Bank has decided to determine L1 through bids submitted on GeM portal. Bidders shall bear the cost of registration on the GeM portal. Bidder is bound to follow rules of GeM portal as per Government guidelines.
2. Bidders at their own responsibility are advised to conduct a mock drill if required.
3. In the event of failure of the internet connectivity (due to any reason whatsoever it may be) Bank will not responsible.



4. In order to ward-off such contingent situation, Bidders are advised to make all the necessary arrangements / alternatives such as back –up power supply, connectivity whatever required so that they are able to circumvent such situation and still be able to participate in the Auction successfully.
5. However, the bidders are requested to not to wait till the last moment to quote their bids to avoid any such complex situations.
6. Failure of power at the premises of bidders during the E-Tendering cannot be the cause for not participating in the E-Tendering.
7. On account of this, the time for the E-Tendering cannot be extended and BANK is not responsible for such eventualities.
8. Bank will not have any liability to Bidders for any interruption or delay in access to site of E-Tendering irrespective of the cause.

Tender Schedule (Key Dates)

The Bidders are strictly advised to follow the Dates and Times as indicated in the Time Schedule in the detailed tender Notice for the Tender. All the online activities are time tracked and the electronic Tendering System enforces time-locks that ensure that no activity or transaction can take place outside the Start and End Dates and time of the stage as defined in the Tender Schedule.

At the sole discretion of the tender Authority, the time schedule of the Tender stages may be extended.

18. INTEGRITY PACT

Each Participating bidder/s shall submit Integrity Pact as per attached Annexure 9 duly stamped for ₹500. Integrity pact should be submitted by all participating bidders at the time of submission of bid documents or as per satisfaction of the Bank. The Non submission of Integrity Pact as per time schedule prescribed by Bank may be relevant ground of disqualification for participating in Bid process.

Bank has appointed Independent External Monitor (hereinafter referred to as IEM) for this pact, whose name and e-mail ID are as follows:

1. Shri Anant Kumar [Mail ID: anant_in@yahoo.com]
2. Shri Nirmal Anand Joseph Deva [Mail ID: meghanadeva2022@gmail.com]
 - For any clarifications/issues, bidders are requested to contact with Bank's personnel in the below mail-id before contacting with IEM.
smitcsoc@centralbank.co.in
cminfosec@centralbank.co.in
smitpurchase@centralbank.co.in
 - IEM's task shall be to review – independently and objectively, whether and to what extent the parties comply with the obligations under this pact
 - IEM shall not be subjected to instructions by the representatives of the parties and perform his functions neutrally and independently

- Both the parties accept that the IEM has the right to access all the documents relating to the project/procurement, including minutes of meetings.

19. COMMERCIAL OFFERS

Commercial Bids of only technically qualified Bidders shall be opened based on technical proposal.

The Commercial Offer (CO) should be complete in all respect. It should contain only the price information as per Bill of Material

- The commercial offer should be in compliance with technical configuration / specifications as per Technical Specifications.
- The price to be quoted for all individual items and it should be unit price in Indian rupees.
- In case there is a variation between numbers and words, the value mentioned in words would be considered. The Bidder is expected to quote unit price in Indian Rupees (without decimal places) for all components and services on a fixed price basis, as per the commercial Bid inclusive of all costs. GST (Goods and Services Taxes) shall be payable as per applicable structure laid down under GST Law. The Bank will not pay any other taxes, cost, or charges. The price would be inclusive of all applicable taxes under the Indian law like customs duty, freight, forwarding, insurance, delivery, etc. including applicable GST, which shall be paid/ reimbursed on actual basis on production of bills with GSTIN. Any increase in GST will be paid in actuals by the Bank or any new tax introduced by the government will also be paid by the Bank. The entire benefits/ advantages, arising out of fall in prices, taxes, duties or any other reason, must be passed on to Bank. The price quoted by the Bidder should not change due to exchange rate fluctuations, inflation, market conditions, and increase in custom duty. The Bank will not pay any out-of-pocket expense. The Selected Bidder will be entirely responsible for license fee, road permits, insurance etc. in connection with the delivery of products at site advised by the Bank including incidental services and commissioning.
- The price is inclusive of taxes i.e. Goods and Services Tax, which shall be paid as per actuals.
- Bank will award the contract to the successful Bidder, whose bid has been determined as the **Lowest Commercial bid (L1) through** GeM Portal.
- Bank reserves the rights to negotiate with L1 bidder, if required.

20. EVALUATION & ACCEPTANCE

- Technical offers will be evaluated on the basis of compliance with eligibility criteria, technical specification, other terms & conditions stipulated in the RFP. Only those bidders who qualify in the technical evaluation would be considered for evaluating the commercial bid. Bank may, at its sole discretion, waive any non-conformity or deviations.
- Bank reserves the right to reject the bid offer under any of the following circumstances: a) If the bid offer is incomplete and / or not accompanied by all stipulated documents. b) If

the bid offer is not in conformity with the terms and conditions stipulated in the RFP. c) If there is a deviation in respect to the technical specifications of hardware items.

3. The Bank shall be under no obligation to mandatorily accept the lowest or any other offer received and shall be entitled to reject any or all offers without assigning reasons

21. EVALUATION PROCESS

The competitive bids shall be evaluated in three phases:

- Stage 1 – Eligibility Criteria Evaluation Stage - Bidder have to qualify each and every criteria as mentioned in the section 2 of the RFP, to qualify for the next stage of evaluation.
- Stage 2 – Technical Evaluation Stage - Bidders Qualify in Stage 1 have to score minimum 70% marks in technical evaluation scoring matrix as per section 21.2 of the RFP to qualify for stage 3. The score given by the Bank will be final and Bank reserves the right to increase/decrease minimum qualifying marks.
- Stage 3 – Commercial Bid process

21.1 ELIGIBILITY CRITERIA EVALUATION

Central Bank of India is looking for Supply, Installation and Management of Next-Generation Cyber Security Operation Centre Solution and associated hardware at the Bank. It includes supply, installation, Implementation and maintenance of the Solution(s).

Only those Bidders who fulfil the eligibility criteria are eligible to respond to the RFP. Offers received from Bidders who do not fulfil any of the eligibility criteria will be summarily rejected.

Bidder will be responsible for delivering the end-to-end solution and will be the single point of contact for the implementation, integration, support and maintenance for the entire project. Bidder will also be solely responsible for ensuring adherence to the Service Levels, terms & condition and Service Quality for each of the deliverables executed. However, OEM or its authorized service partners will be responsible for implementation.

Note:

- All relevant documents / certificates should be attached as proof in support of the claims made. The bidder should provide relevant additional information wherever required in the eligibility criteria. Central Bank of India reserves the right to verify /evaluate the claims made by the Bidder independently. Any decision of Central Bank of India in this regard shall be final, conclusive, and binding upon the Bidder.
- In case of business transfer where bidder has acquired a Business from an entity (“Seller”), work experience credentials of the Seller in relation to the acquired business may be considered.
- In-case of corporate restructuring the earlier entity’s incorporation certificate, financial statements, Credentials, etc. may be considered.

21.2 TECHNICAL EVALUATION CRITERIA

The bidder must fulfil the criteria mentioned in the Annexure-2 Technical Specification of this RFP. All the technical specifications requirements mentioned in Annexure-2 are mandatory and 100% compliance of the technical specifications is required.

Note:

All relevant documents / certificates should be attached as proof in support of the claims made. The bidder should provide relevant additional information wherever required in the eligibility criteria. Central Bank of India reserves the right to verify /evaluate the claims made by the Bidder independently. Any decision of Central Bank of India in this regard shall be final, conclusive, and binding upon the Bidder.

In case of business transfer where bidder has acquired a Business from an entity (“Seller”), work experience credentials of the Seller in relation to the acquired business may be considered.

In-case of corporate restructuring the earlier entity’s incorporation certificate, financial statements, Credentials, etc. may be considered.

Detailed Evaluation Criteria



| SN | Criteria | Parameters | Document Required | Max Marks | Marks Scheme |
|----|---------------|--|--|-----------|---|
| 1 | Bidder | Bidder's experience in implementing and managing SOC with on-premises SIEM solution with minimum 30,000 Events Per Second (EPS) or 1TB / Day in at least one BFSI*/RBI/NPCI/BSE/NSE/SEBI/Govt./PSU in India. | Purchase Order along with anyone documents of out of (i) Performance Certificate or (ii) E-mail confirmation from the Official mail ID or (iii) Installation Certificate to be submitted. (iv) Reference letter Details such as Make, Model, EPS etc. should be available in either of the documents. | 20 | One implementation of 30,000 EPS or 1 TB/ Day to 50,000 EPS or 1.6 TB /Day to - 10 Marks |
| | | (*BFSI must be an organization having minimum of 1000 branches/ offices in India) | | | One implementation of 50,000 and Above or 1.6 TB/ Day - 20 Marks |
| 2 | | Bidder's experience in supply & implementation of SIEM Solution in Organization(s) in BFSI segment as on date of Bid submission. | Purchase Order along with any one documents of out of (i) Performance Certificate or (ii) E-mail confirmation from the Official mail ID or (iii) Installation Certificate to be submitted. (iv) Reference Letter Details such as Make, Model, EPS etc. should be available in either of the documents. | 10 | Less than 2 Organization - 2 Marks |
| | | | | | 2 Organizations - 5 Marks |
| | | | | | 3 Organizations - 7 Marks |
| | | | | | 4 or more Organizations - 10 Marks |



| | | | | | |
|---|-----|--|--|----|--|
| 3 | | Bidder's experience in implementing and managing any of the solutions as part of NG-SOC Implementation (SOAR, UEBA) along with SIEM. | Purchase Order along with anyone documents from customer (i) E-Mail confirmation from the Official E-Mail ID (ii) Installation Certificate (iii) Reference Letter Details such as Make, Model, No. of User & Entity, No. of Analyst License, EPS Count etc. should be available in either of the documents. | 20 | SIEM with UEBA or SOAR- 15 Marks |
| | | | | | SIEM with UEBA & SOAR both- 20 Marks |
| | | | | | |
| 4 | OEM | Proposed OEM's SIEM solution with minimum 60,000 EPS or 2 TB/ Day in at least two BFSI*/RBI/NPCI/BSE/NSE/SEBI/ Govt./PSU in India during the last seven years. (*BFSI must be an organization having minimum of 1000 branches/ offices in India) | Purchase Order along with any one documents of out of (i) Performance Certificate or (ii) E-mail confirmation from the Official mail ID with solution details or (iii) Installation Certificate to be submitted including solution details. (iv) Reference Letter Details such as Make, Model, EPS etc. should be available in either of the documents. | 20 | Two Implementa tion of minimum 60,000 EPS or 2 TB Data/ Day – 10 Marks |
| | | | | | Out of two implementa tion of minimum 60,000 EPS or 2 TB Data/day one implementa tion of 1,00,000 EPS and above or 3.5 TB – 20 Marks |



RFP for Supply, Implementation & Management of Next-Generation Security Operations Centre (NG-SOC) Solutions
Central Bank of India – Tender No – GEM/2025/B/6180729

| | | | | | |
|---|--|---|--|----|---|
| 5 | | Proposed OEM's operational presence in India | Purchase order/work order/contract from client/distributor/system integrator to substantiate the proposed OEM's operational presence in India. | 10 | Upto 7 Years – 5 Marks |
| | | | | | More than 7 Years - 10 Marks |
| 6 | | Offered UEBA solution should be deployed at least One BFSI*/RBI/NPCI/BSE/NSE/SEBI/Govt./ PSU in India) during the last seven years. (*BFSI must be an organization having minimum of 1000 branches/ offices in India) | Purchase Order along with any one documents of out of (i) Performance Certificate or (ii) E-mail confirmation from the Official mail ID with solution details or (iii) Installation Certificate to be submitted including solution details. (iv) Reference Letter Details such as Make, Model, Number of Users etc. should be available in either of the documents. In case of UEBA deployment other than User based licensing, then bidder/OEM is required to produce a reference letter from the client clearly specifying the no. of simultaneous users being supported by the deployed UEBA solution. | 10 | Above 15,000 User's Licences – 3 Marks |
| | | | | | 15,001 to 25,000 User's Licences – 5 Marks |
| | | | | | 25,001 to 35,000 User's Licences – 7 Marks |
| | | | | | For above 35,000 User's Licences – 10 Marks |

| | | | | | |
|---|--|---|---|----|--------------------------------------|
| 7 | | Offered SOAR solution shall have been deployed at least One BFSI*/RBI/NPCI/BSE/NSE/SEBI/Govt./ PSU in India) during the last seven years. (*BFSI must be an organization having minimum of 1000 branches/ offices in India) | Purchase Order along with any one documents of out of (i) Performance Certificate or (ii) E-mail confirmation from the Official mail ID with solution details or (iii) Installation Certificate to be submitted including solution details. (iv) Reference Letter Details such as Make, Model, Number of Analyst License etc. should be available in either of the documents. | 10 | For 1 Implementation – 3 Marks |
| | | | | | 2 to 3 Implementation – 5 Marks |
| | | | | | 4 and above Implementation –10 Marks |

Note:

1. The minimum qualifying score will be 70 marks and bidder has to score minimum 30 marks in each section of criteria i.e. Bidder and OEM.
2. Bank reserves the right to increase or decrease the minimum qualifying score.
3. If required, Bank may call for presentation(s), product walkthroughs, on the features of the solution offered etc., from the bidders based on the technical bids submitted by them.
4. Based upon the compliance of the minimum technical specifications of the proposed product / solution, shortlisting would be made of the eligible bidders for final commercial bidding.
5. Bank reserves the right to conduct reference site visits at the Bidder's client sites.
6. If the OEM has undergone merger/acquisition/de-merger then the earlier entity's reference shall also be considered.

21.3 COMMERCIAL EVALUATION CRITERIA

The Commercial offers of only those Bidders, who are short-listed after technical evaluation, would be opened. The format for quoting commercial bid set out in Annexure-1-Commercial Bill of Material. The commercial offer should consist of comprehensive cost for required solution. Bidder must provide detailed cost breakdown, for each and every category mentioned in the commercial bid. The Bank will determine whether the Commercial Bids are complete, unqualified and unconditional. Omissions, if any, in costing any item shall not entitle the firm to be compensated and the liability to fulfil its obligations as per the Scope of the RFP within the total quoted price shall be that of the Bidder.

Bidder (L1) quoting the lowest commercial bid will be selected on the basis of Total Cost of Ownership (TCO) Price mentioned in the Summary Cost of Annexure 1-Commercial Bid.

22. PAYMENT TERMS

The term of the contract will be 5 years. Hardware to be provided for execution of project should be sized for 5 years by considering functional & technical requirements as per in-scope solutions. However, if it is found that the hardware is not sized adequately or the hardware utilization goes beyond the threshold limit of 70%, the Bidder has to provide additional hardware at no additional cost to meet the performance parameters set by the Bank. The Bidder must accept the payment terms proposed by the Bank as proposed in this Section. The financial offer submitted by the Bidder must be in conformity with the payment terms proposed by the Bank. Any deviation from the proposed payment terms would not be accepted.

The scope of work is divided in different areas and the payment would be linked to delivery and acceptance. All / any payments will be made subject to compliance of Service Levels defined in the RFP document. The Bank shall have the right to withhold any payment due to the Bidder, in case of delays or defaults on the part of the Bidder. Such withholding of payment shall not amount to a default on the part of the Bank. If any of the items / activities as mentioned in the price bid is not taken up by the Bank during the course of the assignment, the Bank will not pay the fees quoted by the Bidder in the price bid against such activity / item.

Payment for the Supply of required HW, SW, Design, Installation, Implementation, and Commission of the NG-SOC solutions shall be made by Bank as per the solutions in scope as mentioned in the Scope of Work.

22.1 PROCEDURE FOR CLAIMING PAYMENTS

The Bidder's requests for payment shall be made to the Bank in writing accompanied by Original Invoice detailing the systems, software delivered, installed and accepted by the Bank. The payment after deducting applicable TDS will be released by the Bank. All payments will be made only by electronic transfer of funds either by NEFT or RTGS. The Bidder therefore has to furnish the Bank account number to where the funds have to be transferred for effecting payments. Payments as per the schedule given below will be released only on acceptance of the order and on signing the agreement / contract by the selected Bidder and also on submission of Performance Bank Guarantee.

The Bidder will have to submit a document explaining the AMC / ATS costs. The scope of work is divided in different areas, the payment would be linked to delivery, and acceptance of each area as explained below:

| S. No | Deliverables | % Of Payment | Payment Milestone (On completion of the activities) |
|-------|--------------|--------------|---|
| 1. | Hardware | 60% | Against delivery of respective components. |



| S. No | Deliverables | % Of Payment | Payment Milestone (On completion of the activities) |
|-------|---|--------------|--|
| | | 30% | Against successful installation and Sign-off of respective components. |
| | | 10% | 3 months after successful Go-Live signoff of respective components. |
| 2. | Software (Including OS & other associated software) | 70% | Against delivery of respective components |
| | | 20% | After sign-off and go-live of respective components. |
| | | 10% | 3 months after successful Go-Live signoff of respective components. |
| 3. | One Time Implementation Charges | 70% | After sign-off and go-live of respective components. |
| | | 30% | After 3 months of go-live of respective components. |
| 3 | For FM Support | - | Payment for on-site support charges will be paid quarterly in arrears. |

22.2 AMC/ATS PAYMENT TERMS

- AMC/ATS amount payable would be paid quarterly in arrears at the end of each quarter.
- First quarter for AMC/ATS payment would begin from 1st of the next month of the date of completion of the warranty period.
- In case bidder fails to have agreement with respective OEM's for back-to-back support after 3 years for hardware & software post warranty, the bank reserves the right to not make any payment for the duration for which Bidder was unable to produce the back-to-back agreement with the respective OEM to the Bank.

22.3 AMC & ATS and Warranty Costs

Bidder shall provide the maintenance (Warranty, AMC & ATS) for a period of five years from the date of GO-Live of the product in the Bank. Warranty period for the new components should be for the first three years for which the cost should be factored in the Product cost and AMC/ATS shall be factored for the subsequent two years. Bidder must factor the costs in the Bill of Material accordingly. As part of warranty, AMC & ATS support the Bidder must:

- Provide on-site comprehensive support for Next-Gen Security Operation Centre(NG-SOC) Solutions and associated hardware provided as part of this RFP
- Have back-to-back arrangements with respective OEMs for the maintenance services (Warranty/AMC/ATS)



- Warrant all the NG-SOC solutions and associated hardware against defects arising out of faulty design, materials, and media workmanship etc., for a period of five years from the date of acceptance of the Solutions.
- Provide maintenance of NG-SOC Solutions hardware as well as repair or replacement activity after hardware problem has occurred. If the supplied equipment are to be replaced permanently due to the Bidder's inability to provide spares or maintain the equipment, the Bidder shall replace the equipment of same make/ model/configuration or of higher configuration at no extra cost to the Bank. However, the Bank may accept different make/model/ configuration at its discretion, if the original make/model/ configurations are not available in the market due to obsolescence or technological up gradation
- Provide support services like repair, replacement to resolve the problem as per the service levels defined in this RFP.
- Defective hardware shall be replaced by the Bidder at his own cost, including the cost of transport etc. The Bidder shall not charge the Bank any extra charges related to this activity during the period of contract.
- Bidder may provide adequate spares for the critical components of the NG-SOC Solutions and associated hardware to meet the SLA.
- Provide expert person for onsite support during DR Drills / cyber drills / attack simulation exercises / audit etc as required by the Bank.
- The Bank will not be liable to pay any additional amounts in respect of any sort of maintenance covered under the scope of this tender during the tenure of the contract. Free on-site maintenance services shall be provided by Bidder during the period of warranty
- Bidder should undertake system maintenance and replacement or repair of hardware.
- In case equipment taken away for repairs, Bidder shall provide similar standby equipment so that the equipment can be put to use in the absence of the originals/ replacements without disrupting the Bank's regular work
- If during operation, the down time of any piece of equipment or component thereof does not prove to be within reasonable period, Bidder shall replace the unit of component with another of the same performance and quality or higher, at no cost to the Bank
- Further provided that the Bank may, during the contract, shift the goods wholly or in part to other location(s) within the Country and in such case the Bidder undertakes to continue to warrant or maintain the goods at the new location without any other additional cost to the Bank
- In case the Bank desires to get the services delivered by their appointed Bidder or System Integrator, then the OEM shall transfer such services to that preferred Bidder at no additional cost to the Bank.
- In case of any issue with NG-SOC Solution and associated hardware supplied by Bidder, Bank shall log a call with Bidder (who has supplied the Solution) it is responsibility of Bidder to resolve the issue with the assistance of the OEM if deemed

necessary. The Bank or its appointed System Integrator shall promptly notify Bidder in writing/e-mail of any claims arising under the maintenance services.

- Provide all future software upgrades and patches for all components of the solution and assist the Bank or its System Integrator to install the same if Bank desires during period of contract at free of cost.
- Bidder warrants that the Goods supplied under the Contract are new & unused, of the most recent or current models and incorporate all recent improvements in design and materials unless provided otherwise in the RFP
- Bidder further warrants that all the Goods supplied under as part of this RFP shall have no defect arising from design, materials, or workmanship (except when the design and/or material is required by the Bank's Specifications) or from any act or omission of Bidder, that may develop under normal use of the supplied Goods in the conditions prevailing at the final destination
- Bidder's hardware engineer will report at the Bank's premises within one hour of reporting of breakdown and repair the same at the earliest.

The payments will be released through NEFT / RTGS/account credit after deducting the applicable LD/Penalty, TDS if any, on submission of invoices to Information Security Department, Central Office, CBD- Belapur. The Successful Bidder has to provide necessary Bank Details like Account No., Bank's Name with Branch, IFSC Code, GSTIN, State Code, State Name, HSN Code etc.

Fixed Price

The commercial offer shall be on a fixed price basis, inclusive of all taxes and levies. No price variation relating to increases in customs duty, excise tax, dollar price variation etc. will be permitted. The bidder shall pay any other applicable Taxes being applicable after placement of order, during currency of the project only.

Taxes

1. The consolidated fees and charges required to be paid by the Bank against each of the specified components under this RFP shall be all-inclusive amount with currently (prevailing) applicable taxes. The bidder shall provide the details of the taxes applicable in the invoices raised on the Bank. Accordingly, the Bank shall deduct at source, all applicable taxes including TDS from the payments due/ payments to bidder. The applicable tax shall be paid by the bidder to the concerned authorities.
2. In case of any variation (upward or downward) in Government levies / taxes / etc. up-to the date of providing services , the benefit or burden of the same shall be passed on or adjusted to the Bank. If the service provider makes any conditional or vague offers, without conforming to these guidelines, the Bank will treat the prices quoted as in conformity with these guidelines and proceed accordingly.
3. Goods and Services Taxes (GST) and its Compliance:-
 - i. Goods and Services Tax Law in India is a Comprehensive, multi-stage, destination-based tax that will be levied on every value addition. Bidder shall have to follow GST

Law as per time being enforced along with certain mandatory feature mentioned hereunder

- ii. TDS (Tax Deducted on Source) is required to deduct as per applicable under GST Law on the payment made or credited to the supplier of taxable goods and services. It would enhance the tax base and would be compliance and self-maintaining tax law based on processes. The statutory compliances contained in the statutes include obtaining registration under the GST law by the existing assesses as well as new assesses, periodic payments of taxes and furnishing various statement return by all the registered taxable person.
 - iii. It is mandatory to pass on the benefit due to reduction in rate of tax or from input tax credit (ITR) to the Bank by way of commensurate reduction in the prices under the GST Law.
 - iv. If bidder as the case may be, is backlisted in the GST (Goods and Services Tax) portal or rating of a supplier falls below a mandatory level, as decided time to time may be relevant ground of cancellation of Contract.
4. Bank shall deduct tax at source, if any, as per the applicable law of the land time being enforced. The Service provider shall pay any other taxes separately or along with GST if any attributed by the Government Authorities including Municipal and Local bodies or any other authority authorized in this regard.

23. ORDER CANCELLATION

Bank reserves its right to cancel the order in the event of one or more of the following situations:

1. Delay in delivery beyond the specified period for delivery.
2. Serious discrepancy in hardware/software noticed during Installation or during maintenance period
3. Any other lapse pertaining to the order.
4. Penalty beyond 10% of the Total Project cost. In addition to the cancellation of purchase order, Bank reserves the right to appropriate the damages by foreclosing the performance bank guarantee.

