Central Bank of India

Information Security Department

Tender No. GEM/2025/B/6984238

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..... 8
2. Eligibility Criteria..... 11
3. EMD / Bid Security..... 16
4. Performance Bank Guarantee..... 17
5. Cost of Bidding.....17
6. Manufacturer's Authorization Form.....18
7. Scope of Work..... 19
7.1 Implementation Methodology:.....22
7.2 Setting up NG-SOC.....23
7.3 Transition from existing SOC to NG-SOC:.....28
7.4 Scope Of Work For Proposed Solutions.....29
7.5 SERVICES.....37
7.6 SECURITY DASHBOARDS.....39
7.7 OEM'S RESPONSIBILITIES ENGAGED BY THE BIDDER..... 41
7.8 NG-SOC OPERATIONS, FACILITY MANAGEMENT, AMC & ATS.....42
7.9 MANPOWER REQUIREMENT & DESIRED SKILLSET..... 49
7.10 TRAINING TO BANK EMPLOYEES..... 59
8. GENERAL RESPONSIBILITY OF THE BIDDER.....59
9. Project Timelines.....62
10. Staggered delivery of the equipment's.....63
11. Contract Renewal.....63
12. SLA compliance.....63
12.1 Service Level Agreements (SLA)..... 63
12.2 SERVICE LEVELS DURING IMPLEMENTATION PHASE.....64
12.3 SERVICE LEVELS POST ACCEPTANCE OF SOLUTIONS BY THE BANK.....64
13. Responsibility Matrix.....70
14. Escalation Matrix..... 70
15. Liquidated damage.....71
16. Land Border Sharing Clause.....71
17. Monitoring & Audit..... 73
18. Bid Submission..... 73
19. Integrity Pact.....75
20. Commercial Offers.....75

21. Evaluation & Acceptance....76
22. Evaluation Process....76
23. Payment Terms....88
23.1 PROCEDURE FOR CLAIMING PAYMENTS....88
23.2 AMC/ATS PAYMENT TERMS.... 90
23.3 AMC & ATS and Warranty Costs....91
24. Order Cancellation....93
25. Project Review....95
26. Indemnity....95
27. Confidentiality & Non-Disclosure....98
28. Force Majeure.... 98
29. Resolution of Disputes....99
30. Independent Contractor....100
31. Assignment....100
32. Insurance.... 101
33. Execution of Contract, SLA & NDA....101
34. SUCCESSFUL Bidder's Liability....101
35. Information Ownership....102
36. Inspection, Audit, Review, Monitoring & Visitations....103
37. Information Security....104
38. Limitation of Liability....105
39. Intellectual Property Rights....106
40. Visitorial Rights....107 41. Termination....108
Grounds of Termination .... 108 Types of Termination 108
Effect of Termination 109
Right to Transfer IT outsourcing Arrangements 109
42. Exit option and Contract Re-Negotiation....109
43. Privacy & Security Safeguards....110
44. Governing Law and Jurisdiction.... 111
45. Compliance with Laws.... 111

46. Regulatory compliance....112
47. Violation of Terms....113
48. Data localization....113
49. Corrupt & Fraudulent Practices....113
50. Publicity....113
51. APPLICABILITY OF PREFERENCE TO MAKE IN INDIA, ORDER 2017 (PPP-MII ORDER) 114
52. compliance to RBI master direction on outsourcing of it services (rbi Circular dated April 2023) 114
53. Sustainable Sourcing....117
54. Entire Agreement; Amendments.... 117
55. Adherence to Cyber Security Policy....117
56. Survival and Severability....118
57. Amendments to Bidding Documents....118
58. Period of Validity....119
59. Ownership, Grant and Delivery....119
60. Last Date and Time for Submission of Bids....119
61. Authorized Signatory.... 119
62. Late Bids....119
63. Modifications and/or Withdrawal of Bids....119
64. Waiver....120
65. Signing of Contract....120
66. Checklist for Submission....120
67. Annexure-1 Bill of Material....123
68. Annexure 2: Minimum Technical Specifications.... 131
69. Annexure 3: Conformity Letter....158
70. Annexure 4: Bidder's Information.... 159
71. Annexure 5: Letter for Conformity of Product as per RFP.... 160
72. Annexure 6: Undertaking for Acceptance of Terms of RFP....161
73. Annexure 7: Manufacturer's Authorization Form.... 163
74. Annexure 8: Integrity Pact....164
75. Annexure 9: Non-Disclosure Agreement....169
76. Annexure 10: Performance Bank Guarantee....174
77. Annexure 11: Bid Security (Earnest Money Deposit)....177
78. Annexure 12: Bidder's Particulars....179

79. Annexure 13: NPA/PENDING LITIGATION/BLACKLISTING Undertaking..... 180
80. Annexure 14: Undertaking letter (Land Border Sharing).....181
81. Annexure 15: Cover Letter..... 184
82. Annexure 16: Pre-bid Query Format..... 185
83. Annexure 17: Eligibility Criteria Compliance.....186
84. Annexure 18: Self declaration for compliance to RBI master direction on outsourcing of IT services..... 191
85. Annexure 19: GOI Guidelines for preference to Make in India.....193
86. Annexure 19a: Certificate of Local Content.....196
87. Annexure 20: Guidelines on banning of business dealing.....197
88. Annexure 21: Undertaking for 5 Years Roadmap..... 207
89. Annexure 22: Undertaking For Information Security.....208
90. Annexure 23: undertaking for authenticity of the product.....209
91. Annexure 24: List of Software and Hardware Components required for implementation.....210
92. Annexure 25: Proposed Team Profile.....212

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
BFSI	Banking Financial Services and Insurance
"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
RMA	Return Material Authorization
RO	Regional Office
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SCB	Scheduled Commercial Bank
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 4600 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 for the contract period of 5 years.

The details are given below:

Date of RFP Issue	10/12/2025
Bid Security (EMD)	An amount of Rs. 2,60,00,000/- (Rupees Two Crore Sixty Lakh 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	smit2infosec@centralbank.bank.in, smitcsoc@centralbank.bank.in, smitpurchase@centralbank.bank.in
Last Date for submission of pre-bid queries	Latest by 18/12/2025 up to 16:00 hrs. As per the format given in Annexure-16
Date and time for Pre-Bid Meeting,	22/12/2025 at 15:00hrs.
Last Date and Time submission of Bids Mode of bid submission & online	16/01/2026 up to 15:00 hrs.
Time & Date of Opening of technical bids	16/01/2026 at 15:30 hrs.
Mode of Submission	Government e Marketplace (GeM)
Response Types	1.Technical Bid plus Bid Security/EMD 2.Commercial Bid
Address for Communication	CISO, Central Bank Of India Information Security Department, Plot no-26, Sector-11, CBD Belapur, Navi Mumbai- 400614 Mail address:

	smit2infosec@centralbank.bank.in, smitcsoc@centralbank.bank.in, smitpurchase@centralbank.bank.in
Contact Telephone Numbers	022- 67123669,67123586

For any clarification with respect to this RFP, the bidder may send their queries/suggestions, valuable inputs. 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 16.

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) 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.

CISO,
Central Bank Of India
Information Security Department,
Plot no-26, Sector-11,
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 Criteria for Bidder / OEM	Documents to be submitted	Compliance (Y / N)
	Bidder Criteria		
1.	The 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 bid.	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.	The bidder must 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. 1000 crores each year in the last three financial years (i.e. 202223, 2023-24,2024-2025) as an individual company and not as group of companies.	Copy of Audited Balance Sheet and Certificate of the Chartered Accountant for the last three financial years (i.e. 2022-23, 2023-24,2024-2025)	
4.	The bidder must have made operating profit in at least two financial years out of last three financial years (i.e. 2022-23, 2023-24,2024-2025)	Copy of Audited Balance Sheet and Certificate of the Chartered Accountant for the last three financial years (i.e. 2022-23, 2023-24,2024-2025)	
5.	The bidder must have a positive net worth in last three financial years (i.e. 2022-23, 2023-24,2024-2025)	Copy of Audited Balance Sheet and Certificate of the Chartered Accountant for the last three financial years (i.e. 2022-23, 2023-24,2024-2025)	

6.	At the time of bidding, the Bidder and OEM must not have been blacklisted/debarred/ by any Govt. / IBA/RBI/PSU /PSE/ or Banks, Financial institutes for any reason including nonimplementation/delivery of the order. Self-declaration to that effect should be submitted along with the technical bid.	Undertaking on Company's letter head	
7.	At the time of bidding, there must not have been any pending litigation or any legal dispute, before any court of law between the Bidder or OEM and the Bank.	Submit the undertaking self-declaration on Company's letter head	
8.	The bidder and OEM must not have NPA with any Bank /financial institutions in India Any case pending or otherwise, with any organization in India which affects the credibility of the Bidder in the opinion of Central Bank of India to service the needs of the Bank may be a ground for rejection of the bid at the discretion of the Bank.	Submit self-declaration on Company's letter head.	
9.	The bidder must have service/support centre or should make the arrangements 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 must be registered with the Competent Authority.	Certified copy of the registration certificate	

11.	The Bidder should have implemented or managed onpremise SIEM solution and currently in use with minimum 1,00,000 Events Per Second (EPS) or 3.4TB / Day in at least ONE Scheduled Commercial Bank (SCB)*/RBI/NPCI/BSE/NSE/ SEBI in India during last 5 years *(SCB – with minimum 1000 Branches in India)	Letter of acceptance (LoA)/ purchase order along with completion certificate or any relevant document acceptable to Bank/ work order/ contract/ completion certificate Deployment Certificate issued by client to the bidder/Particulars confirming relevant experience. The Bank may also reach out to the concerned organization for verification of this criteria / point.	
12.	The Bidder should have implemented or managed onpremise SOAR solution in at least ONE Scheduled Commercial Bank (SCB)*/RBI/NPCI/BSE/NSE/SEBI/ in India during last 5 years *(SCB – with minimum 1000 Branches in India)	Letter of acceptance (LoA)/ purchase order along with completion certificate or any relevant document acceptable to Bank/ work order/ contract/ completion certificate Deployment Certificate issued by client to the bidder/Particulars confirming relevant experience. The Bank may also reach out to the concerned organization for verification of this criteria / point.	

13.	The Bidder should have implemented or managed onpremise UEBA solution in at least ONE Scheduled Commercial Bank (SCB)*/RBI/NPCI/BSE/NSE/SEBI/ in India during last 5 years *(SCB – with minimum 1000 Branches in India)	Letter of acceptance (LoA)/ purchase order along with completion certificate or any relevant document acceptable to Bank/ work order/ contract/ completion certificate Deployment Certificate issued by client to the bidder/Particulars confirming relevant experience. The Bank may also reach out to the concerned organization for verification of this criteria / point.	

14.	The Bidder must have minimum of 50 IT Security permanent resources with experience inscope solutions on their payroll with certifications such as CISSP/ CEH/CISM.	Undertaking on bidder letter head needs to submit along with certification details and relevant evidence.	
15.	The Bidder should be authorized partner of the OEMs of proposed solutions (SIEM, SOAR, UEBA, TIF, BRAND PROTECTION).	Bidder to submit duly filled and signed Manufacturer Authorization form (MAF) on OEM's letter head in the Bank's format and declaration about back-to-back support from respective OEMs.	
	OEM Criteria		

16	The OEM's proposed SIEM solution to the Bank must have been implemented and currently in use with minimum 1,00,000 Events Per Second (EPS) or 3.4 TB/Day in at least one SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE /NSE/SEBI/ in India during the last 5 years. *(SCB – with minimum 1000 Branches in India)	Letter of acceptance (LoA)/ purchase order along with completion certificate or any relevant document acceptable to Bank/ work order/ contract/ completion certificate Deployment Certificate issued by client /Particulars confirming relevant experience. The Bank may also reach out to the concerned organization for verification of this criteria / point.	
17	The OEM's proposed SOAR solution must have been implemented in at least One SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/ NSE/SEBI in India) during the last 5 years. *(SCB – with minimum 1000 Branches in India)	Letter of acceptance (LoA)/ purchase order along with completion certificate or any relevant document acceptable to Bank/ work order/ contract/ completion certificate Deployment Certificate issued by client/Particulars confirming relevant experience. The Bank may also reach out to the concerned organization for verification of this criteria / point.	
18	The OEM's proposed UEBA solution must have been implemented in at least One SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/ NSE/SEBI in India) during the last 5 years. *(SCB – with minimum 1000 Branches in India)	Letter of acceptance (LoA)/ purchase order along with completion certificate or any relevant document acceptable to Bank/ work order/ contract/ completion certificate Deployment Certificate issued by client /Particulars confirming relevant experience. The Bank may also reach out to the concerned organization for verification of this criteria / point.	

19	The OEM's proposed Threat Intel Feeds (TIF) solution must have been integrated in at least three out of top 10 SCHEDULED COMMERCIAL BANKs (SCB)*/RBI/NPCI/BSE/NSE/SEBI in India) during the last 5 years. *(SCB – with minimum 1000 Branches in India)	Letter of acceptance (LoA)/ purchase order along with completion certificate or any relevant document acceptable to Bank/ work order/ contract/ completion certificate Deployment Certificate issued by client /Particulars confirming relevant experience. The Bank may also reach out to the concerned organization for verification of this criteria / point.	
20	The OEM's proposed Brand Protection solution / services must have been provided in at least One SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/ NSE/SEBI/ in India) during the last 5 years. *(SCB – with minimum 1000 Branches in India)	Letter of acceptance (LoA)/ purchase order along with completion certificate or any relevant document acceptable to Bank/ work order/ contract/ completion certificate Deployment Certificate issued by client /Particulars confirming relevant experience. The Bank may also reach out to the concerned organization for verification of this criteria / point.	

*Note: In case of unaudited Balance Sheet for FY 2024-25, Bidder needs to submit Provisional Balance Sheet along with CA Certificate of Auditor for FY 2024-25.

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 ₹ 2,60,00,000/- (Rupees Two Crore Sixty Lakh 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 10, 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 theissuing 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 whateverreason, 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 schedulesgiven 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 thecontract 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 proposed OEM Product.

7. SCOPE OF WORK

Central Bank of India intends to implement Next Generation Security Operations Centre (NGSOC) 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, appliances, 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 willbe 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 atleast once in year from OEM review of the implemented NG-SOC solutions with concurrence of the Bank.

4. Supply all required infrastructure (appliances, servers, storages, NAS, tape library,tapes etc any hardware / equipment required for NG-SOC deployment) 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 ofthe 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. In this context, Threat Hunting Hypothesis to be prepared and shared with Bank on time to time basis. Frequency of Threat hunting will be decided with successful bidder.

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 theassets under the scope of NG-SOC solutions.

10. Managing reporting and logging of security alerts /incidents through ticketing tool andclosing 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 withInternational 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 ofspecifications, 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. Bidder hasto provide required support to Bank / Regulator appointed forensic investigation agency / vendor / consultant / company / auditor in such scenario.

15. Ensure continual improvement of NG-SOC operations, incorporating industry bestpractices, closure of audit observations and regulatory guidelines.

16. Ensure graceful transition from existing CSOC of the Bank to new NG-SOC alongwith migration activities.

17. The proposed solutions implemented by the Bidder should adopt evolving threats andtechnological advancements, including Quantum Computing and AI based threat.

18. All the tools/ application/ OS/hardware supplied as part of the project should be onpremise, latest and supplied with Enterprise-wide Licenses and all the licenses / subscriptions 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. In case of amalgamation / merger of Bank / s, Bank will have the right to continue or discontinue product / services without assigning any reason.

19. If a solution fails to meet the technical requirements of RFP during the implementation/before sign-off phase, Bank reserves the right to reject the solution with no cost to the Bank and recover all payments made for that solution. However, in such

cases the bidder may offer alternate solution to the Bank which fulfil technical requirements of the RFP with no extra cost to the Bank.

20. If during the contract period, the solution is not performing as per specifications/requirements in this RFP, bidder shall upgrade/enhance the devices or place additional devices and reconfigure the system without any extra cost to the bank till the required performance is achieved.

21. Bank's expectation is that successful bidder is required to manage the existing SOCfor another one year after expiry of existing contract in Jan'27.

22. Monitoring and Management

22.1 Configuration management. The successful bidder must ensure that all supplied & installed infrastructure & solutions are updated with the latest configuration and both the sites (DC & DR) have consistent configuration.

22.2 Patch Management - The successful bidder must ensure that all supplied & installed infrastructure & solutions are updated with patches as and when they are released after due testing. Critical patches should be applied immediately as per Bank Policy.

22.3 Service Level Management, Service reporting- Maintain the service levels as per the RFP and provide a periodic report to the Bank assessing all device performance under the scope of RFP against the Service Levels. Service Levels will include Availability measurements and Performance parameters (Utilization of CPU, RAM, storage, TPS, performance, uptime/downtime, EPS etc.) The Bidder should provide the requisite tools to measure availability of Hardware, OS, platform, other solutions as per RFP.

22.4 Change Management. The successful bidder must ensure that all supplied & installed infrastructure & solutions related changes are properly updated and recorded with version controlling and to have consistent setup both the sites (DC & DR).

22.5 Operation Management - Successful bidder should monitor measures, evaluates, and records status and performance information about all the equipment and software brought in by the bidder to aid in performance monitoring and tuning of the environment. Performance metrics should include utilization, throughput and other critical system needs. The successful bidder shall implement proactive procedures to address trends identified from performance and monitoring data. The successful bidder should provide standard reports that are to be provided to designated Bank personnel.

Successful bidder shall fix any security findings/vulnerabilities identified by various security agencies hired/consulted by the Bank without any additional cost during the contract period. Further, if the security observation(s) cannot be closed by applying updates/patches/fixes/upgrades to the supplied equipment and replacement is the only option to close the observation(s), then the successful bidder has to replace the device(s) with device meeting all the specifications of the RFP at no extra cost to the Bank.

However, the Bank reserves the right to waive off the hardware replacement depending on the type of vulnerability and its associated risk.

22.6 End of Sales / End of support: The Bidder has to ensure that any solution/equipment supplied as part of this RFP should not have either reached or announced 'End of Sales' (1 years from last date of submission of Bid.) or end of support for at least 5 years from the date of issue of purchase order. In the event if any equipment supplied by the bidder reaches end of support, within the 5 years period from the date of supply, the bidder has to replace the equipment with devices having equivalent or upgraded specification, at no additional cost to the Bank or revamp the entire solution (if required).

The Solution including Application & Hardware shall have a road map for 5 years from the Project Sign Off date. A certificate to this effect had been provided by the bidder/OEM and in Annexure 21.

The bidder shall provide mission critical support for both hardware and software for proposed solution. The mission critical support includes 24x7x365 support with site engineers for hardware and software.

23. Online Access/Remote Access will not be provided by the Bank during implementationor for troubleshooting purpose. Onsite Resources should be deployed for implementations and for troubleshooting purpose.

24. Seating Space and Workstations for onsite implementation and FMS Teams will beprovided by Bank at DC, Mumbai / Navi Mumbai and DRC, Hyderabad.

25. The Bank shall give Bidder/OEM and their personnel physical access to the designatedhardware & equipment at the Bank/Support Location to enable Bidder/OEM to provide the support for Installation, Maintenance, Troubleshooting & any other Support Services. Any mode of remote access will not be allowed from any Network outside Bank's Network.

26. Depending on the requirement, Bank reserves the right to extend the contract with the successful bidder including Subscription, AMC, ATS and Onsite FM Services of the supplied Platform and Solution for 2 more years i.e. 6th and 7th year on the same terms and conditions wherein enhancements/cost escalation quoted for 4th and 5th year would be taken as the price reference for the extension of the contract.

27. Implement and test procedures for backup and recovery of configurations, logs, andother critical components of the solutions. Perform an annual security audit to ensure that the systems remain compliant with regulatory requirements and that any vulnerabilities or gaps are addressed.

7.1 Implementation Methodology:

Implementation, Integration and Commissioning of Solutions will be performed onsite i.e. at Bank premises only at DC and DR. Comprehensive Project Plan along with detailed sub milestones of implementation and high level and low-level data flow diagrams should be shared with the Bank during kick-off meeting post issuance of purchase Order.

Project Director should be available ONSITE on all regular days and should update the project status on daily basis. The complete Implementation Team should also be stationed at Bank's location in Mumbai/Navi-Mumbai. The successful bidder should provide enough resources to complete the project as per the timelines mentioned in the RFP document considering various dependencies on integration with internal & external channels.

7.2 Setting up NG-SOC

1. Supply, install, integrate, operate, maintain and manage all NG-SOC technologiestogether 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 shouldleverage self-learning, analytic 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-SOCsolution suite with 30 Security Analysts equivalent license plus 15 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. Configure each solution based on the Bank's specific requirements, ensuring optimalperformance, security, and compatibility with existing systems (e.g., Security Operations Centre (SOC), network devices, servers, etc.).
6. Proposed Next-Gen solutions should provide automated remediation of threats on ITinfrastructure (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.
7. The intention should be to free up the personnel resources/ NG-SOC analysts/ ITteams from routine job and encourage them to invest their time more into threat hunting and advanced threat detection & prevention efforts.
8. The successful bidder should guarantee that the solution allows for the inclusion ofmanual changes within automated workflows within time frame defined by Bank.
9. There should be feature to import the logs of any endpoint/server/device(s) into thesystem for analysis based on various parameters/inputs and processed data and findings should be available on screen and for download & export to various entities.
10. Bidder should study the entire bank environment, identify data required for User & Entity Behavioural Analytic (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.
11. 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.
12. The bidder shall ensure that the proposed solution should not create multiple datalakes/ 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.
13. The proposed solution must be self-contained solution to provide the ease of addingfunctionalities such as UEBA, Threat hunting, Automation & Orchestration etc. Solution should use centralized Data Lake instead of traditional DB approach to avoid performance degradation during threat hunting.

14. Solution must provide unified GUI platform to manage and monitor the solutionsought under NG-SOC solutions e.g. SIEM, UEBA, SOAR and should also support for Threat Hunting etc.
15. The real-time view of events with relevant severity score.
16. Storage of logs should be encrypted by using highest level encryption such as AES256 or equivalent or above.
17. Compression of event logs should be minimum of 1:8 or more.
18. Threat hunting should be deployed on top of the existing real time/historical events forarresting of incidents. Log extraction should be seamless.
19. The bidder must propose NG-SOC solutions i.e. SIEM, UEBA and SOAR from singleOEM only. Further, there should be single & common dashboard/console/Database of all mentioned NG-SOC technologies in the RFP.
20. The proposed solution shall be capable of dual forwarding/streaming/replicating ofany raw logs from DC to DRC and vice versa. Storage must be arranged accordingly such that near zero RPO can be achieved.
21. The bidder must ensure that logs should be collected from each datacentre with thehelp of connectors and should be sent to respective data repository/data lake layer in the data centre. 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.
22. Every technology deployed in the NG-SOC should not have only rule based correlation system but also have analytics & AI/ML based correlation system for logs, vulnerabilities & threat intelligence together for accurate risks prediction.
23. NG-SOC shall support curated knowledge base and model for cyber adversary behaviour, reflecting the various phases of an adversary's attack life cycle and the platforms they are known to target like MITRE ATT&CK framework.
24. The NG-SOC should have following major technologies and related services withdeep 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 Data Lake (SDL)
- User and Entity Behaviour Analytic (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 1,00,000 EPS or equivalent TB data/day. In case ofData volume ingestion, raw log size of event to be factored as 500 bytes and enriched logs of events (Raw + CEF) to be factored as 700 bytes for storage & licensing purpose. While the solution (Including hardware) should be scalable to support 1.5 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. Bank may also opt for additional SIEM licenses as per requirement which should bepart of TCO and bidder should quote the price for pack of additional 10,000 EPS.
22. Bidder has to implement the similar setup at both DC (Mumbai/Navi Mumbai) andDR (Hyderabad) locations.
23. UEBA Sustained EPS/Volume/No of User 40,000 EPS or equivalent TB per Day or 40,000 users.
24. UEBA & SOAR Should leverage only on SIEM or Common Data Repository storageas per architecture proposed by the bidder..

25. 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. Data retention period will be the entire contract period. As per the regulatory guidelines all relevant data has to be stored for minimum 10 years. 6 Months data should be available online and should be stored in highest speed of storage. Another 12 months data should be in warm node that can be accessible through the application. Beyond that till contract period, Data should be in Archival node.

26. 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.

27. All the licenses and infrastructure provided as part of BoM should strictly adhere torequirements 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.

28. Bank may deploy the resources at both DC- Mumbai/Navi Mumbai and DR Hyderabad site as per Bank's requirement.

29. Minimum number of manpower to available in NG-SOC as per the shift, bidder has tofactor adequate resources considering management of shift. Bank may increase/decrease the manpower as per requirement of the bank.

30. 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.

31. The hardware/appliances that is going to be deployed at DC and DR locations shouldbe identical and each component should be in High availability mode.

32. All the Hardware devices should be with latest processor and releases date should notbe earlier than one year from the date of RFP.
33. All the hardware should be supplied as per EPS requirement asked by the Bank.
34. System should be capable for external and Internal disk space monitoring and alertingin 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.
35. Storage should attach Backup device which also encrypt the data stored in the externalback up media.
36. Any kind of Open Source Software/tools are not allowed as part of NG-SOC solutions. Offered software/tool must have enterprise/OEM support.
37. The solution must offer all the below built-in/custom-built compliance modules at no additional cost but not limited to:

    a) PCI-DSS Compliance Module

    b) MITRE

    c) NIST

    d) DPDP/GDPR Compliance Module

    e) ISO Compliance Module and other regulatory compliance which is applicable toBank

7.3 TRANSITION FROM EXISTING SOC TO NG-SOC:

- Integrate all existing log sources with NG-SOC.
- The bidder shall co-ordinate with existing vendor for extraction of data/logs from the available data/logs at existing SIEM/SOC as and when required by investigating agency, regulators etc.
- Migrate configurations, rules, use cases, other settings, logs from existing SOC.
- 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 NGSOC, ensure the existing SOC is up & running in steady state. Ensure that the reports are extracted from online / warehouse storage etc. Restore the logs from backup, if 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.

7.4 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, analyse, 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 by the means of continuous monitoring.
- 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.
  The solution should be capable of continuous monitoring and real-time auditing.
- 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.
  - Conduct comprehensive testing of the security solutions in a controlled environment to verify functionality, performance, and integration compatibility before full deployment. After installation and configuration, the Service Provider will work with Bank's designated personnel to conduct user acceptance testing

(UAT) to ensure the solutions meet specified requirements and performance expectations.

- Provide detailed documentation for each solution deployed, including installation steps, configuration settings, and operational procedures.

- 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 nonreporting 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.
  - Logs 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.
- SAN storage Systems should support Storage virtualization centralized management and SAN Storage should support 99.99% Data Availability

- 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 analyse 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-Tandeum, 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 monthly rule review or as decided by Bank 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 by obtaining permission from Bank 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. 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 analyse 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.

III. User and Entity Behaviour Analytics (UEBA)

- UEBA as a part of analytical engine of NG-SOC shall deeply compliment SIEM.
- It should profile and analyse 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 behaviour 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 behaviour 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.

IV. Threat Intelligence Feeds

- The feeds should demonstrate exceptional expertise in delivering high-quality, actionable threat intelligence that enables proactive threat detection and response by integrating this intelligence into Bank's existing IT security infrastructure. The comprehensive feeds should provide real-time insights into emerging threats, vulnerabilities, and adversary tactics, techniques, and procedures (TTPs).

- The bidder shall be solely responsible for provisioning all components necessary for implementation, including but not limited to the solution platform, services, software licenses, APIs, integration mechanisms, and any other tools or utilities required for the effective functioning of the Threat Intelligence Feed solution.
- The bidder must submit a comprehensive Plan of Action (PoA) outlining the methodology, intended use, integration points, operationalization process, and utilization strategy for the Threat Intelligence Feed tailored to the Bank's cybersecurity framework.
- The bidder shall be the single point of contact for all technical assistance and ongoing support. They will be responsible for ensuring the agreed-upon availability and uptime of the solution, including proactive monitoring, incident resolution, and performance tuning.
- The bidder shall be responsible for ensuring comprehensive and detailed training is provided by the Original Equipment Manufacturer (OEM).

V. Brand Protection Services including Dark Web Monitoring

The proposed Brand Protection solution should be able to address the following key areas but not restricted:

- 24x7 anti-phishing, anti-Trojan, anti-malware service to scan critical websites and Mobile Apps identified by Bank for the tenure of the project.
- Scan the Dark web for mentions of Bank's brand, product or services. Track specific keywords related to Bank including product names, executive names and brand slogans.
- Identify and block phishing attempts using Bank's brand name or logo.
- Collect and analyse data from dark web sources, including forums, marketplaces and chatrooms.
- Set up an alert system to notify Bank of potential brand protection incidents. Any newly launched websites and Mobile Application by the Bank in future to be scanned without any cost incurred to the Bank

- The bidder should be able to Initiate the responses as per Bank‘s request and permission

The Bidder needs to ensure that the solution should be able to takedown websites and Mobile App as per Bank‘s request and permission.

- Access to Dashboard view of the ―risks and threats‖ identified through the Anti-Phishing and threat intelligence services
- Monitoring of all major mobile application marketplaces for counterfeit, copycat apps, or apps infringing trademarks, linking to pirated content, attempting phishing attacks or distributing malware
- Prompt submission of enforcement notices and for the removal of rogue or infringing applications
- Fake Website detection impersonating Bank, work with domain registrars and hosting providers to shutdown / takedown such websites with Bank’s permission.
- Monitor for unauthorized use of Brand logo.
- Social Media tracking, analytics, reporting and influencer identification.
- Brand abuse reporting.
- Trademark, copyright, patent monitoring.
- Bidder must have capability for monitoring of similar sounding domain name registrations and alerting the Bank if this is detected. The Bidder is expected to perform the following activities:
  - Deploy the Brand Protection services for DC and DR location
  - Configure the Brand Protection policies as per Bank’s requirement
  - Daily reports must be submitted for Banks‘s review which highlights the threats, risks and respective mitigation actions taken as mentioned above.
  - Provide training to the identified Bank personnel/ SOC team on the product architecture, functionality and the solution design – to be provided before the implementation of solution.
  - Provide hands-on training to the Bank personnel/ SOC team on Brand Protection policy configuration, alert monitoring, problem mitigation and etc. post implementation.
  - Bidder should ensure the maintenance of the solution and provision of logs on daily basis for review with the Bank

7.5 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.
- The supplied enterprise class servers and storage should meet the requirement of high availability and fault tolerance without any component having single point of failure.
- The supplied server should be provided with Management Console for installation, provisioning, configuration, monitoring and maintenance of the supplied Hardware Infrastructure.
- 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 Service Provider will manage the end-of-life (EOL) of hardware and software components, ensuring that any outdated or unsupported solutions are properly decommissioned and replaced in a timely manner.
- Ensure that data on decommissioned equipment is securely wiped or destroyed, in compliance with Bank policies and regulatory requirements.

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 incyber security) for the threat hunting exercise
4. The threat hunting team must provide the threat hunting plan before every threathunting exercise
5. The threat hunting team must ensure the rules used by the SIEM are updated todetect the latest threats
6. They should share the list of IOC provider's intelligence feeds.

7.6 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 diskspace 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 / Analysed/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)

7.7 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 as per Bank's requirement 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: o Validation of solution design and architecture.
  o 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.

7.8 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 including L3 and Project Director, before onboarding of any such resource(s). Any such resource will be onboarded only after getting approval from Bank. Bank reserves the right to reject onboarding of any resource found not suitable.
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 Director 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, analysed 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. Project Director and L3 resources should be completely responsible for successfactor of C-SOC project including other tools / services.
12. Participate and contribute in every DR drill, cyber security drill, table-top exercises or any other exercises by the Bank, regulators or any third party.
13. Conduct DR drill of the NG-SOC on quarterly interval or as and when requiredby the Bank. The capacity of DR should be equivalent to 100% of current load and should be scalable as per annual growth.
14. Develop custom plug-ins, parsers, connectors, agents, adopters for all the systemsin the Bank or related to the Bank periodically or as and when needed without any extra cost to bank during the contract period.

15. Develop the baseline for the level of logs to be enabled across the differentcomponents 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.
16. Perform fortnightly & monthly gap analysis of current levels of logs enabled inOS, databases, web servers, business applications and devices and entire IT infrastructure & recommend and implement remedial actions.
17. 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.
18. 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.
19. The bidder should provide the on-site support for 24/7 around the year (365 days) for the period of warranty, AMC and ATS. Project Director 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.
20. Creating new reports and customize existing reports, dashboards, rules, queries,user interface in all forms to meet the dynamic requirements of the Bank.
21. Define formats for MIS reporting that includes daily, weekly and monthly or anyperiodical or ad-hoc reports, dashboards as per the Bank's requirements.
22. There should be alert generated and sent to concerned Application owner(s) forevery 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.