24. INDEMNITY

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

- i. Bank's authorized / bonafide use of the Deliverables and/or the Services provided by Bidder under this RFP or any or all terms and conditions stipulated in the SLA (Service level Agreement) or PO and/or



- ii. Relating to or resulting directly from infringement of any third party patent, trademarks, copyrights etc. or such other statutory infringements in respect of all components provided to fulfil the scope of this project.
- iii. An act or omission of the Bidder, employees, agents, sub-contractors in the performance of the obligations of the Bidder under this RFP or, any or all terms and conditions stipulated in the SLA(Service level Agreement) or Purchase Order(PO) and/or
- iv. Claims made by employees or subcontractors or subcontractors' employees, who are deployed by the Bidder, against the Bank and/or
- v. Breach of any of the term of this RFP or breach of any representation or false representation or inaccurate statement or assurance or covenant or warranty of the Bidder under this RFP or; any or all terms and conditions stipulated in the SLA (Service level Agreement) or PO 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 Bidder contained in this RFP or; any or all terms and conditions stipulated in the SLA (Service level Agreement) or PO and/or
- viii. Negligence or gross misconduct attributable to the Bidder or its employees, agent or sub-contractors.

The Bidder shall further indemnify the Bank against any loss or damage arising out of claims of infringement of third-party copyright, patents, or other intellectual property issued or registered in India, provided however,

- (i) The Bank notifies the Bidder in writing immediately on aware of such claim,
- (ii) The Bidder has sole control of defense and all related settlement negotiations,
- (iii) The Bank provides the Bidder with the assistance, information and authority reasonably necessary to perform the above, and
- (iv) The Bank does not make any statement or comments or representations about the claim without prior written consent of the Bidder, except under due process of law or order of the court. It is clarified that the Bidder shall in no event enter into a settlement, compromise or make any statement (including failure to take appropriate steps) that may be detrimental to the Bank's (and/or its customers, users and Bidders) rights, interest and reputation.

The Bidder shall compensate the Bank for direct financial loss suffered by the Bank, if the Bidder fails to fix bugs, provide the Modifications / Enhancements / Customization as required by the Bank as per the terms and conditions of this RFP and to meet the Service Levels as per satisfaction of the Bank.

Additionally, the Bidder shall indemnify, protect and save the Bank against all claims, losses, costs, damages, expenses, action, suits and other proceedings, suffered by bank due to the following reasons:



- i. that the Deliverables and Services delivered or provided under this Agreement infringe a patent, utility model, industrial design, copyright, trade secret, mask work or trademark in any country where the Deliverables and Services are used, sold or received; and/or The Bidder shall indemnify the Bank in case of any mismatch of ITC (Input Tax Credit) in the GSTR 2A, where the Bank does not opt for retention of GST component on supplies.
- ii. all claims, losses, costs, damages, expenses, action, suits and other proceedings resulting from infringement of any patent, trade-marks, copyrights etc. or such other statutory infringements under any laws including the Copyright Act, 1957 or Information Technology Act, 2000 or any Law, rules, regulation, bylaws, notification time being enforced in respect of all the Hardware, Software and network equipment or other systems supplied by them to the Bank from whatsoever source, provided the Bank notifies the Bidder in writing as soon as practicable when the Bank becomes aware of the claim however:
 - a. The Bidder has sole control of the defense and all related settlement negotiations.
 - b. The Bank provides the Bidder with the assistance, information and authority reasonably necessary to perform the above and bidder is aware of the rights to make any statements or comments or representations about the claim by Bank or any regulatory authority. Indemnity would be limited to court or arbitration awarded damages and shall exclude indirect and incidental damages and compensations.

Bidder shall have no obligations with respect to any Infringement Claims to the extent that the Infringement Claim arises or results from:

- (i) Bidder's compliance with Bank's specific technical designs or instructions (except where Bidder knew or should have known that such compliance was likely to result in an Infringement Claim and Bidder did not inform Bank of the same);
- (ii) Inclusion in a Deliverable of any content or other materials provided by Bank and the infringement relates to or arises from such Bank materials or provided material;
- (iii) Modification of a Deliverable after delivery by Bidder to Bank if such modification was not made by or on behalf of the Bidder;
- (iv) operation or use of some or all of the Deliverable in combination with products, information, specification, instructions, data, materials not provided by Bidder; or (v) use of the Deliverables for any purposes for which the same have not been designed or developed or other than in accordance with any applicable specifications or documentation provided under the applicable Statement of Work by the Bidder; or
- (v) Use of a superseded release of some or all of the Deliverables or Bank's failure to use any modification of the Deliverable furnished under this Agreement including, but not limited to, corrections, fixes, or enhancements made available by the Bidder.

In the event that Bank is enjoined or otherwise prohibited, or is reasonably likely to be enjoined or otherwise prohibited, from using any Deliverable as a result of or in connection with any claim for which Bidder is required to indemnify Bank under this section according to a final decision of the courts or in the view of Bidder, Bidder, may at its own expense and option:

- (i) Procure for Bank the right to continue using such Deliverable;
- (ii) Modify the Deliverable so that it becomes non-infringing without materially altering its capacity or performance;
- (iii) replace the Deliverable with work product that is equal in capacity and performance but is non-infringing; or (iv) If such measures do not achieve the desired result and if the infringement is established by a final decision of the courts or a judicial or extrajudicial settlement, the Bidder shall refund the Bank the fees effectively paid for that Deliverable by the Bank subject to depreciation for the period of Use, on a straight line depreciation over a 5 year period basis. The foregoing provides for the entire liability of the Bidder and the exclusive remedy of the Bank in matters related to infringement of third party intellectual property rights.

The Bank warrants that all software, information, data, materials and other assistance provided by it under this Agreement shall not infringe any intellectual property rights of third parties, and agrees that it shall at all times indemnify and hold Bidder harmless from any loss, claim, damages, costs, expenses, including Attorney's fees, which may be incurred as a result of any action or claim that may be made or initiated against it by any third parties alleging infringement of their rights.

25. CONFIDENTIALITY & NON-DISCLOSURE

The bidder is bound by this agreement for not disclosing the Banks data and other information. Resources working in the premises of the Bank are liable to follow the rules and regulations of the Bank.

The document contains information confidential and proprietary to the Bank. Additionally, the bidder will be exposed by virtue of the contracted activities to the internal business and operational information of the Bank, affiliates, and/or business partners, disclosure of receipt of this tender or any part of the aforementioned information to parties not directly involved in providing the requested services could result in the disqualification of the bidders, premature termination of the contract, or legal action against the bidder for breach of trust.

No news release, public announcement or any other reference to the order, relating to the contracted work if allotted with the assignment or any program hereunder shall be made without written consent from the Bank.

As the bidder providing support services for multiple Banks, the bidder at all times should take care to build strong safeguards so that there is no mixing together of information/ documents, records and assets is happening by any chance.

The bidder should undertake to maintain confidentiality of the Banks information even after the termination / expiry of the contracts. The successful bidder shall keep all confidential information of the Bank secure and will not disclose or use it for any purpose other than fulfilling this agreement, both during and after the term, as outlines in the Non-disclosure Agreement.

The Non-Disclosure Agreement (NDA) should be entered in to between the Bank and the successful bidder within a period of 21 days from, the date of acceptance of purchase order.

Guarantee on Software License

The bidder shall guarantee that the software supplied under this contract to the Bank is licensed and legally obtained. Software supplied should not have any embedded malicious and virus programs.

26. FORCE MAJEURE

The parties shall not be liable for default or non-performance of the obligations under the contract, if such default or non-performance of the obligations under this contract is caused by any reason or circumstances or occurrences beyond the control of the parties, as a result of force majeure. For the purpose of this clause, “Force Majeure” shall mean an event beyond the control of the parties, including but not limited to, due to or as a result of or caused by acts of God, wars, epidemic/pandemic, insurrections, riots, earth quake and fire, 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, each party shall notify the other party in writing of such circumstances and the cause thereof immediately within seven business days. Unless otherwise directed by the other party, the party pleading Force Majeure shall continue to perform/render/dischage other obligations as far as they can reasonably be attended/fulfilled and shall seek all reasonable alternative means for performance affected by the Event of Force Majeure.

In such a case, the time for performance shall be extended by a period(s) not less than the duration of such delay. If the duration of delay continues beyond a period of three months due to force majeure situation, the parties shall hold consultations with each other in an endeavour to find a solution to the problem. However bidder shall be entitled to receive payments for all services actually rendered upto the date of termination of date of agreement. The financial constraints by way of increased cost to perform the obligations shall not be treated as a force majeure situation if the obligations can otherwise be performed.

27. RESOLUTION OF DISPUTES

The Bank and the bidder shall make every effort to resolve amicably, by direct informal negotiation, any disagreement or dispute arising between them under or in connection with the contract. If after thirty days from the commencement of such informal negotiations, the Bank

and the Bidder have been unable to resolve amicably a contract dispute, either party may require that the dispute be referred for resolution by formal arbitration.

All questions, disputes or differences arising under and out of, or in connection with the contract shall be referred to a sole arbitrator to be appointed mutually by the parties and in case of failure to appoint a sole arbitrator within 15 days from the raising of dispute the same shall be referred to the Arbitration Tribunal: one Arbitrator to be nominated by the Bank and the other to be nominated by the Bidder and the Presiding Arbitrator shall be appointed by the two Arbitrators appointed by the parties.

The decision of the Arbitration Tribunal shall be final and binding on the parties. The Arbitration and Reconciliation Act 1996 shall apply to the arbitration proceedings and the venue of the arbitration shall be Mumbai. The Language of Arbitration will be English. Notwithstanding the existence of a dispute, and/or the commencement of arbitration proceedings, bidder will continue to perform its contractual obligations and the Bank will continue to pay for all products and services that are accepted by it, provided that all products and services are serving as per the agreed scope between the parties.

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) on the date of acknowledgment signed by the receiver or (iii) the business date of receipt, if sent by courier.

This RFP shall be governed and construed in accordance with the laws of India. The courts of Mumbai alone and no other courts shall be entitled to entertain and try any dispute or matter relating to or arising out of this RFP.

28. INDEPENDENT CONTRACTOR

Nothing herein contained will be construed to imply a joint venture, partnership, principal agent relationship or co-employment or joint employment between the Bank and Bidder. Bidder, in furnishing services to the Bank hereunder, is acting only as an independent contractor. Bidder does not undertake by this Agreement or otherwise to perform any obligation of the Bank, whether regulatory or contractual, or to assume any responsibility for the Bank's business or operations. The parties agree that, to the fullest extent permitted by applicable law; Bidder has not, and is not, assuming any duty or obligation that the Bank may owe to its customers or any other person. The bidder shall follow all the rules, regulations statutes and local laws and shall not commit breach of any such applicable laws, regulations etc. In respect of sub-contracts, as applicable – If required by the Bidders, should provide complete details of any subcontractor/s used for the purpose of this engagement. It is clarified that notwithstanding the use of sub-contractors by the Bidder, the Bidder shall be solely responsible for performance of all obligations under the SLA/NDA (Non-Disclosure Agreement) irrespective of the failure or

inability of the subcontractor chosen by the Bidder to perform its obligations. The Bidder shall also have the responsibility for payment of all dues and contributions, as applicable, towards statutory benefits including labour laws for its employees and sub-contractors or as the case may be. The bidder should ensure that the due diligence and verification of antecedents of employees/personnel deployed by him for this project are completed and is available for scrutiny by the Bank.

29. ASSIGNMENT

Bank may assign the Project and the solution and services provided therein by Bidder in whole or as part of a corporate reorganization, consolidation, merger, or sale of substantially all of its assets. The Bank shall have the right to assign such portion of the facilities management services to any of the Contractor/sub-contractor, at its sole option, upon the occurrence of the following: (i) Bidder refuses to perform; (ii) Bidder is unable to perform; (iii) termination of the contract with Bidder for any reason whatsoever; (iv) expiry of the contract. Such right shall be without prejudice to the rights and remedies, which the Bank may have against Bidder. Bidder shall ensure that the said sub-contractors shall agree to provide such services to the Bank at no less favourable terms than that provided by Bidder and shall include appropriate wordings to this effect in the agreement entered into by Bidder with such sub-contractors. The assignment envisaged in this scenario is only in certain extreme events such as refusal or inability of Bidder to perform or termination/expiry of the contract/project.

30. EXECUTION OF CONTRACT, SLA & NDA

The bidder and Bank should execute

1. Contract, which would include all the services and terms and conditions of the services to be extended as detailed herein and as may be prescribed by the Bank and
2. Non-disclosure Agreement.
3. The bidder should execute the contract, SLA and NDA within 21 days from the date of acceptance of the Purchase Order.
4. The term of the contract shall be for a period of 5 years from the date of Go live.
5. In case of any discrepancy among RFP, Purchase Order and SLA, the RFP clauses shall prevail.

31. SUCCESSFUL BIDDER'S LIABILITY

The successful bidder's aggregate liability in connection with obligations undertaken as a part of the project regardless of the form or nature of the action giving rise to such liability (whether in contract, tort or otherwise), shall be at actuals and limited to the value of the contract. The successful bidder's liability in case of claims against the Bank resulting from misconduct or gross negligence of the successful bidder, its employees and subcontractors or from infringement of patents, trademarks, copyrights(if any) or breach of confidentiality obligations shall be unlimited. In no event shall the Bank be liable for any indirect, incidental or consequential damages or liability, under or in connection with or arising out of this tender and

subsequent agreement or services provided. The successful bidder should ensure that the due diligence and verification of antecedents of employees/personnel deployed by him for execution of this contract are completed and is available for scrutiny by the Bank.

32. INFORMATION OWNERSHIP

All information transmitted by successful Bidder belongs to the Bank. The Bidder does not acquire implicit access rights to the information or rights to redistribute the information unless and until written approval sought in this regard. The Bidder understands that civil, criminal, or administrative penalties may apply for failure to protect information appropriately, which is proved to have caused due to reasons solely attributable to bidder. Any information considered sensitive by the bank must be protected by the successful Bidder from unauthorized disclosure, modification or access. The bank's decision will be final if any unauthorized disclosure have encountered. Types of sensitive information that will be found on Bank system's which the Bidder plans to 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. The successful Bidder shall not publish or disclose in any manner, without the Bank's prior written consent, the details of any security safeguards designed, developed, or implemented by the Bidder or existing at any of the Bank location. The Bidder will have to 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 Bank's prior written consent, the details of any security safeguards designed, developed, or implemented by the Bidder or existing at any Bank location.

33. INSPECTION, AUDIT, REVIEW, MONITORING & VISITATIONS

All OEM/Bidder records with respect to any matters / issues covered under the scope of this RFP/project shall be made available to the Bank at any time during normal business hours, to audit, examine, and make excerpts or transcripts of all relevant data. Such records are subject to examination. The cost of such audit will be borne by the Bank. Bidder shall permit audit by internal/external auditors of the Bank or RBI to assess the adequacy of risk management practices adopted in overseeing and managing the outsourced activity/arrangement made by the Bank. Bank shall undertake a periodic review of service provider/BIDDER outsourced process to identify new outsourcing risks as they arise. The BIDDER shall be subject to risk management and security and privacy policies that meet the Bank's standard. In case the BIDDER outsourced to third party, there must be proper Agreement / purchase order with concerned third party. The Bank shall have right to intervene with appropriate measure to meet the Bank's legal and regulatory obligations. Access to books and records/Audit and Inspection would include:-

- a. Ensure that the Bank has the ability to access all books, records and information relevant to the outsourced activity available with the bidder. For technology outsourcing, requisite audit trails and logs for administrative activities should be retained and accessible to the Bank based on approved request.

- b. Provide the Bank with right to conduct audits on the bidder whether by its internal or external auditors, or by external specialist appointed to act on its behalf and to obtain copies of any audit or review reports and finding made on the service provider in conjunction with the services performed for the bank.
- c. Include clause to allow the reserve bank of India or persons authorized by it to access the bank's documents: records of transactions, and other necessary information given to you, stored or processed by the bidder within a reasonable time. This includes information maintained in paper and electronic formats.
- d. Recognized the right of the reserve bank to cause an inspection to be made of a service provider of the bank and its books and account by one or more of its officers or employees or other persons. Banks shall at least on an annual basis, review the financial and operational condition of the bidder. Bank shall also periodically commission independent audit and expert assessment on the security and controlled environment of the bidder. Such assessment and reports on the bidder may be performed and prepared by Bank's internal or external auditors, or by agents appointed by the Bank.
- e. Any such audit shall be conducted expeditiously, efficiently, and at reasonable business hours after giving due notice to the Bidder which shall not be less than 10 days. The Bank shall not have access to the proprietary data of, or relating to, any other customer of Bidder, or a third party or Bidder's cost, profit, discount and pricing data. The audit shall not be permitted if it interferes with Bidder's ability to perform the services in accordance with the service levels, unless the Bank relieves Bidder from meeting the applicable service levels. The audit shall not be performed by any competitor of the Bidder. The auditor including regulatory auditor shall sign the confidentiality undertaking with the Bidder before conducting such audit.

Monitoring

Compliance with Information security best practices may be monitored by periodic Information security audits performed by or on behalf of the Bank and by the RBI. The periodicity of these audits will be decided at the discretion of the Bank. These audits may include, but are not limited to, a review of: access and authorization procedures, physical security controls, backup and recovery procedures, network security controls and program change controls. To the extent that the Bank 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 Service Provider shall afford the Bank's representatives access to the Bidder's facilities, installations, technical resources, operations, documentation, records, databases and personnel. The Bidder must provide the Bank access to various monitoring and performance measurement systems (both manual and automated). The Bank has the right to get the monitoring and performance measurement systems (both manual and automated) audited by prior notice to the Bidder.

Visitations

The Bank shall be entitled to, either by itself or its authorized representative, visit any of the Bidder's premises by prior notice to ensure that data provided by the Bank is not misused.

The Bidder shall cooperate with the authorized representative(s) of the Bank and shall provide all information/ documents\required by the Bank.

34. INFORMATION SECURITY

System should have standard input, communication, processing and output validations and controls. System hardening should be done by bidder. Access controls at DB, OS, and Application levels should be ensured. Bidder should comply with the Information Security Policy of the Bank. The Product offered should comply with regulator's guidelines. The bidder shall disclose security breaches if any to the Bank, without any delay.

35. INTELLECTUAL PROPERTY RIGHTS

The Bidder claims and represents that it has obtained appropriate rights to provide the Deliverables upon the terms and conditions contained in this RFP. The Bank agrees and acknowledges that same as expressly provided in this RFP, all Intellectual Property Rights in relation to the Hardware, Software and Documentation and any adaptations, translations and derivative works thereof whether protectable as a copyright, trade mark, patent, trade secret design or otherwise, provided by the Bidder during, in connection with or in relation to fulfilling its obligations under this RFP belong to and shall remain a property of the Bidder or its licensor. During the Term of this Project and, if applicable, during the Reverse Transition Period, Bank grants Bidder a right to use at no cost or charge the Hardware and Software licensed to the Bank, solely for the purpose of providing the Services. The Bidder shall be responsible for obtaining all necessary authorizations and consents from third party licensors of Hardware and Software used by Bidder in performing its obligations under this Project. If a third party's claim endangers or disrupts the Bank's use of the Hardware and Software, the Bidder shall at no further expense, charge, fees or costs to the Bank, (i) obtain a license so that the Bank may continue use of the Software in accordance with the terms of this tender and subsequent Agreement and the license agreement; or (ii) modify the Software without affecting the functionality of the Software in any manner so as to avoid the infringement; or (iii) replace the Software with a compatible, functionally equivalent and non-infringing product. All third party Hardware/software / service/s provided by the bidder in the scope of the RFP will be the responsibility of the bidder if any discrepancy or infringement is encountered. The Bank shall not be held liable for and is absolved of any responsibility or claim/Litigation or penal liability arising out of the use of any third party software or modules supplied by the Bidder as part of this Project.

Bidder's Proprietary Software and Pre-Existing IP:- Bank acknowledges and agrees that this is a professional services agreement and this agreement is not intended to be used for licensing of any Bidder's proprietary software or tools. If Bidder and Bank mutually agree that the Bidder provides to Bank any proprietary software or tools of Bidder or of a third party, the parties shall negotiate and set forth the applicable terms and conditions in a separate license agreement and the provisions of this Clause shall not apply to any deliverables related to customization or implementation of any such proprietary software or products of Bidder or of



a third party. Further, Bank acknowledges that in performing Services under this Agreement Bidder may use Bidder's proprietary materials including without limitation any software (or any part or component thereof), tools, methodology, processes, ideas, know-how and technology that are or were developed or owned by Bidder prior to or independent of the Services performed hereunder or any improvements, enhancements, modifications or customization made thereto as part of or in the course of performing the Services hereunder, ("Bidder Pre-Existing IP"). Notwithstanding anything to the contrary contained in this Agreement, Bidder shall continue to retain all the ownership, the rights title and interests to all Bidder Pre-Existing IP and nothing contained herein shall be construed as preventing or restricting Bidder from using Bidder Pre-Existing IP in any manner. To the extent that any Bidder Pre-Existing IP or a portion thereof is incorporated or contained in a deliverable under this Agreement, Bidder hereby grants to Bank a non-exclusive, perpetual, royalty free, fully paid up, irrevocable license, with the right to sublicense through multiple tiers, to use, copy, install, perform, display, modify and create derivative works of any such Bidder Pre-Existing IP in connection with the deliverables and only as part of the Deliverables in which they are incorporated or embedded. The foregoing license does not authorize Bank to (a) separate Bidder Pre-Existing IP from the deliverable in which they are incorporated for creating a stand-alone product for marketing to others; (b) independently sell, lease, exchange, mortgage, pledge, license, sub license, assign or in any other way convey, transfer or alienate the Bidder Pre-Existing IP in favour of any person (either for commercial consideration or not (including by way of transmission), and/or (c) except as specifically and to the extent permitted by the Bidder in the relevant Statement of Work, reverse compile or in any other way arrive at or attempt to arrive at the source code of the Bidder Pre-Existing IP.

Residuary Rights. Each Party shall be entitled to use in the normal course of its business and in providing same or similar services or development of similar deliverables for its other clients, the general knowledge and experience gained and retained in the unaided human memory of its personnel in the performance of this Agreement and Statement of Work(s) hereunder. For the purposes of clarity the Bidder shall be free to provide any services or design any deliverable(s) that perform functions same or similar to the deliverables being provided hereunder for the Client, for any other customer of the Bidder (including without limitation any affiliate, competitor or potential competitor of the Bank. Nothing contained in this Clause shall relieve either party of its confidentiality obligations with respect to the proprietary and confidential information or material of the other party

36. TERMINATION

Termination for Default

The Bank, without prejudice to any other remedy for breach of contract, by 30 (Thirty) days written notice of default sent to the Successful Bidder, may terminate this Contract in whole or in part:

a. if the Successful Bidder fails to deliver any or all of the deliverables / milestones within the period(s) specified in the Contract, or within any extension thereof granted by the Bank



provided the failure is for the reasons which are solely and entirely attributable to the Bidder and not due to reasons attributable to Bank and/or its other vendors or due to reasons of Force Majeure; or;

b. If the Successful Bidder fails to perform any other material obligation(s) under the contract provided the failure is for the reasons which are solely and entirely attributable to the Bidder and not due to reasons attributable to Bank and/or its other vendors or due to reasons of Force Majeure.

c. If the Successful Bidder, in the judgment of the Bank has engaged in corrupt or fraudulent practices in competing for or in executing the Contract.

Prior to providing a written notice of termination to the Selected Bidder, Bank shall provide the selected bidder with a written notice of 30 days to cure any breach of the Contract. The decision to terminate the contract shall be taken only if the breach continues or remains unrectified, for reasons within the control of Bidder, even after the expiry of the cure period.

In case the contract is terminated then all undisputed payment for the services delivered till the date of termination will be given to vendor, but disputed payment shall be discussed and will be paid once the dispute is resolved.

Termination for Insolvency

If either party becomes bankrupt or insolvent, has a receiving order issued against it, with its creditors, or, a resolution is passed or order is made for its winding up (other than a voluntary liquidation for the purposes of amalgamation or reconstruction), a receiver is appointed over any part of its undertaking or assets, or if either party takes or suffers any other analogous action in consequence of debt; then other party plans to, at any time, terminate the contract by giving written notice of 60 days to the party becoming bankrupt etc. If the contract is terminated by either party in terms of this Clause, Bank shall be liable to make payment of the entire amount due under the contract for which services have been rendered by the Selected Bidder.

Termination- Key Terms & Conditions

Notwithstanding anything contain in this RFP, the Bank shall entitled to terminate the agreement with the service provider without assigning any reason at any time by giving 30 days prior written notice to the successful bidder . Bidder shall have to comply the same.

Either Party shall also be entitled to terminate the agreement at any time by giving notice if the other party.

- i. has a winding up order made against it; or
- ii. has a receiver appointed over all or substantial assets; or
- iii. is or becomes unable to pay its debts as they become due; or
- iv. enters into any arrangement or composition with or for the benefit of its creditors; or
- v. Passes a resolution for its voluntary winding up or dissolution or if it is dissolved.

Exit Option & Contract Re-Negotiation

The Bank reserves the right to cancel the contract in the event of happening one or more of the following Conditions:

- i. Failure of the successful bidder to accept the contract and furnish the Performance Guarantee within 21 days of receipt of purchase contract
- ii. Substantial delay in delivery, performance or implementation of the solution beyond the specified period.
- iii. Serious discrepancy in functionality to be provided or the performance levels agreed upon, which have an impact on the functioning of The Bank. Inability of the Bidder to remedy the situation within 60 days from the date of pointing out the defects by The Bank. (60 days will be construed as the notice period)

In addition to the cancellation of purchase contract, Bank reserves the right to appropriate the damages through encashment of Bid Security / Performance Guarantee given by the Bidder.

Notwithstanding the existence of a dispute, and/or the commencement of arbitration proceedings, the Bidder will be expected to continue to provide services to the Bank as per the contract. Bank will continue to pay for all products and services that are accepted by it provided that all products and services as serving as per the agreed scope between the parties. The Bank shall have the sole and absolute discretion to decide whether proper reverse transition mechanism over a period of 6 to 12 months, has been complied with. In the event of the conflict not being resolved, the conflict will be resolved through Arbitration. The Bank and the Bidder shall together prepare the Reverse Transition Plan. However, The Bank shall have the sole decision to ascertain whether such Plan has been complied with. Reverse Transition mechanism would typically include service and tasks that are required to be performed / rendered by the Bidder to The Bank or its designee to ensure smooth handover and transitioning of Bank's deliverables, maintenance and services.

Notwithstanding anything contained in this RFP, Bank reserve the right to cancel the contract by giving 90 days notice period without assigning any reason as per its convenience.

37. PRIVACY & SECURITY SAFEGUARDS

- i. The Bidder shall not publish or disclose in any manner, without the Bank's prior written consent, the details of any security safeguards designed, developed, or implemented by the Bidder or existing at any Bank location. The Bidder will have to 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 Bank data and sensitive application software. The Bidder will have to also ensure that all subcontractors who are involved in providing such security safeguards or part of it shall not publish or disclose in any manner, without the Bank's prior written consent, the details of any security safeguards designed, developed, or implemented by the Bidder or existing at any Bank location.
- ii. The Bidder hereby agrees and confirms that they will disclose, forthwith, instances of security breaches.

iii. The Bidder hereby agrees that they will preserve the documents.

38. GOVERNING LAW AND JURISDICTION

The provisions of this RFP and subsequent Agreement shall be governed by the laws of India. The disputes, if any, arising out of this RFP/Agreement shall be submitted to the jurisdiction of the courts/tribunals in Mumbai.

Statutory and Regulatory Requirements

The solution must comply with all applicable requirements defined by any regulatory, statutory or legal body which shall include but not be limited to RBI or other Regulatory Authority, judicial courts in India and as of the date of execution of Agreement. This requirement shall supersede the responses provided by the Bidder in the technical response. During the period of warranty / AMC, Bidder / Bidder should comply with all requirements including any or all reports without any additional cost, defined by any regulatory authority time to time and which fall under the scope of this RFP / Agreement. All mandatory requirements by regulatory / statutory bodies will be provided by the bidder under change management at no extra cost to the bank during the tenure of the contract.

39. COMPLIANCE WITH LAWS

1. Compliance with all applicable laws: Successful bidder shall undertake to observe, adhere to, abide by, comply with the Bank 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 scope of work.
2. Compliance in obtaining approvals/permissions/licenses: 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.
3. The Annual Technical Support under the RFP should comply with all the Regulatory/ Compliance guideline of the Banks/ Regulatory authority in India. Bank has right to change the compliance/ guideline at any point of time and the service provider has to comply with the guidelines. Bank has right to audit by regulatory authority or any agency appointed by the Bank, as a part of Vendor Audit. The service should comply with Bank IT/ Information Security (IS) / BCP Policy. It will be mandatory to protect the data privacy, as per Indian Data Privacy Law. Service provider should comply with all such laws in existence currently or introduced in future by the Govt. agencies or any other regulatory body.

40. VIOLATION OF TERMS

The Bank clarifies that the bank 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 bidder from committing any

violation or enforce the performance of the covenants, obligations and representations contained under the RFP/Agreement. These injunctive remedies are cumulative and are in addition to any other rights and remedies the bank 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-

41. CORRUPT & FRAUDULENT PRACTICES

As per Central Vigilance Commission (CVC) directives, it is required that Bidders / Suppliers / Contractors observe the highest standard of ethics during the procurement and execution of such contracts in pursuance of this policy:

“Corrupt Practice” means the offering, giving, receiving or soliciting of anything of values to influence the action of an official in the procurement process or in contract execution AND

“Fraudulent Practice” means a misrepresentation of facts in order to influence a procurement process or the execution of contract to the detriment of The Bank and includes collusive practice among Bidders (prior to or after offer submission) designed to establish offer prices at artificial non-competitive levels and to deprive The Bank of the benefits of free and open competition.

The Bank 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. The Bank reserves the right to declare a firm 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.

42. PUBLICITY

Any publicity by either party in which the name of the other party is to be used should be done only with the explicit written permission of such other party.

43. APPLICABILITY OF PREFERENCE TO MAKE IN INDIA, ORDER 2017 (PPP-MII ORDER)

Government guidelines on Public Procurement (Preference to Make in India), Order 2017 (PPP-MII Order) and subsequent revision vide Order No. 45021/2/2017-PP(BE-II) dated 16.09.2020 and any revision thereto will be applicable for this RFP.

44. COMPLIANCE TO RBI MASTER DIRECTION ON OUTSOURCING OF IT SERVICES (RBI CIRCULAR DATED APRIL 2023)

a). Regular Monitoring And Assessment Of The Service Provider By Bank

The Bank shall have the right to conduct regular monitoring and assessment including periodic audits, reviews, and security checks of Successful bidder 's performance, security practices,

and compliance with the terms of this agreement. The Successful bidder shall cooperate with the Bank during these assessments and take corrective actions as required.

Type of material adverse events and the incidents required to be reported to Bank by the service provider

- i. The Successful bidder shall promptly report any material adverse events, including (but not limited to)
 - a. Data breaches
 - b. Denial of service attacks
 - c. Service unavailability
 - d. Security vulnerabilities
 - e. Unauthorized access
 - f. System failures
 - g. Any other incidents that may impact Bank's operations or data integrity.
- ii. Such incidents shall be reported to the Bank immediately upon identification, enabling the Bank to take prompt risk mitigation measures and ensure compliance with statutory and regulatory guidelines.
- iii. The Successful bidder shall provide all relevant details and updates regarding the incident, including the nature, scope, impact, and corrective actions taken, in accordance with the Bank's incident reporting procedures.

b). Storage of data only in India as per extant regulatory requirements

The Prospective Successful bidder (Service Provider) shall ensure that Bank's data processed or handled under this agreement is stored exclusively within India, in compliance with the extant regulatory requirements.

c). Service provider to provide details of data (related to Bank and its customers) captured, processed and stored

The Successful bidder shall provide the Bank with details of all data related to the Bank and its customers that it captures, processes, and stores, upon receiving an approved request.

d). Controls for maintaining confidentiality of data of Bank and its customers', and incorporating service provider's liability to Bank in the event of security breach and leakage of such information

With related to confidentiality of data,

- a) The Successful bidder shall treat all data of the Bank and its customers as confidential and shall not disclose or allow access to such data to any unauthorized third party without the prior written consent of the Bank.
- b) The Successful bidder shall implement all necessary measures to protect the confidentiality and integrity of the data throughout the term of this Agreement and thereafter.
- c) The Successful bidder shall implement and maintain industry-standards controls to safeguard Bank related data.

e). Types of data/information that the service provider (successful bidder) is permitted to share with Bank's customer and/or any other party



The Successful bidder shall define and ensure the types of data/information that is shared with the Bank's customers and/or any other parties:

- i. Is shared with explicit written consent or authorization from the Bank.
- ii. Is required by law or regulation, including legal processes such as subpoenas.
- iii. Is shared with approved third-party successful bidder or sub-processors.

f). Contingency plan(s) to ensure business continuity and testing requirements

- i. The Successful bidder shall have a documented Business Continuity Plan in place, which outlines the strategies for maintaining service availability in the event of an unexpected incident. The Business Continuity Plan should include, but not limited to:
 - a. Detailed procedures for mitigating and recovering from various business disruptions.
 - b. Identification of key personnel, roles, and responsibilities in a crisis.
 - c. Communication plans to inform both Successful bidder and Bank, of significant disruptions and progress towards recovery.
- ii. The Successful bidder shall maintain a Disaster Recovery Plan to restore critical services and infrastructure in the event of a disaster, including:
 - a. Specific recovery objectives, such as Recovery Time Objective (RTO) and Recovery Point Objective (RPO), to be met for each service.
 - b. Procedures for data backup, storage, and retrieval.
 - c. Clear steps to restore services to full functionality, including resource allocation and escalation procedures.

g). Right to seek information from the service provider about the third parties (in the supply chain) engaged by the former

The Bank reserves the right to seek information from the Successful bidder about its third parties or sub-contractors engaged in the supply chain or any sub-contracted work.

h). Making the service provider contractually liable for the performance and risk management practices of its sub-contractors

The Successful bidder shall be contractually liable for the performance and risk management practices of its sub-contractors. The Successful bidder will remain fully responsible for ensuring that its sub-contractors adhere to the same performance standards, security protocols, and risk management practices as outlined in the agreement with the Bank. The Successful bidder should be obligated to manage and mitigate any risks arising from its sub-contractors' actions or failures, and to promptly address any issues related to sub-contractor performance that could impact the quality of service or compliance with the agreement.

i). Need of prior approval/consent of the Bank for use of sub-contractors by the service provider for all or part of an outsourced activity

The Successful bidder shall obtain the Bank's prior written consent before sub-contracting or outsourcing all or part of activities covered under this agreement.

j). Termination rights of the Bank, including the ability to orderly transfer the proposed IT-outsourcing arrangement to another service provider, if necessary or desirable

In the event of termination, the Bank shall have the right to transition of the IT outsourcing arrangement to another sub-successful bidder, either in whole or in part, at its discretion. The

Successful bidder agrees to fully cooperate with the Bank to ensure an orderly and seamless transfer of services, including the transfer of data, systems, and knowledge, and to provide necessary support to the new Service Provider. The Successful bidder shall also assist in mitigating any risks associated with the transition and shall ensure that all customer data and confidential information is securely handled during the transition process.

k). Obligation of the service provider to co-operate with the relevant authorities in case of insolvency/resolution of the Bank

If the Bank becomes subject to insolvency proceedings, financial restructuring, or resolution by relevant authorities (e.g., governmental bodies, regulatory agencies, or liquidators), the Successful bidder shall co-operate fully with the relevant authorities in accordance with applicable laws and regulations.

l). Provision to consider skilled resources of service provider who will provide core services as “essential personnel” so that a limited number of staff with back-up arrangements necessary to operate critical functions can work on-site during exigencies (including pandemic situations)

- a. The Successful bidder shall designate and maintain a pool of skilled resources who will be considered "essential personnel" for the delivery of core services under this agreement.
- b. These personnel will be responsible for ensuring the continuity of critical functions, particularly during exigent circumstances such as emergencies, natural disasters, or pandemics.
- c. In the event of such situations, the Successful bidder shall implement necessary backup arrangements to ensure that a limited but enough essential personnel are available to work on-site to support critical operations.
- d. The Successful bidder shall make reasonable efforts to ensure the safety and well-being of these personnel while maintaining the uninterrupted delivery of critical services.
- e. The Successful bidder shall notify the Bank promptly of any significant changes to the availability or capacity of essential personnel, as well as any potential impact on service delivery.

m). Suitable back-to-back arrangements between service providers and the OEMs

The Successful bidder shall ensure that suitable back-to-back arrangements are in place with Original Equipment Manufacturers (OEMs) to guarantee the provision of required products, services, and support. These arrangements must align with the terms and service levels defined in this agreement, ensuring that the Successful bidder can meet its obligations to the Bank and address any issues related to the OEM products or services in a timely and efficient manner. The Successful bidder is responsible for ensuring that the OEM's support and performance meet the agreed-upon standards, and for providing any necessary escalations or resolutions in the event of failure by the OEM to meet such standards.

45. SUSTAINABLE SOURCING

The Supplier shall adhere to Sustainable Sourcing practices including but not limited to the use of environment friendly materials, ethical labor practices and compliance with relevant local and international regulations. The Supplier shall provide documentation or certifications

demonstrating their commitment to Sustainable Sourcing upon request. Failure to comply with these requirements may result in contract termination.

46. ENTIRE AGREEMENT; AMENDMENTS

This RFP sets forth the entire agreement between the Bank and the Successful bidder and supersedes any other prior proposals, agreements and representations between them related to its subject matter, whether written or oral. No modifications or amendments to this Agreement shall be binding upon the parties unless made in writing, duly executed by authorized officials of both parties.

47. SURVIVAL AND SEVERABILITY

Any provision or covenant of the RFP, which expressly, or by its nature, imposes obligations on successful bidder shall so survive beyond the expiration, or termination of this Agreement. The invalidity of one or more provisions contained in this Agreement shall not affect the remaining portions of this Agreement or any part thereof; and in the event that one or more provisions shall be declared void or unenforceable by any court of competent jurisdiction, this Agreement shall be construed as if any such provision had not been inserted herein.

Bidding Document

The bidder is expected to examine all instructions, forms, terms and conditions and technical specifications in the Bidding Document. Submission of a bid not responsive to the Bidding Document in every respect will be at the bidder's risk and may result in the rejection of its bid without any further reference to the bidder.

48. AMENDMENTS TO BIDDING DOCUMENTS

The Bank reserves the right to change/modify the dates/terms & conditions without assigning any reasons, mentioned in this RFP document as per its requirement, which will be communicated to the Bidders through Bank's Website. The amendments / clarifications to the tender, if any, will be posted on the Bank website (www.centralbankofindia.co.in) / GEM Portal. It may be noted that notice regarding corrigenda, addendums, amendments, time-extensions, clarifications, response to bidders' queries etc., if any to RFP, will not be published through any advertisement in newspapers or any other media. Prospective bidders shall regularly visit Bank's website for any changes / development in relation to this RFP. The amendments / clarifications to the tender, if any, will be posted on the Bank website.

49. PERIOD OF VALIDITY

Bids shall remain valid for 120 days from the last date of bid submission. A bid valid for shorter period shall be rejected by the bank as non-responsive.

50. OWNERSHIP, GRANT AND DELIVERY

The Bidder shall procure and provide a non-exclusive, non-transferable, perpetual license to the Bank for all the software to be provided as a part of this project.

The Bank reserves the right to use the excess capacity of the hardware, licenses and other infrastructure supplied by the Bidder for any internal use of the Bank or its affiliates, subsidiaries or regional rural Bank at no additional cost other than the prices mentioned in the commercial bid. The Bidder agrees that they do not have any reservations on such use and will not have any claim whatsoever against such use of the hardware, licenses and infrastructure.

Further, the Bidder also agrees that such use will not infringe or violate any license or other requirements as per applicable intellectual property right.

51. LAST DATE AND TIME FOR SUBMISSION OF BIDS

Bids must be submitted not later than the specified date and time as specified in the Bid Document. Bank reserves the right to extend the date & time without mentioning any reason.

52. LATE BIDS

Any bid received after the deadline for submission of bids will be rejected and/or returned unopened to the Bidder, if so desired by him.

53. MODIFICATIONS AND/OR WITHDRAWAL OF BIDS

- a. Bids once submitted will be treated as final and no further correspondence will be entertained on this.
- b. No bid will be modified after the deadline for submission of bids.
- c. No bidder shall be allowed to withdraw the bid, if the bidder happens to be a successful bidder.

Clarification of Bids

To assist in the examination, evaluation and comparison of bids the bank may, at its discretion, ask the bidder for clarification and response, which shall be in writing and without change in the price, shall be sought, offered or permitted.

Bank's Right to Accept or Reject Any Bid or All Bids

The bank reserves the right to accept or reject any bid and annul the bidding process and reject all bids at any time prior to award of contract, without thereby incurring any liability to the affected bidder or bidders or any obligation to inform the affected bidder or bidders of the ground for the bank's action.

54. SIGNING OF CONTRACT

The successful bidder(s) to be called as bidder, shall be required to enter into an Agreement with the Bank, within 21 days of the award of the work order (when provided) or within such extended period as may be specified by the bank.



55. CHECKLIST FOR SUBMISSION

| # | Particulars | Bidders Remark Yes/No |
|----|---|--------------------------|
| 1 | Certificate of incorporation | |
| 2 | GSTN Registration Certificate | |
| 3 | Audited Balance sheets of last three years 2021-22, 2022-23 & | |
| 4 | CA certificate for three years average turnover for financial years 2021-22, 2022-23 & 2023-24. | |
| 5 | CA certificate for operating profit for last three financial years 2021-22, 2022-23 & 2023-24. | |
| 6 | CA certificate for net worth for last three financial years 2021-22, 2022-23 & 2023-24. | |
| 7 | Self-declaration on Company's letter head should not have been Blacklisted /debarred/ by any Govt. / IBA/RBI/PSU /PSE/ or Banks, Financial institutes for any reason or non-implementation/ delivery of the order. Self-declaration to that effect should be submitted along with the technical bid. | |
| 8 | Self-declaration on Company's letter head Bidder/OEM should not have any pending litigation or any dispute in the last five years, before any court of law between the Bidder or OEM and the Bank regarding supply of goods/services. | |
| 9 | Self-declaration by the Authorized Signatory for not have filed for bankruptcy in any country including India on company letter head | |
| 10 | Self-declaration on Company's letter-head for not having <ul style="list-style-type: none"> NPA with any Bank /financial institutions in India Any case pending or otherwise, with any organization across the globe which affects the credibility of the Bidder in the opinion of Central Bank of India to service the needs of the Bank Pending | |
| 11 | Self-declaration by the Authorized Signatory for having support / service center or having support arrangement in Mumbai and Hyderabad | |
| 12 | Reference Letters / Purchase Orders for Eligibility Criteria 11 | |
| 13 | Details of Resources on Company's letter for Eligibility Criteria 12 | |
| 14 | Reference Letters / Purchase Orders for Eligibility Criteria 13 | |
| 15 | Reference Letters / Purchase Orders for Eligibility Criteria 14 | |
| 16 | Document Cost | |
| 17 | Annexure 1: Bill of Material | |
| 18 | Annexure 2: Minimum Technical Specifications | |
| 19 | Annexure 3: Conformity Letter | |
| 20 | Annexure 4: Bidder's Information on company letter head | |



सेंट्रल बैंक ऑफ़ इंडिया
Central Bank of India

1911 से आपके लिए "केन्द्रीय" "CENTRAL" TO YOU SINCE 1911

**RFP for Supply, Implementation & Management of Next-Generation Security Operations Centre (NG-SOC) Solutions
Central Bank of India – Tender No – GEM/2025/B/6180729**

| # | Particulars | Bidders Remark Yes/No |
|----|--|--------------------------|
| 21 | Annexure 5: Letter for Conformity of Product as per RFP Bidder's | |
| 22 | Annexure 6 : Undertaking for acceptance of terms of RFP | |
| 23 | Annexure 7: MAF on OEM's letter head | |
| 24 | Annexure 8: Integrity Pact | |
| 25 | Annexure 9: Non-Disclosure Agreement | |
| 26 | Annexure 10: Performance Bank Guarantee | |
| 27 | Annexure 11: Pro forma for Bid Security (EMD) | |
| 28 | Annexure 12: Bidders Particulars in Company Letter Head | |
| 29 | Annexure 13: NPA UNDERTAKING | |
| 30 | Annexure 14: Undertaking letter (Land Border Sharing) | |
| 31 | Annexure 15: Cover Letter | |
| 32 | Annexure 16: Pre-Bid Query Format | |
| 33 | Annexure 17: Eligibility Criteria Compliance | |
| 34 | Annexure 18: Self declaration for compliance to RBI master direction on outsourcing of it services | |
| 35 | Annexure 19: GOI Guidelines For Preference To Make In India | |
| 36 | Annexure 19A: Certificate of Local Content | |
| 37 | Annexure 20: Guidelines on banning of business dealing | |



56. ANNEXURE 1: BILL OF MATERIAL

Bidder needs to provide the compliance on below Bill of Materials and Also share the details of Hardware & Software proposed with the NG-SOC solutions on Bidder's letter head.

Summary of Bill of Material (Summation of Tables: A to G)

| Commercial Table: Summary Of Cost | | | | |
|-----------------------------------|--------------------------------------|--------------|-----|-----------------------------------|
| S. No. | Item | Total Amount | GST | Total Cost in Rs. (including GST) |
| 1 | Hardware(s) Cost (Table A) | | | |
| 2 | Software(s) Cost (Table B) | | | |
| 3 | Implementation Cost (Table C) | | | |
| 4 | AMC Cost (Table D) | | | |
| 5 | ATS Cost (Table E) | | | |
| 6 | FMS Cost (Table F) | | | |
| 7 | Professional Services Cost (Table G) | | | |
| 8 | Any other Cost | | | |
| Total Cost of Ownership (TCO) | | | | |

Table – A (Infrastructure Hardware Cost)

| Price Schedule For Next Generation Security Operation Center Solution - Hardware Cost With Three Years Warranty | | | | | | |
|---|--|--------------|---------------|-------------------|---------|--------------------------|
| SNO | Item Description | Quantity (Q) | Unit Rate (R) | Total Price T=QxR | GST Amt | Total Cost including GST |
| 1 | SERVERS/APPLIANCE | | | | | |
| 2 | STORAGE | | | | | |
| 3 | SAN SWITCH IF ANY | | | | | |
| 4 | HIGH SPEED BACKUP DEVICE FULL SET | | | | | |
| 5 | 2*2 Video wall with 55" display with hardware based controller of 16 inputs and 4 outputs (4K) | 1 | | | | |
| 6 | Any other item | | | | | |
| Cost of Table - A | | | | | | |

Table – B (Software Cost)

| Price Schedule For Next Generation Security Operation Center Solution - Licenses/Software Cost With Three Years Warranty | |
|--|--|
|--|--|



| SNO | Item Description | Quantity (Q) | Unit Rate (R) | Total Cost T=QxR | GST Amt | Total Cost including GST |
|--------------------------|-------------------------------------|--------------|---------------|---------------------|---------|--------------------------|
| 1 | SIEM License for DC And DR Location | 60000 | | | | |
| 2 | UEBA Licenses | 40000 | | | | |
| 3 | SOAR | 10 Analysts | | | | |
| 4 | Threat Intelligence Feed | | | | | |
| 5 | Operating System | | | | | |
| 6 | Database Software | | | | | |
| 7 | Any Other Item | | | | | |
| Cost of Table – B | | | | | | |

Table – C (Implementation Cost)

| SNO | Item Description | Total Cost | GST Amt | Total Cost including GST |
|--------------------------|---|------------|---------|--------------------------|
| 1 | SIEM Implementation | | | |
| 2 | UEBA Implementation | | | |
| 3 | SOAR Implementation | | | |
| 4 | Threat Intelligence Feed Implementation | | | |
| 5 | Any Other Item | | | |
| Cost of Table – C | | | | |

Table – D (AMC Cost)

| Price Schedule For Next Generation Security Operation Center Solutions – AMC Cost (2 Years) – 4th & 5th Year | | | | | |
|---|------------------|-----------------------|-------------------|---------|--------------------------|
| SNO | Item Description | Per Year AMC Cost (Q) | Total Price T=Qx2 | GST Amt | Total Cost including GST |



| | | | | | |
|--------------------------|--|---|--|--|--|
| 1 | SERVICES/APPLIANCE | | | | |
| 2 | STORAGE | | | | |
| 3 | SAN SWITCH IF ANY | | | | |
| 4 | HIGH SPEED BACKUP DEVICE FULL SET | | | | |
| 5 | 2*2 Video wall with 55" display with hardware based controller of 16 inputs and 4 outputs (4K) | 1 | | | |
| 6 | Any other item | | | | |
| Cost of Table - D | | | | | |

Table – E (ATS Cost)

| Price Schedule For Next Generation Security Operation Center Solution - Licenses/Software ATS Cost (2 Years)- 4th & 5th Year | | | | | |
|---|--------------------------|------------------------------|--------------------------|----------------|---------------------------------|
| SNO | Item Description | Per Year ATS Cost (Q) | Total Price T=Qx2 | GST Amt | Total Cost including GST |
| 1 | SIEM | | | | |
| 2 | UEBA | | | | |
| 3 | SOAR | | | | |
| 4 | Threat Intelligence Feed | | | | |
| 5 | Operating System | | | | |
| 6 | Database Software | | | | |
| 7 | Any Other Item | | | | |
| Cost of Table - E | | | | | |

Table – F (Facility Management Support Cost)

| Price Schedule For Next Generation Security Operation Center Solutions Facility Management Support Cost for 5 Years | | | | | | |
|--|-------------------------|------------------------------------|------------------------------------|----------------------------------|----------------|-----------------------------------|
| SNO | Manpower details | Minimum Number of Resources | Cost Per Resource/ Per Year | Total Cost for Five years | GST Amt | Total Amount including GST |
| | | (A) | (B) | A x B x 5 | | |
| 1 | L3 | 1 | | | | |



| | | | | | | |
|--------------------------|----|----|--|--|--|--|
| 2 | L2 | 6 | | | | |
| 3 | L1 | 11 | | | | |
| Cost of Table - F | | | | | | |

Table – G (Professional Services Cost)

| Price Schedule For Next Generation Security Operation Center Solutions | | | | | | |
|---|--|-----------------|----------------------------------|---------------------------|---------|----------------------------|
| Professional Services Cost for 5 Years | | | | | | |
| SNO | Professional Services details | No. of Man Days | Professional Cost / Per Man Days | Total Cost for Five years | GST Amt | Total Amount including GST |
| | | (A) | (B) | A x B x 5 | | |
| 1 | Professional Services for SIEM, SOAR, UEBA, Threat Intelligence Feed, etc. | 15 | | | | |
| Cost of Table - G | | | | | | |

- The Bidder is expected to quote for all items required for fully complying with the requirements of the RFP.
- The Bank is not responsible for any omission/skip of any component required for complying with the RFP requirement and bidder will have to fulfil the entire requirement without any additional cost to Bank.
- Bank is not responsible for any arithmetic errors in the commercial bid details submitted by the bidder.
- The bidder may insert any additional line item as applicable based on the solution offered by the bidder.