23. Transfer the knowledge to the Bank's SOC employees and/or Banks' InfoSecteam about day to day operations, system / backend level troubleshooting, dashboarding, creating basic and advanced rules & analytical models, creation and customization of reports &queries etc.
24. 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 L3 & L2 resources.
25. There should not be any disruption or degradation in the Bank's network bandwidth utilization and availability due to excessive log transmission.
26. Bidder to conduct periodic health check of the NG-SOC systems/solutions byrespective 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.
27. Secure configuration baseline should be benchmarked and updated on a periodicbasis with standards including SANS, NIST, CIS etc. followed by Bank's policies, CERT-IN, IDRBT, RBI, NCIIPC guidelines as updated from time to time.
28. The bidder should provide incident management/case management tool and should integrate with Bank's ITSM (Motadata) for ticketing system, tracking, incident management etc as per Bank's requirement. 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.
29. All deliverables including reports, incidents/alerts, their closure, vulnerabilitiesreported 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 Director of the bidder should define quality metrics, measurement frequency and reporting periodicity in consultation with the Bank.

30. 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.
31. For the security of the NG-SOC setup, bidder should integrate the complete NGSOC 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.
32. The NG-SOC setup must be complete in all the respect with different solutioncomponents 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.
33. 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.
34. The bidder should perform the advanced threat hunting on continuous basis.They should perform activities and incorporate changes based on global threat intelligence. If required Threat Intelligence should be shared with external agencies as per industry adopted formats / protocols.
35. Successful bidder is required to support the Bank or it's appointed vendor duringthe digital forensic investigation process as and when required during the contract period
36. Bidder should engage the Subject Matter Expert (SME) as and when required foranalytics, 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.

37. Monitor, detect, prevent and appropriately respond against any known and unknowns security threat, risk, bots identification etc.
38. Bidder must provide the brief summary & presentation before going for anymajor hardware/firmware/middleware/software version upgrade to cover all new functionalities, features and bug fixes that are coming with new version/upgrade.
39. During the entire Contract period at any point of time, if the performance of anysystem 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.
40. 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.
41. 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.
42. All proposed engineer, ought to be work at Bank's site, shall be on the companypayroll and no subcontracting resources will be allowed to work on NG-SOC project.
43. Email and Telephonic Support should also be provided by the back end experts tothe On-site support team.
44. The warranty period for the hardware will be three years and for Software /Solution will be for 1 year from the date of Go-live followed by 3 years AMC and 4 years ATS as applicable.
45. Post the completion of warranty period, the successful bidder should providecomprehensive AMC & ATS for proposed solution, including other software, associated modules, hardware and services required to meet the requirements in the RFP.
46. 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 without additional cost to Bank.

47. 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.

7.9 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 at the same rate and same will be notified to bidder in advance.

Threat & Incident Management / Threat Hunting				
Analyst Type	Morning	General	Afternoon	Night
L1	4	0	4	3
L2	2	1	2	1
L3	0	1	0	0
SIEM, SOAR,TIF & UEBA, Brand Protection Engineer/ Use case Engineering & Automation				
Analyst Type	Morning	General	Afternoon	Night
L1	1	1	1	1
L2	1	1	1	1
L3	0	1	0	0
Infrastructure Management				
Analyst Type	Morning	General	Afternoon	Night

L1	1	0	1	1
L2	0	1	0	0
L3	0	0	0	0
Project Director				
Analyst Type	Morning	General	Afternoon	Night
Project Director	0	1	0	0

L3 Resource shall have the responsibilities of Project Manager also and should be able to handle / monitor all of the above mentioned responsibilities and co-ordinate / guide L2 and L1 resources and continuously improve the SOC status. Project Director will be wholly responsible for success and continuous improvements in SOC.

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)	Total - 11 SOC Location: The resources may be deployed at both Primary and DR SOC situated in Mumbai/Navi Mumbai and Hyderabad respectively
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	

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 1-2 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 - Threat & Incident Management / Threat Hunting		
S. No	Role & Responsibilities	Resources/Shift
1	24*7 analysis of the alerts escalated by the L1 Team	Total - 6
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 3-4 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		
S.No	Role & Responsibilities	Resources/Shift
1	Analysis of the alerts escalated by the L2 or L1 Team and call support for critical issues	2 Resources 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 analyseevidence from compromised systems.	
6	Conduct malware analysis to understand the behaviour and impact of malicious code.	
7	Analyse 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 postincident 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. Detailed Responsibilities
29	Provide leadership and direction to the SOC team, ensuring alignment with Bank's goals and objectives
30	Manage the day-to-day operations of the SOC, including staffing, scheduling, and performance management
31	Oversee the incident response process, ensuring incidents are identified, investigated, and resolved promptly

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

1	Minimum 5 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	Preferably shall have any two certifications from the mentioned list, Cyber Security - Any One 1) CISSP (Certified Information Systems Security Professional) 2) CISM 3) CISA 4) CEH Incident and Program Management - Any One 5) ITIL (Information Technology Infrastructure Library) 6) PMP (Project Management Professional)	
L1 & L2 Infrastructure Management		
S.No	Role & Responsibilities	Resources/Shift
1	Provide support for critical infrastructure issues	

2	Log Source Management, Ensure timely integration of log sources	L1 – 3 resources L2 – 1 resource
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 contextto support security investigations.	
7	Platform Management: The installation, configuration, maintenance, update, upgrade of SIEM, UEBA & SOAR and 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 L1 engineer shall have minimum 1-2 years of experience in managing the similar solutions with OEM certification.	

8	The L2 engineer shall have minimum 3-4 years of experience in managing the similar solutions with OEM certification.	

SIEM, SOAR,TIF & UEBA, Brand Protection Engineer/ Use case Engineering & Automation		
S.No	Role & Responsibilities	Resources/Shift
1	Provide support for critical issues	4 – L1 resources 4 – L2 resources 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-tuningalerting 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 feeds) 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	L2 resource must have 3-4 Years of experience and proposed OEM certifications	
8	L1 resource must have 1-2 Years of experience and proposed OEM certifications	

1. The FMS team will be responsible for the complete end-to-end project management, installation, re-installation, configuration, re-configuration, implementation, integration, monitoring, patch management, VA/PT closure and troubleshooting of all the components supplied by the successful bidder including but not limited to the hardware infrastructure, all supplied software, Container Platforms (if any), Load Balancers (if any), any other Tools supplied for the project and its supporting hardware during the contract period of 5 years.

2. In case of exigency, support arrangements should be available during off-hours as a part of the crisis / incident management process. Bank at it's discretion may deploy resources at it's Data Center or Disaster Recovery site as per requirement of the project. Successful bidder shall be notified in advance.

3. The number of onsite resources mentioned in the RFP is minimum indicative requirement from Bank. However, the bidder may propose and quote adequate number of onsite resources with relevant skillset for achieving effective operation and management of proposed Solutions. However, payment will be made on the basis of actual number of resources deployed onsite.

4. If the FMS Team member is found to be not qualified / suitable / his performance is not satisfactory, the bidder will have to replace the engineer within 30 days of written communication from the Bank regarding the same.
5. The bidder shall be responsible for providing resolution of issues and implementation of the same. If the issue requires OEMs intervention, bidder has to take up with the OEM, obtain the solution and implement it for the resolution of the issue.

7.10 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 at-least 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 provide "certificate of participation" to the trainees identified by Bank.

Provide training for the Bank's IT and security personnel on how to operate, maintain, and manage the deployed IT security solutions. For the IT/security team on advanced configuration, troubleshooting, and management of the solutions. To prepare the team for handling security incidents and integrating security orchestration capabilities into response workflows. Ensure that the Bank's personnel are fully capable of managing and maintaining the security solutions post-deployment.

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. Following Oracle database and security products are available with Bank :

i. Database Enterprise Edition Licenses
ii. Partitioning Licenses
iii. Diagnostic Pack
iv. Tuning Pack
v. Real Application Clusters
vi. Audit Vault Database Firewall
vii. Data Masking & Subletting
viii. Database Vault
ix. Advanced Security Option
x. WebLogic License

- 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.
- The server rack(s) should be spacious enough and Industry standard with redundant Power Distribution Units, cable management arm, perforated front & back doors, mounted wheels, exhaust fans and Lock & Non generic Key. Rack Dimension: 42 U Rack, 600 mm*1000 mm.
- All the hardware equipment should be Rack Mountable and should have dual Power supply units.
- LTO-10 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. All media related to backup is to be provided by bidder till the end of the contract period and even in case of the extended period.
- 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.

- Any other Hardware, Software, Tools, Utilities, Databases etc. required for the successful implementation of the project should be provided by the bidder and should be mentioned in the commercial bill of material.

- 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. In case of OEM authorised partner OEM certificate should be presented to Bank mentioned authorisation to the partner.
- 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:

Sl. No.	Activity	Timelines
1	Acceptance of Purchase Order by successful bidder.	T
2	Delivery of all the equipment (software and hardware) as quoted in the bill of materials for SIEM, SOAR, UEBA, TIF and Brand Protection. Date of delivery of last item shall be taken as date of delivery for all items. *Note : Software licenses to be delivered post delivery of hardware upon getting confirmation from Bank.	T+10 Weeks
Implementation of below mentioned in-scope solutions/ services. Date of implementation of last items shall be taken as date of installation of all items.		
3	Installation of Hardware and System Software, configuration, baselining etc as per Bank's policies.	T+12 weeks

4	Implementation of SIEM and integrate all the required log sources (all network devices, AD, AV/EDR, DAM, Security Tools etc, approximately 3500 Servers and all critical Applications as prescribed by the Bank).	T+24 weeks
5	Integration of TIF and Brand Protection services with SIEM and/or SOAR and/or UEBA.	T+26 weeks
6	Implementation of SOAR, integration with SIEM and automation of minimum 10 playbooks as per Bank's requirement, integration of remaining applications with SIEM.	T+34 Weeks
7	Implementation of UEBA, integration with SIEM and SOAR.	T+37 Weeks
8	Migration of existing policies, rules, scenarios, logs etc . Fine tuning and acceptance by Bank for fully operational SOC and other solutions / services and Project Go-live.	T + 40 weeks

The above mentioned milestones will be treated as complete and successful only after obtaining sign off from Bank team at each milestone.

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 2 years (2 X 1 or 1 X 2 depending on Bank's requirement) time on same / mutually agreed terms with the successful Bidder. However, any of the component should not be EOS for extended 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:

(Total contracted minutes in a month – Downtime minutes within contracted minutes)

$$\frac{\text{Total contracted minutes in a month}}{\text{Total contracted minutes in a month}} * 100$$

- 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, Dashboard and the services offered by the bidder should have high uptime and penalties will be calculated for any unscheduled downtime as mentioned below:	Uptime % calculated on monthly basis for each solution.	
			Uptime 99.90% and above	No Penalty
			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 charges
		95% to 97.99%	3% of monthly NG-SOC operations charges
		90% to 94.99%	5% of monthly NG-SOC operations charges

<table>
<tr><td></td><td></td><td>Notify Low priority events within 90 minutes of the event identification.
99.9 % and above</td><td>NA</td></tr>
<tr><td></td><td></td><td>98% to 99.9</td><td>2% of monthly NG-SOC operations charges</td></tr>
<tr><td></td><td></td><td>95% to 97.99%</td><td>3% of monthly NG-SOC operations charges</td></tr>
<tr><td></td><td></td><td>90% to 94.99%</td><td>5% of monthly NG-SOC operations charges</td></tr>
<tr><td>2.</td><td>Incident response</td><td>Response of the incidents is depicted as per the Bank's SLA defined below:
<table><tr><td>Severity</td><td>Response Turnaround Time (TAT)</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>Any violation in meeting the Turnaround time requirements will lead to penalty (Refer below mentioned formula).

Percentage of incidents not meeting the Turnaround time monthly basis = (Total</td><td>Any violation in meeting the Turnaround time requirements will be calculated on monthly basis.

Bank shall impose a penalty of the overall monthly operation charges as mentioned below:

Percentage of incidents not meeting the TAT

5%< - Penalty of 10 percentage of the</td></tr>
<tr><td></td><td></td><td>number of incidents not eeting TAT /Total number of nts)*100
incide</td><td>overall NG-SOC monthly operation charges
2% <=5% - penalty of 5 percentage of the overall NG-SOC monthly operation charges</td></tr>
</table>

3.	Security Intelligence Advisories within 24 hours of vulnerability disclosure/global threat detection for each security device/solution/product as per asset inventory	Failedto take on 5 intelligence action feed/advisory	NA
		Failedto take on 10 intelligence action feed/advisory	2% of monthly NG-SOC operations charges
		Failedto take on 15 intelligence action feed/advisory	3% of monthly NG-SOC operations charges
		Failedto take on 20 intelligence action feed/advisory	5% of monthly NG-SOC operations charges
4.	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 NGSOC once notified by the Bank.
5.	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. Audit observations to be closed as per Bank's TAT (turnaround time).	Penalty of 2% of monthly NG-SOC operations charges per week of delay for complying critical and high observations.
6.	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.

7.	Availability of minimum manpower as per this RFP and add changes agreed from time to time	99.9 % and above	NA
		98% to 99.9	2% of monthly NGSOC FMS charges for each day of absence maximum upto 20%.
		95% to 97.99%	3% of monthly NGSOC FMS charges for each day of absence maximum upto 20%.
		90% to 94.99%	5% of monthly NGSOC FMS charges for each day of absence maximum upto 20%.

In the absence of the assigned resource, a suitable replacement must be provided immediately. If this replacement is not provided, a penalty of 2% of monthly service cost will be applied for each day of absence.

12.3.4 RMA (Return Merchandise Authorization):

For devices at DC/DR: Replacement for faulty equipment's must be done by bidder and follow up with OEM must be done by bidder only. RMA of Faulty equipment's should be received within 4 hours from the date of call lodge. In case bidder fails to provide the RMA of faulty/ damage equipment's penalty of 1% of equipment's cost weekly or part thereof maximum 10% of total contract value. However maximum cap of penalty will be 10% of the Hardware Value.

12.3.5 Availability Service Level Default for Facility Management

a) Bidder will have to guarantee a minimum attendance of 99 % per resource (i.e., attendance of each of the resources), calculated on a monthly basis. Attendance percentage will be calculated as (100% less Person Non-attendance Percentage) Person non-attendance percentage will be calculated as (Unavailable Time divided by Total Available Time), calculated on a monthly basis.
b) The attendance percentage would be calculated on monthly basis and the calculated amount would be adjusted from every subsequent quarter payment.
c) A Service Level Default will occur when the Service Provider fails to meet Minimum uptime (99%), as measured on a monthly basis.
d) In case any resource is not available continuously for more than 4 hours a day (Under normal circumstances) or 1 day in case of unplanned / emergency leave of any resource then the Bidder should immediately provide the Bank with an equivalent standby resource for that resource.
e) If Bidder fails to meet the onsite Resource Availability in any month, then the Bidder will have to pay the following compensation adjusted with every subsequent quarter payment:

(Minimum attendance Percentage – attendance Percentage) x Current Years Monthly Contract value)

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. Escalation Matrix

Bidder is required to submit escalation matrix to the Bank as per below format and inform Bank time to time in case of any update / changes:

Escalation Level	Escalation Point	Contact Details	Time to Acknowledge	Resolution Time
Level 1 (Initial Support)	Vendor's Front-Line Support / Bank IT Operations Team	Vendor: [Support Email / Phone] Bank: [IT Support Email / Phone]	Within 1 hour	Within 4 hours
Level 2 (Technical Support)	Vendor's Technical Support Team / Solution Specialist	Vendor: [Tech Support Email / Phone] Bank: [IT Support	Within 2 hours	Within 12 hours

		Manager Email / Phone]		
Level 3 (Senior Management)	Vendor's Senior Solution Architect / SME Bank's IT or Security Head	Vendor: [Senior Email / Phone] Bank: [Security Manager Email / Phone]	Within 4 hours	Within 24
Level 4 (Executive Escalation)	Vendor's Executive Management Bank's Senior Leadership	Vendor: [Executive Email / Phone] Bank: [CIO/CTO Email / Phone]	Within 8 hours	Within 48 hours

15. 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.

16. 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 14 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 though 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.

17. 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.

18. 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.

CISO
Information Security Department
4th Floor, Central Bank of India
Plot No -26, Sector-11
CBD Belapur, Navi Mumbai, Maharashtra – 400614
Phone -022-67123586

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 successful bidder through QCBS method 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 and Bank will not extend or re-conduct the bid.
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.

19. Integrity Pact

Each Participating bidder/s shall submit Integrity Pact as per attached Annexure 8 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.
  smit2infosec@centralbank.bank.in
  smitcsoc@centralbank.bank.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 parities accept that the IEM has the right to access all the documents relating to the project/procurement, including minutes of meetings.

20. 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

a. The commercial offer should be in compliance with technical configuration / specifications as per Technical Specifications.
b. The price to be quoted for all individual items and it should be unit price in Indian rupees.
c. 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.
d. The price is inclusive of taxes i.e. Goods and Services Tax, which shall be paid as per actuals.
e. Bank will award the contract to the successful Bidder according to the QCBS evaluation determined through GeM Portal.
f. Bank reserves the rights to negotiate with the selected bidder, if required.

21. Evaluation & Acceptance

1. 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.
2. 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

22. Evaluation Process

All bids will be evaluated on the basis of technical competence and the price quoted. The Technical Evaluation and the Commercial Evaluation shall have the weightage of 70% and

30% respectively, and this weightage shall be taken into consideration for arriving at the

Successful Bidder.

Technical & Commercial Scoring

The Commercial Bid of only technically qualified bids shall be opened.

The score(s) will be calculated for all technically qualified bidders using the formula:

H1 = (Minimum Commercial Quote/Quoted Price) x 30% + (Technical Score/Highest Technical Score) x 70%

Technical will carry 70% weightage and Commercial will carry weightage of 30%. Highest scores so obtained using the above method shall be declared as successful bidders. The bidder with the Highest Combined Score (H1) shall be selected. In case of tie between two or more bidders for the Highest Total Combined Score, then the bidder with Highest Technical Score amongst such bidders shall be the successful bidder.

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.

In case, any of the successful bidder is unable to honor in full or part of the contract awarded, Bank shall, at its sole discretion, distribute this shortfall to the other successful bidder(s) equally or in any ratio decided by the Bank.

Bank reserves the right to reject the bid offer under any of the following circumstances:

i). If the bid offer is incomplete and / or not accompanied by all stipulated documents.

ii). If the bid offer is not in conformity with the terms and conditions stipulated in the RFP.

iii). If there is a deviation in respect to the technical specifications of hardware items. 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 The

proposals will be evaluated in three stages.

Stage 1 – Eligibility Criteria Evaluation

Stage 2 – Technical Bid & Presentation Evaluation

Stage 3 – Commercial Bid Evaluation
All bids shall be evaluated by an Evaluation Committee or sub-committee set up for this purpose by the Bank. The evaluation shall be on the basis of technical competence and the price quoted.

Stage 1-Eligibility Criteria Evaluation

Eligibility criterion for the Bidders to qualify this stage is clearly mentioned in Sr no.2 "Eligibility Criteria" of the RFP.

The Bidders who meet all these criteria would only qualify for the second stage of evaluation. The Bidder would also need to provide supporting documents for eligibility proof. All the credentials of the Bidder necessarily need to be relevant to the Indian market.

Stage 2 Technical Bid and Presentation Evaluation

This evaluation will be done in three broad criteria as under :

Section No	Criteria	Maximum Marks	Min. Qualifying marks	Weightage(%)
1	Experience Criteria	770	539	48.125
2	Technical Specifications	430	301	36.875
3	Presentation	400	280	15
Total		1600	1120	

Bidder has to score minimum 70% in each of the above three sections to qualify for the next stage of evaluation.

Example : If bidder X scores : Experience Criteria - 600, Technical Specifications - 350 and Presentation - 300 in Stage -2 above, in such case the Technical Score calculated will be as below,

Step-1 : As bidder has scored more than 70% for each Section i.e (600/770)*100=77.92%, (350/430)*100=81.39% and (300/400)*100=75%, the bidder X qualifies for next step.

Step-2 : The Technical Score of bidder X for each section will be calculated as : (48.125*600)/770=37.5, (36.875*350)/430=30.01 and (15*300)/400=11.25. Accordingly Technical Score of the bidder will be 37.5 + 30.01 + 11.25 = 78.76 out of 100.

Section – 1 – Experience Criteria

SNO	Criteria for Bidder / OEM	Parameters	Document Required	Max Marks	Marks Scheme
1	Bidder	The Bidder should have implemented or managed SOC with on-premises SIEM solution with minimum 1,00,000 Events Per Second (EPS) or 3.4TB / Day in at least one SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/NSE/SEBI in India during last 5 years. *(SCB – with minimum 1000 Branches in India)	Letter of acceptance (LoA)/ purchase order along with completion certificate or any relevant document acceptable to Bank/ work order/ contract/ completion certificate Deployment Certificate issued by client to the bidder/Particulars confirming relevant experience. The Bank may also reach out to the concerned organization for verification of this criteria / point.	100	1 implementation or managed : 60 marks, further additional implementation or managed : 20 marks each
2	Bidder (Solution Capacity	The Bidder should have implemented or managed SOC with any on-premises SIEM solution with minimum 1,00,000 Events	Letter of acceptance (LoA)/ purchase order along with completion certificate or any relevant document acceptable to Bank/ work order/ contract/ completion	50	One Reference of 150,001 EPS / 5.1 TB per day and above - 50 Marks

	Implementation Experience)	Per Second (EPS) or 3.4TB / Day in at least one SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/NSE/SEBI in India during last 5 years. *(SCB – with minimum 1000 Branches in India)	certificate Deployment Certificate issued by client to the bidder/Particulars confirming relevant experience. The Bank may also reach out to the concerned organization for verification of this criteria / point		One Reference of 100,000 EPS / 3.4 TB per day and above upto 1,50,000 EPS - 35 Marks
3	Bidder (Experience)	The Bidder should have implemented or managed any on-premises SOAR solution in at least one SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/NSE/SEBI in India during last 5 years. *(SCB – with minimum 1000 Branches in India)	Letter of acceptance (LoA)/ purchase order along with completion certificate or any relevant document acceptable to Bank/ work order/ contract/ completion certificate Deployment Certificate issued by client to the bidder/Particulars confirming relevant experience. The Bank may also reach out to the concerned organization for verification of this criteria / point.	50	1 implementation : 35 marks, additional implementations : 15 marks each

4	Bidder (Experience)	The Bidder should have implemented or managed any on-premises UEBA solution with minimum 20,000 users in at least one SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/NSE/SEBI in India during last 5 years. *(SCB – with minimum 1000 Branches in India)	Letter of acceptance (LoA)/ purchase order along with completion certificate or any relevant document acceptable to Bank/ work order/ contract/ completion certificate Deployment Certificate issued by client to the bidder/Particulars confirming relevant experience. The Bank may also reach out to the concerned organization for verification of this criteria / point.	40	1 implementation : 25 marks, additional implementations : 15 marks each
5	Bidder (Experience)	The Bidder should have integrated TIF solution with any on-premise SOC in at least one SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/NSE/SEBI in India during last 5 years. *(SCB – with minimum 1000 Branches in India)	Letter of acceptance (LoA)/ purchase order along with completion certificate or any relevant document acceptable to Bank/ work order/ contract/ completion certificate Deployment Certificate issued by client to the bidder/Particulars confirming relevant experience. The Bank may also reach out to the concerned organization for verification of this criteria / point.	40	1 implementation : 20 marks, additional implementations : 10 marks each

6	Bidder (Experience)	The Bidder should have provided services of Brand Protection in at least one SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/NSE/SEBI in India during last 5 years. *(SCB – with minimum 1000 Branches in India)	Letter of acceptance (LoA)/ purchase order along with completion certificate or any relevant document acceptable to Bank/ work order/ contract/ completion certificate Deployment Certificate issued by client to the bidder/Particulars confirming relevant experience. The Bank may also reach out to the concerned organization for verification of this criteria / point.	40	1 implementation : 20 marks, additional implementations : 10 marks each
7	Bidder	The bidder must have minimum 50 IT Security permanent resources with experience in-scope solutions on their payroll with certifications such as CISSP/ CEH/CISM.	Undertaking on bidder letter head needs to submit along with certification details and relevant evidences acceptable to Bank	20	50 Resources - 10 Marks Every Additional 20 Resources - 5 Marks subject to maximum of 20 marks
8	Bidder	Number of data scientist / Engineers in the organization with at least 3 years of experience in implementing / managing AI/ML/Data lake for Cyber Security Operations	Resumes/Profile with the name of the Resources to be submitted and its should be certified by Bidder's HR Head.	20	4 marks for each resource
9	Bidder	Project Director proposed for the current Bank program should have experience in implementation of SOC solutions in last 5 years for	Necessary documentary proof / undertaking on letter acceptable to the Bank to be submitted	30	15 Marks for each implementation

		more than 30,000 EPS with minimum 7 years experience			
10	Bidder	L1 resources proposed for the current Bank program should have min 2 yrs experience in handling SOC solutions having certifications – CEH / CISM / CISA / CISSP	Necessary documentary proof / undertaking on letter acceptable to the Bank to be submitted	10	1 mark for each resource
11	Bidder	L2 resources proposed for the current Bank program should have min 3 yrs experience in handling SOC solutions having certifications - CEH / CISM / CISA / CISSP	Necessary documentary proof / undertaking on letter acceptable to the Bank to be submitted	15	1 marks for each resource
12	Bidder	L3 resources proposed for the current Bank program should have min 5 years experience in handling SOC solutions having certifications - CISSP / CEH / CISM	Necessary documentary proof / undertaking on letter acceptable to the Bank to be submitted	15	5 marks for each resource

13	OEM (Proposed Solution Experience)	The Bidder should have implemented or managed SOC with on-premises SIEM solution with minimum 1,00,000 Events Per Second (EPS) or 3.4TB / Day in at least one SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/NSE/SEBI in India during last 5 years. *(SCB – with minimum 1000 Branches in India)	Letter of acceptance (LoA)/ purchase order along with completion certificate or any relevant document acceptable to Bank/ work order/ contract/ completion certificate Deployment Certificate issued by client to the bidder/Particulars confirming relevant experience. The Bank may also reach out to the concerned organization for verification of this criteria / point.	100	1 implementation or managed : 40 marks, additional implementation or managed : 20 marks each

14	OEM (Proposed Solution Capacity)	OEM's proposed SIEM solution should be successfully implemented in at least one SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/NSE/SEBI in India during last 5 years. *(SCB – with minimum 1000 Branches in India)	Letter of acceptance (LoA)/ purchase order along with completion certificate or any relevant document acceptable to Bank/ work order/ contract/ completion certificate Deployment Certificate issued by client to the bidder/Particulars confirming relevant experience. The Bank may also reach out to the concerned organization for verification of this criteria / point. Details such as Make, Model, EPS etc. should be available in either of the documents.	100	100001 to 125000 EPS (3.4 TB to 4.25 TB) or Equivalent: 60 Marks 125001 to 150000 EPS (4.26 TB to 5.1 TB) or Equivalent: 80 Marks 150001 EPS (5.1 TB) or more: 100 Marks

15	OEM (Experience)	OEM's Proposed SOAR solution should be successfully implemented in at least one SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/NSE/SEBI in India during last 5 years. *(SCB – with minimum 1000 Branches in India)	Letter of acceptance (LoA)/ purchase order along with completion certificate or any relevant document acceptable to Bank/ work order/ contract/ completion certificate Deployment Certificate issued by client to the bidder/Particulars confirming relevant experience. The Bank may also reach out to the concerned organization for verification of this criteria / point.	60	40 marks - 1 reference 10 marks - additional reference
16	OEM (Experience)	OEM's Proposed UEBA solution should be successfully implemented in at least one SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/NSE/SEBI in India during last 5 years. *(SCB – with minimum 1000 Branches in India)	Letter of acceptance (LoA)/ purchase order along with completion certificate or any relevant document acceptable to Bank/ work order/ contract/ completion certificate Deployment Certificate issued by client to the bidder/Particulars confirming relevant experience. The Bank may also reach out to the concerned organization for verification of this criteria / point.	30	10 marks per reference

17	OEM (Experience)	OEM's Proposed Threat Intel Feeds solution should be successfully integrated in at least one SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/NSE/SEBI in India during last 5 years. *(SCB – with minimum 1000 Branches in India)	Letter of acceptance (LoA)/ purchase order along with completion certificate or any relevant document acceptable to Bank/ work order/ contract/ completion certificate Deployment Certificate issued by client to the bidder/Particulars confirming relevant experience. The Bank may also reach out to the concerned organization for verification of this criteria / point.	30	10 marks for each reference
18	OEM (Experience)	OEM's Proposed Brand Protection solution should be successfully integrated in at least one SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/NSE/SEBI in India during last 5 years. *(SCB – with minimum 1000 Branches in India)	Letter of acceptance (LoA)/ purchase order along with completion certificate or any relevant document acceptable to Bank/ work order/ contract/ completion certificate Deployment Certificate issued by client to the bidder/Particulars confirming relevant experience. The Bank may also reach out to the concerned organization for verification of this criteria / point.	20	10 marks for each reference
		Total		770	

Section-2 Technical Specifications

As a part of Technical Evaluation, each line item of Annexure- 2 - Minimum Technical Specifications carries three marks for Mandatory points each, certain other points carrying three marks each and two marks for remaining points each, which will be scaled to 430 marks for evaluation purpose. Non-compliance of Mandatory technical points will lead to disqualification of the bidder. However, other points which are not mentioned as mandatory are also important for Bank and hence effects the scoring of bidder.

Section -3 : Presentation by bidder

Presentation by bidder carries marks for various evaluation criteria as mentioned below -

Sr no	Criteria	Max Marks
1	Solutioning Approach - Cyber Security requirements, Solution Designing, Architecture, Roadmap, Sustainability	50
2	Implementation Approach - Project planning, Proposed setup for Bank, Security Tools Integration, Security Process Development	40
3	Migration and Transition approach - Migration Planning, Data/configuration migration, System Integration, Transition approach	40
4	Experience of Implementation - CSOC Experience, Banking Industry Experience, Best Practices, Lessons Learnt, Use case of successful implementation in similar PSB.	50
5	Project Governance and Methodology - Project Management, Project Execution Methodology, Status Reporting, Success road map	50
6	Resource Planning - Alignment of resources with CSOC goals and objectives, Roles and responsibilities, Efficiency Assessment, Project Director review	40

7	OEM Solution Capabilities - Deployment and Integration Flexibility, Detection and Response capabilities, AI / ML capabilities, Threat Hunting capabilities, CxO Dashboards, Ease of Customization, Automation capabilities, Malware / Ransomeware detection capabilities.	80
8	Value Addition, Innovation and Maturity Road map Reduction in False Positives, Enhanced Threat Detection, Increased Efficiency, Predictive Analysis, Advanced Threat Hunting	50
	Total Marks	400

Bidder qualifying with min. 70% of the each of the experience criteria, technical specifications & presentation sections will be eligible to participate further for commercial evaluation. Stage-3 Commercial Evaluation

a) Only those Bidders who have qualified in Stage 2 above will be eligible for the further participation in the stage 3 of Commercial Evaluation. The total cost of ownership for the purpose of evaluation shall be calculated over the contract period of 5 years, (total cost of products & services).

b) The score(s) will be calculated for all technically qualified bidders using the formula:

S = (30 x C_minimum/C_quoted) + (70 x T_obtained/T_highest)

(Minimum Commercial Quote/Quoted Price) x 30 + (Technical Score/Highest Technical Score) x 70.

Technical will carry 70% weightage and Commercial will carry weightage of 30%)
Bank will award the contract to the successful Bidder whose score "S" is the highest as per the above-mentioned formula.

The Bidder shall not add any conditions / deviations in the Commercial Bid. Any such conditions / deviations may make the bid liable for disqualification.

The commercial evaluation would cover Compliance to the Commercial Bid as in

Annexure 1: The Bidder is expected to provide their "compliance" against each item

stated in the Commercial Bid, this means that the Bidder confirms to the provisioning

of the stated product or service and the terms of the RFP and subsequent addendums.

Deviations to the Compliance requirements may lead to disqualification.