- Bidder must quote as per format of the bill of material only and masked replica of the bill of material should be enclosed in the technical bid without any commercial value.
- All amount in bill of material should be in INR only.
- Any additional number of items (Software, Hardware, FMS etc.) and services to be procured by the Bank in future shall be on pro-rata basis on the rates provided in the bill of material.
- If the bidder has not quoted for any line item mentioned in the bill of material, it will be deemed considered that bidder has factored the cost for the item and no additional charges will be paid by the Bank, other than one mentioned in the bill of material.
- Bidder is required to implement the solution identically both at DC & DRC locations, accordingly bidder has to factor the costs of all the components for DC & DRC locations.
- The bidder shall ensure that AMC rates must be quoted above 5% and ATS rates must be quoted above 10% for the respective product(s).

Signature

Name:

Designation:

Seal of Company

Date:



57. ANNEXURE 2: MINIMUM TECHNICAL SPECIFICATIONS

| 1. Security Information & Event Management(SIEM) | | | |
|---|---|---------------------|-----------------|
| Sl. NO. | Technical & Functional Requirements | Compliance (Yes/No) | Vendor's Remark |
| | Architecture | | |
| 1. | The proposed solution shall be hardware or software based with logically segregated into collections, correlation, and management layer. If the software appliance is proposed, the OEM/bidder shall provide all the required hardware to implement. | | |
| 2. | The solution shall be sized for 60,000 EPS for DC & DR each and sustainable upto 1,00,000 EPS per site during the contract period without dropping or queuing of logs on any proposed SIEM component as per Bank requirement and any additional hardware, software and storage except EPS license. There should not be any limitation on the number of devices like servers, network devices, virtual machines or any other data source(s) that is required to be integrated. | | |
| 3. | The proposed solution shall be capable of dual forwarding/streaming/replicating of any raw logs from DC to DRC and vice versa. Storage must be arranged accordingly. | | |
| | The proposed SIEM Solution should be EPS based at both log management and Correlation layer and must support logs from unlimited devices or sources | | |
| | The proposed SIEM Solution should support security data lake as a single repository for UEBA, SIEM, Threat Hunting etc. Security Data lake is must to ensure search performance in Threat Hunting and analytics. | | |
| 4. | The proposed solution should have the capability to effectively handle burst periods which could be 2 times of regular EPS without dropping logs. It should support burst period for more than 2 hours. | | |
| 5. | SIEM solution should support Disaster Recovery and sized for DR site as well. The solution shall be sized to consider dual forwarding/streaming/replication from DC to DR and vice versa. Bidder shall provide | | |



| | | | |
|-----|--|--|--|
| | necessary load balancer to distribute log ingestion across proposed log collection (in DC and DR) | | |
| 6. | The proposed solution must support the data replication/dual forwarding without relying on other third-party replication technologies on the operating system or storage level. It should also allow admin to decide on replication factor within DC and replication factor for DR. DR should always be active and should be updated with artifacts for any incident analyst is working on. | | |
| 7. | The solution must integrate with 3rd party directory systems as an authentication method. Solution should be integrated with LDAP or Active Directory solution for access provisioning to the SIEM system. | | |
| 8. | SIEM should provide out of box Cloud integrations to retain full visibility into cloud security stack and support hybrid integration (On prem and cloud). If the parser is not available the bidder/ OEM should develop the parsers without any extra cost to bank. | | |
| 9. | SIEM solution should provide MITRE framework mapping and suggest TTPS across rules, alerts, and incidents. | | |
| 10. | The solution must provide an open API mechanism to forward events /incidents /alerts to other platforms such as ITSM, SOAR, and any other SIEM solutions. | | |
| 11. | The solution must use distributed computing to scale data collection and analytics and co-locates analytic processing with collection engines. | | |
| 12. | SIEM solution should have High Availability across all components within the system e.g., log collection, log correlation, management console etc. If it is required to have a LB to achieve the requirement, the bidder should factor the same also must have RAID redundancy (hard drives), Network Redundancy (Mgmt. interfaces), and Power-Supply module redundancy and 4x1G/10G network interfaces per server. (Bidder to explain architecture) | | |
| 13. | High Availability should use cluster set-up so that data could be shared between the nodes. | | |



| | | | |
|-----|--|--|--|
| 14. | The solution collector must support the automatic load balancing and load sharing. | | |
| 15. | The solution must have automated internal health checks and notify Bank in case of problems. | | |
| 16. | The solution should not require additional license to deploy additional nodes/SIEM components i.e., for collection, processing, or HA requirements of the proposed solution. | | |
| 17. | The Proposed solution should have the capability to sync the use cases, configuration from DC to DR automatically. | | |
| 18. | The proposed solution must provide for secure user access via HTTPS, SSH. | | |
| 19. | The solution shall have out of the box parser for the log sources bank would ingest. If the solution does not have a parser for custom application/ log source the bidder / OEM shall develop and implement the same within the agreed timelines. The bidder shall ensure the relevancy of the custom developed parser are maintained throughout the tenure of the contract. | | |
| 20. | If the proposed solution has data replication functionalities, the same has to be achieved without relying on other third-party replication technologies on the operating system or storage level. | | |
| 21. | The solution should also provide incident management tool and solution should be able to integrate with Bank's existing ticketing/service tool. | | |
| 22. | The solution should have the ability to gather information on real time threats and zero day attacks from anti-virus, IPS and IDS and analyses data against the information for any threats | | |
| 23. | The solution shall be able to provide the contextual enrichment for the parsed data to help triage alerts faster. This information can include details about the user, asset, IP address, geolocation, threat intelligence and vulnerability scan results. | | |
| 24. | The OEM shall provide Premium/ Enterprise Support. | | |
| 25. | Solution must support STIX/TAXII and API method for consumption of threat intel feeds from different platforms. Also, it must have | | |



| | | | |
|-----------------------|--|--|--|
| | capacity to ingest custom threat intel feeds manually. | | |
| 26. | Proposed solution should be perpetual software based solution. To deploy the proposed Software based SIEM, the HW, OS and Storage related configuration details should be submitted over OEM letterhead | | |
| Log Storage | | | |
| 27. | The bidder shall provision hardware to retain six months events online and 1 year in warm node (Six months + 12 months) and beyond that in Archival node. | | |
| 28. | SAN storage Systems should support Native Storage virtualization centralized management and SAN Storage should support 99.99% Data Availability. | | |
| 29. | SAN storages should be an end-to-end NVMe SSDs storage with dual controllers in Active-Active architecture and must support Scale Up & Scale Out. | | |
| 30. | End to End SAN Storage monitoring from a single management suite. | | |
| 31. | SAN system should support native remote replication for backup/DR purposes, i.e., 2-way replication with Synchronous and Asynchronous. | | |
| 32. | SAN system should allow intelligent compression & de-duplication without degrading the performance. | | |
| 33. | The system must have dual controller and file system heads with automatic failover capabilities in case of one controller or head failure. | | |
| 34. | During the Contract period, the bidder shall provide to bank all new versions, releases and updates of standard software/ hardware/ application etc., as well as related technical support. | | |
| 35. | Storage should support in built Data at rest Encryption, FIPS. | | |
| Log Management | | | |
| 36. | The Proposed solution should have capability to collect logs from different platforms like Microsoft Windows, Linux (All flavours), LinuxONE, UNIX, MAC OS, AIX, Solaris, Firewalls, EDR, AV, WAF, Tenable - Nessus, Network devices, 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, OpenStack) & cloud services (Aws/Azure/GCP/OCI), SAAS Solutions, 0365, etc. as required by the Bank. | | |
| 37. | The solution must support auto discovery of assets that are being protected or monitored and make them available in an asset database within the system with critical fields like server IP, Server hostname, OS Name, OS Version, Criticality, Date of discovery etc. to be populated automatically. | | |
| 38. | The network assets are often changing IP addresses. The solution must maintain the asset database correctly even when IP address changes. | | |
| 39. | Solution must support industry log collection methods (syslog, WMi, JDBC, SNMP, IPsec, ODBC, HTTP etc.) | | |
| 40. | The solution must support information (users, groups, etc.) collected from Directories (i.e., AD, LDAP) products. | | |
| 41. | The solution must not block, drop, or place grace period when system exceeds purchased EPS license/subscriptions limit. | | |
| 42. | The solution must integrate with other security and network devices such as Firewalls, IPS, WAF, EDR, other security solutions including but not limited to NAC, DLP etc. | | |
| 43. | Solution must have a log collection and archive architecture that supports both short-term (online) and long-term (offline) event storage | | |
| 44. | Solution must provide agent-based collection of event logs preferably wherever not possible agent less log collection has to be provided without any additional license cost. Agent must be single lightweight agent. Solution must have a light footprint and agent based / agentless solution must have minimal / no impact on performance of end points. | | |
| 45. | Solution must provide the ability to distribute both event collection and processing across the entire SIEM deployment. | | |



| | | | |
|-----|---|--|--|
| 46. | SIEM shall support Connector Development tool/SDK / API availability for developing collection mechanism for home-grown or any other unsupported devices/ applications. The respective tool should be provided without any extra cost to Bank | | |
| 47. | The solution must ensure the communication between the SIEM components are encrypted. | | |
| 48. | SIEM solution collector should forward the data to processing unit/ component in real time without any delay. | | |
| 49. | The solution must normalize common event fields (i.e., usernames, IP addresses, hostnames, and log source device, etc.) from disparate devices across a multi-vendor network. | | |
| 50. | The system shall be able to capture all details in raw log, events and alerts and normalize them into a standard format for easy comprehension. | | |
| 51. | The system should be able analyse logs with different event formats e.g.. well-structured logs, natural language logs, multi-line logs etc. | | |
| 52. | The solution must provide a common taxonomy of events. | | |
| 53. | The solution must provide the ability to normalize and aggregate event fields that are not represented by the out-of-the-box normalized fields. | | |
| 54. | The SIEM must provide searching & data/log management including free form search. | | |
| 55. | The solution must provide near-real-time analysis of events. | | |
| 56. | The solution must provide more advanced event drill down when required. | | |
| 57. | The solution must provide a real-time streaming view that supports full filtering capabilities. | | |
| 58. | The solution must provide a mechanism to capture all relevant aspects of a security incident in a single logical view. This view should include relevant events, network activity data, correlated alerts, etc. | | |
| 59. | The solution must allow for custom defined tagging of events. | | |



| | | | |
|-----|--|--|--|
| 60. | The proposed solution should be horizontally scalable to support increase in EPS and should have global correlation capability on raw or metadata/normalized events (i.e., correlation of events if processed on multiple hardware/appliances). | | |
| 61. | The solution must support user extended taxonomy of events and fields. The user must be able to add their own unique event names. | | |
| 62. | Solution should be able to define purging and retention rules for log storage. | | |
| 63. | The solution must monitor and alert when there is a disruption in log collection from a device. In other words, if logs are not seen from a server in 15 minutes, then generate an alert (report / SMS /email). In the event of same device generating multiple device types of logs (For Example, same device generating Application logs and System logs), the log disruption should be identified properly without any false positives. | | |
| 64. | The solution must provide an out of the box mechanism to discover and classify assets by system type (i.e., mail servers vs. data base servers) to minimize false positives associated with poor asset classification. Please describe how your solution meets this requirement. | | |
| 65. | The platform shall help to explore current and potential log source type MITRE-mapping coverage per rule, and suggest how the rule coverage can expand if new log source types are added to the environment. | | |
| 66. | Solution should do baselining of normal log ingestion rate regularly and alert for any unusual log ingestion rate(dips/spikes) per log source using ML/AI models. | | |
| 67. | The solution must allow the adding/modifying/removing of log parsers from UI console without impacting log collection. | | |
| 68. | The proposed solution must allow access to the rules written in Sigma/Generic SIEM and EDR/DR query languages. It supports common data schemas of SIEM along with the integration with content service to | | |



| | | | |
|-----------------|---|--|--|
| | directly deploy rules from threat detection marketplace. | | |
| 69. | Solution should have ability to restore / replay older logs for reporting, analysis, correlation, investigation, and forensics. | | |
| 70. | Solution should support IPV6 format. | | |
| 71. | The proposed solution must support integration of Custom Application's logs. | | |
| 72. | The solution should provide a no-code/low-code, drag- and-drop-based response design for the creation of simple or advanced security use cases. | | |
| Analysis | | | |
| 73. | The solution must provide alerting based on observed anomalies and behavioural changes in network and security events. | | |
| 74. | The solution must support and maintain a history of user authentication activity on a per asset basis. | | |
| 75. | The solution must support a web-based GUI for management, analysis, and reporting. | | |
| 76. | Solution should offer a global threat feed which must allow the analyst to perform search across various parameter like IPv4, IPv6, URL, vulnerability, Applications name, Malware, Spam. | | |
| 77. | Solution should allow analyst to perform manual ad-hoc check to determine if the organization is infected with any Zero-day attack. | | |
| 78. | There should be provision available to create complex searches by means GUI, to support advance investigation on the data available in the platform. | | |
| 79. | The platform should provide a search experience which shall guides analysts in defining what they want to search for with ability to change. | | |
| 80. | The solution must provide alerting based on observed security threats from monitored devices and network activity. | | |
| 81. | The solution must support a distributed model for correlation such that counters, sequences, identity lookups, etc. are shared across all collectors/loggers/aggregators. | | |
| 82. | Proposed solution should provide capability to add the following systems for effective | | |



| | | | |
|-----|---|--|--|
| | incident detection and correlation post completion of the SIEM deployment. a) Flow and packet-based threat Detection b) User Behaviour analysis by Integration with flow analysis/ packet capture tool c) Threat Intelligence | | |
| 83. | The solution must provide the ability to correlate information across potentially disparate devices and flows information. | | |
| 84. | The solution must provide alerting based on observed anomalies and behavioural changes in network activity (flow) data, Describe any pre-packaged alerts and method for adding user-defined anomaly and behaviour alerts. | | |
| 85. | The solution must observe anomalies other than just simple threshold basis. | | |
| 86. | The solution must chain alerts into one single incident record, so when different rules are triggered and these activities are related with one single offense, then these triggers will generate only one incident record to avoid overloading the security operation team. | | |
| 87. | The solution must provide alerting based upon established policy. | | |
| 88. | The solution must generate and alert when a new service appears on the network or when new assets appear where they shouldn't or are not planned. | | |
| 89. | The solution must provide the ability to transmit alerts using multiple protocols and mechanisms to other management solutions. | | |
| 90. | The solution must provide UI based wizard/ capabilities to minimize false positives and deliver accurate results. | | |
| 91. | The solution must limit the presentation of multiple similar alerts. | | |
| 92. | The solution must support the ability to take action upon receiving an alert. For example, the solution should support the ability to initiate a script or send an email message. The solution should also have feature to capture analyst details who have worked analyzed/ investigate the alerts. | | |
| 93. | The solution must support the ability to correlate against 3 rd party security data feeds (i.e., geographic mapping, known botnet channels, known hostile networks, etc.). | | |



| | | | |
|------|---|--|--|
| | These 3 rd party data feeds should be updated automatically in the proposed SIEM solution. | | |
| 94. | The solution must support correlation for a missing sequence. Example service stopped not followed by the service restarting within 10 minutes. | | |
| 95. | The solution must support Chain of Custody and Evidence Locker for securing and sharing artifacts like logs, files, and annotations | | |
| 96. | The solution must support correlation for additive values over time. For example, alert when any Source IP sends more than 1GB of data to a single port on a single Destination IP in a one-hour period of time. | | |
| 97. | The solution must provide a mechanism, to optimize rule tuning, which allows for the grouping of similar input values of a correlation rule that can be used by multiple rules. This grouping mechanism should allow for both static groups and groups that are dynamically created by other correlation rules. For example, the user of the system can define a group of banned ports/protocols that should be used across multiple correlation rules that monitor for inappropriate network activity. | | |
| 98. | The solution must support historical correlation so users can re-run past events and flows on historical data, so new rules can be tested more precisely. | | |
| 99. | The solution must be able to be updated regularly, to stay aware of the latest threat information and research available. | | |
| 100. | The solution must be able to analyse user activity to detect malicious insiders and determine if a user's credentials have been compromised. | | |
| 101. | The platform should Visualize alerts, network data, threats, malicious user behaviour, and cloud environments from around the world in geographical maps, and auto updating charts. | | |
| 102. | The platform should offer an interface to help user in browsing the existing rule mapping across MITRE Framework & enabling them to map their custom rules to MITRE ATT&CK tactics and techniques. | | |



| | | | |
|------|---|--|--|
| 103. | The platform should offer user to tune their environment with the help of built-in analysis capability. | | |
| 104. | The platform should suggest new insights to prioritize the rollout of new use cases/apps to effectively strengthen the security posture. | | |
| 105. | The platform must automatically detect any logical or performance issues in the default or custom use cases/rules and provide a visual interface indicating the issue. | | |
| 106. | The platform must detect logical or performance issues, such as when a rule calls referenceable data but the object is blank for example: when a rule calls referenceable data of a bad process but the object/folder does not contain a list of bad processes. | | |
| 107. | The platform must detect logical or performance issues such as no rule referring to a data/object/folder. | | |
| 108. | The platform must detect any logical or performance-related issues. Such a rule uses a normalized event property/field, but the field is deactivated at the system level. | | |
| 109. | The platform must detect logical or performance issues, such as a rule that uses a performance-intensive test condition, such as regex or unparsed raw payload content, and so on. | | |
| 110. | The platform must provide information about the rules that are available with OEM (as part of the OEM update or content packs) but not deployed on the platform, as well as the name of the content pack and the coverage of the use case/rules from MITRE perspective. | | |
| 111. | Platform must be capable of Identify the topmost alert generating rules or event generating rules, and then provide the guide/steps to tune them. | | |
| 112. | Platform must help in Reducing the number of false positives by reviewing the most common configuration features like update network details, common reusable content, and server discovery based on recommendations. | | |
| 113. | Should support integrating to Bank's existing VA tools (Tenable)or any new tool procured by the Bank, bidirectionally to tag the | | |



| | | | |
|----------------------------------|---|--|--|
| | offenses with list of vulnerabilities present in the associated assets of that offense. | | |
| Reporting & Dashboard | | | |
| 114. | The solution must provide a 'Dashboard' for quick visualization of security and network information. | | |
| 115. | The solution must support the automated distribution of reports. | | |
| 116. | The solution must support the capability to provide historical trend reports. | | |
| 117. | Platform must provide capability to generate rules related reports from predefined templates, such as searches based on rule response and actions, log source coverage, and many others. | | |
| 118. | The platform shall support provision for dashboard specific to a single incident, which can offer various widgets, provision for sharing notes, representation of data in a graphical manner over a certain period and various rules triggered, rules, models responsible in triggering of the offense. | | |
| 119. | The platform should allow to import and export dashboards or share dashboard links with colleagues. | | |
| 120. | The platform should allow user to create dashboard items that use the full power of native query language, dynamic search, and generic APIs. | | |
| 121. | The platform should allow user to fine-tune there with complete flexibility in dashboard layout and dashboard item refresh rates. | | |
| 122. | The platform should allow user to Assign thresholds. | | |
| 123. | The solution must offer all the below built-in compliance modules out of the box at no additional cost but not limited to: a) PCI-DSS Compliance Module b) NIST c) DPDP Compliance Module d) ISO Compliance Module and other regulatory bodies which is applicable to Bank | | |
| 124. | The proposed solution must offer all the reports out of the box at no additional cost. | | |
| 125. | The proposed solution must have real-time visualization options, features and capabilities of the dashboard. A) Blacklist-based correlation. | | |



| | B) Whitelist based correlation | | |
|---|--|----------------------------|------------------------|
| 126. | Proposed solution should have a dashboard to see the real time and history of EPS, Data sources integrated for the last 6 months. | | |
| 127. | Solution should have option to check non reporting event sources and non-triggered/ zero hit use cases within the given timeframe. | | |
| <u>2. User & Entity Behavioral Analytics</u> | | | |
| Sl. No. | Technical & Functional Requirements | Compliance (Yes/No) | Vendor's Remark |
| <u>Architecture & General Specifications</u> | | | |
| 1. | The proposed solution is required to be deployed at on-premises. The bidder is required to size all the component for the solution proposed. If there is any performance issue during the contract period, bidder is required to provide software / hardware at no additional cost to the Bank | | |
| 2. | Proposed UEBA should be from the same OEM of the proposed SIEM solution. | | |
| 3. | The solutions deployed should be modular, scalable and should be able to address Bank's requirements for the next five years, with the deployed hardware and software. | | |
| 4. | The architecture should have High Availability in inbuilt into the product. The solution shall be deployed at Data Center and Disaster Recovery Center of the Bank in high availability. | | |
| 5. | The solution shall have 40,000 User & Entity licenses and provision to procure additional licenses as per the requirement without compromising on system functionality or performance. | | |
| 6. | The solution shall be sized to maintain six months data online. | | |
| 7. | The solution shall have native integration available with existing AD, EDR, ticketing tool, proposed SOAR and SIEM solution. | | |
| 8. | The solution should have role-based access control. It should support SMS, Email and App based MFA. | | |
| <u>Analysis</u> | | | |
| 9. | The solution should leverage Artificial Intelligence and machine learning for detecting anomalies. | | |



| | | | |
|-----|--|--|--|
| 10. | The solution shall be able to detect risky and potentially abnormal user activity within the Bank's network such as but not limited to privilege escalation, lateral movement etc. | | |
| 11. | The solution shall be able to identify identity threat behavior such as account hijacking and abuse of user accounts. | | |
| 12. | The solution must be able to detect when strange users access a specific host, learn what users connect with specific assets such as a point-of-sale terminal and then alert when new users login. | | |
| 13. | The solution shall provide high privilege access anomaly detection for misuse, sharing, or takeover user accounts. | | |
| 14. | The solution shall have self-learning behavioral analysis and dynamically model to identify any anomalous activity that falls outside of the normal pattern. | | |
| 15. | <p>The solution shall use unsupervised or supervised machine learning algorithms for anomaly detection mentioned below</p> <p>(a) Access high-value assets such as User starts accessing and downloading high-value assets with increased frequency.</p> <p>(b) Usage changes over time such as User activity deviates from normal over a short period of time or a gradual change over an extended period of time.</p> <p>(c) Assess frequency of assets such as User's volume of activity suddenly spikes or access to number of assets increases rapidly.</p> <p>(d) Usage deviates from peer group such as User pattern of activity starts deviating from the peer group.</p> <p>(e) Change in account privileges such as User attempts to change privileges on existing account or open new accounts on other systems.</p> <p>(f) Application misuse by sequence of actions: User performs a sequence of actions which no other user is performing.</p> <p>(g) Sensitive data leakage such as User manipulates http request/response parameter to download sensitive data.</p> <p>(h) Application misuse by malware or bots such as A bot or malware attacks an application or access sensitive data.</p> | | |