The Bank may go through a process of technical and/ or commercial evaluation and

normalization of the bids to the extent possible and feasible to ensure that Bidders are more or

less on the same technical ground. After the normalization process, if the Bank feels that any

of the bids need to be normalized and that such normalization has a bearing on the Commercial Bid; the Bank may at its discretion ask all the technically shortlisted Bidders to resubmit the updated technical and Commercial Bids once again for scrutiny. The Bank can repeat this normalization process at every stage of technical submission till the Bank is reasonably satisfied. The Bidders agree that they have no reservation or objection to the normalization process and all the technically short-listed bidders will, by responding to this detailed document, agree to participate in the normalization process and extend their co-operation to the Bank during this process. The Bidders, by submitting the response to this detailed document, agree to the process and conditions of the normalization process. Any non-compliance to the normalization process may result in disqualification of the concerned Bidder. Bank may call for any clarifications/ additional particulars required, if any, on the technical/Commercial Bids submitted. The Bidder has to submit the clarifications/ additional particulars in writing within the specified date and time. The Bidder's offer may be disqualified, if the clarifications/ additional particulars sought are not submitted within the specified date and time. Bank shall call for presentation(s), product demo/walkthroughs, on the features of the solution offered etc., from the bidders based on the technical bids submitted by them. Bank also reserves the right to conduct reference site visits at the Bidder's client sites. Based upon the final technical scoring, short listing would be made of the eligible bidders for final Commercial Bidding.
Note: Tendering process need not be cancelled merely on the grounds that a single tender was received provided that the single bid received is evaluated to be substantially responsive and deemed fit for award. Bank reserves right to proceed and award the tender to single bidder in case only one bidder participates in the tender / qualifies in the technical bid evaluation. Bank can negotiate with such single bidder, if required.

Note : As per GeM regulations Bank may scale down over all score of each bidder according to the maximum marks of 100.

23. 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 inscope 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.

23.1 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, on signing the agreement / contract by the selected Bidder, on submission of Performance Bank Guarantee and obtaining sign-off for respective payment milestones. Payment for Project Director and other FMS resources (L1,L2,L3) will commence post Go-live of the NG-SOC project and through scrutinization process.

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	40%	On post-delivery inspection of the Hardware
		50%	Against successful installation and acceptance testing signoff by Bank at DC, DRC
		10%	3 months after successful installation signoff of software / solution / service and signoff by Bank at DC, DRC
2.	Software license (OS, Application & other associated software and services) For Each of the following Software Solution / Service 1. SIEM 2. SOAR 3.UEBA 4.TIF 5.Brand Protection	30%	On post-delivery of the licenses
		50%	Against successful implementation and acceptance testing of respective software / solution / service (i.e. SIEM, SOAR, UEBA, TIF, Brand Protection) and signoff by Bank at DC, DRC
		10%	After Successful Migration of existing policies, rules, scenarios, logs, VAPT compliance and completion of one DR Drill
		10%	3 monthsafter successful implementation signoff
3.	Implementation Charges For Each of the following Software Solution / Service 1. SIEM 2. SOAR	70%	On successful implementation of respective software / solution / service (i.e. SIEM, SOAR, UEBA, TIF, Brand Protection) of the RFP in DC, DR and its sign off and acceptance by the Bank
		10%	Fine tuning and acceptance by Bank for fully operational SOC and other solutions / services, Issuance of Go-Live Certificate by the Bank.
S. No	Deliverables	% Of Payment	Payment Milestone (On completion of the activities)

	3.UEBA 4.TIF 5.Brand Protection	20%	3 months after fully operational and completion of migration of logs, existing policies etc, Golive signoff and satisfactory working of each solution / service.
4	Charges for migration from existing SIEM and SOAR system and Transition	70%	Migration of existing policies, rules, scenarios, logs etc .
		10%	Fine tuning and acceptance by Bank for fully operational SOC and other solutions / services, Issuance of Go-Live Certificate by the Bank.
		20%	3 months after fully operational , Go-live signoff and satisfactory working of each solution / service.
5	AMC Charges		AMC charges will be paid quarterly in arears and on satisfactory working of the hardware infrastructure.
6	ATS / Subscription Charges		ATS charges will be paid quarterly in arears and on satisfactory working of the software / solution Subscription charges will be paid yearly in advance from 2nd year onwards. 1st year Subscription charges will be paid after Go-live of the project.
7	FM Support Charges (32 resources)	-	Payment for on-site support charges will be paid on actuals on quarterly basis in arrears.
8	Professional Services Cost	-	Professional Services cost will be paid on actuals on availing the services by Bank

23.2 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 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 backto-back agreement with the respective OEM to the Bank.

23.3 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 hardware components should be for the first three years for which the cost should be factored in the Product cost and AMC shall be factored for the subsequent two years. Bidder must factor the costs in the Bill of Material accordingly. ATS of Software from 2nd year onwards will be paid quarterly in arrears. 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, destinationbased 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.

24. Order Cancellation

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

24.1 Bank reserves the right to cancel the contract placed on the successful bidder and recover expenditure incurred by the Bank under the following circumstances.

24.2 Delay in delivery beyond the specified period for delivery.

24.3 Serious discrepancy in hardware/software noticed during Installation or during maintenance period

24.4 Any other lapse pertaining to the order from successful bidder / OEM's end.

24.5 If the service provider commits a breach of any of the terms and conditions of the bid, or if the service provider goes into liquidation, voluntarily or otherwise, the Bank reserves the right to cancel the contract.

24.6 Additionally, if an attachment is levied or continues to be levied for a period of seven days upon the effects of the bid, the Bank may take appropriate action.

24.7 If the service provider fails to complete the assignment as per the timelines prescribed in the RFP and any extension allowed, it will be considered a breach of contract, and the Bank reserves its right to cancel the order in the event of delay and forfeit the bid security/performance bank guarantee as liquidated damages for the delay.

24.8 Penalty / Liquidated Damages 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.

24.9 After the award of the contract, if the service provider does not perform satisfactorily or delays execution of the contract, the Bank reserves the right to get the balance contract executed by another party of its choice by giving one month's notice for the same. In this event, the service provider is bound to make good the additional expenditure that the Bank may have to incur in executing the balance contract. This clause is applicable if, for any reason, the contract is cancelled. The Bank reserves the right to recover any dues payable by the service provider from any amount outstanding to the credit of the service provider, including pending bills and/or invoking the bank guarantee under this contract.

24.10 In addition to the cancellation of the purchase order, the Bank reserves the right to appropriate the damages from the Bid Security / Performance Bank Guarantee given by the service provider and/or foreclose the bank guarantee given by

the service provider against the advance payment and may take appropriate action. Further, in case of failure to adhere to the terms and conditions of the RFP in totality, concealment of facts in the tender documents, or failure to fulfil the contractual obligations of the Purchase order, the Bank may debar/blacklist the service provider from participating in future tender processes. The Bank reserves the right to inform IBA/other banks about blacklisting the service provider in case of default in service or delay leading to financial or reputational loss, loss of time of the bank.

25. Project Review

The parties agree to conduct periodic project reviews at key milestones throughout the IT security solution procurement process to assess progress, adherence to scope, schedule, and budget, identify any issues or risks, ensure the quality and functionality of the solution, and implement corrective actions as needed, with summary reports documenting the outcomes and proposed adjustments.

26. 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 / bona fide 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 theinfringement 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 wasnot 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 anymodification 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 itscapacity or performance;

(iii) replace the Deliverable with work product that is equal in capacity and performance butis 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.

27. 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.

28. Force Majeure

Force Majeure is herein defined as any cause, which is beyond the control of the service provider or the Bank as the case may be which they could not foresee or with a reasonable

amount of diligence could not have foreseen and which substantially affect the performance, such as:

i. Natural phenomenon, including but not limited to floods, droughts, earthquakes, epidemics,
ii. Situations, including but not limited to war, declared or undeclared, priorities, quarantines, embargoes.
iii. Terrorist attacks, public unrest in work area.

Provided either party shall within seven (7) days from the occurrence of such a cause notify the other in writing of such causes. The Service provider or the Bank shall not be liable for delay in performing his/her obligations resulting from any Force Majeure cause as referred to and / or defined above. The decision regarding whether a particular event as informed by the bidder being a force majeure event, should be regarded as a force majeure event, shall be solely the decision of the bank. Financial reasons or escalation in prices will not fall under "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 up to 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.

29. Resolution of Disputes

The Bank and the competent authority of 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.

30. 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.

31. 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.

32. INSURANCE

The equipment (hardware/software, etc.) supplied under the contract shall be fully insured by the bidder against loss or damage incidental to manufacture or acquisition, transportation, storage, delivery, and installation. The insurance shall be obtained by the Service Provider, naming Central Bank of India as the beneficiary, for an amount equal to 100% of the invoiced value of the goods on an "all risks" basis, covering risks such as damage, theft, fire, or natural disasters. The period of insurance shall remain in effect until the supplied components are accepted by the Bank, and the rights to the property are transferred to the Bank at its premises. In the event of any loss or damage, the bidder shall initiate and pursue the claim until settlement. Additionally, the bidder must promptly make arrangements for the repair and/or replacement of any damaged items, irrespective of the settlement of the claim by the underwriters. Furthermore, the Service Provider shall ensure that the insurance policy remains valid throughout the supply, transportation, and installation period, and any gaps in coverage shall be rectified immediately. The Service Provider shall also provide the Bank with necessary documentation of the insurance policy, claim details, and any associated correspondence with the underwriters.

33. 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.

34. SUCCESSFUL BIDDER'S LIABILITY

The Bidders 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 Bidders liability in case of claims against the Bank resulting from wilful misconduct or gross negligence of the 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 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.

Subject to any law to contrary, and to the maximum extent permitted by law neither party shall be liable to other for any remote and indirect loss or damages arising out of this tender and subsequent agreement or services provided."

This limitation shall not apply to third-party claims arising from:

Intellectual Property (IP) Infringement Indemnity: The Bidder's liability for any claim or damages arising from infringement or alleged infringement of third-party intellectual property rights shall not be subject to the above limitation.

Bodily Injury, Death, and Property Damage: The Bidder shall be fully liable for any bodily injury (including death) or damage to real property or tangible property caused by the Bidder's negligence, fraud, or misrepresentation, or that of its employees, representatives, or subcontractors.

35. 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.

36. 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.

37. 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.

The following mandatory security controls must be ensured by the Bidder for proposed Solutions:

a. There should be mechanisms in place to secure the Data from loss, misuse, or disclosure.

b. The platform and solution should encrypt/tokenize data at rest.

c. There should be encryption and integrity protection in place for all internal network traffic that potentially carries sensitive information (including passwords, emails, files, source code, management traffic, etc.)

d. The passwords should be encrypted.
e. The Solution should handle personally identifiable information (PII) as per the statutory guidelines.
f. Testers and developers should be prevented from accessing production systems.
g. The application should have role-based access for customers and third-party users.
h. The system should define groups of leads that are only accessible to certain specified users for marketing purposes.
i. The system should define groups of assets (emails, landing pages, etc.) that can only be accessed by certain specified users.
j. The solution should ensure PII data security.
k. The bidder should comply with various guidelines issued by regulatory / statutory bodies such as Govt of India, RBI, UIDAI, NCIIPC, EASE such as RBI Working group document on "Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds" dated Jan 2011, such as for confidentiality and security and Cyber Security guideline June' 2016, RBI February 2021 Master Circular on Digital Payments Security, RBI circular on "Storage of Payment System Data" dated April 6, 2018, RBI's Master Directions on Outsourcing of Information Technology Services dated 10th April 2023, Digital Personal Data Protection (DPDP) Act 2023 of Government of India etc. with respect to implementation and maintenance of proposed Solutions.
l. Scalability and Availability: The solution's architecture must support high scalability and availability. The vendor should provide a high-level architectural design of the application including this network topology.

38. Limitation of Liability

Bidder's aggregate liability under the contract shall be limited to a maximum of the contract value. For the purpose of this section, the contract value at any given point of time means the aggregate value of the purchase orders placed by the Bank on the Bidder that gave rise to the claim, under this Request for Proposal (RFP).

This limitation shall not apply to third-party claims arising from:

Intellectual Property (IP) Infringement Indemnity: The Bidder's liability for any claim or damages arising from infringement or alleged infringement of third-party intellectual property rights shall not be subject to the above limitation.

Bodily Injury, Death, and Property Damage: The Bidder shall be fully liable for any bodily injury (including death) or damage to real property or tangible property caused by the Bidder's

negligence, fraud, or misrepresentation, or that of its employees, representatives, or subcontractors.

Indirect, Consequential, Incidental, or Special Damages: Notwithstanding the above, the SP shall be liable for any indirect, consequential, incidental, or special damages arising under this agreement or purchase order. These types of damages may include, but are not limited to, lost profits, loss of business opportunities, loss of use, or other similar damages, even if the Bidder has been advised of the possibility of such damages.

Liability for Subcontractor Practices: The Service Provider shall be contractually liable for the performance of its subcontractors and must ensure that its subcontractors adhere to the same level of risk management practices as required by the Bank. This includes ensuring that subcontractors meet the agreed-upon standards of performance, compliance, and quality.

39. 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 Banka 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 PreExisting 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 authorizes 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

40. VISITORIAL RIGHTS

The Bank and its authorized representatives reserve the right to visit any of the Bidder's premises without 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. Non-cooperation by the bidder in this regard will be treated as breach of agreement/Purchase Order and will follow the consequences accordingly.

41. TERMINATION

Central Bank of India reserves the right to cancel the work/purchase order or terminate the Service Level Agreement (SLA) by providing 90 (ninety) days' prior written notice and recovering any damages, costs, and expenses incurred by the Bank under the following circumstances:

GROUNDS OF TERMINATION

i. Breach of Terms: If the bidder commits a breach of any of the terms and conditions of the Request for Proposal (RFP) or the Service Level Agreement (SLA) to be executed between the Bank and the SP.

ii. Insolvency: If the bidder goes into liquidation, voluntarily or otherwise.

iii. Violation of Laws: If the bidder violates any laws, rules, regulations, byelaws, guidelines, or notifications.

iv. Legal Attachment: If an attachment is levied or continues to be levied for a period of seven days on the effects of the bid.

v. Failure to Meet Timelines: If the bidder fails to complete the assignment as per the timelines prescribed in the Work Order/SLA, including any extensions granted.

vi. Excess Liquidated Damages: If the deductions due to liquidated damages exceed 10% of the total work order.

vii. Failure to Deliver Resources: If the bidder fails to deliver the required resources as stipulated in the delivery schedule, the Bank reserves the right to procure similar resources from alternative sources at the risk, cost, and responsibility of the bidder.

viii. Non-Performance: If after the award of the contract, the bidder fails to perform satisfactorily or causes delays, the Bank reserves the right to have the remaining contract executed by another party of its choice. The bidder must cover any additional expenditure incurred by the Bank in this regard.

ix. Outstanding Dues: The Bank reserves the right to recover any dues payable by the bidder from any amount outstanding, including pending bills and/or invoking the Performance Bank Guarantee under this contract.

TYPES OF TERMINATION

i. Termination for Insolvency: The Bank may terminate the contract if the bidder becomes bankrupt or insolvent, with termination being without compensation to the bidder. However, this does not affect any accrued rights or remedies of the Bank.

ii. Termination for Default: The Bank may terminate the contract in whole or in part, by providing written notice in case of a default by the bidder.

iii. Termination for Convenience: The Bank may terminate the contract at its convenience, in whole or in part, with written notice.

EFFECT OF TERMINATION

i. Transition and Business Continuity: Upon termination, the Bank is entitled to impose necessary obligations and conditions to ensure smooth transition and business continuity of the services. The bidder must take all steps to minimize loss caused by termination and allow the next successor bidder to take over the obligations.

ii. Post-Termination Assistance: If the contract expires or is not extended, the bidder must assist the successor or the Bank's representative with the transition. This may include providing training or any other necessary support even beyond the contract's termination period.

RIGHT TO TRANSFER IT OUTSOURCING ARRANGEMENTS

In the event of termination, the Bank reserves the right to orderly transfer the proposed IT outsourcing arrangement to another service provider, if necessary or desirable, to ensure minimal disruption of services. This transfer shall be managed in an efficient manner, with the bidder cooperating fully with the Bank to facilitate this process, including transferring knowledge, data, and providing assistance as required.

The termination shall not affect any accrued rights or liabilities of either party and will not affect the provisions that are intended to continue after termination.

42. EXIT OPTION AND CONTRACT RE-NEGOTIATION

i.The Bank reserves the right to cancel the contract and debar bidder from participating in future procurement processes if one or more of the following conditions occur:

a.Failure of bidder to accept the contract or purchase order and to furnish the Performance Guarantee within 21 days of the acceptance of the purchase contract.

b.Delay in offering the required deliverables or services.

c.Delay in commissioning the project beyond the specified period.

d.Delay in completing commissioning, implementation, and acceptance tests/checks beyond the specified periods.

e.Serious discrepancies in the project noticed during the testing phase.

f.Serious discrepancies in the functionality to be provided or the performance levels agreed upon, which negatively affect the functioning of the Bank.

g.Serious discrepancies in the completion of the project.

ii.In addition to cancelling the purchase contract, the Bank reserves the right to appropriate damages by encashing the Bid Security or Performance Guarantee provided by bidder.

iii.The Bank reserves the right to purchase the equipment from third-party suppliers if such equipment is available at a lower price, and if bidder's offer does not match that lower price. However, this will be done only if:

a.The equipment is available at more favourable terms in the industry.

b.The equipment procured from third parties is functionally similar to the original equipment, ensuring that bidder can maintain it.

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.

43. Privacy & Security Safeguards

i. The Bidder shall not publish or disclose in any manner, without the Bank's prior writtenconsent, 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 ofsecurity breaches. iii. The Bidder hereby agrees that they will preserve the documents.

44. 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.

45. 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.

46. REGULATORY COMPLIANCE

a. The bidder must ensure that the proposed Solutions, platform and implementation, architecture should adheres to guidelines issued by regulatory / statutory bodies such as Govt of India, RBI, UIDAI, SEBI, IRDAI, NCIIPC, TRAI including but not limited to RBI Working group document on "Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds" dated Jan 2011, for confidentiality and security and Cyber Security guideline June' 2016, RBI February 2021 Master Circular on Digital Payments Security, RBI circular on "Storage of Payment System Data" dated April 6, 2018, RBI's Master Directions on Outsourcing of Information Technology Services dated 10th April 2023, Digital Personal Data Protection (DPDP) Act 2023 of Government of India, ISO 27001, ISO 22301, ISO 27701.

b. Any implementation/changes//customizations/enhancements forming part of existing and future statutory and regulatory requirements under the directives of Government of India (GOI), Reserve Bank of India (RBI), MeITY, Cert-In, NCIIPC, UIDAI etc. should be carried out by the Bidder during the entire contract period without any cost to the Bank.

c. 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.

d. 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.

e. The warranty and AMC of the proposed software shall include all version upgrade, patches/fixes, upgrades, compliance of mandates (legal guidelines of GOI as per Gazette of India, regulatory authorities, RBI, etc.) and maintenance support, troubleshooting, performance fine tuning, problem resolution for the OS, database, middleware and the application software for total solution provided by the Bidder.

f. Bidder should carry out the backup, storage and restoration as part of the scope of the RFP document to enable the Bank to achieve regulatory compliance and as per Bank's ISMS & BCMS Policies, RBI, NCIIPC (National Critical Information Infrastructure Protection Centre), NCRF guidelines.

47. 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.

48. Data localization

The service provider shall ensure that all data, as applicable to the concerned bank, is stored exclusively within India, in full compliance with the extant regulatory requirements set forth by the relevant authorities. The service provider shall not store or process any data outside of India without prior written consent from the bank and approval from regulatory bodies.

49. 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.

50. 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.

51. 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.

52. 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 RecoveryPoint 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 andescalation 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.

The bidder agrees to provide all necessary information, documentation, and assistance as requested by the relevant authorities, including but not limited to access to data, records, systems, and personnel, to ensure a smooth transition or orderly resolution process.

In the event of insolvency or resolution of the Bank, the bidder shall continue to perform its obligations under this Agreement unless otherwise directed by the relevant authorities or instructed by Bank.

The bidder shall notify the Bank promptly upon learning of any insolvency, liquidation, or resolution proceedings involving the Bank, and shall comply with any directions provided by the relevant authorities.

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 wellbeing 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.

53. Sustainable Sourcing

The Supplier shall adhere to Sustainable Sourcing practices including but not limited to the use of environment friendly materials, ethical labour 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.

54. 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.

55. Adherence to Cyber Security Policy

Bidder is responsible for complying with the security standards or desired security aspects of all the ICT resources in line with regulatory guidelines from time to time as well as Bank's IT/Information Security / Cyber Security Policy guidelines. Such guidelines will be shared with bidder. Bidder should ensure Data Security and protection of facilities/application managed by them.

The deputed persons should be aware about Bank's IT/IS/Cyber security policy guidelines and have to maintain the utmost secrecy & confidentiality of the bank's data including process performed. At any time, if it comes to the notice of the bank that data has been compromised/disclosed/misused/misappropriated then bank would take suitable action as deemed fit and selected bidder would be required to compensate the bank to the fullest extent of loss incurred by the Bank.

Bidder has to agree and provide undertaking not to disclose any Bank information and will maintain confidentiality of Bank information as per policy of the Bank and will sign "NonDisclosure Agreement" document provided by Bank.

The Service provider Shall put in place necessary controls within its organization for maintaining confidentiality of the Bank's and its customers data.

56. 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.

57. 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.bank.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.

58. 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.

59. 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.

60. 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.

61. Authorized Signatory

The bidder shall indicate the authorized signatories who can discuss and correspond with Bank, with regard to the obligations under the contract. The bidder shall submit at the time of signing the contract a certified copy of the resolution of their board, authenticated by the company secretary, authorizing an official or officials of the bidder to discuss, sign agreements/contracts with Bank, raise invoice and accept payments and also to correspond. The bidder shall provide proof of signature identification for the above purposes as required by Bank.

62. 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.

63. 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 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.

64. Waiver

No waiver of any provision of this Agreement or any of the rights or obligations hereunder shall be effective unless in writing and executed by both parties. A waiver of any breach of any provision of this Agreement shall not be construed as a waiver of any subsequent breach of the same or any other provision. The failure of either party to enforce any provision of this Agreement shall not be deemed a waiver of that provision or of the right of that party thereafter to enforce the same. Any waiver, consent, or approval under this Agreement shall be effective only if it is in writing and signed by the party giving such waiver, consent, or approval.

65. 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.

66. Checklist for Submission

#	Particulars	Bidders Remark Yes/No
1	Certificate of incorporation	
2	GSTN Registration Certificate	
3	Copy of Audited Balance sheets of last three years 2022-23, 2023-24 & 2024-25 of the bidder	
4	CA certificate for three years average turnover for financial years 2022-23, 2023-24 & 2024-25 of the bidder	

5	CA certificate for operating profit for last three financial years 2022-23, 2023-24 & 2024-25 of the bidder	
6	CA certificate for net worth for last three financial years 2021-22, 2022-23, 2023-24 & 2024-25 of the bidder	

#	Particulars	Bidders Remark Yes/No
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 • 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	Certified copy of the registration certificate if the bidder is from a country which shares a land border with India	
13	Letter of acceptance (LoA)/ purchase order along with completion certificate or any relevant document acceptable to Bank/ work order/ contract/ completion certificate Deployment Certificate issued by client to the bidder/Particulars confirming relevant experience for Eligibility Criteria 11	
14	Letter of acceptance (LoA)/ purchase order along with completion certificate or any relevant document acceptable to Bank/ work order/ contract/ completion certificate Deployment Certificate issued by client to the bidder/Particulars confirming relevant experience for Eligibility Criteria 12	

15	Letter of acceptance (LoA)/ purchase order along with completion certificate or any relevant document acceptable to Bank/ work order/ contract/ completion certificate Deployment Certificate issued by client to the bidder/Particulars confirming relevant experience for Eligibility Criteria 13	
16	Undertaking on company letter head for Eligibility Criteria 14	
17	Letter of acceptance (LoA)/ purchase order along with completion certificate or any relevant document acceptable to Bank/ work order/ contract/ completion certificate Deployment Certificate issued by client to the bidder/Particulars confirming relevant experience for Eligibility Criteria – 17	
18	Letter of acceptance (LoA)/ purchase order along with completion certificate or any relevant document acceptable to Bank/ work order/ contract/ completion certificate Deployment Certificate issued by client to the bidder/Particulars confirming relevant experience for Eligibility Criteria – 18	

#	Particulars	Bidders Remark Yes/No
19	Letter of acceptance (LoA)/ purchase order along with completion certificate or any relevant document acceptable to Bank/ work order/ contract/ completion certificate Deployment Certificate issued by client to the bidder/Particulars confirming relevant experience for Eligibility Criteria – 19	
20	Letter of acceptance (LoA)/ purchase order along with completion certificate or any relevant document acceptable to Bank/ work order/ contract/ completion certificate Deployment Certificate issued by client to the bidder/Particulars confirming relevant experience for Eligibility Criteria – 20	
21	Letter of acceptance (LoA)/ purchase order along with completion certificate or any relevant document acceptable to Bank/ work order/ contract/ completion certificate Deployment Certificate issued by client to the bidder/Particulars confirming relevant experience for Eligibility Criteria – 21	
22	Copy of the power of Attorney of signing authority / executor	
23	Annexure 1: Bill of Material	
24	Annexure 2: Minimum Technical Specifications	
25	Annexure 3: Conformity Letter	
26	Annexure 4: Bidder's Information on company letter head	

27	Annexure 5: Letter for Conformity of Product as per RFP Bidder's	
28	InformationAnnexure 6 :onUndertakingcompany letterfor acceptanceheadof terms of RFP	
29	Annexure 7: MAF on OEM's letter head in Bank's format	
30	Annexure 8: Integrity Pact	
31	Annexure 9: Non-Disclosure Agreement	
32	Annexure 10: Performance Bank Guarantee	
33	Annexure 11: Pro forma for Bid Security (EMD)	
34	Annexure 12: Bidders Particulars in Company Letter Head	
35	Annexure 13: NPA UNDERTAKING / PENDING LITIGATION / BLACKLISTING	
36	Annexure 14: Undertaking letter (Land Border Sharing)	
37	Annexure 15: Cover Letter	
38	Annexure 16: Pre-Bid Query Format	
39	Annexure 17: Eligibility Criteria Compliance	
40	Annexure 18: Self declaration for compliance to RBI master direction on outsourcing of it services	
41	Annexure 19: GOI Guidelines For Preference To Make In India	
42	Annexure 19A: Certificate of Local Content	
43	Annexure 20: Guidelines on banning of business dealing	
44	Annexure 21 : Undertaking for 5 years Roadmap	
45	Annexure 22 : Undertaking for Information Security	
46	Annexure 23 : Undertaking for Authenticity of the product	
#	Particulars	Bidders Remark Yes/No
47	Annexure 24 : List of Hardware and Software required for Implementation	
48	Annexure 25 : Proposed Team Profile	

67. 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 H)

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	Migration and Transition Cost (Table D)			
5	AMC Cost (Table E)			
6	ATS / Subscription Cost (Table F)			
7	FMS Cost (Table G)			
8	Professional Services Cost (Table H)			
9	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	Make, Model and Configuration	Quantity (Q)	Unit Rate (R)	Total Price T=QxR	GST Amt	Total Cost including GST
1	SERVERS						
2	APPLIANCE						
3	STORAGE						
4	H/W LOAD BALANCER (IF ANY)						

5	SAN SWITCH IF ANY						
6	HIGH SPEED BACKUP DEVICE FULL SET						
7	2*2 Video wall with 55" display with hardware based controller of 16		1				
	inputs and 4 outputs (4K)						
8	Any other item						
	Cost of Table - A						

Table – B (Software Cost)

Price Schedule For Next Generation Security Operation Center Solution Licenses/Software Cost With One Year Warranty							
SNO	Item Description	OEM name and Application / Soft ware Details	Quantity (Q)	Unit Rate (R)	Total Cost T=QxR	GST Amt	Total Cost including GST
1	SIEM License for DC And DR Location		1,00,000 EPS / 3.4 TB				
2	UEBA Licenses		40,000				
3	SOAR		25 Analysts				
4	Threat Intelligence Feeds						
5	Brand Protection Services (including Deep Dark Web						

	Monitoring)						
6	Operating System						
7	Database Software						
8	Backup Software						
9	Additional SIEM Licenses		Additional10,000 EPS license pack				
10	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 Feeds Implementation			
5	Brand Protection Services (including Deep Dark Web Monitoring) implementation			
6	Any Other Item			
Cost of Table – C				

Table – D (Migration and Transition Cost)

SNO	Item Description	Total Cost	GST Amt	Total Cost including GST
1	Migration and Transition Cost			
2	Any Other Item			
Cost of Table – D				

Table – E (AMC Cost)

	Price Schedule For Next Generation Security Operation Center Solutions – HARDWARE AMC Cost (2 Years) – 4th & 5th Year					
SNO	Item Description	4th Year AMC Cost (P)	5th Year AMC Cost (Q)	Total Price T=P+Q	GST Amt	Total Cost including GST
1	SERVERS					
2	APPLIANCES					
3	STORAGE					
4	H/W LOAD BALANCER (IF ANY)					
5	SAN SWITCH IF ANY					
6	HIGH SPEED BACKUP					
	DEVICE FULL SET					
7	2*2 Video wall with 55" display with hardware based controller of 16 inputs and 4 outputs (4K)	1				
8	Any other item					
Cost of Table - E						

Table – F (ATS/Subscription Cost)

Price Schedule For Next Generation Security Operation Center Solution Licenses/Software ATS/Subscription Cost -4 Years

SNO	Item Description	2nd[t] Year Cost (A)	3rd Year Cost (B)	4th Year Cost (C)	5th Year Cost (D)	Total Price T=A+B+ C+D	GST Amt	Total Cost including GST
1	SIEM							
2	UEBA							
3	SOAR							
4	Threat Intelligence Feeds							
5	Brand Protection Services (including Deep Dark Web Monitoring) implementation							
6	Operating System							
7	Database Software							
9	Backup Software							
10	Additional 10,000 SIEM Licenses							
11	Any Other Item							
Cost of Table - F								

Table – G (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 for 1st Year	Cost Per Resource for 2nd	Cost Per Resource for 3rd	Cost Per Resource for 4th Year	Cost Per Resource for 5th Year	Total Cost for Five years	GST Amt	Total Amount including GST

				Year	Year					
		(A)	(B)	(C)	(D)	(E)	(F)	A x (B+C+D+E+F)		
1	Project Director	1								
1	L3	2								
2	L2	11								
3	L1	18								
Cost of Table - G										

Table – H (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	Cost Per Man Days for 1st Year	Cost Per Man Days for 2nd Year	Cost Per Man Days for 3rd Year	Cost Per Man Days for 4th Year	Cost Per Man Days for 5th Year	Total Cost for Five years	GST Amt	Total Amount including GST
		(A)	(B)	(C)	(D)	(E)	(F)	A x (B+C+D+E+F)		
1	Professional Services for SIEM, SOAR, UEBA, Threat Intelligence	25								

	Feed, Brand									
	Protection (including Dark Web) etc.(on need basis)									
Cost of Table - H										

- All products quoted / offered by bidder must be having 24 x 7 x 365 enterprise supported version from OEM.
- 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.
- Successful bidder is required to submit Software Bill of Material (SBOM) and Crypto Graphic Bill of Material (CBOM) in Bank's format as and when required.
- 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. Failure to comply with submission of masked replica of BOM on the letterhead of the bidder, duly signed and sealed by an authorized signatory will be liable to rejection of the bid.
- 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 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 8% and ATS rates must be quoted above 12% for the respective product(s).

Signature

Name:
Designation:
Seal of Company
Date:

68. ANNEXURE 2: MINIMUM TECHNICAL SPECIFICATIONS

S. No.	SIEM Requirement Specifications	Compliance (Y/N)	Vendor Remark and supporting documentary proof from OEM
Mandatory Specifications (3 marks for each point)			
1	The proposed solution must include Next Gen SIEM, Security Analytics, Big Data Analytics with necessary automation capabilities. To avoid maintaining multiple data repositories, proposed solution should have a single central data repository including security logs which should act as common data lake for SIEM, UEBA & SOAR.		
2	The proposed solution should be sized for 1,00,000 sustained EPS and should be scalable up to 1,50,000 sustained EPS without dropping or queuing of logs as per bank requirement. There should not be 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	To virtually segregate different types of data, proposed solution should support unlimited virtual storage groups or indexes. Each index/ virtual storage group should be used for searching specific data and retention period should be configurable as per storage groups or indexes and should not be hardcoded.		
4	The proposed solution must support the data replication natively without relying on other third party replication technologies on the operating system or storage level with near zero RPO and RTO. Solution 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.		
5	The proposed solution should provide a test/dev license as part of the solution. It should also provide a tool in-built or integrable, that allows to create test bed environment which can help to simulate blue team and red team attacks to test use cases, train analysts etc.		

6	The proposed solution should be able to receive, ingest and index		
	structured or unstructured data without schema or normalization and no events should be dropped if log source changes the format of log data.		
7	Machine learning should be embedded across the platform (SIEM, DATA LAKE, SOAR & UEBA). It should empower every user in the SOC with ML. Security analyst to become citizen data scientist i.e. used predefined ML algorithms to detect & predict threats, threat hunters to build their own ML models with steps to build, train and implement model and data scientists should be able to integrate various ML frameworks.		
8	The solution must ensure that if data ingested is not parsed then with the new parser old data ingested should also be parsed without need to re-ingest data in the SIEM throughout the minimum retention period of online 180 days and 365 days of archival.		
9	The proposed solution should have Out of The Box support for identifying data gap for deploying MITRE ATTACK & Kill Chain use cases. It should help to check data availability and guide on data sources are required to implement MITRE ATTACK Technique & Sub techniques.		
10	The proposed solution should be deployable on commodity HW including Physical and Virtual and should be IPv6 compatible in both Standalone and High Availability deployments		
11	Log Filtering – Logs can be filtered by the source system, times, or by other rules defined by the SIEM administrator.		
12	The solution should use a distributed, horizontally scalable architecture for large-scale designs to support high-performance search queries. It should not rely on legacy relational databases nor impose limitations on the event database for larger architectures.		
General Specifications (2 marks for each point)			

13	The proposed solution should have physical or logical separation of the collection module, logging module and analysis / correlation module with the ability for adding more devices, locations, applications, etc.		
14	The proposed solution must support caching mode of transfer for data collection, to ensure data is being logged in the event of loss of network connectivity, and resume sending of data upon network connection.		
15	The proposed solution must have a user-friendly interface to convert statistical results to dashboards with a single click. The real-time dashboard should support Realtime updates ensuring analyst assess to the most current and relevant information at all the times the dashboard should publish/populate the real-time log in structured format containing all the relevant details.		
16	The proposed solution must provide an interface that allows the query string to be configured as an alert, report or a dashboard panel. Same query string with minimum modifications should also be capable of being used for security data lake & SIEM.		
17	OEM / OEM certified partner to provide n number of parsers for data ingestion for all the current data sources and their respective upgrades (in maximum 15 business days from data of intimation of the same) during the contract period. If any new data source is added during the contract period, the OEM / OEM certified partner will provide parsers for data ingestion in maximum 15 business days from date of intimation of the same.		
18	The proposed solution must be scalable and have a distributed architecture with native replication of data across DC & DR. DR should be active all the time to ensure continuous security monitoring. The dual forwarding feature should be configurable as per bank requirements and capability for enabling & disabling should be available depending on the device, IP address, and other related parameters.		

19	The proposed solution must support single site or multiple site clustering allowing data to be replicated across the peer's nodes and across multiple sites with near zero RTO & RPO. This solution should keep full copy of data at at least two sites - DC and DR		
20	The proposed solution should be able to promptly notify the designated personnel in case of any component failure. This notification should be real-time and capable of delivering alerts via multiple channels such as SMS or integration with incident management platforms		
21	The proposed solution should support RADIUS, Active Directory, PAM, LDAP and SSO for authentication		

22	The proposed solution must support a configurable replication factor of N where it can tolerate the failure of N-1 peer nodes or should handle failure of a node in the solution. Also, the solution should be able to handle up to 3 days of data at the log source, in case of failure of connectivity with central log store.		
23	The proposed solution must be software based allowing flexible deployment models and architecture.		
	Supported Data Sources (2 marks for each point)		
24	The proposed solution must be able to support both real-time and on-demand access to data sources from files, network ports, database connections, custom APIs, public cloud, private cloud and interfaced incl. text, XML, JSON and other evolving format, and normalize the data		
25	The proposed solution must be able to read data input from the following log file formats: a. Archived Log Files (Single line, Multi-line, and Complex XMLand JSON Structure) b. Windows Events Logs c. Standard Log Files from applications such as Web (HTTP) servers, FTP servers, Email (SMTP/Exchange) servers, DNS servers, DHCP servers, Active Directory servers, etc.		

26	The proposed solution must be able to accept the following indicative live data streams feeding through the network: a. Syslog Messages b. Security Alerts c. JSON streaming over HTTP/HTTPS		
27	The proposed solution must support the decoding of the following indicative network protocols from log data or picking the meta data from network traffic: HTTP, FTP, DNS, MySQL, SMTP, SNMP, SMB, TCP, UDP, NFS, Oracle (TNS), LDAP/AD, PostgreSQL, Sybase/SQL Server (TDS), IMAP, POP3, RADIUS, IRC, SIP, DHCP, AMQP, DIAMETER, MAPI,		
28	The proposed solution must come with out-of-the-box integration and dashboards, reports, rules etc. to provides rapid insights and operational visibility into large-scale CentOS, Windows, Unix and Linux environments machine data: syslog, metrics and configuration files.		

	Index, Search, Filter, Analyze and Investigate (2 marks for each point)		
29	The proposed solution must be able to index all data from any application, server or network device including logs, configurations, messages, traps and alerts, metrics and performance data without any custom adapters for specific formats so that the analyst can have end to end visibility of the ecosystem. Indicative		
30	The proposed solution must be able to build an unstructured index or store data in its original format without any rigid schema and without tampering or altering with the raw data/logs/events along with support of log encryption in transit and at rest		
31	The proposed solution's licensing should be based on post filtering of events. If log events are filtered, then they should not be counted in license.		

32	Proposed solution should forward data to multiple destinations apart from its own SIEM processing/data storage layer. Log collector should be able to forward data to multiple destinations and should have ability to create dashboards / reports for log reconciliation.		
33	The proposed solution should support external storage integration (such as but not limited to low cost storage, tape drives, etc.) for log storage and archival		
34	The proposed solution will be continuously used in the SOC so that solution builds specific repository which includes categories like including event types, tags, lookups, parsing/normalizing, actions and saved searches etc. It should help to discover and analyze various aspects in data. For example, event types should enable analyst to quickly classify and group similar events; then use to perform analytics on events.		
	Monitor, Alert and Reporting Functions (2 marks for each point)		
35	The proposed solution must be able to run any search on a schedule and set alerting conditions based on thresholds and deltas in the number and distribution of results across a time range or days like a histogram visualization.		
36	The proposed solution must be able to execute automated corrective or follow-on actions via scripted alerts.		
37	The proposed solution must support viewing of the same log data in different formats or should support multiple schema views during search time or report building time without redundant storage or reindexing so that complex report or user defined reports can be built.		
38	The proposed solution must be able to support sophisticated statistical and summary analysis by pipelining advanced search commands together in a single search.		

39	The proposed solution must be able to support mathematics functions to perform calculations on field values, examples Converting bytes to kilobytes, mega-bytes, absolute value functions, highest integers, standard deviation, command length etc.; Finding the time duration between time stamp values. These functionalities should be available as a search, report, alert or dashboard etc. so that analyst can build any kind of report required.		
40	The proposed solution must be able to support predictive analytics to predict future values of single or multi-valued fields. This will help security analytics to predict the attack patters or specific attacks using multiple fields in the alerts or logs.		
41	The proposed solution must possess built-in function for Predictive Analysis: a. Uses historical data as a baseline to forecast future patterns,thresholds and tolerances b. Ability to identify the future needs of critical system resources,no prior knowledge in predictive modelling algorithms required to use this functionality, and the ability to easily interpret and customize the results.		
42	The proposed solution must come with pre-packaged alerting capability, flexible service-based hosts grouping, and easy management of many data sources, and provide analytics ability to quickly identify performance and capacity bottlenecks and outliers in Unix and Linux environment. It should quickly compare resources and capacity utilization across many hosts.		
43	The proposed solution should be able to audit all changes made to all of its components		
44	The proposed solution should provide dashboards for insight into resource consumption of desired systems, service availability status		

	of critical services, integration with NMS tools for network status visibility, security alerts, risky users & entities, anomalies and outliers across all the data etc. from a single dashboard.		

45	The proposed solution must possess built-in feature for anomaly detection: a. Uses historical data as a baseline to forecast future patterns, thresholds and tolerances b. Ability to identify the future needs of critical system resources,no prior knowledge in predictive modeling algorithms required to use this functionality, and the ability to easily interpret and customize the results		
46	The proposed solution should give visualization of operational health of the Windows, Linux & Unix environment through a single dashboard customizable to service-groupings in your environment.		
47	The proposed solution should have the capability to collaborate and orchestrate with 3rd party solutions and the solution should be able to be embedded in third-party business applications such as SharePoint, WordPress, Wiki, etc.		
	Artificial Intelligence Machine Learning (2 marks for each point)		
48	The proposed solution must provide GUI that can easily help to build, built-in or custom machine learning models using the predefined sequence and should be able to integrate with a collection of NLP and classical machine learning libraries, generic machine learning tools like tensor flow, pytorch, R, Python, Scala etc.		
49	The proposed solution machine learning capabilities must include API access for searching & data extraction, role-based access controls for machine learning models.		
50	The proposed solution machine learning capabilities must allow addition of custom machine learning algorithms from popular libraries like NLP, Python etc.		
51	The proposed solution should natively have ML capabilities and should not have separate engine/compute requirements for running ML models.		
	Search and Reporting (2 marks for each point)		

52	Reports can be scheduled in a dynamic fashion with schedule windowing and prioritization to improve run priority of high value scheduled reports and manage concurrently running reports to meet the requirements of completing reports under 24 hours. The report should be parameterized, and the user should be able to scale the parameter as needed. And Out of box aging analysis of incident should be available.		
53	The solution must provide drill down functionality that is user defined, allowing users to drill down into another report, dashboard, raw events or passing URL parameters to any third party website. The Report should be scalable IP-wise, device- wise, user-wise, data-wise, location-wise based on requirement between any two dates.		
54	The product internal logs must be ingested within the product for ease of troubleshooting and investigation and those logs do not consume the product license.		
55	The solution must provide granular license utilization down to devices, log sources and data store or additional lookups of devices to agencies by the minute and the retention of granularity can be extended to the project requirement.		
56	The proposed solution should support historical correlation and to search for matching historical data using new correlation rule		
57	The solution must provide the same search language for search, investigate, alert, report and visualize license utilization. It should be able to support Boolean-style search patterns, complex regular expressions and free text searches. A proper error handling screen should be available.		
58	The solution should have capability to support more than 1000 correlation rules which should be available out of the box		
59	The solution's reports should run fast on large data sets. Proposed solution should use next generation functionalities like creating set of data from the main index or data store. This will avoid running the queries on large index or full index and faster response for searching and reporting.		
	Fields, Schema and Log Parsing (2 marks for each point)		

60	The solution must support viewing data in different formats or schemas without re-consumption, re-indexing, redundant storage. Historical data also should be viewed as per new format or schema without re-consumption or without additional storage utilization.		
61	The solution must allow the adding/modifying/removing of log parsers without impacting log collection from the web interface.		
62	The solution must provide a field extraction wizard that is used to create parsers and allow testing and validation with existing live or historical data within the system from the web interface.		
63	Old data should be parsed with new parser without re-consumption or re-indexing the data. Any additional license or storage should not be consumed because of parsing through new parser.		
	Security Analytics Platform (3 marks)		
64	The proposed solution must provide the following capabilities as a Security Analytics Platform: a. One single syntax that can be used universally for search queries,alerts, reports or dashboards, SIEM and preferably for Data repository lake also. b. Incident management technique to facilitate incident tracking,investigation, pivoting and closure c. Risk management technique to apply risk scores to any asset oruser based on relative importance or value to the business d. Threat intelligence technique that automatically collect, aggregate, indicators of compromise from threat feeds. The solution should have capability to alert in case duplicate indicators of compromise is added.		
	Security Analytics Platform (2 marks for each point)		
65	The proposed solution must be fully integrated with the log platform without the need to duplicate the collected raw logs.		

66	The solution should be able to assign risk score with Scoring for various identified entities like user & assets should be possible based on the threats or correlations that particular host, username, entity, location has contributed.		
67	The proposed solution must be able to assign any arbitrary risk score based on self-defined query based on any correlated events,		
	statistical analysis, threat indicator match, importance to the business.		
68	The Proposed solution must offer all the below built-in threat detection techniques out of the box: Detect Web Application Threats. Detect APT Threats Integrate with any Honeypot/Deception solutions Integrate with any NBAD tools Detect threats indicated by advisories Give visibility of endpoints also by integrating with EDR, Antivirus etc. for endpoint analytics.		
69	The proposed solution must be able to retrieve from any threat feeds without restriction, retrieve threats in various ASCII/UTF- 8 file formats like text, csv, xml. Must be able to automatically parse IOC from STIX and Open IOC formats. Must be able to support multiple transport mechanisms such as TCP or Trusted Automated exchange of Indicator Information (TAXII).		

70	The proposed solution must be able to support at least 8 out the following indicative list: a) Network b) HTTP Referrer, User Agent, Cookie, Header, Data, URL c) IP d) Domain e) Endpoint f) File Hash, Name, Extension, Path and Size g) Registry Hive, Path, Key Name, Value Name, Value Type, Value Text, Value Data h) Process Name, Arguments, Handle Name, Handle Type i) Service Name, Description j) Certificate k) Certificate Alias, Serial, Issuer, Subject, Start Time, End Time,Version, Handshake Type, Public key Algorithm, Signature Algorithm l) Email m) Email Address, Subject Body		
71	Beside event matching signature use cases, the proposed solution must have the following analytical capabilities to address anomalies and behavioral based use cases.		
72	Basic Statistical analysis that can be applied to any fields like calculating the length of command line arguments, HTTP user agent string, sub domains, URLs, standard deviation of count of		
	events over time		
73	The proposed solutions should use multiple technologies like using distance formula, geo Database, etc. to detect geographically improbable access		
74	The proposed solutions should use randomness to measure domain names that can be potentially from malware domain generated algorithms.		

75	The proposed solution should use statistic functions or techniques like percentile or standard deviation to detect unusual activities that can be applied to insider or fraudulent use cases. Other analysis: Find common or rare events using cluster or most commonly and widely used means clustering method Find percentage of times two fields exist in the same events correlating all the fields. Indicative		
76	The proposed solution should find relationship between pairs of fields (in event or desired metadata) by change in randomness in pair of fields.		
77	The proposed solution's detection use cases should be comprised of guidance that provides an assessment of the Security Threat and how it helps detect and investigate it using the proposed solution. In addition, it should provide a summary of how the attack or detection technique maps to the following: ATT & CK MITRE, an adversary behavior model that describes the actions an adversary might take. Kill-Chain, a model that identifies the phases an adversary must complete to achieve their objective. CIS Critical Security Controls Data types that are referenced within the rules/ search and that need to be populated. Technologies, example technologies that map to the data types. There should be template to upload advisories in an automated manner. There should be templates to design and trigger work flows automatically. Any other customizable templates as per bank requirements.		
78	The proposed solution should also guide administrator on data sources required to implement detection technique from the same console (ATTACK MITRE, CIS, NIST, Kill Chain etc.)		
	Incident Response (3 marks for each point)		

79	The proposed solution must provide investigation auditing capability to enable analysts to easily: Track searches and activities Review activities at any point Select and place into timeline for temporal analysis Help remember searches, steps taken, provide annotation support		

80	The solution must be able to provide a built-in facility to centralize incident analysis of entities in one location.		
	Incident Response (2 marks for each point)		
81	The proposed solution should be able to trigger actions. These actions can be automatically triggered by correlation alerts or offences or manually run on an ad hoc basis from the Incident.		
82	The proposed solution should have integration with major commercially available tools OOTB for triggering actions or integration with all commercially available SOAR for initiating action to be taken.		
83	The proposed solution should be integrated with the SOAR, UEBA, TIF and Brand Protection solutions.		
84	The proposed solution must provide out-of-the-box (OOTB) dashboards for MTTD, MTTR, and MTTI in SIEM incident management through integration with SOAR.		
85	The proposed solution should ensure real-time replication of analyst comments and all other incident updates from the primary data center (DC) to the disaster recovery (DR) site.		
86	The proposed solution must not rely on third-party or open-source components. It should include its own proprietary agent for collecting logs from operating systems such as Windows, Linux, and Solaris.		
S. No	SOAR Requirements Specifications	Compliance (Y/N)	REMARKS and supporting documentary proof from OEM
	Mandatory Specifications (3 marks for each point)		
1	The proposed solution must have an orchestrator ability to direct and oversee all activities from beginning to end.		

2	The proposed solution orchestrator must be able to ingest security data from any source and in any format. Example: Email based alerts SIEM Based alerts		
3	The proposed solution orchestrator must be able to poll data sources or pull data into the platform.		
4	The proposed solution orchestrator must be able to interpret the data and make it usable by the platform. Example: extracting indicators from emails IP address Domains File Hashes		
5	The ability to extract indicators from various files attachments such as PDFs, emails, or raw text. Example: .txt .eml like Outlook Email Messages PDF Docx CSV HTML		
6	The proposed solution orchestrator must be able to initiate automation upon creation of new events with artifacts or existing events with new artifacts without human intervention.		
7	The proposed solution orchestrator must be able to dispatch automation tasks from its queue at the appropriate and optimal time, passing them to the automation engine for execution.		
8	The proposed solution orchestrator must be able to introduce human supervision if necessary, pausing the automation engine for an approval by asset owner is needed to execute a security action on a target.		
9	The proposed solution orchestrator must ensure output data from one action is properly parsed, so that future actions can make use of		
	it.		

10	Consistent, Standardized naming conventions for actions. Normalized action names in a Virtualization / Abstraction layer allows easy transition across API action calls and/or products		
	General Specifications (2 marks for each point)		
11	The proposed solution must provide a built-in visual automation editor.		
12	The proposed solution built-in visual automation editor must enable users to construct comprehensive and sophisticated playbooks to fully validate, investigate and resolve incident using drag and drop capabilities visually without needing the expert ability to code.		
13	The proposed solution built-in visual automation editor must be able to represent code using blocks and blocks can be connected in a one-to-one, one-to-many and many-to-one fashion to dictate an order of execution.		
14	The proposed solution built-in visual automation editor must be able to provide an interface where testing and debug can take place allowing transition from edit mode to test mode seamlessly.		
15	The proposed solution must provide an open and extensible interface for new integrations to connect the platform to any of the thousands of point products available in the security market today.		
16	The proposed solution must provide easy transition in and out of other security technologies without negatively impacting automated playbooks.		
17	The proposed solution must provide users with the framework and open control of integrating with other technologies without relying on the solution provider for development work.		
18	The proposed solution must standardize on one language like Python for developing integrations with other technologies for custom actions and custom handling of playbooks confined in a block while retaining the original visual playbook editor functionality for the entire playbook.		
19	The ability to run multiple playbooks and actions while retaining the		

	data in the containers/events/cases.		
20	Retaining the data of all multiple runs of playbooks ensure the retention of key artifacts especially with dynamic information like reputation information.		
21	The proposed solution must have documented REST API access that allows full control over the platform.		
22	The proposed solution must have ability to label the nature of the event.		
23	The proposed solution must have ability to store attachment as part of the user manual workflow or as part of the automated playbook.		
24	The proposed solution must be able to extract and store attachments from ingested emails.		
25	The proposed solution must have the ability to mark artifacts as evidence.		
26	The proposed solution must be able to provide an indicator view to quickly pivot investigation of an indicator to past incident occurrences.		
27	The proposed solution must allow case or task assignment in relation to a ticket or an incident to other team members or group.		
28	The proposed solution must provide fine grained role-based access into actions and assets, so users can be granted with investigative actions and not containment actions.		
29	The proposed solution should have an out of the box guidance by offering suggestions to help investigate, contain, eradicate, and recover from a security event, allowing newer analyst to take and validate choices of more experienced analysts.		
30	The proposed solution must have an activity log of actions taken (automated and manual), results returned by actions, chat and comment history in each event.		

31	The proposed solution must provide central management of incidents and administrative functions from a single web-based user interface.		
32	The proposed solution must provide multi-tenancy support allowing multiple departments or business units to use the same solution with		
	appropriate segregations/separations.		

Sr No	UEBA Requirement Specifications	Compliance (Y/N)	Remarks and supporting documentary proof from OEM
	Mandatory Specifications (3 marks for each point)		
1	The UEBA must be able to monitor all the users in the organization. UEBA should not have separate data repository and should consume and operate on data lake or SIEM data repository.		
2	The UEBA must create a heuristic baseline of user activity by analyzing behavior, so it must perform multidimensional baselining, enabling the modeling of a broad set of user behaviors. Baselines are used to detect anomalous behavior via machine learning and other statistical analysis techniques.		
3	Proposed solution should use behavior modeling, peer-group analysis, and machine learning to uncover hidden threats in our environment. It should automatically detect anomalous behavior from users, devices, and applications, combining those patterns into specific, actionable threats.		
4	The proposed UEBA solution should perform identity resolution to find the real-time association between IP addresses, host names, endpoints, endpoints location and users, and maintain these associations over time.		

5	Investigate and respond to detected threats using a streamlined threat review workflow that provides visibility into anomalous activity and supporting evidence. Should increases the effectiveness of our security analysts by helping them focus on threats and malicious activities with kill chain and geographical visualizations.		
	General Specifications (2 marks for each point)		

6	Proposed solution should detect threats by normalizing device and domain names, and associate all AD accounts.		
7	The proposed solution should use unsupervised machine learning algorithms to analyze the data for activity deviating from normal behavior.		
8	The proposed solution should have threat detection technique and models to distill anomalies down to a real handful threat. A single violation might not represent a legitimate threat in our environment. Over time, however, a series of violations should tell a story about a threat that must be investigated. Threat detection models should stitch together anomalies to provide an end-to-end story about a high-fidelity threat.		
9	Proposed solution should leverage the data in SIEM platform and not build its own data store and maps the fields in the data to UEBA-specific fields.		
10	The proposed solution should have anomaly detection models to analyze the data in UBEA and create anomalies or violations based on a variety of factors.		
11	The proposed solution should be able to create new anomaly detection models or clone existing models from the GUI.		
12	The above categories typically should correspond to stages of the kill chain and make it possible for the threat logic to place anomalies into the correct sections of the chain.		
13	The proposed solution should find deviations from typical behavior or detection of interesting patterns like beaconing.		

14	The proposed solution should detect threats using graph-based threats, which are computed based on groups of similar anomalies rather than anomalies grouped by user or device. Example graph-based threats are public-facing website attack or fraudulent website activity.		
15	The proposed solution should detect threats like Lateral Movement and Data Ex-filtration. These should collect data about anomalies and users or devices to determine the likelihood of a threat.		
16	UEBA should perform identity resolution to find the real-time association between endpoints, IP addresses, host names,		

	endpoint location, and users, and maintain these associations over time.		
Sr. No	Threat Intelligence Feeds(TIF) Requirement Specification	Compliance (Y/N)	Remarks and supporting documentary proof from OEM
	Mandatory Specifications (3 marks for each point)		
1	The solution must provide intelligence of entities, proprietary or OSINT sourced, in a single viewing pane; (i) IP Addresses (ii) Domains (iii) Hashes (iv) URLs (v) Malwares (vi) TTP (vii) Threat Actors		

2	Solution should support automated machine based Natural Language Processing for deep analysis on at least 14 most common Cyber Criminal languages used like (i) Arabic (ii) Chinese (both simplified and traditional script) (iii) English (iv) Farsi (Persian) (v) French (vi) German (vii) Italian (viii) Japanese (ix) Portuguese (x) Russian (xi) Spanish (xii) Swedish (xiii) Korean (xiv)Ukrainian		

3	Intelligence should include provisioning of hunting tools, such as YARA rules, SNORT rules, Sigma Rules, MITRE ATT&CK Identifiers to assist in hunting for adversaries, malware, or traffic of interest wherever available.		
4	The YARA rules should be able to be downloaded directly from the Threat Intelligence Portal.		
5	Solution should support Unlimited Yara Rule generation with help of AI without having deep knowledge of YARA to avoid false positive.		
6	Enrich IoC/IoA received from other sources like RBI, CERT-IN, NCIIPC and other regulatory bodies with help of Browser Extension.		
7	Identify potential exploits for vulnerabilities linking and alerting only for technologies in making at Proof of concept stage before Day-0 Exploits and Vulnerabilities with customized alerts for technology stack being used in the our environment.		

8	Threat actor (Nation State Sponsors, Financially Motivated and APT groups) profile description : Detailed information on at least 3500+ unique Threat Actor's origin, targets and Motive, TTP and active exploit along with its reputation		
9	Dedicated Industry Threat Dashboard to monitor the business industry and relevant Partners, peers and 3rd party for cyber trends.		
10	The solution must provide a direct link to the source, or a cached copy of metadata posted on dark web in near real time without analyst actually going onto Dark web to look for evidence.		
11	Solution should provide up to 15+ years Historical and current data around IoC/Malwares/Actors for detailed analysis. OEM should be established for at least 15+ years in industry.		
12	The offered solution must have a capability to create a custom Threat Actor heat map curated for Bank based on Intent and Capability of the threat actors.		

13	Threat Intel OEM must be in existence for more than 15 years and the offered solution should have readily searchable data (for up to last 15 years) with the specific dates of event. The OEM may be required to demonstrate the same at the time of technical evaluation.		
	General Specifications (2 marks for each point)		
14	The solution should have Mobile App for access to the Threat Intelligence and critical alerts on the move from anywhere on Smart phones with Internet Access mobile app available via Apple Store on Google Play store. It should support Search and AI bot capability for user friendly access.		
15	Solution should support IP Deprecation from Firewall blocklist to clean up the Firewall		

16	The solution must identify if Organization's partners and suppliers are ransomware victim irrespective of the public disclosure by monitoring the Ransomware extortion sites.		
17	The Sandbox solution should support below features and abilities, (i) More than 1000 analysis per day & File size of more than2Gb (ii) Support sandbox service for Files, URLs, Source Code andQR codes (iii) Support for Windows, Linux, Android and MACOS environments for sandboxing. (iv) Support for interactive mode where Organization's analystcan have live interaction with the endpoint and modify things while the file analysis in in progress. (v) Access to the screen recording of the file analysis overvirtual machine. (vi) Should have big scale and repository of analyzing morethan 1 Million Malware samples per day.		
18	The Sandbox solution should be native and owned by same OEM		
19	Threat Intelligence vendor should have native Browser Extension for Quick triage and Enrichment of IoC		

20	The browser extension must have the capability to export the IOC such as IP, Domains, URLs, Hash files into separate CSV files directly from the browser plugin.		
21	AI based Chatbot search, Query and Auto Report generation should be supported		
22	Malware Hunt (Live Hunts and Retro hunts)		
23	Contextual and Evidence based API Feeds for IP, Domains, URL and Malware hashes to be integrated with SIEM like Qradar, Splunk, Logrhythm etc.		
24	API feeds should support more than 10000 API calls per day to support correlation and enrichment of IoC.		

25	OEM's Solution should be GDPR complied		
26	Threat Intelligence Vendor should be serving more than 1000 Customers globally for threat intelligence solution		
27	Threat Intelligence vendor should have all of the mentioned Certifications ISO 27001, ISO 9001, ISO 27701, ISO 27017, SOC 2 Type 2, and NIST 800-218 SSDF certified		
28	Threat Intelligence Vendor should have spent over $50M across its research, development, and intelligence services to provide the world's leading intelligence platform Over the last twelve months.		
29	OEM should have registered entity in India.		
30	On-boarding, Quarterly Reviews and Technical Trainings should be led directly by Threat Intelligence OEM.		
31	The Threat intel Feeds (TIF) OEM should not be blacklisted by any organization in India.		
32	Bidder should offer Threat Intelligence solution and feed other than the ones already present currently in Bank environment.		
33	The solution should offer the IoC score update every one hour for faster time to action.		
34	The solution must be offered with a Technical Account Manager/Customer Success Manager directly from the OEM to offer the following services :		

	Provide enablement around licensed product and services Handle customer support escalations and feature request Provide insights into the product usage and benchmarking of alerts against Industry peers Provide training and enablement on new product features and services. Provide in person Threat Briefings /Custom workshops and tabletop exercises/ Detailed reporting on topics/events/industries of customer interest considering 1 such activity twice a year		

35	The Brand Intelligence and the Threat Intelligence feeds should be from different OEM.		

Sr	Brand Protection (including Dark Web Monitoring) Specifications	Compliance (Y/N)	Remarks and supporting documentary proof from OEM
	Mandatory Specifications (3 marks for each point)		
1	Social Media Monitoring: The platform should monitor all the major social media platform, including, but not limited to; Twitter, Facebook, YouTube, Instagram, LinkedIn, Tiktok, Vimeo, RSS etc		
2	All data sources should be collectively analyzed for the use of Bank's brand. These should be reviewed by bidder's / OEM's Security Analysts, manually verified, and evaluated to determine the extent of any abuse or fraud. If abuse is suspected, Bank should be immediately notified to take the site down or seek to have the post removed via the normal Incident Response channel.		
3	Platform should monitor & do unlimited take downs of : - Phishing sites & Campaigns - Fake Mobile Apps on Appstore, Play store & other 3rd party Application stores - Fake Customer Service Contact details - Fake Social Media profiles - Fake Domains/URLs and Web pages - Fake recruitment drives & Hiring Scams - Fake Videos or Images using Bank Logos		

4	The Bidder/OEM should be member of International Anti-Phishing Working Group (APWG).		
5	Solution should provide the visibility of DNS records, Who-is records, MX records, screenshot tagged to a typo squatted domain		
6	Solution should provide Domain Watch listing feature, to get instant alert whenever there's a change in the status of domain		
7	Platform should be capable of doing Image/Logo monitoring to identify profile impersonation		
8	Platform should provide : Website Watermarking Website Defacement monitoring		
9	Platform should monitor and report- - CXOs fake social media profiles, posts, pages and groups, takedown is also expected here. -Exposed Executive credentials - Executive mentions / Discussion on Executive on Dark Web - physical threats to executives keeping them informed about potential physical threats during their travel with risk assessment and threat analysis of destination.		
10	Deepfakes of Executives/Heads of the government/ministries used for disinformation campaigns should be detected		

11	Proposed solution provide an early intelligence on the Compromised Identities including the intel on endpoints, Cookies & Session keys of customer internal application available for sale in Dark web Marketplaces.		
	General Specifications (2 marks for each point)		

12	Platform should provide the System Information including the Application details, Username, IP address , OS Type (Windows, Mac), Autofill files etc for the compromised access available for sale on DW marketplace		
13	Platform should provide visibility of critical files leaked from the enterprise systems due to malware attacks		
14	Solution should also provide clear distinction between internal assets or internal employees & the other stakeholders like customers/citizens & partners in the case of exposed credentials		
15	Intelligence provided must have reference to the source of information including Dark web and Deep web and Paste bin sites, either through a direct link to the source or a cached copy without Customer actually going onto Dark web to look for evidence.		
16	The Platform must be able to create, monitor, automate alert and report for threat on Dark Web but is not limited to, the following:		
	-Employee compromised credentials		
	-Sensitive information Leakage such as Username Password Secret token access keys		
	-Compromised PII such as Email ID, Phone number and Address.		
	-information about the compromised system such as device ID, host name, IP address etc to help in forensic investigation		
	-Malware and Malicious Infrastructure related to Customer domain		
	-Private / Sensitive Documents relating to the business.		