| | | | |
|-----|---|--|--|
| | (i) Dynamic adjustment of risk scores such as Dynamically adjust the risk score of rules when triggered against particular user or users. | | |
| 16. | UEBA should activate a rule for a set of users until a specified condition or specified time window. | | |
| 17. | The solution should leverage Machine learning to perform analytics to gain additional insight into user behavior with predictive modelling. | | |
| 18. | UEBA should perform the below mentioned scenario's as well. Use Case for UEBA: Access and Authentication | | |
| | Account accessing more high value assets than normal | | |
| | More data being transferred then a normal to and from servers and / or external location | | |
| | Privileged account accessing high-value servers from a new location for the first time | | |
| | Account used for the first time in a long time | | |
| | Rare privilege escalation | | |
| | Accounts being used from peculiar locations | | |
| | User involved in previously malicious or threatening behavior | | |
| | User an outlier within their peer group | | |
| 19. | Exfiltration | | |
| | Data Exfiltration by Print | | |
| | Data Exfiltration by Removable Media | | |
| | Data Loss Possible | | |
| | Initial Access Followed by Suspicious Activity on critical servers | | |
| | Large Outbound Transfer by High-Risk User | | |
| | Multiple Blocked File Transfers Followed by a File Transfer | | |
| 20. | Browsing behavior | | |
| | Browsed to Entertainment Website | | |
| | Browsed to Gambling Website | | |
| | Browsed to Information Technology Website | | |
| | Browsed to Mixed Content/Potentially Adult Website | | |
| 21. | DNS Analysis | | |
| | Potential Access to Blacklist Domain | | |
| | Potential Access to DGA Domain | | |
| | Potential Access to Squatting Domain | | |
| | Potential Access to Tunnelling Domain | | |



| | | | |
|------------------------------|---|--|--|
| 22. | Admin/Activity Based | | |
| | Anomalous Account Created from New Location | | |
| | User Access from Multiple Locations | | |
| | User Geography Change | | |
| | User Geography, Access from Unusual Locations | | |
| Dashboard and Reports | | | |
| 23. | The solution shall provide customizable dashboards, configurable policies, and risk model optimization | | |
| 24. | The solution shall provide various visualization options for deep-dive investigation, compliance, and reporting . | | |
| 25. | The solutions shall have a "Single-pane-of-glass" view into high-risk user/ entity showing behavior pattern with respect to activities, locations, devices, sessions, usage, and risk trends. | | |
| 26. | The solution shall enable bank to export report in CSV, Email, PDF format. | | |
| 27. | The solution should have ability to schedule the report. | | |
| 28. | UEBA UI/panel should be integrated in SIEM dashboard. Thus, which will help in monitor desired elements of users' behaviors, risks, and trends from a single screen. | | |
| 29. | The solution should provide Privilege Access Intelligence via Access information & Activity Log to alert most Risky events as per device, User, Access, and behavior. | | |
| 30. | The solution should support contextual natural language search for query, investigation & threat hunting purpose. It should provide baselines, Peer Groups (Static & Dynamic) Analysis and User contextual Data while doing the investigation. | | |
| 31. | The solution should provide 360-degree view and single pane of glass for user/entity activities across all resources using linked analysis. The tool should be capable to provide Risky Activities, Anomalies/ Outliers, Risk profiling, Asset & Device Usage, Transaction Timeline, MITRE ATT&CK Mapping information, Incident Information, Access & Peer Group Information as a single view, for quick analysis. This 360 degree view should be | | |



| | | | |
|-----|--|--|--|
| | exportable as a Report with above mentioned information. | | |
| 32. | The solution should provide Cyber Kill chain mapping using the MITRE ATT&CK framework and suggest remediation. | | |
| 33. | The solution should provide analytical capabilities pertaining to ML models. | | |
| 34. | The solution should support the creation of personalized Dashboards & Sharing of Dashboards & Queries with specific Users & Roles (SOC Analyst, Auditor etc.). | | |
| 35. | The solution should detect slow attacks, advance persistent threats, and file less attacks, zero-day attacks, in-memory attacks, leveraging in-built self-learning and analytics leveraging AI / ML. | | |
| 36. | The solution should support bidirectional integration with core NG-SOC solutions (SIEM, SOAR, threat Intel etc.) | | |

3.Security Orchestration, Automation & Response (SOAR)

| Sl. No | Technical Requirement | Compliance (Yes/No) | Remarks |
|--|---|---------------------|---------|
| Architecture, Integration & General Requirement | | | |
| 1. | The proposed platform shall be hosted on-prem that integrates with all on-premises and hybrid, multi cloud architecture security components. The bidder shall provide all the required hardware which includes compute and storage to retain the data defined by the Bank | | |
| 2. | Proposed SOAR solution should be from the same OEM of the proposed SIEM & UEBA solutions. All the hardware/software required for the solution shall be provisioned by the bidder. | | |
| 3. | The solution must be able to support multi-tenancy. | | |
| 4. | The proposed solution should support High Availability in DC and DR site, the same shall be offered as part of the solution. | | |
| 5. | The solution should auto replicate all the rules, data, etc., to DR site and vice versa for continuing the operations without any loss in data | | |
| 6. | The proposed solution should have Development environment where integration and playbooks shall be tested before deploying it to the production deployment | | |



| | | | |
|-----|---|--|--|
| 7. | The solution should be able to consume security alerts/incidents from SIEM, EDR, TIP, directly from any other Next Gen SOC and Cyber security solutions. | | |
| 8. | The solution should be able to provide bidirectional integration with All the solution and tools proposed as a part of Next Gen SOC | | |
| 9. | The solution shall have 500+ out of the box integration available from day one. SI to develop any new integration as and when required by the Bank with no extra cost. | | |
| 10. | Solution should include out-of-the- box playbooks for incidents like Ransomware Attack, Data Leakage, Malware Attack, DoS and DDoS attack, Phishing Attack, etc. and should support creation of multiple playbooks without any additional cost to Bank | | |
| 11. | In solution there should not be any limit on number of playbooks and playbook steps or playbook execution or action execution | | |
| 12. | The solution should have the integrated Ticketing tool to manual/auto-assigning of incidents/tickets based on the type of alert/incident, asset owner/department, based on the availability of personnel in shift. | | |
| 13. | All the basic and advanced integrations have to be provided by the OEM without any extra charge to bank. In case of new customizations, the SI/OEM should leverage the Onsite engineering resources in developing the same within 30 days of providing the requirement. or OEM has to provide ,required professional services for 10 customized connectors every year or 50 customized playbooks during contract period without any extra cost to Bank. | | |
| 14. | Workflow and playbook capabilities: a. The solution should auto assign playbooks for each alert along with recommendation to a particular analyst. b. The solution should provide simulation environment to test playbooks without any dependency on real environment. c. The solution should repeat workflow until all assigned tasks are completed and the solution should be able to raise alert in case of failure. d. The solution should provide exception report, detailed analysis of failure and corrective steps. | | |



| | | | |
|-----|---|--|--|
| | e. The solution should have a versioning mechanism to save and maintain multiple versions for the playbooks. f. The solution should allow for viewing version history for all or selected playbook and provide option for restoring to an older version. | | |
| 15. | The solution should provide contextual analysis / quick reference into an indicator/object/event when viewing incident investigation data by auto-correlation with TIP, VM, EDR etc. without requiring navigating away from incident investigation. | | |
| 16. | AI Capabilities: a. Auto assigning analyst – The solution should have capability to auto assign incidents/ tickets based on type of incident, asset owner, concerned department, availability in shift, workload on analyst etc. | | |
| 17. | The solution should suggest contextual between incidents using machine learning. | | |
| 18. | The solution should provide shift management feature to upload shift schedule of users in any suitable format. | | |
| 19. | Chat/messaging capabilities: a. The solution should provide platform for users to discuss and collaborate. b. The solution should support auto documentation of chats/ actions. | | |
| 20. | The platform must provide capability to quickly integrate the existing security tools to generate deeper insights into threats, orchestrate actions and automate responses—all while leaving the data where it is i.e., using federated searches | | |
| 21. | The solution should be able to parse all necessary fields from proposed NG-SOC solutions (SIEM, UEBA) alerts, including but not limited to creation time, update time, source/destination IP, source country, category, system, rule-name, severity, etc. | | |
| 22. | The proposed solution should take response actions to Users like Password reset, Force Sign out, Disable User Account, etc. | | |
| 23. | The solution should provide visual representation of an incident, correlation of its elements, history of investigation and so on. | | |
| 24. | The Platform must supports the integration with multiple 3rd party directory systems for authentication via SAML 2.0 etc. | | |



| | | | |
|---|--|--|--|
| 25. | The Platform must offer API's so that 3rd Party solutions such as ITSM tool can integrated with the platform and fetch/update alerts/cases/offense | | |
| 26. | The Platform must support Granular Role based access control. The administrator must be able to define role based access to various functional areas of the solution. This includes being able to restrict a users access to specific functions of the solution that is not within the scope of a users role including, but not limited to, administration, reporting, incident assignment, playbook creation. Please describe how your solution meets this requirement. | | |
| 27. | Bank shall have 10 user licenses and 2 read only licenses from day one. | | |
| Analysis and Incident Management | | | |
| 28. | The platform should provide a single, integrated platform for analyzing log, flow, vulnerability, user and asset data providing full visibility into all networks, applications, and user activity. | | |
| 29. | The platform shall have threat visibility and investigation depth, speed and consistency with AI based automated analysis of EDR, NDR and SIEM telemetry sources | | |
| 30. | The Platform must support documenting Investigation notes/outcome and presented it in chronologically order | | |
| 31. | The Platform must support export Investigation notes/outcome in pdf or csv format | | |
| 32. | The Platform must provide information in such a way that analysts can quickly understand the source and impact of an attack, enabling teams to respond more effectively | | |
| 33. | Platform must have inbuilt Ability to gather actionable IOC based on the organization vertical/Geo and then run automated searches for related indicators of compromise across different datastores in the organization like SIEM, EDR, NDR, Data lake etc. | | |
| 34. | Bidder should have their own threat intelligence service which shall be integrated with SOAR to check threat score, reputation etc. | | |
| 35. | The Platform provides a visual representation of enriched information HTML, markdown, feature-rich GUI | | |



| | | | |
|-----|---|--|--|
| 36. | The Platform must support Evidence retention, case notes, and attached artifacts should be retained six months logs online and 1 year in warm node (Six months + 12 months) and beyond that in Archival node. | | |
| 37. | The Platform must support the creation of custom incident types, artifact tagging and any additional custom fields as you see fit. | | |
| 38. | The proposed platform must have built-in MITRE ATT&CK alignment for all the Automated/manual based investigation and should overlay the playbooks depicting the coverage against MITRE ATT&CK TTPs. | | |
| 39. | The platform must have the ability to create custom hunting rules or hypotheses using Universal Threat Hunting Language. | | |
| 40. | The solution must be able to create incident by parsing email notification. | | |
| 41. | The solution must provide UI based wizard to manually create incidents. | | |
| 42. | The solution must be able to support creation and deletion of automated incidents via API, Web URL, SIEM, Ticketing System. | | |
| 43. | The solution must be able to automatically extract email attachments from emails and store that for the related incidents as attachments. | | |
| 44. | The solution must be able to support storing of incident related files not limited to malware specimens, logs, screenshots. | | |
| 45. | The solution must include out-of-the-box playbooks based on SANS and NIST for incidents like Malware, Phishing, DOS and should support creation of multiple playbooks based on the SOC's Use case. | | |
| 46. | The solution must be able to provide incident response playbooks that consist of phases and tasks that guides the user on how to adequately response to the incident; integrating people, processes and technology. | | |
| 47. | The solution must provide a visual workflow editor to enforce sequencing of incident response activities | | |
| 48. | The solution must include a in-product script editor with autocomplete and syntax highlighting, to support automation of incident response workflow. | | |



| | | | |
|-----|---|--|--|
| 49. | The solution must include a in-product script editor with run buttons to facilitates debug and perform tests on scripts. | | |
| 50. | The solution must allow organizations simulate incidents, to test response plans, allowing them to identify gaps and refine processes before a real incident happens. | | |
| 51. | The Proposed Solution should have out-of-the-box bi-directional integration with the proposed SIEM solution & App on both platform (SIEM & SOAR) | | |
| 52. | The proposed solution should have out-of-the-box provision of closing incident simultaneously on SIEM and the proposed SOAR platform. | | |
| 53. | The proposed solution should have out-of-the-box capability to query or add IOC/Artifact to existing watchlist of the deployed SIEM solution. | | |
| 54. | The Proposed solution should have web based application store which should host latest integrations available from the OEM this integration can be downloaded with no additional cost. | | |
| 55. | The proposed solution should have community portals and knowledgebase which can be used to learn about sample integration and forum to discuss issue or use cases. | | |
| 56. | The solution should have bidirectional integration capability with proposed SIEM solutions i.e. create case/ticket/incident from the alert raised by SIEM / EDR, pull raw logs from SIEM /EDR, pull information related to rules triggered the alert, pull asset vulnerability details, update alert in SIEM /EDR and close SIEM / EDR alert. | | |
| 57. | The solution should have capability to create flexible, multi-conditional and complex workflows | | |
| 58. | The solution should allow creation of manual tasks, automated tasks, combination of both and conditional tasks in playbooks | | |
| 59. | The solution should also allow scheduling and customization of tasks. | | |
| 60. | The solution should provide capability to embed scripts (Python or any other language) in the playbooks. | | |
| 61. | The solution should be capable to provide automated detailed post incident report about all | | |



| | | | |
|-----|---|--|--|
| | the actions taken, root cause, collaborative actions/chats etc. | | |
| 62. | The solution must support creation of workflow which can have multiple task which can be executed sequentially or parallelly where parallel task can be executed independently while sequential task will depend on closure of previous task. In case any task or workflow encounter any issue, same should be displayed on the tool as part of status. | | |
| 63. | Solution should provide analysis about failed tasks/workflow in the UI itself | | |
| 64. | SOAR solution must allow analyst to create multiple playbooks and allow them to be manually or automatically saved with different names or versions | | |
| 65. | The solution should allow for viewing playbook name/version history for all or selected playbook either within the system or outside the system and provide option for restoring to an older playbook. | | |
| 66. | The solution must provide central management of incidents and administrative functions from a single web based user interface. | | |
| 67. | The solution must support the ability to correlate against 3rd party security data feeds. These 3rd party data feeds should be updated automatically by the solution. | | |
| 68. | The solution must dynamically augment incident playbooks in real time to support a specific incident response workflow. | | |
| 69. | The solution must provide the ability to contextually link incidents with similar artifacts. | | |
| 70. | The solution must provide the means for analysts to review the enrichments performed on the incident to arrive at conclusions about a security incident. | | |
| 71. | The solution must out-of-the-box integrate with external threat intelligence feed providers to provide data enrichment of incident artifacts. | | |
| 72. | The solution must, out-of-the-box, must provide visualization of incident correlation across IOCs and other artifacts automatically with timeline support. | | |
| 73. | The solution must allow users to take remedial steps directly from within the visualization of incident correlation enabling a rapid and efficient response. | | |



| | | | |
|----------------------------------|---|--|--|
| 74. | The solution should offer graphical representation of all the artifact associated to a particular incident along with the timeline. It should enable the analyst to take action from withing the graphical view on any artifact i.e., this could be blocking a IP address or doing further investigation using any of the threat service available to solution. | | |
| 75. | The Solution should offer Timeline graph for each incident allowing display that can be set to display days, weeks, and months. It should also allow analyst to add milestones to call out important events within the timeline. Where the analyst can add a date, title, and description of your milestone. | | |
| 76. | The solution should allow adding custom table to incident layout allowing organization to track relevant fields based on use case. Such as Approval flow, Response time, Actions performed to name a few. | | |
| 77. | The solution must offer out-of-the-box support for auto creation of incident artifacts. | | |
| 78. | The solution must be able to support logical segregation of incidents. This will be used to assign a specific group of incidents to a specific group of users/analysts | | |
| 79. | The solution must enable to delegate tasks to another user and to assign due dates | | |
| 80. | The solution must be able to support creation of Knowledge portal. This enables organizations to add important information, guidelines, and reference material for the Incident Response team. | | |
| 81. | The solution must provide long term trend analysis of incidents. Please describe how this requirement is met by the solution. | | |
| 82. | The solution must provide more advanced incident drill down when required. Please describe how this requirement is met by the solution. | | |
| 83. | The solution must provide the ability to correlate artifacts across potentially disparate incidents. | | |
| 84. | The solution must support the ability to trigger action on external systems, for a related to an incident. For example, the solution should support the ability to block an intruder. | | |
| Reporting & Dashboard | | | |



| | | | |
|-----|--|--|--|
| 85. | The solution must support a web-based GUI for management, analysis and reporting. | | |
| 86. | The solution must provide the ability to deliver multiple dashboards that can be customized to meet the specific requirements of different users of the system. | | |
| 87. | Provide automated reports and dashboards for real-time measurement of key performance indicators (KPIs) such as MTTD and MTTR for overall SOC | | |
| 88. | The solution must deliver sample dashboards out-of-the-box (not limited to - Incident Over Time by Type, Open Incidents by Phase, Close Incident by Duration). | | |
| 89. | The solution must deliver customizable dashboard widgets that can present relevant incident information to the users. | | |
| 90. | The solution must maintain a database of incidents. The user must be able to search this database. | | |
| 91. | The solution must support and maintain a history of user activity per incident. | | |
| 92. | The solution must provide reporting templates, to report on incident information, for the management team as well as the IT Security team via the GUI. Describe how the solution provides the ability to configure reports. | | |
| 93. | The solution should support reporting templates where users can add content blocks with preconfigured text or visual elements, such as charts, images, tables, and saved graphs, or placeholder sections that users can fill in after they create a report from the template | | |
| 94. | The solution must provide configurable reporting engine for customized report creation. | | |
| 95. | The solution must support importing and exporting of configuration settings. | | |
| 96. | The Solution must support a flexible dashboard environment that allows users to leverage searches and views that can easily be deployed to a user's workspace. | | |
| 97. | The solution should serve as end-to-end incident management, incident response, investigation platform and single evidence repository | | |
| 98. | The Solution should provide ticketing functionality for the security team/IR team | | |
| 99. | The Solution should be able assign an incident to a user or a team | | |



| | | | |
|------|--|--|--|
| 100. | The solution shall have feature to configure SLAs pertaining to MTTD, MTTR, MTTC and have capabilities to notify respective incident owner / manager for any potential SLA breach through SMS, email | | |
| 101. | The solution should be able to set reminders for tasks | | |
| 102. | The solution should be able to group incidents (e.g., Malware outbreak with time delay, every incident with this malware in one parent incident) | | |
| 103. | The solution should have customizability available for incident management | | |
| 104. | The solution should offer any auto-casing / auto-population based on the incident type or other relevant incident attributes | | |
| 105. | The solution must provide tagging capabilities on tickets. Tags must be customizable. | | |
| 106. | The solution must be able to aggregate information from past investigations on the ticket (such as link to a data source, comments, involved analyst, etc.) | | |
| 107. | The solution must be able to detect redundant alerts and hence, aggregate duplicates in one and only ticket (Number of aggregated tickets must be displayed) | | |

Hardware based Video Wall controller Technical Specification

| Sr. | Technical Requirement | Compliance (Yes/No) | Vendor's Remark |
|-----|---|---------------------|-----------------|
| 1 | 16 HDMI Inputs | | |
| 2 | 8 HDMI Outputs | | |
| 3 | 4U Chassis | | |
| 4 | 500 Watt Redundant Power Supply | | |
| 5 | Audio Input support | | |
| 6 | Wall Management Software | | |
| 7 | Touch LCD Panel Inbuilt in Videowall controller for easy Preset Management | | |
| 8 | Input Sources Audio Management with mute/Unmute option on every input sources | | |
| 9 | Any Source on Any Display | | |
| 10 | Source Overlapping | | |
| 11 | Should be able to show minimum 16 same or different sources in one single display | | |
| 12 | PIP and POP | | |
| 13 | Auto Source Detection | | |
| 14 | Ticker Scrolling Text | | |
| 15 | Unlimited Layouts | | |



| | | | |
|----|---|--|--|
| 16 | upto 16 Layouts can be Controlled by Crestron/AMX devices | | |
| 17 | Multi Videowall Supports | | |
| 18 | Scheduling of Layouts | | |
| 19 | Supports Control by Web Browser with Live Preview | | |
| 20 | Hot Swappable Graphic Card, Fan & Power Supply | | |
| 21 | Support 4K Resolution Base Image on Whole Video Wall | | |
| 22 | 09 Slot Chassis with capabilities to add Input and Output using any slot. | | |
| 23 | Expandable upto 56 Inputs / outputs without adding external chassis | | |
| 24 | expansion of Outputs without Loop in Loop out | | |
| 25 | User Management With Authentication, upto 3 Levels Admin, Technical officer, User | | |
| 26 | Custom Resolution for All types of display technology | | |

| Video Wall Display Specifications | | | | |
|-----------------------------------|----------------------|--|----------------------|-----------------|
| Sr. No | Parameters | Features | Compliance (Yes /No) | Vendor's Remark |
| 1 | Screen Size | 55" | | |
| 2 | Panel Technology | IPS(In plane Switching) | | |
| 3 | Back Light Type | Direct/Edge LED for Slim depth of display | | |
| 4 | Aspect Ratio | 16:09 | | |
| 5 | Native Resolution | 3840 x 2160 (4K), | | |
| 6 | Brightness | 500 nits or Higher | | |
| 7 | Dynamic CR | 450,000:1 or Better | | |
| 8 | Viewing Angle(H x V) | 178 X 178 angle to cover Max viewing angle from any location of Room | | |
| 9 | Response Time | 8 ms | | |
| 10 | Life time(Typ.) | 60,000Hrs(Typ.) or High | | |
| 11 | Operation Hours | 24Hrs grade panel | | |



| | | | | |
|----|-------------------------|--|--|--|
| 12 | Orientation | Portrait & Landscape | | |
| 13 | Inputs ports | HDMI -2,DP-1,DVI-D-1,USB-1,RJ45(LAN-1) or high | | |
| 14 | Output ports | Display Port (DP) for daisy chain to run FHD contents with out Controller, RJ45(LAN-1) and RS232C both | | |
| 15 | Calibration | Auto Calibration possible as well as calibration through Remote Control and Image gap to reduce | | |
| 16 | Daisy Chain | LAN in/LAN out for Daisy Chain | | |
| 17 | Internal Memory | 8GB(4GB usable) | | |
| 18 | Bezel to Bezel (Gap) | Less than or equal 1 mm | | |
| 19 | Key Feature required | Temperature Sensor, Auto Source Selection, Energy Saving, Calibration Mode, Failover ,Wake on LAN, No Signal Screen, Daisy Chain of LAN to take control of Panels from remote location/Long distance, USB Plug and play, OPS Type Compatible | | |
| 20 | Color Calibration | Sensor less Inbuilt continuous calibration with 144 points calibration in one display | | |
| 21 | Operation Humidity | 10 % to 80 % | | |
| 22 | Power Supply | 100-240V~, 50/60Hz | | |
| 23 | Power Consumption- Typ. | 250 Watts or less | | |
| 24 | CERTIFICATION's | UL for safety, FCC for Electro Magnetic Communication , | | |
| 25 | Operating System | Inbuilt Windows/Web OS for Secure Content | | |
| 26 | Warranty | 3 years | | |
| 27 | Installation | SITC installation with OEM approved Push Pull Bracket | | |

58. ANNEXURE 3: CONFORMITY LETTER

Date

To,

General Manager (IT),
Central Bank of India,
DIT, Sector 11,
CBD Belapur,
Navi Mumbai – 400614

Sir,

Sub: RFP for Supply, Implementation and Management of Next-Generation Security Operations Centre (NG-SOC) Solutions

Tender No. GEM/2025/B/6180729

Further to our proposal dated _____, in response to the RFP document (hereinafter referred to as “RFP DOCUMENT”) issued by Central Bank of India (“Bank”) we hereby covenant, warrant and confirm as follows:

We hereby agree to comply with all the terms and conditions / stipulations as contained in the RFP document and the related addendums and other documents including the changes made to the original tender documents issued by the Bank.