	-Hacking documents/tools specifically targeting client; Leaked Source Code.		
	-Intellectual property exposed or leaked		
	-Copyright / Trademark infringement.		
	-Technical Information / Data that could be used to compromise corporate systems.		
	- Mentions of IP Addresses and Infrastructure		
	-Use of BIN and other PII serial numbers to identify client-related accounts and credentials.		
	-Stolen / Compromised Login Credentials and Customer Account Information.		
	- Exposure in 3rd Party Breaches		
17	The platform should incorporate a range of multilayered monitoring services and analysis techniques and correlates data across a range of resources including:		
	- .onion sites, I2P sites and alternative networks;		
	- Dark Net blogs, forums, chat rooms;		
	- Infostealer Marketplaces, Logs and Cookies		
	- IRC conversations;		
	- Black market and criminal auction sites		
	- Ransomware forums		
	- Telegram		
	- Discord		
	- Paste sites		

18	Platform should be able to correlate all data that was exposed on the dark web and provide customized reports using AI prompts. Bank should have possibility of adding prompts to modify reports as per wishes and create schedules around the reports for weekly/monthly etc hunting and reporting needs		
19	AI based prompting should also allow for hunting specific keywords in various forums automatically and generate reports or summary		

Minimum Technical Specifications for Video Wall Display				
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,USB1,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	Colour 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		

ANNEXURE

69. 3: CONFORMITY LETTER

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

Date :

To,

CISO,
Central Bank Of India,
Information Security Department,
Plot no-26, 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/6984238

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

70. 4: BIDDER'S INFORMATION

#	Particulars	Details
1.	Name of bidder	

ANNEXURE

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.) 2022-23 – 2023-24 – 2024- 25 –	
9.	Operating Profits (In Rs.) 2022-23 – 2023-24 – 2024- 25 —	
10.	Net Worth (In Rs.) 2022-23 – 2023-24 – 2024- 25 –	
11.	Whether OEM or authorized vendor	
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:

ANNEXURE

71. 5: LETTER FOR CONFORMITY OF PRODUCT AS PER RFP

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

Date :

To,

CISO,
Central Bank Of India
Information Security Department,
Plot no-26, 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/6984238

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		
Eligibility Criteria		

Signature

Name:
Designation:
Seal of Company

Date:

72. Annexure 6: Undertaking for Acceptance of Terms of RFP

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,

CISO,
Central Bank Of India
Information Security Department,
Plot no-26, 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/6984238

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 as mentioned in the RFP. 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.
5. We undertake to provide SBOM and CBOM as and when required by Bank in Bank's prescribed format.

Signature

Name:
Designation:
Seal of Company
Date:

73. ANNEXURE 7: MANUFACTURER'S AUTHORIZATION FORM

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,

CISO,
Central Bank Of India
Information Security Department,
Plot no-26, 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/6984238

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/OEM duly signed & sealed by an authorized signatory)

Note : MAF not submitted in Bank's format mentioning the tender number along with Bid will by liable for rejection.

74. 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 undisclosedagreement 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/PCAct; 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 ofthe 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: _____
Date: _____	Date: _____

75. 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

The ……..bidder 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.

6. 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.

7. 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.

8. 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.

9. 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.

10. 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.

11. 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.

12. 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: _____

76. 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) 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/- ----------

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

To,

CISO,
Central Bank Of India
Information Security Department,
Plot no-26, Sector-11,
CBD Belapur, Navi Mumbai- 400614

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 theperiod 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

78. 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:

79. ANNEXURE 13: NPA/PENDING LITIGATION/BLACKLISTING 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 (NGSOC) Solutions on their official letter-head Date :

To,
CISO,
Central Bank Of India,
Information Security Department,
Plot no-26, 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/6984238

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 in India which affects our credibility to service the bank.
- Further, we are not blacklisted/debarred/ by any Govt. / IBA/RBI/PSU /PSE/ or Banks, Financial institutes for any reason including non-implementation/delivery of any order.

Yours faithfully,

Authorised Signatory

Designation

Bidder's corporate name

80. 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 Date :

To,
CISO,
Central Bank Of India,
Information Security Department,
Plot no-26, 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/6984238

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.:

List of documents enclosed:

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

ANNEXURE

81. 15: COVER LETTER

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

Date :
To,
CISO,
Central Bank Of India,
Information Security Department,
Plot no-26, 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/6984238

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

ANNEXURE

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

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

82. 16: PRE-BID QUERY FORMAT

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 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)

83. 17: ELIGIBILITY CRITERIA COMPLIANCE

Bidder needs to comply with the eligibility criterion mentioned below. Non-compliance with any of these criterions 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.

ANNEXURE

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.

Date :
To,
CISO,
Central Bank Of India,
Information Security Department,
Plot no-26, 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/6984238

We Certify that we comply with below listed Eligibility Criteria as per the requirement of RFP,

#	Eligibility Criteria for Bidder / OEM	Documents to be submitted	Compliance (Y / N)
	Bidder Criteria		
1.	The 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 bid.	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.	The 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. 1000 crores each year in the last three financial years (i.e. 2022-23, 2023-24,2024-2025) of individual company and not as group of companies.	Copy of Audited Balance Sheet and Certificate of the Chartered Accountant for the last three financial years (i.e. 2022-23, 2023-24,2024-2025)	
4.	The bidder should have made operating profit in at least two financial years out of last three financial years (i.e. 2022-23, 2023-24,2024-2025)	Copy of Audited Balance Sheet and Certificate of the Chartered Accountant for the last three financial years (i.e. 2022-23, 2023-24,2024-2025)	
5.	The bidder should have a positive net worth in last three financial years (i.e. 2022-23, 2023-24,2024-2025)	Copy of Audited Balance Sheet and Certificate of the Chartered Accountant for the last three financial years (i.e. 2022-23, 2023-24,2024-2025)	
6.	At the time of bidding, the Bidder and OEM should not have been blacklisted/debarred/ by any Govt. / IBA/RBI/PSU /PSE/ or Banks, Financial institutes for any reason including nonimplementation/delivery of the order. Self-declaration to that effect should be submitted along with the technical bid.	Undertaking on Company's letter head	

7.	At the time of bidding, there should not have been any pending litigation or any legal dispute, before any court of law between the Bidder or OEM and the Bank.	Submit the undertaking self-declaration on Company's letter head	
8.	The bidder and OEM should not have NPA with any Bank /financial institutions in India Any case pending or otherwise, with any organization in India 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.	The bidder should have service/support centre or should make the arrangements 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 or managed onpremise SIEM solution and currently in use with minimum 1,00,000 Events Per Second (EPS) or 3.4TB / Day in at least ONE Scheduled Commercial Bank (SCB)*/RBI/NPCI/BSE/NSE/ SEBI in India during last 5 years *(SCB – with minimum 1000 Branches in India)	Letter of acceptance (LoA)/ purchase order along with completion certificate or any relevant document acceptable to Bank/ work order/ contract/ completion certificate Deployment Certificate issued by client to the bidder/Particulars confirming relevant experience. The Bank may also reach out to the concerned organization for verification of this criteria / point.	

12.	The Bidder should have implemented or managed onpremise SOAR solution in at least ONE Scheduled Commercial Bank (SCB)*/RBI/NPCI/BSE/NSE/SEBI/ in India during last 5 years *(SCB – with minimum 1000 Branches in India)	Letter of acceptance (LoA)/ purchase order along with completion certificate or any relevant document acceptable to Bank/ work order/ contract/ completion certificate Deployment Certificate issued by client to the bidder/Particulars confirming relevant experience. The Bank may also reach out to the concerned organization for verification of this criteria / point.	
13.	The Bidder should have implemented or managed onpremise UEBA solution in at least ONE Scheduled Commercial Bank (SCB)*/RBI/NPCI/BSE/NSE/SEBI/ in India during last 5 years *(SCB – with minimum 1000 Branches in India)	Letter of acceptance (LoA)/ purchase order along with completion certificate or any relevant document acceptable to Bank/ work order/ contract/ completion certificate Deployment Certificate issued by client to the bidder/Particulars confirming relevant experience. The Bank may also reach out to the concerned organization for verification of this criteria / point.	
14.	The Bidder must have minimum of 50 IT Security permanent resources with experience in-scope solutions on their payroll with certifications such as CISSP/ CEH/CISM.	Undertaking on bidder letter head needs to submit along with certification details and relevant evidence.	
15.	The Bidder should be authorized partner of the OEMs of proposed solutions (SIEM, SOAR, UEBA, TIF, BRAND PROTECTION).	Bidder to submit duly filled and signed Manufacturer Authorization form (MAF) on OEM's letter head in the Bank's format and declaration about back-to-back support from respective OEMs.	
	OEM Criteria		

16	The OEM's proposed SIEM solution to the Bank must have been implemented and currently in use with minimum 1,00,000 Events Per Second (EPS) or 3.4 TB/Day in at least one SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE /NSE/SEBI/ in India during the last 5 years. *(SCB – with minimum 1000 Branches in India)	Letter of acceptance (LoA)/ purchase order along with completion certificate or any relevant document acceptable to Bank/ work order/ contract/ completion certificate Deployment Certificate issued by client /Particulars confirming relevant experience. The Bank may also reach out to the concerned organization for verification of this criteria / point.	
17	The OEM's proposed SOAR solution must have been implemented in at least One SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/ NSE/SEBI in India) during the last 5 years. *(SCB – with minimum 1000 Branches in India)	Letter of acceptance (LoA)/ purchase order along with completion certificate or any relevant document acceptable to Bank/ work order/ contract/ completion certificate Deployment Certificate issued by client/Particulars confirming relevant experience. The Bank may also reach out to the concerned organization for verification of this criteria / point.	
18	The OEM's proposed UEBA solution must have been implemented in at least One SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/ NSE/SEBI in India) during the last 5 years. *(SCB – with minimum 1000 Branches in India)	Letter of acceptance (LoA)/ purchase order along with completion certificate or any relevant document acceptable to Bank/ work order/ contract/ completion certificate Deployment Certificate issued by client /Particulars confirming relevant experience. The Bank may also reach out to the concerned organization for verification of this criteria / point.	

19	The OEM's proposed Threat Intel Feeds (TIF) solution must have been integrated in at least three out of top 10 SCHEDULED COMMERCIAL BANKs (SCB)*/RBI/NPCI/BSE/NSE/SEBI in India) during the last 5 years. *(SCB – with minimum 1000 Branches in India)	Letter of acceptance (LoA)/ purchase order along with completion certificate or any relevant document acceptable to Bank/ work order/ contract/ completion certificate Deployment Certificate issued by client /Particulars confirming relevant experience. The Bank may also reach out to the concerned organization for verification of this criteria / point.	
20	The OEM's proposed Brand Protection solution / services must have been provided in at least One SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/ NSE/SEBI/ in India) during the last 5 years. *(SCB – with minimum 1000 Branches in India)	Letter of acceptance (LoA)/ purchase order along with completion certificate or any relevant document acceptable to Bank/ work order/ contract/ completion certificate Deployment Certificate issued by client /Particulars confirming relevant experience. The Bank may also reach out to the concerned organization for verification	
		of this criteria / point.	

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)

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

(on Bidder's letterhead)

Date :
To,
CISO,
Central Bank Of India,
Information Security Department,
Plot no-26, 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/6984238

We, M/s_____ hereby state that we have gone through the RBI Master Circular: RBI/2023-24/102 DoS.CO.CSITEG/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)

85. 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 1692020 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 14-92017 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 16092020, para 9(h).

Note:

a) Bidder has to submit the Make in India Class-I / Class-II local supplier certificate as perattached 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 inclass 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 localsupplier', 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 localsupplier', the contract will be awarded to L1.

• If L1 is not 'Class-I local supplier', the lowest bidder among the 'Class-I local supplier', willbe 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-Ilocal 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.

86. 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)

Date :
To,
CISO,
Central Bank Of India,
Information Security Department,
Plot no-26, 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/6984238

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)

87. 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 andinclude 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 followingfeatures:

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, CENTRALBANK 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 totake 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 theconduct 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 mala fide / 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 Bankwide / 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/recommendationswithin 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) toissue 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 byED (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 defence.

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) Forbanning 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 interconnected 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

ANNEXURE

88. 21: UNDERTAKING FOR 5 YEARS ROADMAP

(This undertaking should be on the letterhead of the bidder duly signed by an authorized signatory)

Date :
To,
CISO,
Central Bank Of India,
Information Security Department,
Plot no-26, 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/6984238

We, _____ hereby confirm that as a bidder and the product provider, would Supply, Implementation & Management of Next-Generation Security Operations Centre (NG-SOC) Solutions along with Facility Management Services. We also commit to support the proposed Solutions for a minimum period of 5 years and further period of another 2 years if extended.

Yours faithfully,

Signature of Authorized Signatory:
Name of Signatory:
Designation:
Seal of Company:

Date:
Place:

89. 22: UNDERTAKING FOR INFORMATION SECURITY

(This undertaking should be on the letterhead of the bidder duly signed by an authorized signatory)

Date :
To,
CISO,

ANNEXURE

Central Bank Of India,
Information Security Department,
Plot no-26, 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/6984238

We hereby undertake that the proposed solution / software to be supplied will be free of malware, free of any obvious bugs and free of any covert channels in the code (of the version of the application being delivered as well as any subsequent versions/ modifications done).

Also, undertake that the proposed solution / software to be supplied will be complying to Bank's Information Security Policy (of the version of the application being delivered as well as any subsequent versions/modifications done). And new Information Security requirement will be compiled within the timeline set by Bank / Regulatory agencies.

Yours faithfully,

Signature of Authorized Signatory:
Name of Signatory:
Designation:
Seal of Company:

Date:
Place:

90. 23: UNDERTAKING FOR AUTHENTICITY OF THE PRODUCT

(This undertaking should be on the letterhead of the bidder duly signed by an authorized signatory)

Date :
To,
CISO,
Central Bank Of India,
Information Security Department,
Plot no-26, Sector-11,
CBD Belapur, Navi Mumbai- 400614

Sir,
Sub: RFP for Supply, Implementation and Management of Next-Generation Security

ANNEXURE

Operations Centre (NG-SOC) Solutions
Tender No. GEM/2025/B/6984238

With reference to RFP for Supply, Implementation & Management of Next-Generation Security Operations Centre (NG-SOC) Solutions

We hereby undertake to produce the certificate from our OEM supplier in support of this undertaking at the time of delivery/installation. It will be our responsibility to produce such letters from our OEM suppliers at the time of delivery or within a reasonable time.

In case of default and we are unable to comply with the above at any time, we agree to take back the Licenses without demur, if already supplied and return the money if any paid to us by you in this regard.

Yours faithfully,

Signature of Authorized Signatory:
Name of Signatory:
Designation:
Seal of Company:

Date:
Place:

91. 24: LIST OF SOFTWARE AND HARDWARE COMPONENTS REQUIRED FOR IMPLEMENTATION

(This undertaking should be on the letterhead of the bidder duly signed by an authorized signatory)

Date :
To,
CISO,
Central Bank Of India,
Information Security Department,
Plot no-26, 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/6984238

ANNEXURE

With reference to RFP for Supply, Implementation & Management of Next-Generation Security Operations Centre (NG-SOC) Solutions

The below software are proposed for implementation of scope mentioned in RFP. If Bank would like to procure the below licenses (Complete or partial) independently, we will support and co-operate with Bank for procurement of licenses in line with CVC guidelines.

Sr. No.	Software / Tool or Component Required	OEM Name	Justification (Why Software is needed)	Licensing Metric for software (User Based/ Processor Based/ any other)

The below Hardware items are proposed for implementation of scope mentioned in RFP. If Bank would like to procure the below items (Complete or partial) independently, we will support and co-operate with Bank for procurement of licenses in line with CVC guidelines

Sr. No.	Hardware Item or Component Required	Quantity	OEM Name	Size of Hardware for provisioning Racks space	Number of Power Inputs and Power consumption for device

Date:
Place:
Signature of Authorized Signatory:
Name of Signatory:
Designation:
Seal of Company:

92. ANNEXURE 25: PROPOSED TEAM PROFILE

(This undertaking should be on the letterhead of the bidder duly signed by an authorized signatory)

Date :
To,
CISO,
Central Bank Of India,
Information Security Department,
Plot no-26, 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/6984238

With reference to RFP for Supply, Implementation & Management of Next-Generation Security Operations Centre (NG-SOC) Solutions

S.NO	TYPE OF WORK	NAME OF TEAM MEMBERS	QUALIFICATION & CERTIFICATION	PREVIOUS BANKS WHERE TEAM MEMBER WAS ASSOCIATED	DURATION OF TEAM MEMBER ASSOCIATION	NO. OF YEARS OF EXPERIENCE

We hereby acknowledge that the information provided by us is true and to the Best of our Knowledge
Date:

Place:
Signature of Authorized Signatory:
Name of Signatory:
Designation:
Seal of Company:

****
*

CORRIGENDUM 1 - GEM/2025/B/6984238 - 21/01/2026

Additions / Amendments

Sr No	Page No	Type of Change	RFP Clause	Ammended / Added Clause	
1	132	Amendment	The proposed solution must be scalable and have a distributed architecture with native replication of data across DC & DR. DR should be active all the time to ensure continuous security monitoring. The dual forwarding feature should be configurable as per bank requirements and capability for enabling & disabling should be available depending on the device, IP address, and other related parameters.	The proposed solution must be scalable and have a distributed architecture with native replication of data across DC & DR. DR should be active all the time to ensure continuous security monitoring. The dual forwarding feature should be configurable as per bank requirements and capability for enabling & disabling should be available depending on the device, IP address, and other related parameters. DC and DR should be in sync all the time i.e. data, logs, configuration, usecases, rules etc should be replicated between DC & DR and vice versa on real-time basis with near zero RPO & RTO.	
2	NA	Addition	NA	Bidder has to demonstrate bench-marking / load testing of the proposed solution vis-à-vis Bank's requirement of 1,50,000 EPS as a part of Sign off process.	

3	NA	Addition	NA	Bank will conduct Proof of Concept (POC) of the proposed solution before actual deployment and Sign-off.		
4	8	Amendment	Last Date and Time for submission of Bids	6th February 2026 15:00 hrs Mode of bid submission online on GeM Portal		
5	8	Amendment	Time & Date of Opening of technical bids	6th February 2026 15:30 hrs		
Response to Pre-bid Queries						
Sr No	Page #	RFP Clause No.	Clarification point as stated in the tender document	Bidder Comment/ Suggestion	Bank's Response	Status Corrigendum /Addition/No Change/Deletion/Clarification

1	26	7.2 SETTING UP NG-SOC Point 20	SIEM Sustained EPS / Volume 1,00,000 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 700 bytes for storage & licensing purpose. While the solution (Including hardware) should be scalable to support 1.5 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.	For solutions that ingest Raw data we have to consider 1,00,000 EPS with 500 bytes per event for license and 1.5lakh EPS with 500 bytes for hardware sizing. The total expected ingestion in DC/DR combined will be max 1.5lakh EPS Please confirm If this understanding is accurate	Please abide by the RFP requirement	Clarification

2	26	7.2 SETTING UP NG-SOC Point 25	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. Data retention period will be the entire contract period. As per the regulatory guidelines all relevant data has to be stored for minimum 10 years. 6 Months data should be available online and should be stored in highest speed of storage. Another 12 months data should be in warm node that can be accessible through the application. Beyond that till contract period, Data should be in Archival node.	As per requirement, 6 months data Online + 12 Month data in warm storage, assuming Archival to be for 3.5years, please clarify	Please abide by the RFP requirement	Clarification
3	27	7.1 IMPLEMENTATION METHODOLOGY: Point No. 34	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.	In case of the threshold exceed 70% of disk capacity in a quarter the additional storage should be provisioned in such a way that the max disk capacity for the quarter should be 70% of the new disk capacity after addition of the storage	Please abide by the RFP requirement	No Change

4	28	7.3 TRANSITION FROM EXISTING SOC TO NG-SOC:	Migrate configurations, rules, use cases, other settings, logs from existing SOC.	It is assumed that the use cases mapping might not be 1-to-1, however the existing detecting coverage should available in the new SIEM.	Please abide by the RFP requirement	Clarification

5	28	7.3 TRANSITION FROM EXISTING SOC TO NG-SOC:	Migrate configurations, rules, use cases, other settings, logs from existing SOC.	Log migration from existing SOC to NG-SOC should be in RAW / Non Proprietary format	Bank is not expecting to migrate all the logs from existing solution, and hence asked to run current set up parallelly for three years	Clarification
6	30	7.4 SCOPE OF WORK FOR PROPOSED SOLUTIONS	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).	It is assumed that API's of existing ITSM(Motadata) can be leveraged for the integration, inputs required for the integration will be provided by the bank or the vendor	Please abide by the RFP requirement	Clarification

7	135	68. ANNEXURE 2: MINIMUM TECHNICAL SPECIFICATIONS	The proposed solution should provide dashboards for insight into resource consumption of desired systems, service availability status of critical services, integration with NMS tools for network status visibility, security alerts, risky users & entities, anomalies and outliers across all the data etc. from a single dashboard.	Please clarify NSM tool vendor	Details will be shared with successful bidder	Clarification

8	13	Section 2 Point 11 : Eligibility Criteria	The Bidder should have implemented or managed onpremise SIEM solution and currently in use with minimum 1,00,000 Events Per Second (EPS) or 3.4TB / Day in at least ONE Scheduled Commercial Bank (SCB)*/RBI/NPCI/BSE/NSE/ SEBI in India during last 5 years *(SCB – with minimum 1000 Branches in India)	The above experience clause is restricting participation from otherwise eligible bidders. Already the same experience has been asked from OEM side.It is right that you are asking OEMs to have min 1Lakh EPS experience in SCB/ RBI/ NPCI/ BSE/ NSE/SEBI . However, asking same experience from both bidders and OEMs are not making much sense. Bidder experience may differ. It may be noted that last time when this bid has been flaoted , 30 K EPS with experience in Government sector has been asked.	Please abide by the RFP requirement	No Change

9	13	Section 2 Point 12 : Eligibility Criteria	The Bidder should have implemented or managed onpremise SOAR solution in at least ONE Scheduled Commercial Bank (SCB)*/RBI/NPCI/BSE/NSE/SE BI/ in India during last 5 years *(SCB – with minimum 1000 Branches in India)	The above experience clause is restricting participation from otherwise eligible bidders. Already the same experience has been asked from OEM side.It is right that you are asking OEMs to have SOAR experience in SCB/ RBI/ NPCI/ BSE/ NSE/SEBI . However, asking same experience from both bidders and OEMs are not making much sense. Bidder experience may differ.	Please abide by the RFP requirement	No Change

10	13	Section 2 Point 13 : Eligibility Criteria	The Bidder should have implemented or managed onpremise UEBA solution in at least ONE Scheduled Commercial Bank (SCB)*/RBI/NPCI/BSE/NSE/SE BI/ in India during last 5 years *(SCB – with minimum 1000 Branches in India)	The above experience clause is restricting participation from otherwise eligible bidders. Already the same experience has been asked from OEM side.It is right that you are asking OEMs to have UEBA experience in SCB/ RBI/ NPCI/ BSE/ NSE/SEBI . However, asking same experience from both bidders and OEMs are not making much sense. Bidder experience may differ. This PQ criteria is restrictive in nature and we ar not able to qualify against the same. We request you to change this criteria as given below "The Bidder should have implemented or managed onpremise UEBA solution in at least ONE Scheduled Commercial Bank (SCB)*/RBI/NPCI/BSE/NSE/ SEBI/Govt/PSU in India during last 5 years *(SCB – with minimum 1000 Branches in India)"	Please abide by the RFP requirement	No Change

11	14	Section 2 Point 14 : Eligibility Criteria	The Bidder must have minimum of 50 IT Security permanent resources with experience inscope solutions on their payroll with certifications such as CISSP/ CEH/CISM.	This PQ criteria is restrictive in nature and we ar not able to qualify against the same. We request you to change this criteria as given below "The Bidder must have minimum of 50 IT Security permanent resources with experience inscope solutions on their payroll with certifications such as CISSP/ CEH/CISM/ISMS or experience in Network Security/ Cyber Security"	Please abide by the RFP requirement	No Change
12	135	68:Annexure 2: Point No 39	The proposed solution must be able to support mathematics functions to perform calculations on field values, examples Converting bytes to kilobytes, mega-bytes, absolute value functions, highest integers, standard deviation, command length etc.; Finding the time duration between time stamp values. These functionalities should be available as a search, report, alert or dashboard etc. so that analyst can build any kind of report required.	Can you please explain the rational behind the need for the mathematical function.	Please abide by the RFP requirement	Clarification
13	136	68:Annexure 2: Point No 47	The proposed solution should have the capability to collaborate and orchestrate with 3rd party solutions and the solution should be able to be embedded in thirdparty business applications such as SharePoint, WordPress, Wiki, etc.	Can you please clarify on SIEM to be embedded inside 3rd party applications or 3rd party applications inside SIEM. And, where should be orchestration shown.	Please abide by the RFP requirement	Clarification

14	144	SOAR Requirements , Point No 24	The proposed solution must be able to extract and store attachments from ingested emails	Please elaborate this usecase in detail	Please abide by the RFP requirement	Clarification

15	150	TIF Point 26	Threat Intelligence Vendor should be serving more than 1000 Customers globally for threat intelligence solution	We would like to bring to your attention that above clause is restrictive for Indian Local OEMs. As per DPIIT's Public Procurement (Preference to Make in India) Order (PPP-MII), such conditions limit participation of domestic OEMs, which goes against the intent of promoting indigenous solutions under the Make in India initiative. We kindly request you to remove this clause for Make in India companies.	Please abide by the FP requirement	No Change
16	151	Brand Protection Point 4	The Bidder/OEM should be member of International Anti-Phishing Working Group (APWG).	Kindly allow membership with similar threat intelligence group like SPAMHAUS	Please abide by the RFP requirement	No change

17	81	Experience Criteria Section 1 Claue 13	"The OEM should have implemented or managed SOC with on-premises SIEM solution with minimum 1,00,000 Events Per Second (EPS) or 3.4TB / Day in at least one SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/NSE/SEBI in India during last 5 years. *(SCB – with minimum 1000 Branches in India)"	We would like to highlight that the clause is highly restrictive for Indian Local OEMs. As per DPIIT's PPP-MII Order (No. P45021/2/2017-B.E.-II dated 15.06.2017 and revisions) and F.1/15/2018-PPD Procurement Policy/O.M 24/04/2018 from Ministry of Finance procurement should encourage 'Make in India'. However the RFP's clause limits participation of domestic solution providers and go against the intent of promoting indigenous solutions under the Make in India initiative. We kindly request you to remove this clause to ensure compliance with the PPP-MII Order and allow fair opportunity for Make in India companies. We request to remove the clause allowing all deployment models, provided the Overall capability of the offered SIEM meets the specified performance criteria of (≥100,000 EPS or 3.4 TB/day) overall.	Please abide by the RFP requirement	No change

18	36	V. Brand ProteWeb Services inclu Dark Monitoring:	Any newly launched websites and Mobile Application by the Bank in future to be scanned without any cost incurred to the Bank	Please can you specify the current number of Domains/ Brands and a list of these names.	Will be shared with successful bidder	Clarification
19	38	7.5 SERVICES	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.	Please let us know why older versions would be required? New versions would have the latest features in line with the ned of the hour.	Please abide by the RFP requirement	Clarification
20	148	ANNEXURE 2: MINIMUM TECHNICAL SPECIFICATIONS - Threat Intelligence Feeds(TIF) Requirement Specification Point 13	Threat Intel OEM must be in existence for more than 15 years and the offered solution should have readily searchable data (for up to last 15 years) with the specific dates of event. The OEM may be required to demonstrate the same at the time of technical evaluation.	Please can you bring down this requirement to 10 years for OEM Existence ? As most cybersecurity companies are new age companies, it might be had to prove 15 years existence and CBI might lose out on market leading vendors due to this 15 yrs clause.	Please abide by the RFP requirement	No change

21	150	ANNEXURE 2: MINIMUM TECHNICAL SPECIFICATIONS - General Specifications (2 marks for each point) Point 27	Threat Intelligence vendor should have all of the mentioned Certifications ISO 27001, ISO 9001, ISO 27701, ISO 27017, SOC 2 Type 2, and NIST 800-218 SSDF certified	Kindly consider less number of certification requirement, especially the ISOs, as being certified for one ISO usually makes the vendor compliant with other ISO frameworks as well. ISO 27001 usually suffices in case of Cybersecurity providers.	Please abide by the RFP requirement	No Change
22	38	7.5 SERVICES Page No. 38	ii. Threat Hunting Services: 4. The threat hunting team must provide the threat hunting plan before every threat hunting exercise	Is this expected to be hypothesisdriven proactive hunting, or reactive hunting based on alerts/incidents?	Both are required	Clarification
23	130	68. ANNEXURE 2: MINIMUM TECHNICAL SPECIFICATIONS Mandatory Specifications (3 marks for each point) Point 5	The proposed solution should provide a test/dev license as part of the solution. It should also provide a tool in-built or integrable, that allows to create test bed environment which can help to simulate blue team and red team attacks to test use cases, train analysts etc.	Would request Bank to share if there is any specific EPS required for test/dev license	Please abide by the RFP requirement	Clarification

24	131	68. ANNEXURE 2: MINIMUM TECHNICAL SPECIFICATIONS Mandatory Specifications (3 marks for each point) Point 7	Machine learning should be embedded across the platform (SIEM, DATA LAKE, SOAR & UEBA). It should empower every user in the SOC with ML. Security analyst to become citizen data scientist i.e. used predefined ML algorithms to detect & predict threats, threat hunters to build their own ML models with steps to build, train and implement model and data scientists should be able to integrate various ML frameworks.	This is OEM specific point, request you to modify the point/clause as mentioned below: Machine learning should be embedded across the platform (SIEM & UEBA). It should empower every user in the SOC with ML. Ability to use custom ML Model if required to detect and predict threats.	Please abide by the RFP requirement	Clarification

25	135	68. ANNEXURE 2: MINIMUM TECHNICAL SPECIFICATIONS Monitor, Alert and Reporting Functions (2 marks for each point) Point 40	The proposed solution must be able to support predictive analytics to predict future values of single or multi-valued fields. This will help security analytics to predict the attack patters or specific attacks using multiple fields in the alerts or logs.	This requires LLM to run on-prem, can LLM (AI) to run on cloud and SIEM onprem to achieve cost effective solution?	Please abide by the RFP requirement	Clarification

26	136	68. ANNEXURE 2: MINIMUM TECHNICAL SPECIFICATIONS - Artificial Intelligence Machine Learning (2 marks for each point) Point 48	The proposed solution must provide GUI that can easily help to build, built-in or custom machine learning models using the pre- defined sequence and should be able to integrate with a collection of NLP and classical machine learning libraries, generic machine learning tools like tensor flow, pytorch, R, Python, Scala etc.	This is OEM specific point, request you to modify the point/clause as mentioned below: The proposed solution must provide GUI that can easily help to build, built-in or custom machine learning models using the predefined sequence and should be able to integrate machine learning libraries , generic machine learning tools like tensor flow, pytorch, R, Python, Scala etc / Natively Supported ML Tools.	Please abide by the RFP requirement	No change

27	136	68. ANNEXURE 2: MINIMUM TECHNICAL SPECIFICATIONS - Artificial Intelligence Machine Learning (2 marks for each point) Point 50	The proposed solution machine learning capabilities must allow addition of custom machine learning algorithms from popular libraries like NLP, Python etc.	Request Bank to modify the point / clause as below:- The proposed solution machine learning capabilities must allow addition of custom machine learning algorithms from popular libraries or natively supported ML algorithms	Please abide by the RFP requirement	Clarification

28	28	7.3 TRANSITION FROM EXISTING SOC TO NG-SOC	Migrate configurations, rules, use cases, other settings, logs from existing SOC.	Log migration from existing SOC to NG-SOC is possible only if logs are available to process in RAW / Non Proprietary format. What is the volume of existing logs to be migrated to new SIEM.	Bank is not expecting to migrate all the logs from existing solution, and hence asked to run current set up parallelly for three years	Clarification
29	29	7.4 SCOPE OF WORK FOR PROPOSED SOLUTIONS	The bidder should assess, configure/ migrate the use-cases deployed in the current SIEM to the newly procured SIEM.	Pls specify number of use cases that need to be migrated	Will be shared with successful bidder	Clarification
30	20	Scope of Work	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.	will ticketing tool will be provided by client?	Please abide by the RFP requirement	Clarification

31	21	Scope of Work Point 21	Bank'sexpectation is that successful bidder is required to manage the existing SOC for another one year after expiry of existing contract in Jan'27	When is the supply ofyear?lutions expected ? post one pls confirm on the timeline	Supply of solutions is expected as per timelines mentioned in RFP depending on issuance of PO. Irrespective of when the new solution is deployed, the existing solution should be supported by the bidder for additional 3 years	Clarification
32	22	Scope of Work Point 27	Implement and test procedures for backup and recovery of configurations, logs, and other critical components of the solutions. Perform an annual security audit to ensure that the systems remain compliant with regulatory requirements and that any vulnerabilities or gaps are addressed.	Will gap remediation is bidder responsibility? Further should this be independant team or same team handling SOC operations?	Please abide by the RFP requirement	Clarification
33	28	Section 7.3	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.	is the transition timeline to be 1 year or can it be less than 1 year? As above it was mentioned to run existing SOC until Jan 27. Request to clarify on the same	Please abide by the RFP requirement	Clarification

34	36	V. Brand Protection Services including Dark Web Monitoring	24x7 anti-phishing, anti-Trojan, antimalware service to scan critical websites and Mobile Apps identified by Bank for the tenure of the project. Scan the Dark web for mentions of Bank's brand, product or services. Track specific keywords related to Bank including product names, executive names and brand slogans.	number of domains and apps to be received and baselined.	Will be shared with successful bidder	Clarification
35	94	26. 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:	We suggest following changes: Indemnity obligation shall be limited only (i) for breach of thirdparty intellectual property rights arising from the use of deliverables provided by Deloitte and (ii) for third party claim from death or bodily injury or loss to any physical property arising out of gross negligence of Deloitte provided Deloitte is given sole control of defence for such claims. Additionally we disclaim all indemnity and liability related to Product/Solution or OEM if any involved in performance of services.	Please abide by the RFP requirement	No Change

36	101	34. SUCCESSFUL BIDDER'S LIABILITY	The Bidders 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 Bidders liability in case of claims against the Bank resulting from wilful misconduct or gross negligence of the 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 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.	We suggest following changes Notwithstanding anything to the contrary stated anywhere in the RFP or anywhere else, (i) the aggregate liability of the Bidder shall not under any circumstances exceed the total fees received by Bidder for such Service(s)/service attachment/purchase order in the 12-month period preceding to which such losses relate (ii) the Bidder will not be liable for any indirect, special, consequential or punitive damages or losses, including but not limited to loss of business or data or profits or goodwill.	Please abide by the RFP requirement	No Change

37	43	7.8 NG-SOC OPERATIONS, FACILITY MANAGEMENT, AMC & ATS	L1 and L2 to be fully automated in phased manner by the end of first year of operationalizingNG-SOC setup. False positive rate to be less than 5%.	We recommend following changes: L1 and L2 to be automated to the extend possible with mutual discussion, in phased manner by the end of first year of operationalizing NG-SOC setup. Ensure adequate automation and efforts to strive to achieved False positive rate to be less than 5%.	Please abide by the RFP requirement	No Change

38	43	7.8 NG-SOC OPERATIONS, FACILITY MANAGEMENT, AMC & ATS Point 8	Starting from Go-Live date of the NGSOC, it is the responsibility of the Project Director 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, analysed 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 NGSOC 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."	We will raise this as monthly report and not as a certification: Technology reviews are point in time activity and no certification can be provided by us for the security health of the systems of client. We request for change of wordings with mutual agreement.	Please abide by the RFP requirement	No change

39	44	7.8 NG-SOC OPERATIONS, FACILITY MANAGEMENT, AMC & ATS Point 19	The bidder should provide the on-site support for 24/7 around the year (365 days) for the period of warranty, AMC and ATS. Project Director 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.	Digital Forensics shall be separate service, charged at actuals for rate for Incident Retainer Response (IRR) service.	Please abide by the FP requirement	Clarification
40	62	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.	Staggered delivery may affect our cost and there the Bid price and Go-live readiness. It is recommended to agree on the delivery of the solutions well in advance.	Please abide by the RFP requirement	No Change

41	63	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.	It is recommended to change max aggregate capping of penalty for all delays under this contract to 10% of the total Supply cost.	Please abide by the RFP requirement	No Change
42	68	12.3.3 PENALTY ON SERVICE LEVELS DURING OPERATIONS PHASE	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. Audit observations to be closed as per Bank's TAT (turnaround time).	If the closure of the critical/high risk obervations requires code change/product dependenceies, then it will follow OEM's patching cycle. We suggest to restrict this clause to configuration changes and generic OS level only	Please abide by the RFP requirement	No Change
43	68	12.3.3 PENALTY ON SERVICE LEVELS DURING OPERATIONS PHASE	In the absence of the assigned resource, a suitable replacement must be provided immediately. If this replacement is not provided, a penalty of 2% of monthly service cost will be applied for each day of absence.	Absence for reasons of medical, resignation and emergency to be excluded.	Please abide by the RFP requirement	No Change

44	145	UEBA Requirement Specifications (Mandatory Specifications)	The UEBA must create a heuristic baseline of user activity by analyzing behavior, so it must perform multidimensional baselining, enabling the modeling of a broad set of user behaviors. Baselines are used to detect anomalous behavior via machine learning and other statistical analysis techniques.	(Latest/ advance base line models available such as – Anomaly detection, Behaviour profiling, Peer group analysis, risk based profiling etc) Clause To be modified: The UEBA must create a heuristic baseline OR Advance Baseline models such as Anomaly detection, Behaviour profiling, Peer group analysis and risk based profiling of user activity by analyzing behavior, so it must perform multidimensional baselining, enabling the modeling of a broad set of user behaviors. Baselines are used to detect anomalous behavior via machine learning and other statistical analysis techniques.	Please abide by the FP requirement	No Change
45	19	7.SCOPE OF WORK		Request for Clarification: Request Bank to share Number of sites whare solution to be deploy (e.g. Production, DR, UAT) accordingly infra can be sized	Please abide by the RFP requirement	Clarification
46	19	7.SCOPE OF WORK		Request for Clarification: Request Bank to clarify if storage Media/Disk retention required or not?	Please abide by the RFP requirement	Clarification

47	19	7.SCOPE OF WORK		Request for Clarification: Request Bank to share existing network connectivity details so that hardware infra is compatible with existing infra (existing Network Switch details, Port type, Fiber or Copper, placement, length etc)	Will be shared with successful bidder	Clarification
48	59	8. GENERAL RESPONSIBILITY OF THE BIDDER	LTO-10 or above Library based backup solution should be provided with backup software and necessary licenses. Online backup feature should be available.	Request for Clarification: Please clarify if Bidder needs to provide Backup solution along with Tape library? If Yes, Please share the no of drive and slots required in tape?	Please abide by the RFP requirement	Clarification
49	32	7.4 SCOPE OF WORK FOR PROPOSED SOLUTIONS	SAN storage Systems should support Storage virtualization centralized management and SAN Storage should support 99.99% Data Availability	Request for modification: We request Bank to consider below: Proposed OEM should be able to support 100% Data Availability Guarantee in writing in OEMs letter head. Respective OEM should submit the publicly available brochure or publicly available website URL for 100% Data Availability Guarantee.	Please abide by the RFP requirement	No Change

50		Video Wall Controller		Request for Clarification: 1. Adequate wall load-bearing capacity to safely mount the video wall display 2. Availability of a suitable cabletray or raceway pathway to route HDMI cabling from the controller to the user system in an organised and concealed manner. 3. Sufficient dedicated space for controller placement, ensuring proper ventilation and ease of maintenance. 4. The distance between the usersystem and the display must not exceed 15 metres, in line with the maximum supported length for standard HDMI cabling. 5. Detailed room layout drawings,clearly indicating device locations and placement markings.	Please abide by the FP requirement	Clarification
51	152	Pt 8	Platform should provide : Website Watermarking Website Defacement monitoring	Please clarify the requirements for Website Defacement Monitoring	Please abide by the RFP requirement	Clarification
52	152	Pt 9	Platform should Monitor and report to physical threats to executives keeping them informed about potential physical threats during their travel with risk assessment and threat analysis of destination.	Kindly clarify the specific threat analysis expected under this requirement. It would be helpful if the bank could explain the same with a relevant use case for better understanding.	Please abide by the RFP requirement	Clarification

53	154	Pt 16	Stolen / Compromised Login Credentials and Customer Account Information. - Exposure in 3rd Party Breaches	Our Recommendation: The platform must validate credentials associated with official emails or sensitive subdomains/URLs by performing successful login tests and delivering screenshots as evidence for verification.	Please abide by the RFP requirement	No change
54			Recommended Points for Addition	Dark Web, Brand Monitoring etc OEM must have more than 10 years of intelligence collection experience, analysis and tracking across deep web, dark web, OSINT, Social	Please abide by the RFP requirement	No change
55			Recommended Points for Addition	The solution must allow unlimited user licenses.	Please abide by the RFP requirement	No change
56			Recommended Points for Addition	The platform must allow custom dashboards to be built per use case.	Please abide by the RFP requirement	No change
57			Recommended Points for Addition	Favicon Impersonation Detection: The platform must detect websites that mimic the client's brand by copying the favicon (the small icon displayed in browser tabs), which is often used to visually deceive users in phishing or spoofing attempts. It must tag such incidents as 'Favicon Impersonation	Please abide by the RFP requirement	No change

				Detected'.		
58			Recommended Points for Addition	The platform must offer advanced filtering options to isolate unique credentials by excluding duplicates, ensuring a cleaner and	Please abide by the RFP requirement	No change
				more actionable dataset.		
59			Recommended Points for Addition	The OEM should be Class1 Supplier	Please abide by the RFP requirement	No change

60	13	2. ELIGIBILITY CRITERIA	11. The Bidder should have implemented or managed on-premise SIEM solution and currently in use with minimum 1,00,000 Events Per Second (EPS) or 3.4TB / Day in at least ONE Scheduled Commercial Bank (SCB)*/RBI/NPCI/BSE/NSE/SEBI in India during last 5 years *(SCB – with minimum 1000 Branches in India)	Need to change as under : The Bidder should have implemented or managed onpremise SIEM solution and currently in use with minimum 1,00,000 Events Per Second (EPS) or 3.4TB / Day in at least ONE Scheduled Commercial Bank (SCB)*/RBI/NPCI/BSE/NSE/SEBI/PSU in India during last 7 financial years. *(SCB – with minimum 1000 Branches in India)	Please abide by the RFP requirement	No change
61	13	2. ELIGIBILITY CRITERIA	14. The Bidder must have minimum of 50 IT Security permanent resources with experience in-scope solutions on their payroll with certifications such as CISSP/ CEH/CISM.	Request to change the clause as :The bidder shall have minimum 100 skilled resources on the payroll in India in the following areas (Subject Matter Expert): a. Network Security b. Data Security c. Application Security d. Cloud Securitye Vulnerability Management f. Infrastructure Management Or The Bidder must have minimum of 50 IT Security permanent resources with experience in-scope	Please abide by the RFP requirement	No change

				solutions on their payroll.		
62	78	Section – 1 – Experience Criteria	1. The Bidder should have implemented or managed SOC with on-premises SIEM solution with minimum 1,00,000 Events Per Second (EPS) or 3.4TB/ Day in at least one SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/NSE/SEBI in India during last 5 years. *(SCB – with minimum 1000 Branches in India)	Need To Change : The Bidder should have implemented or managed SOC with on-premises SIEM solution with minimum 1,00,000 Events Per Second (EPS) or 3.4TB/ Day in at least one SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/NSE/SEBI/PSU in India during last 7 Financial years.	Please abide by the RFP requirement	No change

63	78	Section – 1 – Experience Criteria	1. Marks Scheme: 1 implementation or managed : 60 marks, further additional implementation or managed : 20 marks each	Need To Change as : 1 implementation or managed of for 1000000 EPS : 60 marks, for below 100000 EPS for further additional implementation or managed : 20 marks each	Please abide by the RFP requirement	No change

64	78	Section – 1 – Experience Criteria	2. The Bidder should have implemented or managed SOC with any on-premises SIEM solutionwith minimum 1,00,000 Events Per Second (EPS) or 3.4TB/ Day in at least one SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/NSE/SEBI in India during last 5 years. *(SCB – with minimum 1000 Branches in India)	Need To Change : The Bidder should have implemented or managed SOC with any onpremises SIEM solution with minimum 1,00,000 Events Per Second (EPS) or 3.4TB/ Day in at least one SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/NSE/SEBI/PSU in India during last 7 Financial years. *(SCB – with minimum 1000 Branches in India)	Please abide by the RFP requirement	No change

65	79	Section – 1 – Experience Criteria	4. The Bidder should have implemented or managed any on-premises UEBA solution with minimum 20,000 users in at least one SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/NSE/SEBI in India during last 5 years. *(SCB – with minimum 1000 Branches in India)	Need To change as : The Bidder should have implemented or managed any on-premises UEBA solution with minimum 20,000 users in at least one SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/NSE/SEBI/PSU. in India during last 5 years. *(SCB – with minimum 1000 Branches in India)	Please abide by the RFP requirement	No change
66	80	Section – 1 – Experience Criteria	5. The Bidder should have integrated TIF solution with any on-premise SOC in at least one SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/NSE/SEBI in India during last 5 years. *(SCB – with minimum 1000 Branches in India)	Need to change as : The Bidder should have integrated TIF solution with any on-premise SOC in at least one SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/NSE/SEBI/PSU in India during last 5 years. *(SCB – with minimum 1000 Branches in India)	Please abide by the RFP requirement	No change
67	80	Section – 1 – Experience Criteria	6. The Bidder should have provided services of Brand Protection in at least one SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/NSE/SEBI in India during last 5 years. *(SCB – with minimum 1000 Branches in India)	The Bidder should have provided services of Brand Protection in at least one SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/NSE/SEBI/PSU/BFSI in any in India during last 5 years. *(SCB – with minimum 1000 Branches in India)	Please abide by the RFP requirement	No change

68	80	Section – 1 – Experience Criteria	7. The bidder must have minimum 50 IT Security permanent resources with experience in-scope solutions on their payroll with certifications such as CISSP/ CEH/CISM.	Need To Change as : The bidder must have minimum 50 IT Security permanent resources with experience in-scope solutions on their payroll.	Please abide by the RFP requirement	No change
69	81	Section – 1 – Experience Criteria	13. The Bidder should have implemented or managed SOC with on-premises SIEM solution with minimum 1,00,000 Events Per Second (EPS) or 3.4TB / Day in at least one SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/NSE/SEBI in India during last 5 years. *(SCB – with minimum 1000 Branches in India)	Need to Change as :OEM's Proposed Solution Experience should have implemented or managed SOC with on-premises SIEM solution with minimum 1,00,000 Events Per Second (EPS) or 3.4TB / Day in at least one SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/NSE/SEBI in India during last 5 years. *(SCB – with minimum 1000 Branches in India)	This is a typographical error please consider this point as related to OEM as "The OEM's proposed SIEM solution to the Bank must have been implemented and currently in use with minimum 1,00,000 Events Per Second (EPS) or 3.4 TB/Day in at least one SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NP	Clarification

					CI/BSE/NSE/SEBI/ in India during the last 5 years. *(SCB – with minimum 1000 Branches in India) "	
70		Additional Marks Scheme	Note : additional Points can be added	The bidder should have below listed certification Cert In Empanelled SOC 2 Type 2 ISO27001 Mark Scheme: All 3 certification 60 marks or each 20 marks	Please abide by the RFP requirement	No change
71		Additional Marks Scheme	Note : additional Points can be added	The bidder having highest level partnership for proposed Infrastructure OEM Mark Scheme: Highest level - 100 marks and N-1 is 50 marks	Please abide by the RFP requirement	No change

72			General Queries	Request for clarification: Request Bank to clarify on UAT Separate Environment requirement, if yes then EPS Count and location for UAT need to specify, also which all feature require for UAT environment kindly that clarify.	Please abide by the RFP requirement	Clarification
73			General Queries	Request for Clarification: EPS License requirement for 100000 is DC and DR separately or combine 100000 EPS in total.	It is separate for DC and DR	Clarification
74	22	22. and Monitoring Management	24. Seating Space and Workstations for onsite implementation and FMS Teams will be provided by Bank at DC, Mumbai / Navi Mumbai and DRC, Hyderabad.	Request for clarification: Please provide bifurcation of Onsite team seating in DC-Mumbai/Navi-Mumbai and DR-Hyderabad Location. This will help us on bifurcating shift and resource backup management. Currently in FMS section, no location specify in RFP.	Will be discussed with successful bidder	Clarification
75	19	7. SCOPE OF WORK	6. Inventory management of all assets (Hardware and Software etc.) supplied as part of the RFP.	Request for Clarification: Does bank require Inventory management software solution along with proposed NG-SOC solution.	Please abide by the RFP requirement	Clarification

76	19	7. SCOPE OF WORK	Integration	Request for Clarification: Request Bank to Clarify number of integration require with SOAR platform and number of playbook require to create automation, this information will help on finalizing project scope timeline and cost.	Will be discussed with successful bidder	Clarification

77	20	7. SCOPE OF WORK	Integration	Request for Clarification: Request Bank to clarify that number of Playbook require in UEBA.	Will be discussed with successful bidder	Clarification
78	20	7. SCOPE OF WORK	16. Ensure graceful transition from existing CSOC of the Bank to new NGSOC along with migration activities.	Request for clarification: Request Bank to clarify on Migration scope from Existing SOC solution to new SOC, what king of migration is expected, is it only related to configuration or existing data log.	Bank is not expecting to migrate all the logs from existing solution, and hence asked to run current set up parallelly for three years	Clarification
79	21	7. SCOPE OF WORK	Sizing	Request for clarification: Request bank to clarify if sizing for NG-SOC need to configure as per 100000 EPS or 150000 EPS or any other specific number as per 5 year tenure including all other proposed solution.	Please abide by the RFP requirement	Clarification

80	88	Payment Terms	Hardware : 40% On post-delivery inspection of the Hardware, 50% - Against successful installation and acceptance, 10%- 3 months after successful installation signoff of software / solution / service and signoff by Bank at DC, DRC testing signoff by Bank at DC, DRC	Request to change the clause as :60% On post-delivery inspection of the Hardware, 35% Against successful installation and acceptance, 5%- 3 months after successful installation signoff of	Please abide by the RFP requirement	No change

81	88	Payment Terms : Software lice (OS, Applicatior other associa software and services) : For ach of the following Softw Solution / Service 1. SIEM 2. SOAR 3.UEBA 4.TIF 5.Brand Protection	30% On post-delivery of the licenses, 50% - Against successful implementation and acceptance testing of respective software / solution / service (i.e. SIEM, SOAR, UEBA, TIF, Brand Protection) and signoff by Bank at DC, DRC, 10%-After Successful Migration of existing policies, rules, scenarios, logs, VAPT compliance and completion of one DR Drill, 10%-3 months after successful implementation signoff	Request to change as : 60% On post-delivery of the licenses, 30% Against successful implementation and acceptance testing of respective software / solution / service (i.e. SIEM, SOAR, UEBA, TIF, Brand Protection) and signoff by Bank at DC, DRC, 5%-After Successful Migration of existing policies, rules, scenarios, logs, VAPT compliance and completion of one DR Drill, 5%-3 months after successful implementation signoff	Please abide by the RFP requirement	No change

82	124	Table – B	Table – B (Software Cost - Price Schedule For Next Generation Security Operation Center Solution - Licenses/Software Cost With One Year Warranty	Licenses to be supplied must be perpetual in nature only?	Bank expects the license to be perpetual	Clarification
83	20	7. SCOPE OF WORK	All the tools/ application/ OS/hardware supplied as part of the project should be on premise, latest and supplied with Enterprise-wide Licenses and all the licenses / subscriptions should be in the name of Central Bank of India.		Bank expects the license to be perpetual	Clarification

84	135	68. ANNEXURE 2: MINIMUM TECHNICAL SPECIFICATIONS SIEM Requirement Specifications	39 The proposed solution must be able to support mathematics functions to perform calculations on field values, examples Converting bytes to kilobytes, mega-bytes, absolute value functions, highest integers, standard deviation, command length etc.; Finding the time duration between time stamp values. These functionalities should be available as a search, report, alert or dashboard etc. so that analyst can build any kind of report required.	Kindly amend the clause as "The proposed solution must be supporting search functionalities and NLP based queries for threat hunting"	Please abide by the RFP requirement	No Change

85	135	68. ANNEXURE 2: MINIMUM TECHNICAL SPECIFICATIONS SIEM Requirement Specifications	40 The proposed solution must be able to support predictive analytics to predict future values of single or multi-valued fields. This will help security analytics to predict the attack patters or specific attacks using multiple fields in the alerts or logs.	Kindly amend the clause as " The proposed solution must support attack pattern detection using multiple fields in the alerts or logs."	Please abide by the RFP requirement	No Change

86	136	68. ANNEXURE 2: MINIMUM TECHNICAL SPECIFICATIONS SIEM Requirement Specifications	48 The proposed solution must provide GUI that can easily help to build, built-in or custom machine learning models using the pre- defined sequence and should be able to integrate with a collection of NLP and classical machine learning libraries, generic machine learning tools like tensor flow, pytorch, R, Python, Scala etc.	Kindly amend the clause as " The proposed solution must provide GUI that can easily help to build, built-in or custom machine learning models using the predefined sequence and should be able to integrate with a collection of NLP and classical machine learning libraries, generic machine learning tools"	Please abide by the RFP requirement	No Change

87	136	68. ANNEXURE 2: MINIMUM TECHNICAL SPECIFICATIONS SIEM Requirement Specifications	75 The proposed solution should use statistic functions or techniques like percentile or standard deviation to detect unusual activities that can be applied to insider or fraudulent use cases. Other analysis: Find common or rare events using cluster or most commonly and widely used means clustering method Find percentage of times two fields exist in the same events correlating all the fields. Indicative	This clause is specific to a particular OEM, Kindly requesting to remove the clause.	Please abide by the RFP requirement	No Change

88	140	68. ANNEXURE 2: MINIMUM TECHNICAL SPECIFICATIONS SIEM Requirement Specifications	77 The proposed solution's detection use cases should be comprised of guidance that provides an assessment of the Security Threat and how it helps detect and investigate it using the proposed solution. In addition, it should provide a summary of how the attack or detection technique maps to the following: ATT & CK MITRE, an adversary behavior model that describes the actions an adversary might take. Kill-Chain, a model that identifies the phases an adversary must complete to achieve their objective. CIS Critical Security Controls Data types that are referenced within the rules/ search and that need to be populated. Technologies, example technologies that map to the data types. There should be template to upload advisories in an automated manner. There should be templates to design and trigger work flows automatically. Any other customizable templates as per bank requirements.	Kindly amend the clause as " The proposed solution's detection use cases should be comprised of guidance that provides an assessment of the Security Threat and how it helps detect and investigate it using the proposed solution. In addition, it should provide a summary of how the attack or detection technique maps to the following: ATT & CK MITRE, an adversary behavior model that describes the actions an adversary might take. Kill-Chain, a model that identifies the phases an adversary must complete to achieve their objective."	Please abide by the RFP requirement	No Change

89	23 124	7.2 SETTING UP NG-SOC Table – B (Software Cost) SOAR 25 Analysts	4. As part of Proposed Next-Gen SIEM solution, SOAR should be part of the NGSOCsolution suite with 30 Security Analysts equivalent license plus 15 view only userlicenses, SOAR must enable the orchestration and automation of security workflows,eliminating manual intervention to reduce mundane tasks. Successful bidder has tofactor the underline hardware and software components for orchestration andautomation of security workflows, etc.	There is a discrepancy in both cases, kindly clarify the number of analyst.	This is a typographical error please consider as 30 instead of 25 and 15 view only user licenses for SOAR	Clarification
90		68. ANNEXURE 2: MINIMUM TECHNICAL SPECIFICATIONS SIEM Requirement Specifications		Kindly confirm if any remote locations are present for the logs to be collected.	Please abide by the RFP requirement	Clarification
91	28	7.3 TRANSITION FROM EXISTING SOC TO NG-SOC:		Kindly provide details of existing SIEM vendor and their model for a clearer understanding	Will be shared with successful bidder	Clarification

92	14	Eligibility Criteria (OEM Criteria)	The OEM's proposed SIEM solution to the Bank must have been implemented and currently in use with minimum 1,00,000 Events Per Second (EPS) or 3.4 TB/Day in at least one SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE /NSE/SEBI/ in India during the last 5 years. *(SCB – with minimum 1000 Branches in India)	Kindly requesting to amend this clause to " The OEM's proposed SIEM solution to the Bank must have been implemented and currently in use with minimum 1,00,000 Events Per Second (EPS) or 3.4 TB/Day in at least one SCHEDULED COMMERCIAL BANK SCB/RBI/NPCI/BSE /NSE/SEBI/GOV/PVT in India during the last 5 years."	Please abide by the RFP requirement	No change

93	81	Section – 1 – Experience Criteria OEM (Proposed Solution Experience)	The Bidder should have implemented or managed SOC with on-premises SIEM solution with minimum 1,00,000 Events Per Second (EPS) or 3.4TB / Day in at least one SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/NSE/SEBI in India during last 5 years. *(SCB – with minimum 1000 Branches in India) 1 implementation or managed : 40 marks, additional implementation or managed : 20 marks each	As per our understanding, bidders can demonstrate their experience in implementing the proposed SIEM solution or similar solutions during the evaluation process. By keeping proposed SIEM Solution only,this clause is restricting multiple Bidders and OEMs of different make and models who have proven experience in large scale deployments to participate in the tender because in each and every bid or tender, the products quoted regularly will change and the bidder always looks at the best commercial models quoted by the OEM. Kindly clarify and include similar solutions also	Please abide by the RFP requirement	No change

94	82	OEM (Proposed Solution Capacity)	OEM's proposed SIEM solution should be successfully implemented in at least one SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/NSE/SEBI in India during last 5 years. *(SCB – with minimum 1000 Branches in India) 100001 to 125000 EPS (3.4 TB to 4.25 TB) or Equivalent: 60 Marks 125001 to 150000 EPS (4.26 TB to 5.1 TB) or Equivalent: 80 Marks 150001 EPS (5.1 TB) or more: 100 Marks	Kindly requesting to amend this clause as: OEM's proposed SIEM solution should be successfully implemented in at least one SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/NSE/SEBI/GOV/Private Organization in India during last 5 years. *(SCB – with minimum 1000 Branches in India) ~~Representation: It~~ is widely recognized that SIEM capability is best assessed through sustained EPS handling, log ingestion scale, correlation efficiency, and operational stability. In the Indian context, several Central Government, State Government, PSU, and large private organizations operate mature, large-scale SIEM deployments comparable to those in financial institutions. Recognizing such implementations will ensure that evaluation reflects current industry practices and real-world operating environments. It is therefore	Please abide by the RFP requirement	No change

				requested that SIEM experience from Central Government, State Government, PSU, and large		

				private organizations be considered, with assessment focused on demonstrated scale, performance, and operational maturity of the proposed SIEM solution.		

95	82	OEM (Experience)	OEM's Proposed SOAR solution should be successfully implemented in at least one SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/NSE/SEBI in India during last 5 years. *(SCB – with minimum 1000 Branches in India) 60 Marks- Max Mark 40 marks - 1 reference 10 marks - additional reference	Kindly amend or modify this clause to "OEM's Proposed SOAR solution should be successfully implemented in at least one SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/NSE/SEBI/GOV/Private Organization in India during last 5 years. Keeping the branch numbers as 1000 branches is restricting major MII Indian companies from participating.We have deployed our solutions in Multi-locations and Multi-sites which includes large scale deployment in critical organizations. So kindly request you to remove the statement "1000 branches" that will allow a healthy participation and also helps more Technical Qualified Indian Make in India Starups such as ours to participate in this opportunity	Please abide by the RFP requirement	No change

96	83	OEM (Experience)	OEM's Proposed UEBA solution should be successfully implemented in at least one SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/NSE/SEBI in India during last 5 years. *(SCB – with minimum 1000 Branches in India) 30 Marks- Max Mark 10 marks per reference	Kindly requesting to amend this clause to "OEM's Proposed UEBA solution should be successfully implemented in at least one SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/NSE/SEBI/GOV/Private Organization in India during last 5 years." Keeping the branch numbers as 1000 branches is restricting major MII Indian companies from participating.We have deployed our solutions in Multi-locations and Multi-sites which includes large scale deployment in critical organizations. So kindly request you to remove the statement "1000 branches" that will allow a healthy participation and also helps more Technical Qualified Indian Make in India Starups such as ours to participate in this opportunity	Please abide by the RFP requirement	No change

97	107	41. Termination	Central Bank of India reserves the right to cancel the work/purchase order or terminate the Service Level Agreement (SLA) by providing 90 (ninety) days' prior written notice and recovering any damages, costs, and expenses incurred by the Bank under the following circumstances:	We recommend addition in the existing clause as below:Termination Central Bank of India reserves the right to cancel the work/purchase order or terminate the Service Level Agreement (SLA) by providing 90 (ninety) days' prior written notice and recovering any damages, costs, and expenses incurred by the Bank under the following circumstances: Termination by the Bidder for Breach: In the event Bank materially breaches this definitive Agreement or any statement of work, which breach is not cured within thirty (30) days after written notice specifying the breach is given to the Bank, the bidder may terminate this defenitive Agreement or any portion thereof or the applicable statement of work by giving written notice to the Bank.	Please abide by the RFP requirement	No Change

98	107	GROUNDS OF TERMINATION	i. Breach of Terms: If the bidder commits abreach of any of the terms and conditions of the Request for Proposal (RFP) or the Service Level Agreement (SLA) to be executed between the Bank and the SP. ii. Insolvency: If the bidder goes into liquidation, voluntarily or otherwise. iii. Violation of Laws: If the bidder violatesany laws, rules, regulations, byelaws,guidelines, or notifications. iv. Legal Attachment: If an attachment is leviedor continues to be levied for a period of seven days on the effects of the bid. v. Failure to Meet Timelines: If the bidder failsto complete the assignment as per the timelines prescribed in the Work Order/SLA, including any extensions granted. vi. Excess Liquidated Damages: If the deductions due to liquidated damages exceed 10% of the total work order. vii. Failure to Deliver Resources: If the bidderfails to deliver the required resources as stipulated in the delivery schedule, the Bank reserves the right to procure similar resources from alternative sources at the risk, cost, and responsibility of the bidder. viii. Non-Performance: If after the award of thecontract, the bidder fails to perform satisfactorily or causes delays, the Bank reserves the right to have the remaining contract executedby another party of its choice. The bidder must cover any	We propose to add changes in the existing clause as below:Grounds of Termination:- i.Breach of Terms: If the bidder commits a breach of any of the terms and conditions of the Request for Proposal (RFP) or the Service Level Agreement (SLA) to be executed between the Bank and the SP,and such breach is proven after providing the bidder a written notice and a reasonable cure period of not less than thirty (30) days to rectify the breach. ii.Insolvency: If the bidder goes into liquidation, voluntarily or otherwise. iii.Violation of Laws: If the bidder violates any laws, rules, regulations, byelaws, guidelines, or notifications. iv.Legal Attachment: If an attachment is levied or continues to be levied for a period of seven days on the effects of the bid. v.Failure to Meet Timelines: If the bidder fails to complete the assignment as per the timelines prescribed in the Work Order/SLA, including any extensions granted. vi.Excess Liquidated Damages: If the deductions due to liquidated damages exceed 10% of the total work order. vii.Failure to Deliver Resources: If the bidder fails to deliver the required resources as stipulated in the delivery schedule, the Bank reserves the right to	Please abide by the RFP requirement	No Change

			additional expenditure incurred by the Bank in this regard.ix. Outstanding Dues: The Bank reserves the right to recover any dues payable by the bidder from any amount outstanding,	procure similar resources from alternative sources at the risk, cost,		

			including pending bills and/or invoking the Performance Bank Guarantee under this contract.	and responsibility of the SP. viii.Non-Performance: If after the award of the contract, the bidder fails to perform satisfactorily or causes delays, the Bank reserves the right to have the remaining contract executed by another party of its choice. The bidder must cover any additional expenditure incurred by the Bank in this regard. ix.Outstanding Dues: The Bank reserves the right to recover any dues payable by the bidder from any amount outstanding, including pending bills and/or invoking the Performance Bank Guarantee under this contract.		