The Bank is not bound by any other extraneous matters or deviations, even if mentioned by us elsewhere either in our proposal or any subsequent deviations sought by us, whether orally or in writing, and the Bank’s decision not to accept any such extraneous conditions and deviations will be final and binding on us.

Yours faithfully,

Authorized Signatory

Designation

Company Name



59. ANNEXURE 4: BIDDER'S INFORMATION

| # | Particulars | Details |
|-----|--|---------|
| 1. | Name of bidder | |
| 2. | Constitution | |
| 3. | Address with Pin code | |
| 4. | Authorized Person for bid | |
| 5. | Contact Details (Mail id & Mob No) | |
| 6. | Years of Incorporation | |
| 7. | Number of years of existence | |
| 8. | Annual Turnover (In Rs.) 2021-22 – 2022-23 – 2023-24 – | |
| 9. | Operating Profits (In Rs.) 2021-22 – 2022-23 – 2023-24 – | |
| 10. | Net Worth (In Rs.) 2021-22 – 2022-23 – 2023-24 – | |
| 11. | Whether OEM or authorized distributor | |
| 12. | Number of service outlets across India | |
| 13. | Good and Service Tax Number | |
| 14. | Income Tax Number | |
| 15. | Name and Address of OEMs | |
| 16. | Brief Description of after sales service facilities available with the bidder. | |
| 17. | Whether all RFP terms & conditions complied with. | |

Signature

Name:

Designation:

Seal of Company

Date:

60. ANNEXURE 5: LETTER FOR CONFORMITY OF PRODUCT AS PER RFP

Date

To,

General Manager (IT),
Central Bank of India,
DIT, Sector 11,
CBD Belapur,
Navi Mumbai – 400614

Sir,

Sub: RFP for Supply, Implementation and Management of Next-Generation Security Operations Centre (NG-SOC) Solutions

Tender No GEM/2025/B/6180729

We submit our Bid Document herewith. If our Bid for the above job is accepted, we undertake to enter into and execute at our cost, when called upon by the bank to do so, a contract in the prescribed form. Unless and until a formal contract is prepared and executed, this bid together with your written acceptance thereof shall constitute a binding contract between us.

We understand that any deviations mentioned elsewhere in the bid will not be considered and evaluated by the Bank. We also agree that the Bank reserves its right to reject the bid, if the bid is not submitted in proper format as per subject RFP.

We undertake that product and services supplied shall be as per the:-

| Compliance | Compliance (Yes/ No) | Remarks |
|---------------------------------|----------------------|---------|
| Terms & Conditions | | |
| Scope of Work | | |
| Technical Specifications (100%) | | |
| Eligibility Criteria | | |

Signature

Name:

Designation:

Seal of Company

Date:

61. ANNEXURE 6: UNDERTAKING FOR ACCEPTANCE OF TERMS OF RFP

Date

To,

General Manager (IT),
Central Bank of India,
DIT, Sector 11,
CBD Belapur,
Navi Mumbai – 400614

Sir,

Sub: RFP for Supply, Implementation and Management of Next-Generation Security Operations Centre (NG-SOC) Solutions

Tender No :GEM/2025/B/6180729

With reference to RFP for Supply, Implementation and Management of Next-Generation Security Operations Centre (NG-SOC) Solutions at the Bank:

We understand that Bank shall be placing Order to the Successful Bidder exclusive/inclusive of taxes only.

1. We confirm that in case of invocation of any Bank Guarantees submitted to the Bank, we will pay applicable GST on Bank Guarantee amount.
2. We are agreeable to the payment schedule as per "Payment Terms" of the RFP.
3. We here by confirm to undertake the ownership of the subject RFP.
4. We hereby undertake to provide latest product/ software with latest version. The charges for the above have been factored in Bill of Material (BOM), otherwise the Bid is liable for rejection. We also confirm that we have not changed the format of BOM.

Signature

Name:

Designation:

Seal of Company

Date:



सेंट्रल बैंक ऑफ़ इंडिया
Central Bank of India

1911 से आपके लिए "केन्द्रीय" "CENTRAL" TO YOU SINCE 1911

**RFP for Supply, Implementation & Management of Next-
Generation Security Operations Centre (NG-SOC) Solutions
Central Bank of India – Tender No – GEM/2025/B/6180729**

62. ANNEXURE 7: MANUFACTURER'S AUTHORIZATION FORM

Date

To,

General Manager (IT),
Central Bank of India,
DIT, Sector 11,
CBD Belapur,
Navi Mumbai – 400614

Tender No. GEM/2025/B/6180729

Dear Sir,

We _____ (OEM Vendor) of _____ product / service / solution hereby authorize M/s. _____ (Selected Bidder / Vendor Name) to offer their quotation, negotiate and conclude the contract with you against the above invitation for the Bid. We hereby extend our full guarantee and comprehensive warranty and AMC & ATS (post expiry of warranty) as per terms and conditions of the tender and the contract for our product / application solution / services offered against this invitation for Bid by the above firm. We also extend our back-to-back service support and assurance of availability of our equipment (Hardware and Software as part of the Bill of Material) and their components as per terms and conditions of the tender, to M/s. _____ (Vendor Name) for a period of five years

Yours Faithfully,

Authorized Signatory

(Name, Phone No., Fax, E-mail)

(This letter should be on the letterhead of the Manufacturer duly signed & seal by an authorized signatory)

63. ANNEXURE 8: INTEGRITY PACT

Integrity Pact

Between

Central Bank of India hereinafter referred to as “The Principal”,

And

..... hereinafter referred to as “The Bidder/
Contractor”

Preamble

The Principal intends to award, under laid down organizational procedures, contract/s for.....The Principal values full compliance with all relevant laws of the land, rules, regulations, economic use of resources and of fairness / transparency in its relations with its Bidder(s) and / or Contractor(s).

In order to achieve these goals, the Principal will appoint an Independent External Monitor (IEM), who will monitor the tender process and the execution of the contract for compliance with the principles mentioned above.

Section 1 – Commitments of the Principal

(1.) The Principal commits itself to take all measures necessary to prevent corruption and to observe the following principles:-

- a. No employee of the Principal, personally or through family members, will in connection with the tender for , or the execution of a contract, demand, take a promise for or accept, for self or third person, any material or immaterial benefit which the person is not legally entitled to.
- b. The Principal will, during the tender process treat all Bidder(s) with equity and reason. The Principal will in particular, before and during the tender process, provide to all Bidder(s) the same information and will not provide to any Bidder(s) confidential / additional information through which the Bidder(s) could obtain an advantage in relation to the tender process or the contract execution.
- c. The Principal will exclude from the process all known prejudiced persons.

(2) If the Principal obtains information on the conduct of any of its employees which is a criminal offence under the IPC/PC Act, or if there be a substantive suspicion in this regard, the Principal will inform the Chief Vigilance Officer and in addition can initiate disciplinary actions.

Section 2 – Commitments of the Bidder(s)/ contractor(s)

(1) The Bidder(s)/ Contractor(s) commit themselves to take all measures necessary to prevent corruption. He commits himself to observe the following principles during his participation in the tender process and during the contract execution.



- a. The Bidder(s)/ Contractor(s) will not, directly or through any other person or firm, offer, promise or give to any of the Principal's employees involved in the tender process or the execution of the contract or to any third person any material or other benefit which he/she is not legally entitled to, in order to obtain in exchange any advantage of any kind whatsoever during the tender process or during the execution of the contract.
- b. The Bidder(s)/ Contractor(s) will not enter with other Bidders into any undisclosed agreement or understanding, whether formal or informal. This applies in particular to prices, specifications, certifications, subsidiary contracts, submission or non-submission of bids or any other actions to restrict competitiveness or to introduce cartelisation in the bidding process.
- c. The Bidder(s)/ Contractor(s) will not commit any offence under the relevant IPC/PC Act; further the Bidder(s)/ Contractor(s) will not use improperly, for purposes of competition or personal gain, or pass on to others, any information or document provided by the Principal as part of the business relationship, regarding plans, technical proposals and business details, including information contained or transmitted electronically.
- d. The Bidder(s)/Contractors(s) of foreign origin shall disclose the name and address of the Agents/representatives in India, if any. Similarly the Bidder(s)/Contractors(s) of Indian Nationality shall furnish the name and address of the foreign principals, if any. Further details as mentioned in the "Guidelines on Indian Agents of Foreign Suppliers" shall be disclosed by the Bidder(s)/Contractor(s). Further, as mentioned in the Guidelines all the payments made to the Indian agent/representative have to be in Indian Rupees only.
- e. The Bidder(s)/ Contractor(s) will, when presenting his bid, disclose any and all payments he has made, is committed to or intends to make to agents, brokers or any other intermediaries in connection with the award of the contract.

(2) The Bidder(s)/ Contractor(s) will not instigate third persons to commit offences outlined above or be an accessory to such offences.

Section 3- Disqualification from tender process and exclusion from future contracts

If the Bidder(s)/Contractor(s), before award or during execution has committed a transgression through a violation of Section 2, above or in any other form such as to put his reliability or credibility in question, the Principal is entitled to disqualify the Bidder(s)/Contractor(s) from the tender process or take action as per the procedure mentioned in the "Guidelines on Banning of business dealings".

Section 4 – Compensation for Damages

(1) If the Principal has disqualified the Bidder(s) from the tender process prior to the award according to Section 3, the Principal is entitled to demand and recover the damages equivalent to Earnest Money Deposit/ Bid Security.

(2) If the Principal has terminated the contract according to Section 3, or if the Principal is entitled to terminate the contract according to Section 3, the Principal shall be entitled to

demand and recover from the Contractor liquidated damages of the Contract value or the amount equivalent to Performance Bank Guarantee.

Section 5 – Previous Transgression

- (1) The Bidder declares that no previous transgressions occurred in the last three years with any other Bank in any country conforming to the anti-corruption approach or with any Public Sector Enterprise in India that could justify his exclusion from the tender process.
- (2) If the Bidder makes incorrect statement on this subject, he can be disqualified from the tender process or action can be taken as per the procedure mentioned in “Guidelines on Banning of business dealings”.

Section 6 – Equal treatment of all Bidders / Contractors / Subcontractors

- (1) The Bidder(s)/ Contractor(s) undertake(s) to demand from his subcontractors a commitment in conformity with this Integrity Pact.
- (2) The Principal will enter into agreements with identical conditions as this one with all Bidders and Contractors.
- (3) The Principal will disqualify from the tender process all bidders who do not sign this Pact or violate its provisions.

Section 7 – Criminal charges against violating Bidder(s) / Contractor(s) / Subcontractor(s)

If the Principal obtains knowledge of conduct of a Bidder, Contractor or Subcontractor, or of an employee or a representative or an associate of a Bidder, Contractor or Subcontractor which constitutes corruption, or if the Principal has substantive suspicion in this regard, the Principal will inform the same to the Chief Vigilance Officer.

Section 8 – Independent External Monitor / Monitors

- (1) The Principal appoints competent and credible Independent External Monitor for this Pact. The task of the Monitor is to review independently and objectively, whether and to what extent the parties comply with the obligations under this agreement.
- (2) The Monitor is not subject to instructions by the representatives of the parties and performs his functions neutrally and independently. It will be obligatory for him to treat the information and documents of the Bidders/Contractors as confidential. He reports to the Chairman & Managing Director, CENTRAL BANK OF INDIA.
- (3) The Bidder(s)/Contractor(s) accepts that the Monitor has the right to access without restriction to all Project documentation of the Principal including that provided by the Contractor. The Contractor will also grant the Monitor, upon his request and demonstration of a valid interest, unrestricted and unconditional access to his project documentation. The same is applicable to Subcontractors. The Monitor is under contractual obligation to treat the information and documents of the Bidder(s)/ Contractor(s)/ Subcontractor(s) with confidentiality. In case of sub-contracting, the Principal Contractor shall take all responsibility of the adoption of Integrity Pact by the sub-contractor. In case of sub-



contracting, the Principal Contractor shall take the responsibility of the adoption of the Integrity Pact by the sub-contractor.

(4) The Principal will provide to the Monitor sufficient information about all meetings among the parties related to the Project provided such meetings could have an impact on the contractual relations between the Principal and the Contractor. The parties offer to the Monitor the option to participate in such meetings.

(5) As soon as the Monitor notices, or believes to notice, a violation of this agreement, he will so inform the Management of the Principal and request the Management to discontinue or take corrective action, or to take other relevant action. The monitor can in this regard submit nonbinding recommendations. Beyond this, the Monitor has no right to demand from the parties that they act in a specific manner, refrain from action or tolerate action. Parties to this agreement agree that they shall not approach the courts while representing the matter to IEM and will await IEM's decision in the matter. Parties to this agreement agree that they shall not approach the courts while representing the matter to IEM and will await IEM's decision in the matter.

(6) The Monitor will submit a written report to the Chairman & Managing Director, CENTRAL BANK OF INDIA within 8 to 10 weeks from the date of reference or intimation to him by the Principal and, should the occasion arise, submit proposals for correcting problematic situations.

(7) If the Monitor has reported to the Chairman & Managing Director CENTRAL BANK OF INDIA, a substantiated suspicion of an offence under relevant IPC/ PC Act, and the Chairman & Managing Director CENTRAL BANK OF INDIA has not, within the reasonable time taken visible action to proceed against such offence or reported it to the Chief Vigilance Officer, the Monitor may also transmit this information directly to the Central Vigilance Commissioner.

(8) The word „Monitor“ would include both singular and plural.

Section 9 – Pact Duration

This Pact begins when both parties have legally signed it. It expires for the Contractor 12 months after the last payment under the contract, and for all other Bidders 6 months after the contract has been awarded.

If any claim is made / lodged during this time, the same shall be binding and continue to be valid despite the lapse of this pact as specified above, unless it is discharged / determined by Chairman & Managing Director of CENTRAL BANK OF INDIA.

Section 10 – Other provisions

(1) This agreement is subject to Indian Law. Place of performance and jurisdiction is the Registered Office of the Principal, i.e. Mumbai.

(2) Changes and supplements as well as termination notices need to be made in writing. Side agreements have not been made.

(3) If the Contractor is a partnership or a consortium, this agreement must be signed by all partners or consortium members.

(4) Should one or several provisions of this agreement turn out to be invalid, the remainder of this agreement remains valid. In this case, the parties will strive to come to an agreement to their original intentions.

(5) In the event of any contradiction between the Integrity Pact and its Annexure, the Clause in the Integrity Pact will prevail.”

Section 11- FALL CLAUSE

11.1. The BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER undertakes that it has not supplied/is not supplying same/exact product/systems or subsystems/services (i.e. same scope, deliverables, timelines, SLAs & pricing terms) at a price lower than that offered in the present bid to any other Bank or PSU or Government Department or to any other organization/entity whether or not constituted under any law and if it is found at any stage that similar product/systems or sub systems/services was supplied by the BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER to any other Bank or PSU or Government Department or to any other organization/entity whether or not constituted under any law, at a lower price, then that very price, with due allowance for elapsed time, will be applicable to the present case and the difference in the cost would be refunded by the BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER to the BUYER, if the contract has already been concluded.

| Signed, Sealed and Delivered for the Principal | Signed, Sealed and Delivered for the Bidder |
|---|--|
| Signature: _____ | Signature: _____ |
| Name: _____ | Name: _____ |
| Designation: _____ | Designation: _____ |
| Address: _____ | Address: _____ |
| Company: _____ | Company: _____ |
| Date: _____ | Date: _____ |
| Company Seal | Company Seal |
| Witness I | Witness II |
| Signature: _____ | Signature: _____ |
| Name: _____ | Name: _____ |
| Designation: _____ | Designation: _____ |
| Address: _____ | Address: _____ |
| Company: _____ | Company: _____ |



सेन्ट्रल बैंक ऑफ़ इंडिया
Central Bank of India

1911 से आपके लिए "केन्द्रीय" "CENTRAL" TO YOU SINCE 1911

**RFP for Supply, Implementation & Management of Next-
Generation Security Operations Centre (NG-SOC) Solutions
Central Bank of India – Tender No – GEM/2025/B/6180729**

Date: _____

Date: _____

64. ANNEXURE 9: NON-DISCLOSURE AGREEMENT

This Agreement made at _____, on this _____ day of _____ 2025

Between

_____ a company incorporated under the Companies Act, 1956/2013 having its registered office at _____ (hereinafter referred to as “-----” which expression unless repugnant to the context or meaning thereof be deemed to include its successors and assigns) of the ONE PART;

AND

CENTRAL BANK OF INDIA, a body corporate constituted under the Banking Companies (Acquisition & Transfer of Undertakings) Act, 1970 and having its head Office at Central Office, Chander Mukhi, Nariman Point, Mumbai – 400 021 (hereinafter referred to as “BANK” which expression unless repugnant to the context or meaning thereof be deemed to include its successors and assigns) of the OTHER PART

Thebidder and BANK are hereinafter individually referred to as party and collectively referred to as “the Parties”. Either of the parties which discloses or receives the confidential information is respectively referred to herein as Disclosing Party and Receiving Party.

WHEREAS:

The Parties intend to engage in discussions and negotiations concerning the establishment of a business relationship between them. In the course of such discussions and negotiations, it is anticipated that both the parties may disclose or deliver to either of the Parties certain or some of its trade secrets or confidential or proprietary information, for the purpose of enabling the other party to evaluate the feasibility of such business relationship (hereinafter referred to as “the Purpose”).

NOW, THEREFORE, THIS AGREEMENT WITNESSETH AND IT IS HEREBY AGREED BY AND BETWEEN THE PARTIES HERETO AS FOLLOWS:

1. Confidential Information

“Confidential Information” means all information disclosed/ furnished by either of the parties to another Party in connection with the business transacted/to be transacted between the Parties and/or in the course of discussions and negotiations between them in connection with the Purpose. Confidential Information shall include customer data, any copy, abstract, extract, sample, note or module thereof.

Either of the Parties may use the Confidential Information solely for and in connection with the Purpose.

Notwithstanding the foregoing, “Confidential Information” shall not include any information which the Receiving Party can show: (a) is now or subsequently becomes legally and publicly available without breach of this Agreement by the Receiving Party, (b) was rightfully in the possession of the Receiving Party without any obligation of confidentiality prior to receiving

it from the Disclosing Party, (c) was rightfully obtained by the Receiving Party from a source other than the Disclosing Party without any obligation of confidentiality, or (d) was developed by or for the Receiving Party independently and without reference to any Confidential Information and such independent development can be shown by documentary evidence.

2. Non-Disclosure

The Receiving Party shall not commercially use or disclose any Confidential Information or any materials derived there from to any other person or entity other than persons in the direct employment of the Receiving Party who have a need to have access to and knowledge of the Confidential Information solely for the Purpose authorized above. The Receiving Party may disclose Confidential Information to its employees, consultants, auditors, sub-contractors ("Representatives") consultants only if such representatives has executed a Non-disclosure Agreement with the Receiving Party that contains terms and conditions that are no less restrictive than these. The Receiving Party shall take appropriate measures by instruction and written agreement prior to disclosure to such employees to assure against unauthorized use or disclosure. The Receiving Party agrees to notify the Disclosing Party immediately if it learns of any use or disclosure of the Disclosing Party's Confidential Information in violation of the terms of this Agreement. Further, any breach of non-disclosure obligations by such employees or consultants shall be deemed to be a breach of this Agreement by the Receiving Party and the Receiving Party shall be accordingly liable therefor.

Provided that the Receiving Party may disclose Confidential information to a court or governmental agency pursuant to an order of such court or governmental agency as so required by such order, provided that the Receiving Party shall, unless prohibited by law or regulation, promptly notify the Disclosing Party of such order and afford the Disclosing Party the opportunity to seek appropriate protective order relating to such disclosure.

3. Publications

Neither Party shall make news releases, public announcements, give interviews, issue or publish advertisements or publicize in any other manner whatsoever in connection with this Agreement, the contents / provisions thereof, other information relating to this Agreement, the Purpose, the Confidential Information or other matter of this Agreement, without the prior written approval of the other Party.

4. Term

This Agreement shall be effective from the date hereof and shall continue till establishment of business relationship between the Parties and execution of definitive agreements thereafter. Upon expiration or termination as contemplated herein the Receiving Party shall immediately cease rights to any and all disclosures or uses of Confidential Information; and at the request of the Disclosing Party, the Receiving Party shall promptly return or destroy all written, graphic or other tangible forms of the Confidential Information and all copies, abstracts, extracts, samples, notes or modules thereof.

Notwithstanding anything to the contrary contained herein, the confidential information shall continue to remain confidential until it reaches the public domain in the normal course.

5. Title & Proprietary Rights

Notwithstanding the disclosure of any Confidential Information by the Disclosing Party to the Receiving Party, the Disclosing Party shall retain title and all intellectual property and proprietary rights in the Confidential Information. No license under any trademark, patent or copyright, or application for same which are now or thereafter may be obtained by such Party is either granted or implied by the conveying of Confidential Information. The Receiving Party shall not conceal, alter, obliterate, mutilate, deface or otherwise interfere with any trademark, trademark notice, copyright notice, confidentiality notice or any notice of any other proprietary right of the Disclosing Party on any copy of the Confidential Information, and shall reproduce any such mark or notice on all copies of such Confidential Information. Likewise, the Receiving Party shall not add or emboss its own or any other any mark, symbol or logo on such Confidential Information.

6. Return of Confidential Information

Upon written demand of the Disclosing Party, the Receiving Party shall (i) cease using the Confidential Information, (ii) return the Confidential Information and all copies, abstract, extracts, samples, notes or modules thereof to the Disclosing Party within seven (7) days after receipt of notice, and (iii) upon request of the Disclosing Party, certify in writing that the Receiving Party has complied with the obligations set forth in this paragraph. The obligation under this clause will not apply where it is necessary to retain any confidential information for the purpose as required by the law or for internal auditing purposes or electronic data stored due to automatic archiving or backup procedures.

7. Remedies

The Receiving Party acknowledges that if the Receiving Party fails to comply with any of its obligations hereunder, the Disclosing Party may suffer immediate, irreparable harm for which monetary damages may not be adequate. The Receiving Party agrees that, in addition to all other remedies provided at law or in equity, the Disclosing Party shall be entitled to injunctive relief hereunder.

8. Entire Agreement, Amendment and Assignment

This Agreement constitutes the entire agreement between the parties relating to the matters discussed herein and supersedes any and all prior oral discussions and/or written correspondence or agreements between the parties. This Agreement may be amended or modified only with the mutual written consent of the parties. Neither this Agreement nor any right granted hereunder shall be assignable or otherwise transferable.

9. Governing Law and Jurisdiction

The provisions of this Agreement shall be governed by the laws of India. The disputes, if any, arising out of this Agreement shall be submitted to the jurisdiction of the courts/tribunals in Mumbai.

10. General

The Receiving Party shall not reverse-engineer, decompile, disassemble or otherwise interfere with any software disclosed hereunder. All Confidential Information is provided “as is”. In no event shall the Disclosing Party be liable for the inaccuracy or incompleteness of the Confidential Information. None of the Confidential Information disclosed by the parties constitutes any representation, warranty, assurance, guarantee or inducement by either party to the other with respect to the fitness of such Confidential Information for any particular purpose or infringement of trademarks, patents, copyrights or any right of third persons.

11. Indemnity

The receiving party should indemnify and keep indemnified, saved, defended, harmless against any loss, damage, costs etc. incurred and / or suffered by the disclosing party arising out of breach of confidentiality obligations under this agreement by the receiving party, its officers, employees, agents or consultants.