99	108	TYPES OF TERMINATION	i. Termination for Insolvency: The Bankmay terminate the contract if the bidder becomes bankrupt or insolvent, with termination being without compensation to the bidder. However, this does not affect any accrued rights or remedies of the Bank. ii. Termination for Default: The Bank mayterminate the contract in whole or in part, by providing written notice in case of a default by the bidder. iii. Termination for Convenience: The Bank may terminate the contract at its convenience, in whole or in part, with written notice.	We propose to add changes in the existing clause as below:- Types of Termination:- i.Termination for Insolvency: The Bank may terminate the contract if the bidder becomes bankrupt or insolvent, with termination being without compensation to the bidder. However, this does not affect any accrued rights or remedies of the Bank. ii.Termination for Default: The Bank may terminate the contract in whole or in part, by providing thirty (30) day's written cure notice, and the bidder shall allowed to remedy the default within this period in case of a default by the bidder. iii.Termination for Convenience: The Bank may terminate the contract at its convenience, in whole or in part, ~~with~~ by providing prior written notice of ninety (90) days to the bidder.	Please abide by the RFP requirement	No Change

100	102	28. FORCE MAJEURE	Force Majeure is herein defined as any cause, which is beyond the control of the service provider or the Bank as the case may be which they could not foresee or with a reasonable amount of diligence could not have foreseen and which substantially affect the performance, such as: i. Natural phenomenon, including but not limited to floods, droughts, earthquakes, epidemics, ii. Situations, including but not limited to war, declared or undeclared, priorities, quarantines, embargoes. iii. Terrorist attacks, public unrest in work area. Provided either party shall within seven (7) days from the occurrence of such a cause notify the other in writing of such causes. The Service provider or the Bank shall not be liable for delay in performing his/her obligations resulting from any Force Majeure cause as referred to and / or defined above. The decision regarding whether a particular event as informed by the bidder being a force majeure event, should be regarded as a force majeure event, shall be solely the decision of the bank. Financial reasons or escalation in prices will not fall under "Force Majeure"	We propose additions in the existing clause as below:Force Majeure:- 1.Force Majeure is herein defined as any cause, which is beyond the control of the service provider or the Bank as the case may be which they could not foresee or with a reasonable amount of diligence could not have foreseen and which substantially affect the performance, such as: i.Natural phenomenon, including but not limited to floods, droughts, earthquakes, epidemics, ii.Situations, including but not limited to war, declared or undeclared, priorities, quarantines, embargoes. iii.Terrorist attacks, public unrest in work area, iv. Any government-imposed lockdowns, supply chain disruptions, or third-party utility outages beyond the control of the service provider. Provided either party shall within seven (7) days from the occurrence of such cause notify the other in writing of such causes. The Service provider or the Bank shall not be liable for delay in performing his/her obligations resulting from any Force Majeure cause as referred to and / or defined above.In the event the Force Majeure event continues beyond thirty (30) days, the parties shall consult in good faith to	Please abide by the RFP requirement	No change

				determine an appropriate course of action. If the event continues beyond a reasonable period without		

				resolution, either party may terminate the agreement without penalty, after providing thirty (30) days' prior written notice.The decision regarding whether a particular event as informed by the bidder being a force majeure event, should be regarded as a force majeure event, shall be solely the decision of the bank. Financial reasons or escalation in prices will not fall under "Force Majeure".		

101		36. 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 accessall 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 auditson 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	We propose changes in the existing clause as below:- 36. 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 upon 15 day's prior written notice to the Bidder 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:-	Please abide by the RFP requirement	No Change

			the service provider in conjunction with the services performed for the bank.	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		

			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. RFP for Supply, Implementation & Management of Next-Generation Security Operations Centre (NG-SOC) Solutions Central Bank of India – Tender No – GEM/2025/B/6984238 103 | P a g e d. Recognized the right of the reserve bank tocause 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	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 upon fifteen (15) days prior written notice to 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 reservebank 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		

			relieves Bidder from meeting the applicable service levels. The audit shall not be performed by any	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		

			competitor of the Bidder. The auditor including regulatory auditor shall sign the confidentiality undertaking with the Bidder before conducting such audit. Monitoring	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.in relation to and as applicable to the scope of the outsourcing arrangement.		

102	104	38. LIMITATION OF LIABILITY	Bidder's aggregate liability under the contract shall be limited to a maximum of the contract value. For the purpose of this section, the contract value at any given point of time means the aggregate value of the purchase orders placed by the Bank on the Bidder that gave rise to the claim, under this Request for Proposal (RFP). This limitation shall not apply to third-party claims arising from: Intellectual Property (IP) Infringement Indemnity: The Bidder's liability for any claim or damages arising from infringement or alleged infringement of third-party intellectual property rights shall not be subject to the above limitation. Bodily Injury, Death, and Property Damage: The Bidder shall be fully liable for any bodily injury (including death) or damage to real property or tangible property caused by the Bidder's negligence, fraud, or misrepresentation, or that of its employees, representatives, or subcontractors. Indirect, Consequential, Incidental, or Special Damages: Notwithstanding the above, the SP shall be liable for any indirect, consequential, incidental, or special damages arising under this agreement or purchase order. These types of damages may include, but are not limited to, lost profits, loss of business opportunities, loss of use, or other similar damages, even if the Bidder has been advised of the possibility of such damages. Liability for Subcontractor Practices: The Service Provider shall be contractually liable for the performance of its subcontractors and must ensure that its subcontractors adhere to the same level of risk management practices as required by the Bank. This includes ensuring that	We propose to amend the clause as below:- 38. LIMITATION OF LIABILITY:Bidder's aggregate liability under the contract shall be limited to a maximum of the contract value. For the purpose of this section, the contract value at any given point of time means the aggregate value of the purchase orders placed by the Bank on the Bidder that gave rise to the claim, under this Request for Proposal (RFP). This limitation shall not apply to thirdparty claims arising from: Intellectual Property (IP) Infringement Indemnity: The Bidder's liability for any claim or damages arising from infringement or alleged infringement of third-party intellectual property rights shall not be subject to the above limitation. Bodily Injury, Death, and Property Damage: The Bidder shall be fully liable for any bodily injury (including death) or damage to real property or tangible property caused by the Bidder's negligence, fraud, or misrepresentation, or that of its employees, representatives, or subcontractors. Indirect, Consequential, Incidental, or Special Damages: Notwithstanding the above, the ~~SP~~ Neither party shall be liable for any indirect, consequential, incidental, or special damages arising under this agreement or purchase order.	Due to typo error the clause is repeated and hence kindly ignore the clause	Clarification

			subcontractors meet the agreed-upon standards of performance, compliance, and quality.	These types of damages may include, but are not limited to, lost profits, loss of business opportunities, loss of use, or other similar damages, even if the		

				~~Bidder~~ either Party has been advised of the possibility of such damages. Liability for Subcontractor Practices: The Service Provider shall be contractually liable for the performance of its subcontractors and must ensure that its subcontractors adhere to the same level of risk management practices as required by the Bank. This includes ensuring thatsubcontractors meet the agreed-upon standards of performance, compliance, and quality.		

103		We Recommend new clause to the RFP		We recommend to add new clause under the RFP as below:- Non-Solicitation:- During the Term of this definitive Agreement and for a period of one year thereafter, neither Party shall (either directly or indirectly through a third party) solicit to employ, cause to be solicited for the purpose of employment to any employee/s (including the employees who have been exposed or introduced to other Party during initial discussion between Parties or engaged to provide/perform the services under any definitive agreement entered between Parties) of the other Party or aid any third person to do so, without the specific written consent of the other Party. The said restriction shall also apply to each Party's affiliates, agents, vendors, contractors, and any third parties with whom such Party has a relationship (collectively, "Representatives"). Parties agree that Representatives are equally restricted from poaching or soliciting or inducing any employees of other Party to leave	Please abide by the RFP requirement	No Change

				their employment or engagement with such other Party.		

104	20	Point 13)	The service delivery (SLA Management) and periodic reporting should be done through automated dashboards.	Request for Clarification: Is the customer expecting these dashboards to be part of the proposed solution, or are they looking for a dedicated third-party dashboard solution to provide the bank with complete visibility and clarity?	Please abide by the RFP requirement	Clarification
105	20	Point 14)	Provide immediate forensic support in case of any security / cyber incident. Bidder has to provide required support to Bank / Regulator appointed forensic investigation agency / vendor / consultant / company / auditor in such scenario.	Request for Clarification: Given that forensic services are comprehensive and involve multiple activities, kindly confirm the number of forensic service hours allocated for each year?	Please abide by the RFP requirement	Clarification

106	20	Point 17)	The proposed solutions implemented by the Bidder should adopt evolving threats and technological advancements, including Quantum Computing and AI based threat.	Request for Clarification: Quantum computing– and AI-based threats are emerging and continuously evolving in nature. In order to ensure accurate compliance with the Bank's expectations, we request detailed clarification on the scope and intent of this requirement. 1) Expectation Clarification Kindly clarify whether the Bank expects: a) Immediate detection and response capabilities for current AI-driven threats, and/or b) Architectural readiness and monitoring capabilities for future quantum-era risks, rather than direct quantum-resistant cryptographic controls. 2) Deployment Model for AI Capabilities Please confirm whether the Bank requires: a) A single SIEM platform with embedded AI capabilities deployed fully on-premises at the Bank's DC and DR, or b) A hybrid architecture where the SIEM is deployed on-premises at DC and DR, while AI/ML analytics are deployed on a secure cloud environment hosted within India, complying with data residency requirements.	Please abide by the RFP requirement	Clarification

				3) Multi-OEM Architecture Acceptance		

				Kindly confirm whether the Bank permits proposing AI/quantum-readiness capabilities from a separate OEM (not the SIEM provider), with such components deployed on-premises at the Bank's DC and DR and integrated with the SIEM.		

107	21	Point 21)	Bank's expectation is that successful bidder is required to manage the existing SOC for another one year after expiry of existing contract in Jan'27.	Request for Confirmation Kindly confirm whether our understanding is correct: as per this requirement, the bidder is expected to operate the existing SOC for a period of one (1) year, followed by a five (5) year contract for the newly proposed SOC solution. This implies that the overall operational engagement would span a total duration of six (6) years post deployment of the new SOC solution.	bidder is expected to run current set up parallelly for three years	Clarification
108	21	22.3 Service Level Management, Service reporting	Maintain the service levels as per the RFP and provide a periodic report to the Bank assessing all device performance under the scope of RFP against the Service Levels. Service Levels will include Availability measurements and Performance parameters(Utilization of CPU, RAM, storage, TPS,performance,uptime/downtime, EPS etc.) The Bidder should provide the requisite tools to measure availability of Hardware, OS, platform, other solutions as per RFP.	Request for Clarification: Kindly confirm whether the bidder's own proprietary solution is acceptable to address this use case, or if the Bank requires a solution from a separate, industryrecognized OEM.	Please abide by the RFP requirement	Clarification

109	22	25. 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. Data retention period will be the entire contract period. As per the regulatory guidelines all relevant data has to be stored for minimum 10 years. 6 Months data should be available online and should be stored in highest speed of storage. Another 12 months data should be in warm node that can be accessible through the application. Beyond that till contract period, Data should be in Archival node.	Request for Clarification: Kindly clarify whether the bidder is permitted to leverage the Bank's existing backup solution for the proposed security solution under this RFP, or if the bidder is required to propose a new backup solution as part of the scope.	Please abide by the RFP requirement	Clarification

110	28	7.3 TRANSITION FROM EXISTING SOC TO NG-SOC:	Migrate configurations, rules, use cases, other settings, logs from existing SOC	Request for Clarification – Migration Scope The RFP mentions migration of configurations, rules, use cases, settings, and logs from the existing SOC. Kindly confirm whether the bidder is expected to migrate historical logs from the existing SIEM at the Bank's DC and DR. Based on industry practice, historical logs stored in SIEMs are typically encrypted and maintained in proprietary OEM-specific formats, making direct migration to a new SIEM technically infeasible. Accordingly, we request confirmation whether the Bank will accept parallel run of the existing and new SOC for a defined transition period (e.g., six months), with migration limited to configurations, rules, use cases, and operational settings only. Requested Modification In view of the above, we request the Bank to consider modifying the scope as follows:	Bank is not expecting to migrate all the logs from existing solution. Kindly read as "Migrate configurations, rules, use cases, and other Supported operational settings from the existing SOC"	No Change

				"Migrate configurations, rules, use cases, and other Supported operational settings from the		

				existing SOC.”		

111	20	7. SCOPE OF WORK	All the tools/ application/ OS/hardware supplied as part of the project should be on premise, latest and supplied with Enterprise-wide Licenses and all the licenses / subscriptions should be in the name of Central Bank of India.		Please abide by the RFP requirement	No change
112	11	2. ELIGIBILITY CRITERIA # 3	The bidder must have minimum annual turnover in India of Rs. 1000 crores each year in the last three financial years (i.e. 2022-23, 2023-24,2024-2025) as an individual company and not as group of companies.	We request to modify the clause as below:- The bidder must have minimum average annual turnover in India of Rs.450 crores in the last three financial years (i.e. 2022-23, 202324,2024-2025) as an individual company and not as group of companies.	Please abide by the RFP requirement	No change

113	79	Section – 1 – Experience Criteria # 4	The Bidder should have implemented or managed any on-premises UEBA solution with minimum 20,000 users in at least one SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/NSE/SEBI in India during last 5 years. *(SCB – with minimum 1000 Branches in India)	We request to modify the clause as below as UEBA comes with Analyst licences hence request you to change with 3 Analyst Section – 1 – Experience Criteria # 4 The Bidder should have implemented or managed any onpremises UEBA solution with minimum 20,000 users in at least one SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/NSE/SEBI in India during last 7 years. *(SCB – with minimum 1000 Branches in India) or The Bidder should have implemented or managed any onpremises UEBA solution with minimum 3 Analyst in at least one SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/NSE/SEBI in India during last 7 years.	Please abide by the RFP requirement	No change

				*(SCB – with minimum 1000 Branches in India)		

114	80	Section – 1 – Experience Criteria # 5	The Bidder should have integrated TIF solution with any on-premise SOC in at least one SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/NS E/SEBI in India during last 5 years. *(SCB – with minimum 1000 Branches in India)	We request to modify the clause as below:- Section – 1 – Experience Criteria # 5 The Bidder should have integrated TIF solution with any on-premise SOC in at least one SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/NS E/SEBI in India during last 7 years. *(SCB – with minimum 1000 Branches in India)	Please abide by the RFP requirement	No change
115	80	Section – 1 – Experience Criteria # 6	The Bidder should have provided services of Brand Protection in at least one SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/NS E/SEBI in India during last 5 years. *(SCB – with minimum 1000 Branches in India)	We request to modify the clause as below:- Section – 1 – Experience Criteria # 6 The Bidder should have provided services of Brand Protection in at least one SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/NS E/SEBI in India during last 7 years. *(SCB – with minimum 1000 Branches in India)	Please abide by the RFP requirement	No change

116	81	Section – 1 – Experience Criteria # 13 OEM (Proposed Solution Experience)	The Bidder should have implemented or managed SOC with on-premises SIEM solution with minimum 1,00,000 Events Per Second (EPS) or 3.4TB / Day in at least one SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/NS E/SEBI in India during last 5 years. *(SCB – with minimum 1000 Branches in India)	Kindly confirm whether this point is applicable to the OEM or the Bidder. As per the criteria for Bidder/OEM, it is mentioned under "OEM (Proposed Solution Experience)"	Please abide by the RFP requirement	clarification

117	63	12.2 SERVICE LEVELS DURING IMPLEMENTATION PHASE	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.	Request Penalty capping of 5% We request to modify the clause as below:- Penalty would be levied for delivery, installation, and implementation delays for each solution and shall be a maximum of 5% of the total cost of that solution from the finalized Bidder for the Bank.	Please abide by the RFP requirement	No change
118	70	15. LIQUIDATED DAMAGE	Liquidated Damages deducted will be pegged at 10% of the total contract value.	Request Penalty capping of 5% We request to modify the clause as below:- Liquidated Damages deducted will be pegged at 5% of the total contract value.	Please abide by the RFP requirement	No change

119	88	23.1 PROCEDURE FOR CLAIMING PAYMENTS Hardware	40% On post-delivery inspection of the Hardware 50% Against successful installation and acceptance testing signoff by Bank at DC, DRC 10% 3 months after successful installation signoff of software / solution / service and signoff by Bank at DC, DRC.	We request to modify the clause as below:- 23.1 PROCEDURE FOR CLAIMING PAYMENTS 60% Against delivery of respective components. 30% Against successful installation and Sign-off of respective components. 10% 3 months after successful Go-Live signoff of respective components.	Please abide by the RFP requirement	No change
120	88	Software (Including OS & other associated software)	30% On post-delivery of the licenses 50% Against successful implementation and acceptance testing of respective software / solution/ service (i.e. SIEM, SOAR, UEBA, TIF, Brand Protection) and signoff by Bank at DC, DRC 10% After Successful Migration of existing policies, rules, scenarios, logs, VAPT compliance and completion of one DR Drill 10% 3 months after successful implementation signoff	We request to modify the clause as below:- 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 GoLive signoff of respective components.	Please abide by the RFP requirement	No change

121	89	Implementation Charges	70% On successful implementation of respective software / solution / service (i.e. SIEM, SOAR, UEBA, TIF, Brand Protection) of the RFP in DC, DR and its sign off and acceptance by the Bank 10% Fine tuning and acceptance by Bank for fully operational SOC and other solutions / services, Issuance of Go-Live Certificate by the Bank. 20% 3 months after fully operational and completion of migration of logs, existing policies etc,	We request to modify the clause as below:- Implementation Charges 70% After sign-off and go-live of respective components. 30% After 3 months of go-live of respective components.	Please abide by the RFP requirement	No change

			Go-live signoff and satisfactory working of each solution / service.			

122	89	23.1 PROCEDURE FOR CLAIMING PAYMENTS	AMC charges will be paid quarterly in arrears and on satisfactory working of the hardware infrastructure.	• AMC/ATS amount payable would be paid Annually Advance in the begining of each year (Because the bidder needs to pay the OEM his money upfront)	Please abide by the RFP requirement	No change
123	131	68. ANNEXURE 2: MINIMUM TECHNICAL SPECIFICATIONS	The solution must ensure that if data ingested is not parsed then with the new parser old data ingested should also be parsed without need to re-ingest data in the SIEM throughout the minimum retention period of online 180 days and 365 days of archival.	(The Search based approach adds more hardware footprint and takes time for detection. While real time corelation will mitigate the risk of delays in detection capability.Most leading vendors licensing is flat model and doesn't charge extra for peak eps consumptions and doesn't charge based on search and for some vendors licensing is based on search / ingestion hence such clauses included.) Clause To be modified SIEM Clause 8- The solution must ensure that if data ingested is not parsed then the old data should be parsed with new parser, without need	Please abide by the RFP requirement	No change

				to re-ingest data, from outside of SIEM Platform & Archival storage and should not be manual process, throughout the data retention period of online 180 days and 365 days of archival		

124	138	68. 2: ANNEXURE MINIMUM TECHNICAL SPECIFICATIONS	The solution must support viewing data in different formats or schemas without reconsumption, re-indexing, redundant storage. Historical data also should be viewed as per new format or schema without re-consumption or without additional storage utilization.	(The Search based approach adds more hardware footprint and takes time for detection. While real time co-relation will mitigate the risk of delays in detection capability.Most leading vendors licensing is flat model and doesn't charge extra for peak eps consumptions and doesn't charge based on search. for some vendors licensing is based on search / ingestion hence such clauses included.) Clause TO BE MODIFIED :The solution must support viewing data in different formats or schemas without re-consumption, ~~re-~~	Please abide by the RFP requirement	No change

				~~indexing~~, redundant storage. Historical data also should be viewed as per new format or schema without re-consumption or without additional storage utilization.		
125	104	Section 37 Information Security : The platform and solution should encrypt/tokenize data at rest.		Query:How many Database servers would be there on which encryption would be applied?	Please abide by the RFP requirement	Clarification

126	104	Section 37 Information S The Solutio should identifiable ersonally information per the (PII) as guidelines. statutory		Query: 1.What is approximate user count whose PII data needs to be encrypted? 2. Whether vault is required to encrypt and tokenize PII data?	Please abide by the RFP requirement	Clarification
127	5	1. - Gene Optio ric Clause n (GeM Document)	OPTION CLAUSE: The buyer can increase or decrease the contract quantity or contract duration up to 25 percent at the time of issue of the contract. However, once the contract is issued, contract quantity or contract duration can only be increased up to 25 percent. Bidders are bound to accept the revised quantity or duration	The prices are dependant on Taxes, Duties (including Custom Duty), Levies, OEM List Price, OEM Discounting, USD-INR exchange rate, Consumer Price Index etc. Kindly request bank to allow for price revision for additional quantity at mutually agreeable prices.	Please abide by the RFP requirement	No Change

128	22	7. SCOPE OF WORK Point 26	Depending on the requirement, Bank reserves the right to extend the contract with the successful bidder including Subscription, AMC, ATS and Onsite FM Services of the supplied Platform and Solution for 2 more years i.e. 6th and 7th year on the same terms and conditions wherein enhancements/cost escalation quoted for 4th and 5th year would be taken as the price reference for the extension of the contract.	The prices are dependant on Taxes, Duties (including Custom Duty), Levies, OEM List Price, OEM Discounting, USD-INR exchange rate, Consumer Price Index etc. Kindly request bank to extend contract at mutually agreeable prices.	Please abide by the RFP requirement	No Change

129	68	12. SLA COMPLIANCE	SLA Penalty	Kindly request the bank to levy SLA penalty upto maximum 10% of monthly SOC operation charges.	Please abide by the RFP requirement	No Change
130	88	23.1 Procedure for Claiming Payments	The payment terms defined in RFP for Hardware is as below: --> Delivery Sign-off of respective components – 40% --> Successful Installation Sign-off of respective components – 50% --> 3 Months after successful installation sign-off of respective components – 10%	Kindly request the bank to modify the Hardware payment terms as per industry standards mentioned below: --> Delivery Sign-off of respective components – 70% --> Successful Installation Sign-off of respective components – 20% --> Against BG of equivalent amount – 10%	Please abide by the RFP requirement	No Change

131	89	23.1 Procedure for Claiming Payments	The payment terms defined in RFP for Software is as below: --> Delivery Sign-off of respective components – 30% --> Successful Installation Sign-off of respective components – 50% --> Successful Migration of existing policies – 10% --> 3 Months after successful installation sign-off of respective components – 10%	Kindly request the bank to modify the Software payment terms as per industry standards mentioned below: --> Delivery Sign-off of respective components – 70% --> Successful Installation Sign-off of respective components – 10% --> Successful Migration of existing policies – 10% --> Against BG of equivalent amount – 10%	Please abide by the RFP requirement	No Change
132	89	23.1 Procedure for Claiming Payments	The installation payment terms metioned in RFP is as below: --> Successful Implementation of respective software Sign-Off – 70% --> Fine tuning and Go-Live – 10% --> 3 Months after successful installation sign-off – 20%	Kindly request the bank to modify the payment term for installation as below: --> Successful Implementation of respective software Sign-Off – 90% --> Against BG of equivalent amount – 10%	Please abide by the RFP requirement	No Change

133	89	23.1 Procedure for Claiming Payments	--> Migration of existing policies – 70% --> Fine tuning and Go-Live – 10% --> 3 Months after successful installation sign-off – 20%	Kindly request the bank to modify the payment term for migration as below: --> Migration of existing policies – 90% --> Against BG of equivalent amount – 10%	Please abide by the RFP requirement	No Change
134	90	23.1 Procedure for Claiming Payments	The ATS subscription charges mentioned in RFP are Quarterly in Arrears	Kindly request the bank to modify the payment term for ATS subscription charges as Annual in Advance.	Please abide by the RFP requirement	No Change
135	108	41. Termination .	iii. Termination for Convenience: The Bank may terminate the contract at its convenience, in whole or in part, with written notice	The bidder would have contracted non-cancellable cotnract with the OEMs to provide back-to-back back-lining of support. Hence request the bank to remove this clause.	Please abide by the RFP requirement	No Change
136	127	67. Annexure 1: Bill of Material	Table – H (Professional Services Cost)	Kindly request the bank to allow Professional Services cost to be quoted for different technologies separately as they are niche technologies and each of them has a different level of skillset requirement.	Please abide by the RFP requirement	No Change
137	129	67. Annexure 1: Bill of Material	The bidder shall ensure that AMC rates must be quoted above 8% and ATS rates must be quoted above 12% for the respective product(s).	Kindly request the bank to allow AMC/ATS rate to be quoted above 4% for respective product.	Please abide by the RFP requirement	No Change

138	Multiple	Indemnities		There are various Indemnities mentioned across the document. We have the following submissions/ Queries:- 1. Indemnities across the document shall be restricted only to:- a. Breach of 3rd Party IPRs; b. Breach of Confidentiality Obligations; c. Personal Injury/ Death caused due to any negligent acts of the Bidder or its personnel; d. Damage to tangible property due to any negligent actions or inactions of the Bidder or its personnel. 2. Para no. 1 of clause 26:- The wordindirect shall be removed. No Indirect damages or Indemnities are agreed in commercial contracts in India as per standard practise. 3. If the Bank proposed to continue thegeneric Indemnities then the same shall be delinked from breach of SLAs/ PO terms. For breach of SLAs there is already a seperate remedy available at the disposal of the Client. Indemnities if generic shall be restricted only to breach of MSA / Agreement terms and since these are	Please abide by the RFP requirement	No Change

				wide open indemnities, they amount shall be restricted to 3 months contract value. 4. If Indemnities are as per 1 above then the same shall be restricted to ACV.		

139	104	38. Limitation of Liability		Since there are blanket indemnities including for Financial losses, etc. it is important that the Bidder shall not be held liable for Indirect Losses. Hence modification to clause 38 is proposed as below:- Indirect, Consequential, Incidental, or Special Damages: Notwithstanding the above, the ~~SP~~ Bidder shall not be liable for any indirect, consequential, incidental, or special damages arising under this agreement or purchase order. These types of damages may include, but are not limited to, lost profits, loss of business opportunities, loss of use, or other similar damages, even if the Bidder has been advised of the possibility of such damages. There are 2 Limitation of Liability clauses one on page no. 101 clause no. 34 and the other on page no. 104 clause no. 38. It order to avoid confusion, clause no. 34 on page no 101 shall be deleted. and clause no. 38 shall be modified to exclude Indirect, special, consequential losses etc.	Due to typo error the clause is repeated and hence kindly ignore the clause	Clarification

140	80	33. Inspection and Audit		Please confirm that Audit shall be restricted to scope of services only. Financial Information like pricing information, Board, Committee Minutes, etc. shall be out of scope of the Audit. The current clause is very broad.	Please abide by the RFP requirement	No Change
141	11	2. ELIGIBILIT CRITERIA		Bidder request to add following criteria under Eligibility - The bidder should have its own/ Captive New Generation SOC Setup in India (technology and customer logs should be stored in Indian jurisdiction only) providing SOC as a service/ managed SOC services including remote log monitoring, correlation and analysis and security incident management services, etc.	Please abide by the RFP requirement	No change
142	19	7. SCOPE OF WORK		What is the current CSOC at the customer location? Are there currently any configured playbooks / runbook / corelations built on the CSOC?Please provide count. DO the same need to be replicated in the New NG SOC?	Please abide by the RFP requirement	Clarification

143	27	7.2 SETTING UP NG-SOC / Point 28		Bank may deploy the resources at both DC- Mumbai/Navi Mumbai and DR Hyderabad site as per Bank's requirement. - Kindly provide clarity on these resources. Are they going to be additional to the ones requested in the RFP?	Will be discussed with successful bidder	Clarification

				resources allocation between DC / DR require to plan weekly shift schedule and week off		
144	27	7.2 SETTING UP NG-SOC / Point 29		from this point, we understand that while the bank has specified the resource count in the RFP, the bidder may increase the count based on the solution requirements. Please confirm. If yes then bidder request to specify the resource count in RFP as per standard roster, e.g. to support 24/7 we need to have 5 resource count.	Please abide by the RFP requirement	Clarification

145	28	7.3 TRANSITION FROM EXISTING SOC TO NG-SOC:		Bidder request to park the scope of managing existing SOC with incumbent partner because bidder do not have any solution visibility of deployed SoC and if Bank still wants new partner to take care of this along with NextGen SoC then bidder request to share complete solution details like architect, over all infra used for existing SoC along with AMC & capacity usage details. we will also need tools in use and the deployed manpower for shadowing purpose	Please abide by the RFP requirement	No change

146	28	7.3 TRANSITION FROM EXISTING SOC TO NG-SOC:		The expectation is to manage the day-to-day operations of the existing SoC setup. Is the bank expecting to onboard resources before the deployment of the NextGen SoC? If so, what is the lead time for onboarding resources from the date of PO release? Additionally, can the bidder start resource billing from the date of onboarding? Bidder also request to specify the skill wise resources count who will be managing the existing SoC solution.	Please abide by the RFP requirement	Clarification

147	33	7.4 SCOPE OF WORK FOR PROPOSED SOLUTIONS / SIEM Use case Management		What are the number of use cases / playbooks to be developed during a year? What are the current number of use cases deployed ? What is the current ratio of False Positives	Will be discussed with successful bidder	Clarification
148	42	7.8 NG-SOC OPERATIONS, FACILITY MANAGEMENT, AMC & ATS / Point 3		Is this Mandatory requirement for all resources or for critical L2 and L3 resources only.	Please abide by the RFP requirement	Clarification
149	42	7.8 (3)		Kindly define Bank interview scheduling lead times	Will be discussed with successful bidder	Clarification
150	44	7.8 NG-SOC OPERATIONS, FACILITY MANAGEMENT, AMC & ATS / Point 14		How much such plug ins, parsers per year we should consider for effort estimation. Please help with your past experience or historical data or can we propose basis the standard practices. Please clarify	Please abide by the RFP requirement	Clarification
151	47	7.8 NG-SOC OPERATIONS, FACILITY MANAGEMENT, AMC & ATS / point 35		NTT Assumes that the existing resources deployed for support will support digital forensic process, no additional resources need to be configured for the same.	Please abide by the RFP requirement	Clarification

152	47	7.8 NG-SOC OPERATIONS, FACILITY MANAGEMENT, AMC & ATS / point 36		how many Man-days effort required for this activity.	Please abide by the RFP requirement	Clarification
153	47	7.8 (42) & 7.8 (4)		Please clarify how short- term OEM SMEs (e.g., AI/ML model tuning, red- team simulations) can be engaged under offsite SME support without violating the 'no subcontracted engineers onsite' clause.	Please abide by the RFP requirement	Clarification
154	48	7.9 MANPOWER REQUIREMENT & DESIRED SKILLSET		The bidder requests the bank to specify the salary slab for each resource type and to outline the requirements for the Client Delivery Manager, MIS, and Quality/Audit resources scope as well.	Please abide by the RFP requirement	Clarification
155	58	7.10 (2) & 12.3.3		Please define ack/restore SLAs for on- call vs onsite coverage during cyber drills/incidents to align with 24x7 exigency support.	Please abide by the RFP requirement	Clarification

156	58	7.10 (Training)		Please confirm role- based curricula (Analyst/Engineer/Admin) for the OEM- led 5- day/year trainings and whether the hands- on lab must replicate Bank's deployed architecture.	Will be shared with successful bidder	Clarification
157	63	12.3.1 UPTIME AND UPTIME PENALTY		Will the billing of deployed resources be released based on the solution uptime SLA or resource availability as per the required service window? Bidder understanding is resources billing will start from date of deployment. Please clarify	Please abide by the RFP requirement	Clarification
158	90	23.1 PROCEDURE FOR CLAIMING PAYMENTS		FM Support Charges (32 resources) however 7.2 SETTING UP NG-SOC / Point 29 said that the bidder may increase the count based on the solution requirements hence total billing will be done total no. of resource deployed instead given 32 resource count.	Please abide by the RFP requirement	Clarification

159	65	12.3.3 PENALTY ON SERVICE LEVELS DURING OPERATIONS PHASE		98% to 99.9,2% of monthly NGSOC FMS charges. NTT assumes that if they provide backup Engineer in place of resigned or on leave engineer, no penalty will be applicable. Please confirm.	Please abide by the RFP requirement	Clarification
160	21–22	7.2 (21)		RFP notes expectation to manage existing SOC for one year after Jan'27. Please clarify commercial model (Table- G vs separate line) and scope boundary (ticketing, upgrades, compliance) for that additional year.	Please abide by the RFP requirement	Clarification
161	24–27	7.2 (25)		Does the 'minimum 10 years regulatory retention' requirement apply to all log types or only relevant data classes? Is tape/offline archival acceptable beyond contract tenure?	Please abide by the RFP requirement	Clarification
162	60	8. GENERAL RESPONSIBILITY OF THE BIDDER		Bidder should be able to provide back up in removable device (tapes) to enable the bank for offsite storage of backup. Please clarify that bank will provide transportation and logistic for offsite tape movement.	Please abide by the RFP requirement	Clarification

163	30–34 & 66	7.4 (Reporting) & 12.3.3 (#1)		Request anonymized 12- month indicative volumes: average daily alerts/events, incident severities, and monthly ITSM ticket counts to finalize team sizing and SLA baselines.	Will be discussed with successful bidder	Clarification