In WITNESS THEREOF, the Parties hereto have executed these presents the day, month and year first hereinabove written:

| Signed, Sealed and Delivered for the Principal | Signed, Sealed and Delivered for the Bidder |
|---|--|
| Signature: _____ | Signature: _____ |
| Name: _____ | Name: _____ |
| Designation: _____ | Designation: _____ |
| Address: _____ | Address: _____ |
| Company: _____ | Company: _____ |
| Date: _____ | Date: _____ |
| Company Seal | Company Seal |
| Witness I | Witness II |
| Signature: _____ | Signature: _____ |
| Name: _____ | Name: _____ |
| Designation: _____ | Designation: _____ |
| Address: _____ | Address: _____ |
| Company: _____ | Company: _____ |
| Date: _____ | Date: _____ |



65. ANNEXURE 10: PERFORMANCE BANK GUARANTEE

To,

Central Bank of India

Mumbai

In consideration of Central Bank of India having Registered Office at Chandermukhi Building, Nariman Point, Mumbai 400 021 (hereinafter referred to as “Purchaser”) having agreed to purchase of software, hardware & other components & services (hereinafter referred to as “Goods”) from M/s ----- (hereinafter referred to as “Contractor”) on the terms and conditions contained in their agreement/purchase order No----- dt.----- (hereinafter referred to as the “Contract”) subject to the contractor furnishing a Bank Guarantee to the purchaser as to the due performance of the computer hardware, as per the terms and conditions of the said contract, to be supplied by the contractor and also guaranteeing the maintenance, by the contractor, of the computer hardware and systems as per the terms and conditions of the said contract;

1) We, ----- (Bank) (hereinafter called “the Bank”), in consideration of the premises and at the request of the contractor, do hereby guarantee and undertake to pay to the purchaser, forthwith on mere demand and without any demur, at any time up to ----- any money or moneys not exceeding a total sum of Rs------(Rupees-----only) as may be claimed by the purchaser to be due from the contractor by way of loss or damage caused to or that would be caused to or suffered by the purchaser by reason of failure of computer hardware to perform as per the said contract, and also failure of the contractor to maintain the computer hardware and systems as per the terms and conditions of the said contract.

2) Notwithstanding anything to the contrary, the decision of the purchaser as to whether computer hardware has failed to perform as per the said contract, and also as to whether the contractor has failed to maintain the computer hardware and systems as per the terms and conditions of the said contract will be final and binding on the Bank and the Bank shall not be entitled to ask the purchaser to establish its claim or claims under this Guarantee but shall pay the same to the purchaser forthwith on mere demand without any demur, reservation, recourse, contest or protest and/or without any reference to the contractor. Any such demand made by the purchaser on the Bank shall be conclusive and binding notwithstanding any difference between the purchaser and the contractor or any dispute pending before any Court, Tribunal, Arbitrator or any other authority.

3) This Guarantee shall expire on -----; without prejudice to the purchaser’s claim or claims demanded from or otherwise notified to the Bank in writing on or before the said date i.e. ----- (this date should be date of expiry of Guarantee).

4) The Bank further undertakes not to revoke this Guarantee during its currency except with the previous consent of the purchaser in writing and this Guarantee shall continue to be enforceable till the aforesaid date of expiry or the last date of the extended period of expiry of



Guarantee agreed upon by all the parties to this Guarantee, as the case may be, unless during the currency of this Guarantee all the dues of the purchaser under or by virtue of the said contract have been duly paid and its claims satisfied or discharged or the purchaser certifies that the terms and conditions of the said contract have been fully carried out by the contractor and accordingly discharges the Guarantee.

5) In order to give full effect to the Guarantee herein contained, you shall be entitled to act as if we are your principal debtors in respect of all your claims against the contractor hereby Guaranteed by us as aforesaid and we hereby expressly waive all our rights of surety ship and other rights if any which are in any way inconsistent with the above or any other provisions of this Guarantee.

6) The Bank agrees with the purchaser that the purchaser shall have the fullest liberty without affecting in any manner the Bank's obligations under this Guarantee to extend the time of performance by the contractor from time to time or to postpone for any time or from time to time any of the rights or powers exercisable by the purchaser against the contractor and either to enforce or forbear to enforce any of the terms and conditions of the said contract, and the Bank shall not be released from its liability for the reasons of any such extensions being granted to the contractor for any forbearance, act or omission on the part of the purchaser or any other indulgence shown by the purchaser or by any other matter or thing whatsoever which under the law relating to sureties would, but for this provision have the effect of so relieving the Bank.

7) The Guarantee shall not be affected by any change in the constitution of the contractor or the Bank nor shall it be affected by any change in the constitution of the purchaser by any amalgamation or absorption or with the contractor, Bank or the purchaser, but will ensure for and be available to and enforceable by the absorbing or amalgamated company or concern.

8) This guarantee and the powers and provisions herein contained are in addition to and not by way of limitation or in substitution of any other guarantee or guarantees heretofore issued by us (whether singly or jointly with other banks) on behalf of the contractor heretofore mentioned for the same contract referred to heretofore and also for the same purpose for which this guarantee is issued, and now existing un-cancelled and we further mention that this guarantee is not intended to and shall not revoke or limit such guarantee or guarantees heretofore issued by us on behalf of the contractor heretofore mentioned for the same contract referred to heretofore and for the same purpose for which this guarantee is issued.

9) Any notice by way of demand or otherwise under this guarantee may be sent by special courier, telex, fax or registered post to our local address as mentioned in this guarantee.

10) Notwithstanding anything contained herein:-

i) Our liability under this Bank Guarantee shall not exceed ₹------(Rupees-----only);

ii) This Bank Guarantee shall be valid up to -----;(date of expiry of PBG) and

iii) We are liable to pay the Guaranteed amount or any part thereof under this Bank Guarantee only and only if you serve upon us a written claim or demand on or before--- ----- (date of expiry of Guarantee plus claim period , if any)



सेंट्रल बैंक ऑफ़ इंडिया
Central Bank of India

1911 से आपके लिए "सेंट्रल" "CENTRAL" TO YOU SINCE 1911

**RFP for Supply, Implementation & Management of Next-
Generation Security Operations Centre (NG-SOC) Solutions
Central Bank of India – Tender No – GEM/2025/B/6180729**

iv) All your rights to bring legal action under this guarantee shall extinguish on..... (date one year from the date mentioned in point no. iii above)

11) The Bank has power to issue this Guarantee under the statute/constitution and the undersigned has full power to sign this Guarantee on behalf of the Bank.

Date this ----- day of ----- 2025 at -----

For and on behalf of ----- Bank.

sd/- -----

66. ANNEXURE 11: BID SECURITY (EARNEST MONEY DEPOSIT)

To,

General Manager-IT
Central Bank of India,
DIT, 1st Floor,
CBD Belapur,
Navi Mumbai -400 614

Dear Sir,

In response to your invitation to respond to your RFP for Supply, Implementation and Management of Next-Generation Security Operations Centre (NG-SOC) Solutions, M/s _____ having their registered office at _____ (hereinafter called the “Bidder”) wishes to respond to the said Request for Proposal (RFP) and submit the proposal for as listed in the RFP document.

Whereas the “Bidder” has submitted the proposal in response to RFP, we, the _____ Bank having our head office _____ hereby irrevocably guarantee an amount of ₹ _____/- (Rupees _____ Only) as bid security as required to be submitted by the, “Bidder” as a condition for participation in the said process of RFQ.

The Bid security for which this guarantee is given is liable to be enforced/ invoked:

1. If the Bidder withdraws his proposal during the period of the proposal validity; or
2. If the Bidder, having been notified of the acceptance of its proposal by the Bank during the period of the validity of the proposal fails or refuses to enter into the contract in accordance with the Terms and Conditions of the RFP or the terms and conditions mutually agreed subsequently. We undertake to pay immediately on demand to Central Bank of India the said amount without any reservation, protest, demur, or recourse. The said guarantee is liable to be invoked/ enforced on the happening of the contingencies as mentioned above and also in the RFP document and we shall pay the amount on any Demand made by Central Bank of India which shall be conclusive and binding on us irrespective of any dispute or difference raised by the Bidder.

Notwithstanding anything contained herein:

1. Our liability under this Bank guarantee shall not exceed ₹ _____/- (Rupees _____ Only)
2. This Bank guarantee will be valid up to _____; and
3. We are liable to pay the guarantee amount or any part thereof under this Bank Guarantee only upon service of a written claim or demand by you on or before _____ (date of expiry of Guarantee plus claim period, if any)
4. All your rights to bring legal action under this guarantee shall extinguish on..... (date one year from the date mentioned in point no. iii above)

In witness whereof the Bank, through the authorized officer has sets its hand and stamp on this _____day of _____ at .

Yours faithfully,

For and on behalf of _____

Bank Authorised Official



सेंट्रल बैंक ऑफ़ इंडिया
Central Bank of India

1911 से आपके लिए "केन्द्रीय" "CENTRAL" TO YOU SINCE 1911

**RFP for Supply, Implementation & Management of Next-
Generation Security Operations Centre (NG-SOC) Solutions
Central Bank of India – Tender No – GEM/2025/B/6180729**

67. ANNEXURE 12: BIDDER'S PARTICULARS

| # | Particulars | |
|----|--|---|
| 1. | Name of the Bidder | |
| 2. | Address with E mail id, Mobile no. and Pin code | |
| 3. | GST Number | |
| 4. | Bank Details | |
| 5. | PAN Number | |
| 6. | Name of Authorised Person Mobile No: Landline No: | |
| 7. | i. Email ID ii. Alternative Email ID | |
| 8. | Details of EMD | BG/UTR/Reference No. date & Amount |
| 9. | Exemption Certificate details (if applicable). Eg: MSE etc. | Please upload copy of the same along with details |

Signature

Name:

Designation:

Seal of Company

Date:

68. ANNEXURE 13: NPA UNDERTAKING

Pro forma of letter to be given by all the bidders participating in RFP for Supply, Implementation & Management of Next-Generation Security Operations Centre (NG-SOC) Solutions on their official letter-head

Date:

To,
General Manager-IT,
Central Bank of India, Central Office,
Sector 11, CBD Belapur,
Navi Mumbai - 400614
Sir,

Sub: RFP for Supply, Implementation & Management of Next-Generation Security Operations Centre (NG-SOC) Solutions

Tender No. GEM/2025/B/6180729

We _____(bidder name), hereby undertake that-

- We have not have been declared NPA by any Bank in India.
- Further, we do not have any pending case with any organization across the globe which affects our credibility to service the bank.

Yours faithfully,

Authorised Signatory

Designation

Bidder's corporate name

69. ANNEXURE 14: UNDERTAKING LETTER (LAND BORDER SHARING)

Pro forma of letter to be given by all the bidders participating in RFP for Supply, Implementation & Management of Next-Generation Security Operations Centre (NG-SOC) Solutions on their official letter-head

To

Date:

General Manager –IT,
Central Bank of India, Central Office,
Sector 11,
CBD Belapur,
Navi Mumbai – 400614

Sir,

Sub: RFP for Supply, Implementation & Management of Next-Generation Security Operations Centre (NG-SOC) Solutions

Tender No. GEM/2025/B/6180729

Dear Sir/Madam,

We, M/s_____ are a private/ public limited company/ LLP/ firm <strike off whichever is not applicable> incorporated under the provisions of the Companies Act, 1956/2013, Limited Liability Partnership Act 2008/ Indian Partnership Act 1932, having our registered office at _____ (referred to as the “Bidder”) are desirous of participating in the Tender Process in response to our captioned RFP and in this connection we hereby declare, confirm and agree as follows:

We, the Bidder have read and understood the contents of the RFP and Office Memorandum & the Order (Public Procurement No.1) both bearing no.F.No.6/18/2019/PPD of 23rd July 2020 issued by Ministry of Finance, Government of India on insertion of Rule 144 (xi) in the General Financial Rules (GFRs) 2017 and the amendments & clarifications thereto, regarding restrictions on availing/ procurement of goods and services, of any Bidder from a country which shares a land border with India and/ or sub-contracting to contractors from such countries.

In terms of the above and after having gone through the said amendments including in particular the words defined therein (which shall have the same meaning for the purpose of this Declaration cum Undertaking), we, the Bidder hereby declare and confirm that:

Strike off whichever is not applicable

1. "I/we have read the clause regarding restrictions on procurement from a bidder of the country which shares a land border with India; I/ we certify that _____ is not from such a country.
2. "I/we have read the clause regarding restrictions on procurement from a Bidder of a country which shares a land border with India; I/we certify that _____ is from such a country. I hereby certify that _____ fulfils all requirements in this regard and is eligible to be considered. [Valid registration by the Competent Authority is attached]"

Further, in case the work awarded to us, I/we undertake that I/we shall not subcontract any of assigned work under this engagement without the prior permission of Bank.

Further, we undertake that I/we have read the clause regarding restrictions on procurement from a bidder of a country which shares a land border with India and on sub-contracting to contractors from such countries; I certify that our subcontractor is not from such a country or, if from such a country, has been registered with the Competent Authority and will not subcontract any work to a contractor from such countries unless such contractor is registered with the Competent Authority. I hereby certify that our sub-contractor fulfils all requirements in this regard and is eligible to be considered. [Valid registration by the Competent Authority]"

We, hereby confirm that we fulfil all the eligibility criteria as per the office memorandum/ order mentioned above and RFP and we are eligible to participate in the Tender process. We also agree and accept that if our declaration and confirmation is found to be false at any point of time including after awarding the contract, Bank shall be within its rights to forthwith terminate the contract/ bid without notice to us and initiate such action including legal action in accordance with law. Bank shall also be within its right to forfeit the security deposits/ earnest money provided by us and also recover from us the loss and damages sustained by the Bank on account of the above.

This declaration cum Undertaking is executed by us through our Authorized signatory/ ies after having read and understood the Office Memorandum and Order including the words defined in the said order.

Dated this _____ by _____ 20__

Yours faithfully,

Authorized Signatory

Name:

Designation:

Bidder's Corporate Name:

Address:

Email & Phone No.:



सेंट्रल बैंक ऑफ़ इंडिया
Central Bank of India

1911 से आपके लिए "केन्द्रीय" "CENTRAL" TO YOU SINCE 1911

**RFP for Supply, Implementation & Management of Next-
Generation Security Operations Centre (NG-SOC) Solutions
Central Bank of India – Tender No – GEM/2025/B/6180729**

List of documents enclosed:

1. Copy of Certificate of valid registration with the Competent Authority (strike off if not applicable)
2. _____
3. _____
4. _____

70. ANNEXURE 15: COVER LETTER

Date:

To

General Manager-IT
DIT, Central Bank of India, Central Office,
Sector 11, CBD Belapur,
Mumbai - 400614

Sub: RFP for Supply, Implementation & Management of Next-Generation Security Operations Centre (NG-SOC) Solutions

Tender No. GEM/2025/B/6180729

Dear Sir/Madam,

1. Having examined the Scope Documents including all Annexures, the receipt of which is hereby duly acknowledged, we, the undersigned offer to supply, deliver, install and maintain all the items mentioned in the 'Request for Proposal' and the other schedules of requirements and services for your bank in conformity with the said Scope Documents in accordance with the schedule of Prices indicated in the Price Bid and made part of this Scope.
2. If our Bid is accepted, we undertake to abide by all terms and conditions of this Scope and also to comply with the delivery schedule as mentioned in the Scope Document.
3. We agree to abide by this bid Offer for 120 days from date of bid (Commercial Bid) opening and our Offer shall remain binding on us which may be accepted by the Bank any time before expiry of the offer.
4. This Bid, together with your written acceptance thereof and your notification of award, shall constitute a binding Contract between us.
5. We undertake that in competing for and if the award is made to us, in executing the subject Contract, we will strictly observe the laws against fraud and corruption in force in India namely "Prevention of Corruption Act 1988".
6. We certify that we have provided all the information requested by the bank in the format prescribed for. We also understand that the bank has the exclusive right to reject this offer in case the bank is of the opinion that the required information is not provided or is provided in a different format.

Authorised Signatory

(Name: Contact Person, Phone No., Fax, E-mail)

(This letter should be on the letterhead of the Bidder duly signed by an authorized signatory)



सेंट्रल बैंक ऑफ़ इंडिया
Central Bank of India

1911 से आपके लिए "केन्द्रीय" "CENTRAL" TO YOU SINCE 1911

RFP for Supply, Implementation & Management of Next-Generation Security Operations Centre (NG-SOC) Solutions
Central Bank of India – Tender No – GEM/2025/B/6180729

71. ANNEXURE 16: PRE-BID QUERY FORMAT

Queries:

| Sr. No. | Page # | Point / Section # | Query | Banks Response (Bidder Should not fill in this column) |
|---------|--------|-------------------|-------|--|
| 1 | | | | |
| 2 | | | | |
| 3 | | | | |
| 4 | | | | |
| 5 | | | | |
| 6 | | | | |
| 7 | | | | |
| 8 | | | | |
| 9 | | | | |

Date:

Authorised Signatory & Stamp

(Name: Contact Person, Phone No., Fax, E-mail)



72. ANNEXURE 17: ELIGIBILITY CRITERIA COMPLIANCE

Bidder needs to comply with the eligibility criterion mentioned below. Non-compliance with any of these criteria would result in outright rejection of bidder's proposal. Bidder is expected to provide proof for each of the points for eligibility evaluation criteria. Any credential detail not accompanied by required relevant proof documents will not be considered for evaluation. All credential letters should be appropriately bound, labeled and segregated in the respective areas. There is no restriction on the number of credentials a bidder can provide.

The decision of Bank pertaining to Eligibility Criteria evaluation would be final and binding on all the bidders. Bank may accept or reject an offer without assigning any reason whatsoever.

The Bidder must fulfil following eligibility criteria

| # | Eligibility of the Bidder | Documents to be submitted | Compliance (Y/N) |
|---|--|--|------------------|
| 1 | Bidder should be a Registered company under Indian Companies Act. 1956/2013 or LLP/Partnership firm and should have been in existence for a minimum period of 5 years in India, as on date of submission of RFP. | Copy of the Certificate of Incorporation issued by Registrar of Companies/Registrar of firms and full address of the registered office of the bidder | |
| 2 | Bidder should be registered under G.S.T and/or tax registration in state where bidder has a registered office. | Proof of registration with GSTIN | |
| 3 | The bidder must have minimum annual turnover in India of Rs. 300 crores per annum in the last three financial years (i.e., 2021-22, 2022-23, 2023-24) of individual company and not as group of companies. | Copy of Audited Balance Sheet and Copy of Certificate of the Chartered Accountant for the last three financial years (i.e., 2021-22, 2022-23, 2023-24) | |
| 4 | The bidder should have made operating profits in at least two financial years out of last three financial years (i.e., 2021-22, 2022-23, 2023-24). | Copy of Audited Balance Sheet and Copy of Certificate of the Chartered Accountant for the last three financial years (i.e., 2021-22, 2022-23, 2023-24) | |
| 5 | The bidder should have a positive net worth in last three financial years (i.e., 2021-22, 2022-23, 2023-24) | Copy of Audited Balance Sheet and Copy of Certificate of | |



| # | Eligibility of the Bidder | Documents to be submitted | Compliance (Y/N) |
|----|---|--|------------------|
| | | the Chartered Accountant for the last three financial years (i.e., 2021-22, 2022-23, 2023-24) | |
| 6 | At the time of bidding, the Bidder should not have been blacklisted/debarred/ by any Govt. / IBA/RBI/PSU /PSE/ or Banks, Financial institutes for any reason including non-implementation/delivery of the order. Self-declaration to that effect should be submitted along with the technical bid. | Submit the undertaking on Company's letter head | |
| 7 | At the time of bidding, there should not have been any pending litigation or any legal dispute in the last five years, before any court of law between the Bidder or OEM and the Bank regarding supply of goods/services. | Submit the undertaking self-declaration on Company's letter head | |
| 8 | Bidder/OEM should not have <ul style="list-style-type: none"> NPA with any Bank /financial institutions in India Any case pending or otherwise, with any organization across the globe which affects the credibility of the Bidder in the opinion of Central Bank of India to service the needs of the Bank | Submit self-declaration on Company's letter head. | |
| 9 | Bidder should have service/support centre or should have arrangement for providing support in Mumbai and Hyderabad. | Submit the undertaking self-declaration on Bidder's letter head | |
| 10 | If the bidder is from a country which shares a land border with India, the bidder should be registered with the Competent Authority. | Certified copy of the registration certificate | |
| 11 | The Bidder should have implemented and managed SOC with on-premises SIEM solution with minimum 30000 Events Per Second (EPS) or 1TB / Day in at least one BFSI*/RBI/NPCI/BSE/NSE/SEBI/Govt./PSU in India. | Letter of acceptance (LoA)/ purchase order/ work order/ contract/ completion certificate Deployment Certificate issued by client to the bidder/Particulars | |



| # | Eligibility of the Bidder | Documents to be submitted | Compliance (Y/N) |
|----|--|---|------------------|
| | (*BFSI must be an organization having minimum of 1000 branches/ offices in India) | confirming relevant experience. | |
| 12 | The bidder shall have minimum 100 skilled resources on the payroll in India in the following areas (Subject Matter Expert): g. Network Security h. Data Security i. Application Security j. Cloud Security k. Vulnerability Management l. Infrastructure Management | List of resources with following details to be provided on company letter head: Name Designation Years of experience | |
| 13 | The proposed OEM's SIEM solution must have been implemented with minimum 60,000 Events Per Second (EPS) or 2 TB/Day in at least two BFSI*/RBI/NPCI/BSE/NSE/SEBI/ Govt./PSU in India during the last seven years. (*BFSI must be an organization having minimum of 1000 branches/ offices in India) | Copies of Completion Certificate/ reference letter/E-Mail from client /copy of purchase order /contract agreement /work order /engagement letter. | |
| 14 | The proposed OEM's UEBA solution must have been implemented in at least One BFSI*/RBI/NPCI/BSE/NSE/SEBI/Govt./ PSU in India) during the last seven years. (*BFSI must be an organization having minimum of 1000 branches/ offices in India) | Copies of Completion Certificate/ reference letter/E-Mail from client /copy of purchase order /contract agreement /work order /engagement letter. | |

Authorised Signatory

(Name: Contact Person, Phone No., Fax, E-mail)

(This letter should be on the letterhead of the Bidder duly signed by an authorized signatory)

73. ANNEXURE 18 – SELF DECLARATION FOR COMPLIANCE TO RBI MASTER DIRECTION ON OUTSOURCING OF IT SERVICES

(on Bidder's letterhead)

Date:

To

General Manager-IT
DIT, Central Bank of India, Central Office,
Sector 11, CBD Belapur,
Mumbai - 400614

Sub: RFP for Supply, Implementation & Management of Next-Generation Security Operations Centre (NG-SOC) Solutions

Tender No. GEM/2025/B/6180729

We, M/s_____ hereby state that we have gone through the RBI Master Circular: RBI/2023-24/102 DoS.CO.CSITTEG/SEC.1/31.01.015/2023-24 dated 10.04.2023 and subsequent circular/guidelines regarding Master Direction on Outsourcing of Information Technology Services and we hereby state that we comply to all the directions and clauses as stated in the aforesaid circular. We along with the resources deployed by us and services provided by us, will also ensure compliance of all the clauses and directions of the aforesaid circular throughout the period of the contract.

Date: _____

Place: _____

Authorised Signatory & Stamp

(Name: Contact Person, Phone No., Fax, E-mail)



74. ANNEXURE 19: GOI GUIDELINES FOR PREFERENCE TO MAKE IN INDIA

Government has issued Public Procurement (Preference to Make in India) [PPP-MII] Order 2017 vide the Department for Promotion of Industry and Internal Trade (DPIIT) Order No.P45021/2/2017-B.E.-II dated 15.06.2017 and subsequent revisions vide Order No. 45021/2/2017-PP(BE-II) dated 16-9-2020 to encourage 'Make in India' and to promote manufacturing and production of goods, services and works in India with a view to enhancing income and employment.

It is clarified that for all intents and purposes, the latest revised order i.e. the order dated 16-9-2020 shall be applicable being revised Order of the original order i.e. Public Procurement (Preference to Make in India) [PPP-MII] Order 2017 dated 15-6-2017.

The salient features of the aforesaid Order are as under:

- 1) Class-I Local supplier - a supplier or service provider, whose goods, services or works offered for procurement, has local content equal to or more than 50%.
- 2) Class-II Local supplier - a supplier or service provider, whose goods, services or works offered for procurement, has local content equal to or more than 20% but less than 50%.
- 3) Non-Local supplier - a supplier or service provider, whose goods, services or works offered for procurement, has local content less than or equal to 20%.
- 4) The margin of purchase preference shall be 20 %., Margin of purchase preference means the maximum extent to which the price quoted by a local supplier may be above the L1 for the purpose of purchase preference.
- 5) "Minimum Local content" for the purpose of this RFP, the 'local content' requirement to categorize a supplier as 'Class-I local supplier' is minimum 50%. For 'Class-II local supplier', the 'local content' requirement is minimum 20%. If Nodal Ministry/Department has prescribed different percentage of minimum 'local content' requirement to categorize a supplier as 'Class-I local supplier'/'Class-II local supplier', same shall be applicable.

Verification of Local contents:

The local supplier at the time of submission of bid shall be required to provide a certificate from the statutory auditor or cost auditor of the company (in the case of companies) or from a practicing cost accountant or practicing chartered accountant (in respect of suppliers other than companies) giving the percentage of local content as per Annexure 5A. Local content certificate shall be issued based upon the procedure for calculating the local content /domestic value addition on the basis of notification bearing no. F. No.33(1) /2017-IPHW dated 14-9-2017 issued by Ministry of Electronics and Information Technology read with Public Procurement (Preference to Make in India) Order 2017 Revised vide the Department for Promotion of Industry and Internal Trade (DPIIT) Order No.P-45021/2/2017-B.E.-II dated 16-09-2020.

False declaration will be in breach of the Code of Integrity under Rule 175(i)(h) of the General Financial Rules for which a bidder or its successors can be debarred for up to two years as per rule 151 of the General Financial Rules along with such other actions may be permissible under law.

A supplier who has been debarred by any procuring entity for violation of this order shall not be eligible for preference under this order for procurement by any other procuring entity for the duration of the debarments. The debarment for such other procuring entities shall take effect prospectively from the date on which it comes to the notice of other procurement entities in the manner prescribed under order No P-45021/2/2017-PP(BE- II) dated 16-092020, para 9(h).

Note:

- a) Bidder has to submit the Make in India Class-I / Class-II local supplier certificate as per attached format.
- b) Bidder has to submit proposal for all line Items.
- c) Any change in classification of Class-I and Class-II, Bidder may submit any change in class level for consideration in subsequent phases.

Purchase Preference:

1) Subject to the provisions of this Order and to any specific instructions issued by the Nodal Ministry or in pursuance of this Order, purchase preference shall be given to 'Class-I local supplier' in procurements undertaken by procuring entities in the manner specified here under,

2) In the procurements of goods or works, which are divisible in nature, the 'Class-I local supplier' shall get purchase preference over 'Class-II local supplier' as well as 'Non-local supplier', as per following procedure:

- Among all qualified bids, the lowest bid will be termed as L1. If L1 is 'Class-I local supplier', the contract for full quantity will be awarded to L1.

- If L1 bid is not a 'Class-I local supplier', 50% of the order quantity shall be awarded to L1. Thereafter, the lowest bidder among the 'Class-I local supplier' will be invited to match the L1 price for the remaining 50% quantity subject to the Class-I local supplier's quoted price falling within the margin of purchase preference, and contract for that quantity shall be awarded to such 'Class-I local supplier' subject to matching the L1 price. In case such lowest eligible 'Class-I local supplier' fails to match the L1 price or accepts less than the offered quantity, the next higher 'Class-I local supplier' within the margin of purchase preference shall be invited to match the L1 price for remaining quantity and so on, and contract shall be awarded accordingly. In case some quantity is still left uncovered on Class-I local suppliers, then such balance quantity may also be ordered on the L1 bidder.

3) In the procurements of goods or works, which are not divisible in nature, and in procurement of services where the bid is evaluated on price alone, the 'Class-I local supplier' shall get purchase preference over 'Class-II local supplier' as well as 'Non-local supplier', as per following procedure:

- Among all qualified bids, the lowest bid will be termed as L1. If L1 is 'Class-I local supplier', the contract will be awarded to L1.

- If L1 is not 'Class-I local supplier', the lowest bidder among the 'Class-I local supplier', will be invited to match the L1 price subject to Class-I local supplier's quoted price falling within the margin of purchase preference, and the contract shall be awarded to such 'Class-I local supplier' subject to matching the L1 price.

- In case such lowest eligible 'Class-I local supplier' fails to match the L1 price, the 'Class-I local supplier' with the next higher bid within the margin of purchase preference shall be invited to match the L1 price and so on and contract shall be awarded accordingly. In case none of the 'Class-I local supplier' within the margin of purchase preference matches the L1 price, the contract may be awarded to the L1 bidder.

4) “Class-2 local supplier” will not get purchase preference in any procurement, undertaken by procuring entities.

All others terms and condition are as per order no. No. P-45021/2/2017-PP (BE-II) dated: 16th September 2020.

Annexure 19A: Certificate of Local Content

(Certificate from the statutory auditor or cost auditor of the company (in case of companies) or from a practicing cost accountant or practicing chartered accountant (in respect of suppliers other than companies) giving the percentage of local content, on their letter head with Registration Number with seal)

To,
 General Manager (IT),
 Central Bank of India,
 DIT, Sector 11,
 CBD Belapur,
 Navi Mumbai – 400614

Sir,

Sub: RFP for Supply, Implementation & Management of Next-Generation Security Operations Centre (NG-SOC) Solutions

Tender No. GEM/2025/B/6180729

This is to certify that proposed (product make____ and model____) is having the local content of % as defined in the above mentioned RFP.

This certificate is submitted in reference to the Public Procurement (Preference to Make in India), Order 2017.

Date: _____

Place: _____

Authorised Signatory & Stamp

(Name: Contact Person, Phone No., Fax, E-mail)

75. ANNEXURE 20: GUIDELINES ON BANNING OF BUSINESS DEALING

GUIDELINES FOR INDIAN AGENTS OF FOREIGN SUPPLIERS

1.0 There shall be compulsory registration of agents for all Global (Open) Tender and Limited Tender. An agent who is not registered with CENTRAL BANK OF INDIA shall apply for registration in the prescribed Application –Form.

1.1 Registered agents will file an authenticated Photostat copy duly attested by a Notary Public/Original certificate of the principal confirming the agency agreement and giving the status being enjoyed by the agent and the commission/remuneration/salary/ retainer ship being paid by the principal to the agent before the placement of order by CENTRAL BANK OF INDIA.

1.2 Wherever the Indian representatives have communicated on behalf of their principals and the foreign parties have stated that they are not paying any commission to the Indian agents, and the Indian representative is working on the basis of salary or as retainer, a written declaration to this effect should be submitted by the party (i.e. Principal) before finalizing the order

2.0 DISCLOSURE OF PARTICULARS OF AGENTS/ REPRESENTATIVES IN INDIA. IF ANY.

2.1 Tenderers of Foreign nationality shall furnish the following details in their offer:

2.1.1 The name and address of the agents/representatives in India, if any and the extent of authorization and authority given to commit the Principals. In case the agent/representative be a foreign Bank, it shall be confirmed whether it is real substantial Bank and details of the same shall be furnished.

2.1.2 The amount of commission/remuneration included in the quoted price(s) for such agents/representatives in India.

2.1.3 Confirmation of the Tenderer that the commission/ remuneration if any, payable to his agents/representatives in India, may be paid by CENTRAL BANK OF INDIA in Indian Rupees only.

2.2 Tenderers of Indian Nationality shall furnish the following details in their offers:

2.2.1 The name and address of the foreign principals indicating their nationality as well as their status, i.e, whether manufacturer or agents of manufacturer holding the Letter of Authority of the Principal specifically authorizing the agent to make an offer in India in response to tender either directly or through the agents/representatives.

2.2.2 The amount of commission/remuneration included in the price (s) quoted by the Tenderer for himself.

2.2.3 Confirmation of the foreign principals of the Tenderer that the commission/remuneration, if any, reserved for the Tenderer in the quoted price (s), may be paid by CENTRAL BANK OF

INDIA in India in equivalent Indian Rupees on satisfactory completion of the Project or supplies of Stores and Spares in case of operation items .

2.3 In either case, in the event of contract materializing, the terms of payment will provide for payment of the commission /remuneration, if any payable to the agents/representatives in India in Indian Rupees on expiry of 90 days after the discharge of the obligations under the contract.

2.4 Failure to furnish correct and detailed information as called for in paragraph-2.0 above will render the concerned tender liable to rejection or in the event of a contract materializing, the same liable to termination by CENTRAL BANK OF INDIA. Besides this there would be a penalty of banning business dealings with CENTRAL BANK OF INDIA or damage or payment of a named sum.

Sr. Contents

1. Introduction
2. Scope
3. Definitions
4. Initiation of banning / suspension
5. Suspension of business dealing
6. Ground on which banning of business dealings can be initiated
7. Banning of business dealings
8. Removal from list of approved agencies –suppliers/contractors
9. Show-cause notice
10. Appeal against the competent authority
11. Review of the decision by the competent authority
12. Circulation of names of agencies with whom business dealings have been banned

1. Introduction

1.1 Central Bank of India, being a Public Sector Enterprise and ‘State’, within the meaning of Article 12 of Constitution of India, has to ensure preservation of rights enshrined in Chapter III of the Constitution. CENTRAL BANK OF INDIA has also to safeguard its commercial interests. CENTRAL BANK OF INDIA deals with Agencies, who have a very high degree of integrity, commitments and sincerity towards the work undertaken. It is not in the interest of CENTRAL BANK OF INDIA to deal with Agencies who commit deception, fraud or other misconduct in the execution of contracts awarded / orders issued to them. In order to ensure compliance with the constitutional mandate, it is incumbent on CENTRAL BANK OF INDIA to observe principles of natural justice before banning the business dealings with any Agency.

1.2 Since banning of business dealings involves civil consequences for an Agency concerned, it is incumbent that adequate opportunity of hearing is provided and the explanation, if tendered, is considered before passing any order in this regard keeping in view the facts and circumstances of the case.

2. Scope

2.1 The General Conditions of Contract (GCC) of CENTRAL BANK OF INDIA generally provide that CENTRAL BANK OF INDIA reserves its rights to remove from list of approved suppliers / contractors or to ban business dealings if any Agency has been found to have committed misconduct and also to suspend business dealings pending investigation. If such provision does not exist in any GCC, the same may be incorporated.

2.2 Similarly, in case of sale of material there is a clause to deal with the Agencies / customers / Buyers, who indulge in lifting of material in unauthorized manner. If such a stipulation does not exist in any Sale Order, the same may be incorporated.

2.3 However, absence of such a clause does not in any way restrict the right of Bank (CENTRAL BANK OF INDIA) to take action / decision under these guidelines in appropriate cases.

2.4 The procedure of (i) Removal of Agency from the List of approved suppliers / contractors; (ii) Suspension and (iii) Banning of Business Dealing with Agencies, has been laid down in these guidelines.

2.5 These guidelines apply to all the Units and subsidiaries of CENTRAL BANK OF INDIA.

2.6 It is clarified that these guidelines do not deal with the decision of the Management not to entertain any particular Agency due to its poor / inadequate performance or for any other reason.

2.7 The banning shall be with prospective effect, i.e., future business dealings.

3. Definitions

In these Guidelines, unless the context otherwise requires:

i) 'Party / Contractor / Supplier / Purchaser / Customer/Bidder/Tenderer' shall mean and include a public limited Bank or a private limited Bank, a firm whether registered or not, an individual, a cooperative society or an association or a group of persons engaged in any commerce, trade, industry, etc. 'Party / Contractor / Supplier / Purchaser / Customer/ Bidder / Tenderer' in the context of these guidelines is indicated as 'Agency'.

ii) 'Inter-connected Agency' shall mean two or more companies having any of the following features:

a) If one is a subsidiary of the other.

b) If the Director(s), Partner(s), Manager(s) or Representative(s) are common;

c) If management is common;

d) If one owns or controls the other in any manner;

iii) ‘Competent Authority’ and ‘Appellate Authority’ shall mean the following:

a) For Bank (entire CENTRAL BANK OF INDIA) wide Banning Executive Director (BSD) shall be the “Competent Authority” for the purpose of these guidelines. Chairman & Managing Director, CENTRAL BANK OF INDIA shall be the “Appellate Authority” in respect of such cases except banning of business dealings with Foreign Suppliers of imported coal/coke.

b) For banning of business dealings with Foreign Suppliers of imported goods, CENTRAL BANK OF INDIA Executive Directors’ Committee (EDC) shall be the “Competent Authority”. The Appeal against the Order passed by EDC, shall lie with Chairman & Managing Director, as First Appellate Authority.

c) In case the foreign supplier is not satisfied by the decision of the First Appellate Authority, it may approach CENTRAL BANK OF INDIA Board as Second Appellate Authority.

d) For Zonal Offices Only

Any officer not below the rank of Deputy General Manager appointed or nominated by the Head of Zonal Office shall be the “Competent Authority” for the purpose of these guidelines. The Head of the concerned Zonal Office shall be the “Appellate Authority” in all such cases.

e) For Corporate Office only

For procurement of items / award of contracts, to meet the requirement of Corporate Office only, Head of Business Support Department (BSD) shall be the “Competent Authority” and concerned Executive Director (BSD) shall be the “Appellate Authority”.

e) Managing Director & CEO, CENTRAL BANK OF INDIA shall have overall power to take suo-moto action on any information available or received by him and pass such order(s) as he may think appropriate, including modifying the order(s) passed by any authority under these guidelines.

iv) ‘Investigating Department’ shall mean any Department or Unit investigating into the conduct of the Agency and shall include the Vigilance Department, Central Bureau of Investigation, the State Police or any other department set up by the Central or State Government having powers to investigate.

v) ‘List of approved Agencies - Parties / Contractors / Suppliers / Purchasers / Customers / Bidders / Tenderers shall mean and include list of approved / registered Agencies - Parties/ Contractors / Suppliers / Purchasers / Customers / Bidders / Tenderers, etc.

4. Initiation of Banning / Suspension

Action for banning / suspension business dealings with any Agency should be initiated by the department having business dealings with them after noticing the irregularities or misconduct on their part. Besides the concerned department, Vigilance Department of each Unit /Corporate Vigilance may also be competent to advise such action.

5. Suspension of Business Dealings

5.1 If the conduct of any Agency dealing with CENTRAL BANK OF INDIA is under investigation by any department (except Foreign Suppliers of imported goods), the Competent Authority may consider whether the allegations under investigation are of a serious nature and whether pending investigation, it would be advisable to continue business dealing with the Agency. If the Competent Authority, after consideration of the matter including the recommendation of the Investigating Department, if any, decides that it would not be in the interest to continue business dealings pending investigation, it may suspend business dealings with the Agency. The order to this effect may indicate a brief of the charges under investigation. If it is decided that inter-connected Agencies would also come within the ambit of the order of suspension, the same should be specifically stated in the order. The order of suspension would operate for a period not more than six months and may be communicated to the Agency as also to the Investigating Department. The Investigating Department may ensure that their investigation is completed and whole process of final order is over within such period.

5.2 The order of suspension shall be communicated to all Departmental Heads within the Plants / Units. During the period of suspension, no business dealing may be held with the Agency.

5.3 As far as possible, the existing contract(s) with the Agency may continue unless the Competent Authority, having regard to the circumstances of the case, decides otherwise.

5.4 If the gravity of the misconduct under investigation is very serious and it would not be in the interest of CENTRAL BANK OF INDIA, as a whole, to deal with such an Agency pending investigation, the Competent Authority may send his recommendation to ED (GAD), CENTRAL BANK OF INDIA Corporate Office along with the material available. If Corporate Office considers that depending upon the gravity of the misconduct, it would not be desirable for all the Units and Subsidiaries of CENTRAL BANK OF INDIA to have any dealings with the Agency concerned, an order suspending business dealings may be issued to all the Units by the Competent Authority of the Corporate Office, copy of which may be endorsed to the Agency concerned. Such an order would operate for a period of six months from the date of issue.

5.5 For suspension of business dealings with Foreign Suppliers of imported goods, following shall be the procedure:-

- i) Suspension of the foreign suppliers shall apply throughout the Bank including Subsidiaries.
- ii) Based on the complaint forwarded by ED (BSD) or received directly by Corporate Vigilance, if gravity of the misconduct under investigation is found serious and it is felt that it would not be in the interest of CENTRAL BANK OF INDIA to continue to deal with such agency, pending investigation, Corporate Vigilance may send such recommendation on the

matter to Executive Director, BSD to place it before Executive Directors Committee (EDC) with ED (BSD) as Convener of the Committee. The committee shall expeditiously examine the report, give its comments/recommendations within twenty one days of receipt of the reference by ED, BSD.

iii) If EDC opines that it is a fit case for suspension, EDC may pass necessary orders which shall be communicated to the foreign supplier by ED, BSD.

5.6 If the Agency concerned asks for detailed reasons of suspension, the Agency may be informed that its conduct is under investigation. It is not necessary to enter into correspondence or argument with the Agency at this stage.

5.7 It is not necessary to give any show-cause notice or personal hearing to the Agency before issuing the order of suspension. However, if investigations are not complete in six months' time, the Competent Authority may extend the period of suspension by another three months, during which period the investigations must be completed.

6. Ground on which Banning of Business Dealings can be initiated

6.1 If the security consideration, including questions of loyalty of the Agency to the State, so warrant;

6.2 If the Director / Owner of the Agency, proprietor or partner of the firm, is convicted by a Court of Law for offences involving moral turpitude in relation to its business dealings with the Government or any other public sector enterprises or CENTRAL BANK OF INDIA, during the last five years;

6.3 If there is strong justification for believing that the Directors, Proprietors, Partners, owner of the Agency have been guilty of malpractices such as bribery, corruption, fraud, substitution of tenders, interpolations, etc.;

6.4 If the Agency continuously refuses to return / refund the dues of CENTRAL BANK OF INDIA without showing adequate reason and this is not due to any reasonable dispute which would attract proceedings in arbitration or Court of Law;

6.5 If the Agency employs a public servant dismissed / removed or employs a person convicted for an offence involving corruption or abetment of such offence;

6.6 If business dealings with the Agency have been banned by the Govt. or any other public sector enterprise;

6.7 If the Agency has resorted to Corrupt, fraudulent practices including misrepresentation of facts and / or fudging /forging /tampering of documents;

6.8 If the Agency uses intimidation / threatening or brings undue outside pressure on the Bank (CENTRAL BANK OF INDIA) or its official in acceptance / performances of the job under the contract;

6.9 If the Agency indulges in repeated and / or deliberate use of delay tactics in complying with contractual stipulations;

6.10 Wilful indulgence by the Agency in supplying sub-standard material irrespective of whether pre-dispatch inspection was carried out by Bank (CENTRAL BANK OF INDIA) or not;

6.11 Based on the findings of the investigation report of CBI / Police against the Agency for malafide / unlawful acts or improper conduct on his part in matters relating to the Bank (CENTRAL BANK OF INDIA) or even otherwise;

6.12 Established litigant nature of the Agency to derive undue benefit;

6.13 Continued poor performance of the Agency in several contracts;

6.14 If the Agency misuses the premises or facilities of the Bank (CENTRAL BANK OF INDIA), forcefully occupies, tampers or damages the Bank's properties including land, water resources, forests / trees, etc.

(Note: The examples given above are only illustrative and not exhaustive. The Competent Authority may decide to ban business dealing for any good and sufficient reason).

7 Banning of Business Dealings

7.1 A decision to ban business dealings with any Agency should apply throughout the Bank Including Subsidiaries.

7.2 There will be a Standing Committee in each Zone to be appointed by Head of Zonal Office for processing the cases of "Banning of Business Dealings" except for banning of business dealings with foreign suppliers of goods. However, for procurement of items / award of contracts, to meet the requirement of Corporate Office only, the committee shall be consisting of General Manager / Dy. General Manager each from Operations, Law & BSD. Member from BSD shall be the convener of the committee. The functions of the committee shall, inter-alia include:

- i) To study the report of the Investigating Agency and decide if a prima-facie case for Bank-wide / Local unit wise banning exists, if not, send back the case to the Competent Authority.
- ii) To recommend for issue of show-cause notice to the Agency by the concerned department.
- iii) To examine the reply to show-cause notice and call the Agency for personal hearing, if required.

iv) To submit final recommendation to the Competent Authority for banning or otherwise.

7.3 If Bank wide banning is contemplated by the banning Committee of any Zone, the proposal should be sent by the committee to ED (BSD) through the Head of the Zonal Office setting out the facts of the case and the justification of the action proposed along with all the relevant papers and documents. GAD shall get feedback about that agency from all other Zones and based on this feedback, a prima-facie decision for banning / or otherwise shall be taken by the Competent Authority. At this stage if it is felt by the Competent Authority that there is no

sufficient ground for Bank wide banning, then the case shall be sent back to the Head of Zonal Office for further action at the Zone level. If the prima-facie decision for Bank-wide banning has been taken, ED (BSD) shall issue a show-cause notice to the agency conveying why it should not be banned throughout CENTRAL BANK OF INDIA.

After considering the reply of the Agency and other circumstances and facts of the case, ED (BSD) will submit the case to the Competent Authority to take a final decision for Bank-wide banning or otherwise.

7.4 If the Competent Authority is prima-facie of view that action for banning business dealings with the Agency is called for, a show-cause notice may be issued to the Agency as per paragraph 9.1 and an enquiry held accordingly.

7.5 Procedure for Banning of Business Dealings with Foreign Suppliers of imported goods.

- Banning of the agencies shall apply throughout the Bank including Subsidiaries.
- Based on the complaint forwarded by ED (BSD) or received directly by Corporate Vigilance, if gravity of the misconduct under investigation is found serious and it is felt that it would not be in the interest of CENTRAL BANK OF INDIA to continue to deal with such agency, pending investigation, Corporate Vigilance may send such recommendation on the matter to Executive Director, BSD to place it before Executive Directors' Committee (EDC) with ED (BSD) as Convener of the Committee.
- The committee shall expeditiously examine the report, give its comments/recommendations within twenty one days of receipt of the reference by ED, BSD.
- If EDC opines that it is a fit case for initiating banning action, it will direct ED (BSD) to issue show-cause notice to the agency for replying within a reasonable period.
- On receipt of the reply or on expiry of the stipulated period, the case shall be submitted by ED (BSD) to EDC for consideration & decision.
- The decision of the EDC shall be communicated to the agency by ED (BSD).

8 Removal from List of Approved Agencies - Suppliers / Contractors, etc.

8.1 If the Competent Authority decides that the charge against the Agency is of a minor nature, it may issue a show-cause notice as to why the name of the Agency should not be removed from the list of approved Agencies - Suppliers / Contractors, etc.

8.2 The effect of such an order would be that the Agency would not be disqualified from Competing in Open Tender Enquiries but Limited Tender Enquiry (LTE) may not be given to the Agency concerned.

8.3 Past performance of the Agency may be taken into account while processing for approval of the Competent Authority for awarding the contract.

9 Show Cause Notice

9.1 In case where the Competent Authority decides that action against an Agency is called for, a show-cause notice has to be issued to the Agency. Statement containing the imputation of misconduct or misbehaviour may be appended to the show-cause notice and the Agency should be asked to submit within 15 days a written statement in its defense.

9.2 If the Agency requests for inspection of any relevant document in possession of CENTRAL BANK OF INDIA, necessary facility for inspection of documents may be provided.

9.3 The Competent Authority may consider and pass an appropriate speaking order:

- a) For exonerating the Agency if the charges are not established;
- b) For removing the Agency from the list of approved Suppliers / Contactors, etc. c) For banning the business dealing with the Agency.

9.4 If it decides to ban business dealings, the period for which the ban would be operative may be mentioned. The order may also mention that the ban would extend to the interconnected Agencies of the Agency.

10 Appeal against the Decision of the Competent Authority

10.1 The Agency may file an appeal against the order of the Competent Authority banning business dealing, etc. The appeal shall lie to Appellate Authority. Such an appeal shall be preferred within one month from the date of receipt of the order banning business dealing, etc.

10.2 Appellate Authority would consider the appeal and pass appropriate order which shall be communicated to the Agency as well as the Competent Authority.

11 Review of the Decision by the Competent Authority

Any petition / application filed by the Agency concerning the review of the banning order passed originally by Competent Authority under the existing guidelines either before or after filing of appeal before the Appellate Authority or after disposal of appeal by the Appellate Authority, the review petition can be decided by the Competent Authority upon disclosure of new facts / circumstances or subsequent development necessitating such review. The Competent Authority may refer the same petition to the Standing Committee/EDC as the case may be for examination and recommendation.

12 Circulation of the names of Agencies with whom Business Dealings have been banned

12.1 Depending upon the gravity of misconduct established, the Competent Authority of the

Corporate Office may circulate the names of Agency with whom business dealings have been banned, to the Government Departments, other Public Sector Enterprises, etc. for such action as they deem appropriate.

12.2 If Government Departments or a Public Sector Enterprise request for more information about the Agency with whom business dealings have been banned, a copy of the report of Inquiring Authority together with a copy of the order of the Competent Authority / Appellate Authority may be supplied.

12.3 If business dealings with any Agency has been banned by the Central or State Government or any other Public Sector Enterprise, CENTRAL BANK OF INDIA may, without any further enquiry or investigation, issue an order banning business dealing with the Agency and its inter-connected Agencies.

12.4 Based on the above, Zonal Offices may formulate their own procedure for implementation of the Guidelines and same be made a part of the tender documents