164	44–47 & 63–68	7.8 & 12.3.3 & 12.3.2		Kindly specify the mandatory back-to- back OEM SLA minimums we must secure (e.g., 4- hour RMA to site, N- 1 patch policy within 90 days, replacement for non- FRU components).	Please abide by the RFP requirement	No change
165	48–58	7.9 (Manpower)		Please share the Mumbai vs Hyderabad split per role and approval TATs for replacement/backfill so that manpower availability penalties do not trigger unfairly.	Will be discussed with successful bidder	Clarification
166	48–58	7.9 (Skills)		Request confirmation that equivalent OEM certifications can substitute for global certifications (CISSP/CISM/GCFA etc.), and whether a minimum % certified per layer (L1/L2/L3) is mandated.	Please abide by the RFP requirement	No change

167	63–68 & 70	12.3.1 & 15		Please confirm downtime exclusions (planned DR drills, Bank dependencies) for uptime penalties and the interplay between SLA penalties and Liquidated Damages.	Please abide by the RFP requirement	Clarification
168	65–67	12.3.3 (#1)		Kindly define 'clock start' for event notification SLAs—event occurrence time, SIEM correlation time, or SOC analyst detection time.	Please abide by the RFP requirement	Clarification
169	68–69	12.3.5 & 12.3.3 (#7)		Please specify Bank approval SLA (days) for onboarding each resource, the background verification dossier format, and any grace period before manpower availability penalties apply.	Please abide by the RFP requirement	Clarification
170	68	Availability Service Level Default for Facility Management		minimum attendance of 99 % per resource means 9 hours a day and 5 days a week so 180 hours of month?	Please abide by the RFP requirement	Clarification

171	87–91	23 & 23.1 (FM/ATS)		Please confirm that pre-Go- Live staffing for dual- run/legacy support is payable under Implementation (Table- C). If not, may FM billing commence from onboarding during dual- run?	Please abide by the RFP requirement	Clarification
172	General	General		we need call dump for security incidence and alerts per month for right team sizing, please help.	Please abide by the RFP requirement	Clarification
173	General	Parser Creation		Are there any custom parsers currently utilised for log ingestion etc. What technologies were these utilised for?	Please abide by the RFP requirement	Clarification
174	General	General		Bidder request to keep the minimum qualification for the deployed resources will be any graduation from an recognized university.	Please abide by the RFP requirement	No change
175	General	General		is rebadging of few of the existing resources who fulfils bidder eligibility criteria, can be considered an option for resource deployment	Please abide by the RFP requirement	Clarification

176	General	Background Verification		Clarify whether police verification/security clearance is required for all deployed resources.	Please abide by the RFP requirement	Clarification

177	49	7.9 MANPOW & REQUIREMENT DESIRED - SKILLSET Infrastructure Management		only 1 L2 engineer in general shift is mentioned does that means there want be L2 engineer required on week off and holiday? Does that also applies to L3 engineer and Program director?	L1, L2 and L3 engineers are must work on 24x7x365 basis. Project Director must be present on all working days. However, project director must be able available onsite in case of need on non-working days and should be available on phone all the time.	Clarification
178	25	7.2 SETTING UP NG-SOC/ Point 24		Please provide volumes of the solutions /tools to be integrated into the NG SOC solution	Will be shared with successful bidder	Clarification
179	25	7.2 SETTING UP NG-SOC / Point 22		Does the bank require hardware based storage on location or a cloud based storage would suffice with DR storage on premise	Please abide by the RFP requirement	Clarification
180				IS the supplier expected to manage the current CSOC setup for 1 Year. Please provide current log ingestion and team size managing the set up.	Bidder is expected to run current set up parallelly for three years.	Clarification

					Remaining	
					details will be shared with successful bidder.	
181				Is the bank looking for a hypotheses based threat hunting approach or is current threat hunting referring to IOC based threat hunting?	Both is required	Clarification
182				What is the current ticket count as recorded by the ITSM. Could you provide us with a security ticket dump for the past 12 months.	Will be shared with successful bidder	Clarification

183	13	2. ELIGIBILITY CRITERIA Point 11	The Bidder should have implemented or managed on premise SIEM solution and currently in use with minimum 1,00,000 Events Per Second (EPS) or 3.4TB / Day in at least ONE Scheduled Commercial Bank (SCB)*/RBI/NPCI/BSE/NSE/SEBI in India during last 5 years *(SCB – with minimum 1000 Branches in India)	Request to bank to include Maharatna CPSEs and BFSI segments for larrger participation	Please abide by the RFP requirement	No Change

184	13	2. ELIGIBILITY CRITERIA Point 11	The Bidder should have implemented or managed on premise SIEM solution and currently in use with minimum 1,00,000 Events Per Second (EPS) or 3.4TB / Day in at least ONE Scheduled Commercial Bank (SCB)*/RBI/NPCI/BSE/NSE/SEBI in India during last 5 years *(SCB – with minimum 1000 Branches in India)	Request to bank to change this to The Bidder should have implemented or managed on premise SIEM solution and currently in use with minimum 50,000 Events Per Second (EPS) or 2 TB / Day in at least ONE Scheduled Commercial Bank (SCB)*/RBI/NPCI/BSE/NSE/SEBI in India during last 5 years *(SCB – with minimum 1000 Branches in India)	Please abide by the RFP requirement	No Change

185	12	2. ELIGIBILITY CRITERIA Point 13	The Bidder should have implemented or managed on premise UEBA solution in at least ONE Scheduled Commercial Bank (SCB)*/RBI/NPCI/BSE/NSE/SEBI/ in India during last 5 years *(SCB – with minimum 1000 Branches in India)	Since Since UEBA adoption is a recent development in the last 3+ years request bank to change The Bidder should have implemented or managed on premise UEBA/UBA solution in at least ONE Scheduled Commercial Bank (SCB)*/RBI/NPCI/BSE/NSE/SEBI/ in India during last 5 years *(SCB – with minimum 1000 Branches in India) UEBA/UBA	Please abide by the RFP requirement	No Change

186	28	7.3 TRANSITION FROM EXISTING SOC TO NG-SOC:	Migrate configurations, rules, use cases, other settings, logs from existing SOC	Our understanding is that bidder has to analyze existing configuration and repliacate to the NGSOC and bank is not looking for log data migration. Migration of logs from existing SIEM to a different proposed SIEM is not possible as every OEM stores data in their own format. The current SIEM will run parallelly to the newly deployed SIEM till the Bank's log retention policy time to fetch the logs if required for forensics or investigation. Request bank to clarify the understanding	Bank is not expecting to migrate all the logs from existing solution, and hence asked to run current set up parallelly for three years	Clarification

187	31	7.4 SCOPE OF WORK FOR PROPOSED SOLUTIONS	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.	Kindly clarify whether the health checkup should be done yearly or half yearly	Please abide by the RFP requirement	Clarification
188	39	7.6 SECURITY DASHBOARDS	The dashboard should be based on secure web based architecture and accessible to users only after verifying identity with Multi Factor Authentication mechanism.	Our understanding is that bank will provide the MFA solution and bidder has to integrate the same for authentication. Kindly clarify	Please abide by the RFP requirement	Clarification

189	60	8. GENERAL RESPONSIBILITY OF THE BIDDER	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.	Request bank to clarify what will be available power per rack to arrive the number of racks needed	Please abide by the RFP requirement	Clarification

190	60	8. GENERAL RESPONSIBILITY OF THE BIDDER Delivery, Installation and Maintenance	Installation of the solutions is to be performed by OEM / OEM authorised partner for each solution. In case of OEM authorised partner OEM certificate should be presented to Bank mentioned authorisation to the partner.	Under section 7.7 OEM resposibilities it is mentioned Implementation should be done by the OEM. Kindly clarify whether the implementation has to be done by OEM or it can be done by authorized partner	Please abide by the RFP requirement	Clarification
191	78	Stage 2 Technical Bid and Presentation Evaluation Section – 1 – Experience Criteria Point 1	The Bidder should have implemented or managed SOC with on-premises SIEM solution with minimum 1,00,000 Events Per Second (EPS) or 3.4TB / Day in at least one SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/NSE/SEBI in India during last 5 years. *(SCB – with minimum 1000 Branches in India)	As the number of SCB having 100000 events are limited request bank to consider marks based on slabs for larger participation like 30000 - 50000, 50000 - 75000, 75000 -100000	Please abide by the RFP requirement	No change

192	78	Point 2 Bidder (Solution Capacity Implementation Experience)	The Bidder should have implemented or managed SOC with any on-premises SIEM solution with minimum 1,00,000 Events Per Second (EPS) or 3.4TB / Day in at least one SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/NSE/SEBI in India during last 5 years. *(SCB – with minimum 1000 Branches in India)	As the number of SCB having 100000 events are limited request bank to consider marks based on slabs for larger participation like 30000 - 50000, 50000 - 75000, 75000 -100000	Please abide by the RFP requirement	No change
193	79	Point 4 Bidder (Experience)	The Bidder should have implemented or managed any on-premises UEBA solution with minimum 20,000 users in at least one SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/NSE/SEBI in India during last 5 years. *(SCB – with minimum 1000 Branches in India)	Requestbank to change it UEBA/UBA	Please abide by the RFP requirement	No change
194	68	Audit/ VAPT of NGSOC 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. Audit observations to be closed as per Bank's TAT (turnaround time).	It is understood that Bank team will run VA scans & Pen Tests on the NGSOC solutions and bidder to close/remediate the findings. Please confirm if the understanding is correct or does Bank expects bidder to run the VA scans & Pen Testing.	Please abide by the RFP requirement	Clarification

195	20	Point 18	18 - Bank will also have a right to relocate any one or all the tools to different locations without any extra cost to the bank	What is the likeliness of Bank deciding to relocate the tools in DC/DR to different locations? We request Bank to give minimum 90 days prior intimation upon such request for the bidder to	Please abide by the RFP requirement	Clarification
				sufficiently prepare for the migration.		
196	36	V. Brand Protection Services including Dark Web Monitoring	Fake Website detection impersonating Bank, work with domain registrars and hosting providers to shutdown / takedown such websites with Bank's permission.	For Brand Monitoring, what is the number of takedowns of malicious content to be factored per year?	Unlimited	Clarification
197		General Query		Can bidder leverage Bank's software distribution/patch management tool for deployment of Log collector Agents on Windows servers for log collection to SIEM?	Will be discussed with successful bidder	Clarification
198	21	Point 21	21. Bank's expectation is that successful bidder is required to manage the existing SOC for another one year after expiry of existing contract in Jan'27	Specify the existing ingestion volume/EPS of the currently deployed SIEM to factor efforts for migration & parallel run.	Will be shared with successful bidder	Clarification

199		Point 28	As per the regulatory guidelines all relevant data has to be stored for minimum 10 years. 6 Months data should be available online and should be stored in highest speed of storage. Another 12 months data should be in warm node that can be accessible through the application. Beyond that till contract period, Data should be in Archival node.	Please specify if the Storage for archival logs should be factored for upto contract period (total 5 years) or 10 years	Upto contract period	Clarification

200	32	Log archival.	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	Please specify whether the archival storeage is needed in NAS or can it be on tape	Please abide by the RFP requirement	Clarification
201	38	7.5 SERVICES	Below services should be offered as part of NG-SOC Offering: i. Security Intelligence Feeds and Services	Does Bank expect this service over and above the ask of Threat Intel Feeds (TIF) solution?	Please abide by the RFP requirement	Clarification
202		General Query		Please specify the existing playbooks configured in SOAR	will be shared with successful bidder	Clarification
203		General Query		Kindly share a high level network diagram of the current setup of Bank with connectivity to efficiently design the new solution with appropriate log collector placement	will be shared with successful bidder	Clarification

204	21		Bank's expectation is that successful bidder is required to manage the existing SOC for another one year after expiry of existing contract in Jan'27.	It is understood that the bidder will just manage the existing SOC operations and not manage the underlying hardware/licenses/DB/storage of the existing SOC	Bidder is expected to manage existing SOC operations along with underlying infrastructure for additional 3 years	Clarification
205	37	7.5 Services		Clarify Training location?, Training Venue to be provided by Bank?	Will be discussed with successful bidder	Clarification
206	58	7.10 TRAINING TO BANK EMPLOYEES		Total yearly Training Duration=5 days please clarify	Will be discussed with successful bidder	Clarification
207	37			Participant size for Pre & Post Training= 5 Pax? Please confrim	Will be discussed with successful bidder	Clarification
208	48	7.8 NG-S OPERATIONS, FACILITY MANAGEMENT, AMC & ATS	44. The warranty period for the hardware will be three years and for Software / Solution will be for 1 year from the date of Go-live followed by 3 years AMC and 4 years ATS as applicable.	Request Bank to amend the clause as under. 44. The warranty period for the hardware and Software will be 3 years from the date of Go-live followed by 2 years AMC and ATS as applicable.	Please abide by the RFP requirement	No change

209	27	7.2 SETTING UP NG-SOC	30. 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.	Request Bank to remove the clause considering OEM will not hold prices for the entire contract period or Bank may place repeat order for next 6 months from the date of acceptance of purchase order.	Please abide by the RFP requirement	No change
210	174	Annexure 11: Bid Security (Earnest Money Deposit)		Request Bank to confirm whether EMD (Bank Guarantee) need to be submitted as per the Annexure 11: Bid Security Format or Format available on GeM Portal.	EMD to be submitted as per format given in RFP	Clarification
211	60	Delivery, Installation and Maintenance	Delivery, Installation and Maintenance Installation of the solutions is to be performed by OEM / OEM authorised partner for each solution. In case of OEM authorised partner OEM certificate should be presented	For the Underlying Hardware Supporting the NGSOC solution (For ex : Servers , Storage , Back up, Tape library ,OS) - Request Bank to confirm if Bidder Resources can be used for Implementation ?	Please abide by the RFP requirement	Clarification

212	58	7.10 TRAINING TO BANK EMPLOYEES	to Bank mentioned authorisation to the partner	For the Underlying Hardware Supporting the NGSOC Solution (For ex : Servers , Storage , Back up, Tape library ,OS- Is training Required for Bank officialls ?	Will be discussed with successful bidder	Clarification
213	44		The warranty period for the hardware will be three years and for Software / Solution will be for 1 year from the date of Go-live followed by 3 years AMC and 4 years ATS as applicable	Basis the Clause mentioned in the adjoining columns : Request confirmation if the Contract is for 5 years (As Server Warranty and AMC is totalling to 6 years) : (3 Yrs warranty , 3 Years AMC)	Please abide by the RFP requirement	Clarification
214	31		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.	Confirm - Half yearly/yearly health check-up to be done on Underlying Hardware Supporting the NGSOC solution. (Yes/No)	Please abide by the RFP requirement	Clarification
215		General		Please confirm structured cabling to be done with proposed NGSOC Solution within the DC ?	Will be shared with successful bidder	Clarification
216		General		Please share CBI standard backup retention policy details (Daily, Weekly, Monthy, Yearly)	Will be shared with successful bidder	Clarification
217	151-154	General Query		Kindly help us with the number of Primary/Top Level Domains to be monitored (currently in use and forecasted over the contract period)	Will be shared with successful bidder	Clarification
218	151-154	16		Kindly help us with the number of brand associated keywords to be monitored	Will be shared with successful bidder	Clarification

219	151-154	3		Please let us know the number of takedowns required in a year	Unlimited	Clarification
220	151-154	9		Please let us know he number of executives to be monitored	Will be shared with successful bidder	Clarification
221	151-154	General Query		How many analystslicenses are required	For SOAR analyst licenses required are 30 plus 15 view only - kindly ignore 25 as it is typographical error	clarification
222	80	Section – 1 – Experience Criteria	7.The bidder must have minimum 50 IT Security permanent resources with experience in-scope solutions on their payroll with certifications such as CISSP/ CEH/CISM. 50 Resources - 10 Marks Every Additional 20 Resources - 5 Marks subject to maximum of 20 marks	RequestBank to amend the marking score as under. Section – 1 – Experience Criteria 7. The bidder must have minimum 50 IT Security permanent resources with experience in-scope solutions on their payroll with certifications such as CISSP/ CEH/CISM. 50 Resources - 20 Marks	Please abide by the RFP requirement	No change
223		General Query		Request Bank to accept references on the name of affiliate company.	Please abide by the RFP requirement	No change

224	130	3	To virtually segregate different types of data, proposed solution should support unlimited virtual storage groups or indexes. Each index/ virtual storage group should be used for searching specific data and retention period should be configurable as per storage groups or indexes and should not be hardcoded.	"This clause is a proprietary feature, favouring a single OEM. Request bank to delete the clause for wider participation. OR To virtually segregate different types of data, the proposed solution should support multiple configurable virtual storage groups or indexes. Each index or virtual storage group should be used for searching specific data, and the retention period should be configurable per storage group or index and should not be hardcoded."	Please abide by the RFP requirement	No change

225	130	4	The proposed solution must support the data replication natively without relying on other third party replication technologies on the operating system or storage level with near zero RPO and RTO. Solution 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.	The proposed solution must support native data replication without relying on third-party replication technologies at the operating system or storage level, with low RPO and RTO. The solution should allow administrators to configure the replication factor within the data center and separately for disaster recovery. The disaster recovery environment should be active and continuously updated with replicated security event data and logs required to support incident investigation and analysis.	Please abide by the RFP requirement	No change

226	131	6	The proposed solution should be able to receive, ingest and index structured or unstructured data without schema or normalization and no events should be dropped if log source changes the format of log data.	"This clause is a proprietary feature, favouring a single OEM. Request bank to delete the clause for wider participation. OR The proposed solution should be able to receive, ingest and index structured or unstructured data with / without schema or normalization and no events should be dropped if log source changes the format of log data."	Please abide by the RFP requirement	No change

227	131	7	"Machine learning should be embedded across the platform (SIEM, DATA LAKE, SOAR & UEBA). It should empower every user in the SOC with ML. Security analyst to become citizen data scientist i.e. used predefined ML algorithms to detect & predict threats, threat hunters to build their own ML models with steps to build, train and implement model and data scientists should be able to integrate various ML frameworks."	Machine learning should be provided through the UEBA component of the platform. It should empower every user in the SOC with ML. Security analyst to become citizen data scientist i.e. used predefined ML algorithms to detect & predict threats, threat hunters to build their own ML models with steps to build, train and implement model and data scientists should be able to integrate various ML frameworks.	Please abide by the RFP requirement	No change

228	131	8	The solution must ensure that if data ingested is not parsed then with the new parser old data ingested should also be parsed without need to re-ingest data in the SIEM throughout the minimum retention period of online 180 days and 365 days of archival.	This clause is a proprietary feature, favouring a single OEM. Request bank to delete the clause for wider participation. OR The solution must ensure that if data ingested was initially unparsed, it should be reprocessed by replaying the data using updated parsers without requiring reingestion from the original data sources, for data retained online for a minimum of 180 days and archived data retained for 365 days.	Please abide by the RFP requirement	No change

229	134	29	The proposed solution must be able to index all data from any application, server or network device including logs, configurations, messages, traps and alerts, metrics and performance data without any custom adapters for specific formats so that the analyst can have end to end visibility of the ecosystem. Indicative		Please abide by the RFP requirement	No change
230	135	42	The proposed solution must come with pre-packaged alerting capability, flexible service-based hosts grouping, and easy management of many data sources, and provide analytics ability to quickly identify performance and capacity bottlenecks and outliers in Unix and Linux environment. It should quickly compare resources and capacity utilization	This clause is oriented toward infrastructure performance and capacity monitoring rather than security analytics and is out of scope for SIEM, SOAR, and UEBA. Request to remove the Clause or consider this optional as this is more a performance monitoring requirement.	Please abide by the RFP requirement	No change
			across many hosts.			

231	136	45	"The proposed solution must possess built-in feature for anomaly detection: a. Uses historical data as a baseline to forecast future patterns, thresholds and tolerances b. Ability to identify the future needs ofcritical system resources, no prior knowledge in predictive modeling algorithms required to use this functionality, and the ability to easily interpret and customize the results"	This is a NMS solution monitoring activity, which any NOC teams perfoms, suggest the SOC team to concentrate more on secuerity related usecases.	Please abide by the RFP requirement	No change
232	136	46	The proposed solution should give visualization of operational health of the Windows, Linux & Unix environment through a single dashboard customizable to service-groupings in your environment.	This is a NMS solution monitoring activity, which any NOC teams perfoms, suggest the SOC team to concentrate more on secuerity related usecases.	Please abide by the RFP requirement	No change
233	136	47	The proposed solution should give visualization of operational health of the Windows, Linux & Unix environment through a single dashboard customizable to service-groupings in your environment.	Request to elaborate on the usecase	Please abide by the RFP requirement	Clarification

234	137	55	The solution must provide granular license utilization down to devices, log sources and data store or additional lookups of devices to agencies by the minute and the retention of granularity can be extended to the project requirement.	Kindly clarify the requirement / use case.	Please abide by the RFP requirement	Clarification

235	137	59	The solution's reports should run fast on large data sets. Proposed solution should use next generation functionalities like creating set of data from the main index or data store. This will avoid running the queries on large index or full index and faster response for searching and reporting.	The solution's reports should execute efficiently on large data sets. The proposed solution should leverage next-generation capabilities such as indexed searches, aggregations, and optimized query mechanisms to avoid running queries across the full data store, thereby enabling faster search and reporting performance.	Please abide by the RFP requirement	No change
236	138	63	Old data should be parsed with new parser without re-consumption or re-indexing the data. Any additional license or storage should not be consumed because of parsing through new parser.	If data was initially ingested without full parsing, the solution should support reprocessing of historical data by replaying preserved raw events through the ingestion pipeline using updated parsers.	Please abide by the RFP requirement	No change
237	138	67	The proposed solution must be able to assign any arbitrary risk score based on self-defined query based on any correlated events, statistical analysis, threat indicator match, importance to the business.	The proposed solution must be able to assign and adjust risk or priority scores based on correlated security events, threat indicator matches, statistical analysis, and business context such as asset criticality, using system-defined scoring logic.	Please abide by the RFP requirement	No change

238	140	76	The proposed solutionshould find relationship between pairs of fields (in event or desired metadata) by change in randomness in pair of fields.	The proposed solution should be able to identify relationships between pairs of event fields or associated metadata by detecting statistically significant deviations or anomalous changes in their historical behavior patterns.	Please abide by the RFP requirement	No change

239	140	77	The proposed solution's detection use cases should be comprised of guidance that provides an assessment of the Security Threat and how it helps detect and investigate it using the proposed solution. In addition, it should provide a summary of how the attack or detection technique maps to the following: ATT & CK MITRE, an adversary behavior model that describes the actions an adversary might take. Kill-Chain, a model that identifies the phases an adversary must complete to achieve their objective. CIS Critical Security Controls Data types that are referenced within the rules/ search and that need to be populated. Technologies, example technologies that map to the data types. There should be template to upload advisories in an automated manner. There should be templates to design and trigger work flows automatically. Any other customizable templates as per bank requirements.	The proposed solution's detection use cases should include descriptive information that explains the purpose of the detection and how it supports security monitoring and investigation. The detection content should provide mappings to relevant frameworks including MITRE ATT&CK techniques, adversary behavior models, and Kill Chain phases. The solution should identify the data types referenced within detection rules or searches and the technologies that typically generate those data types. Where applicable, the solution should support alignment with industry security control frameworks such as CIS Critical Security Controls. The solution should support ingestion of structured threat intelligence content and indicators through supported interfaces and provide templates to design and trigger automated workflows. Additional templates should be customizable to meet bank-specific requirements.	Please abide by the RFP requirement	No change

240	140	78	The proposed solution should also guide administrator on data sources required to implement detection technique from the same console (ATTACK MITRE, CIS, NIST, Kill Chain etc.)	The proposed solution should guide administrators on the data sources required to implement detection techniques, with references to relevant security frameworks such as MITRE ATT&CK, CIS, NIST, and the Kill Chain, through vendor-provided detection content and associated documentation available via supported web-based resources.	Please abide by the RFP requirement	No change
241	141	85	The proposed solution should ensure realtime replication of analyst comments and all other incident updates from the primary data center (DC) to the disaster recovery (DR) site.	The proposed solution should ensure continuous replication of security event from the primary data center (DC) to the disaster recovery (DR) site to enable uninterrupted security monitoring, investigation, and analysis in the event of a failover. The DR site should have access to the replicated security data required to resume investigations based on historical and incoming events.	Please abide by the RFP requirement	No change
242	142	2	The proposed solution orchestrator must be able to ingest security data from any source and in any format. Example: Email based alerts SIEM Based alerts	The proposed solution orchestrator must be able to ingest security data from a wide range of sources and support multiple commonly used formats. Examples include emailbased alerts and SIEM-based alerts.	Please abide by the RFP requirement	No change

243	144	29	The proposed solution should have an out of the box guidance by offering suggestions to help investigate, contain, eradicate, and recover from a security event, allowing newer analyst to take and validate choices of more experienced analysts.	The proposed solution should provide pre-built playbooks, templates, and guided workflows to assist analysts in investigating, containing, eradicating, and recovering from security events, enabling newer analysts to follow and validate actions based on established best practices.	Please abide by the RFP requirement	No change
244	145	5	Investigate and respond to detected threats using a streamlined threat review workflow that provides visibility into anomalous activity and supporting evidence. Should increases the effectiveness of our security analysts by helping them focus on threats and malicious activities with kill chain and geographical visualizations.	Investigate detected threats using a streamlined threat review workflow that provides visibility into anomalous activity and supporting evidence. It should increase the effectiveness of security analysts by helping them focus on threats and malicious activities with kill chain and geographical visualizations.	Please abide by the RFP requirement	No change
245	135	68:Annexure 2: Point No 39	The proposed solution must be able to support mathematics functions to perform calculations on field values, examples Converting bytes to kilobytes, mega-bytes, absolute value functions, highest integers, standard deviation, command length etc.; Finding the time duration between time stamp values. These functionalities should be available as a search, report, alert or dashboard etc. so that analyst can build any kind of report required	Can you please explain the rational behind the need for the mathematical function.	Please abide by the RFP requirement	No change

246	136	68:Annexure 2: Point No 47	The proposed solution should have the capability to collaborate and orchestrate with 3rd party solutions and the solution should be able to be embedded in third-party business applications such as SharePoint, WordPress, Wiki, etc.	Can you please clarify on SIEM to be embedded inside 3rd party applications or 3rd party applications inside SIEM. And, where should be orchestration shown.	Please abide by the RFP requirement	No change
247	144	SOAR Requirements , Point No 24	The proposed solution must be able to extract and store attachments from ingested emails	Please elaboratethis use case in detail	Please abide by the RFP requirement	No change
248	150	TIF Point 26	Threat Intelligence Vendor should be serving more than 1000 Customers globally for threat intelligence solution	We would like to bring to your attention that the clause requiring the Threat Intelligence Vendor to serve more than 1000 customers globally is restrictive for Indian Local OEMs. As per DPIIT's Public Procurement (Preference to Make in India) Order (PPP-MII), such conditions limit participation of domestic OEMs, which goes against the intent of promoting indigenous solutions under the Make in India initiative. We kindly request you to remove this clause for Make in India companies.	Please abide by the RFP requirement	No change

249	81	Experience Criteria Section 1 Claue 13	"The Bidder should have implemented or managed SOC with on-premises SIEM solution with minimum 1,00,000 Events Per Second (EPS) or 3.4TB / Day in at least one SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/NS E/SEBI in India during last 5 years. *(SCB – with minimum 1000 Branches in India)"	We would like to highlight that the clause is highly restrictive for Indian Local OEMs. As per DPIIT's PPP-MII Order (No. P45021/2/2017-B.E.-II dated 15.06.2017 and revisions) and F.1/15/2018-PPD Procurement Policy/O.M 24/04/2018 from Ministry of Finance procurement should encourage 'Make in India'. However the RFP's clause limits participation of domestic solution providers and go against the intent of promoting indigenous solutions under the Make in India initiative. We kindly request you to remove this clause to ensure compliance with the PPP-MII Order and allow fair opportunity for Make in India companies. We request to remove the clause for Make In India companies allowing all deployment models, provided the Overall capability of the offered SIEM meets the specified performance criteria of (≥100,000 EPS or 3.4 TB/day) overall	Please abide by the RFP requirement	No change

250	21	22.6 End of Sales / End of support	The Bidder has to ensure that any solution/equipment supplied as part of this RFP should not have either reached or announced 'End of Sales' (1 years from last date of submission of Bid.) or end of support for at least 5 years from the date of issue of purchase order. In the event if any equipment supplied by the bidder reaches end of support, within the 5 years period from the date of supply, the bidder has to replace the equipment with devices having equivalent or upgraded specification, at no additional cost to the Bank or revamp the entire solution (if required).	There is contradiction in the end of support date. please confirm whether the period of 5 year will be calculated from the date of pO or the date of suppy	Please abide by the RFP requirement	Clarification
251	22	23	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.	Request bank to allow the provisioning of remote support subjected to bank's approvals	Please abide by the RFP requirement	Clarification
252	22	26	Depending on the requirement, Bank reserves the right to extend the contract with the successful bidder including Subscription, AMC, ATS and Onsite FM Services of the supplied Platform and Solution for 2 more years i.e. 6th and 7th year on the same terms and conditions wherein enhancements/cost escalation quoted for 4th and 5th year would be taken	Since the end customer prices are heavily dependedt on USD rate, we request bank to make an exception and allow mutual price discussion in case USD rates are increased by more than10% during the course of the RFP from the date of award of the contract.	Please abide by the RFP requirement	No change

			as the price reference for the extension of the contract			
253	20	16	Ensure graceful transition from existing CSOC of the Bank to new NG-SOC along with migration activities.	Please share details of existing SIEM solution OEM. Count of use cases, playbooks, technologies integrated.	Will be shared with successful bidder	Clarification
254	20	14	Provide immediate forensic support in case of any security / cyber incident.	Please specify if any specific number of hours are to be considered for forensics.	Please abide by the RFP requirement	Clarification
255	28	7.3	The bidder shall co-ordinate with existing vendor for extraction of data/logs from the available data/logs at existing SIEM/SOC as and when required by investigating agency, regulators etc.	This will only be possible for the duration until which the licnese of the SIEM is activated. Please confirm on the licence renewal period.	Please abide by the RFP requirement	Clarification

256	28	7.3	Once all the log sources integrated with existing SOC are migrated to NG-SOC, ensure the existing SOC is up & running in steady state. Ensure that the reports are extracted from online / warehouse storage etc. Restore the logs from backup, if required to extract old logs for forensic investigation, as & when required.	This activity can only be done until the license validity of the existing solution. Please confirm on the license renewal period	Please abide by the RFP requirement	Clarification
257	30	7.4 SCOPE OF WORK FOR PROPOSED SOLUTIONS	The Bidder has to document RCA for applicable incidents e.g. Critical, High priorities incidents ensuring accurate and detailed records are maintained.	RCA is ideally done only for P1/S1 level of incidents. Please confirm	Please abide by the RFP requirement	Clarification

258	30	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		The centralised dashboard will be the dashboard of the proposed SIEM itself. Please confirm.	It is expected tl the requir features should present in t NGSOC solutions	Clarification
259	34	II. Security Orchestration, Automation & Response (SOAR)	Bidder to has to maintain separate UAT environment instance of SOAR.	The proposed solution has inbuilt SOAR and hence mainataing a separate instance is not technically feasible. Please confirm	Please abide by the RFP requirement	Clarification

260	26	25. 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. Data retention period will be the entire contract period. As per the regulatory guidelines all relevant data has to be stored for minimum 10 years. 6 Months data should be available online and should be stored in highest speed of storage. Another 12 months data should be in warm node that can be accessible through the application. Beyond that till contract period, Data should be in Archival node.	6 months online data can be on any type of disk. The objective should be to query online data and get the result. Type of disk will not matter here. Hence, request to remove the "highest speed of storage" and keep it as "6 months online & 12 months offline which can be accessible throught the application"	Please abide by the RFP requirement	Clarification

261	26	25. 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. Data retention period will be the entire contract period. As per the regulatory guidelines all relevant data has to be stored for minimum 10 years. 6 Months data should be available online and should be stored in highest speed of storage. Another 12 months data should be in warm node that can be accessible through the application. Beyond that till contract period, Data should be in Archival node.	Who will provide the Archival storage post 18 months? If bidder has to provide, please confirm it has to be for 3.5 years as the entire contract period is 5 years only.	Please abide by the RFP requirement	Clarification

262	68	Audit/ VAPT of NGSOC solutions		Understanding is that CBoI will be conducting the audits and sharing the report with Bidder for closure. Please confirm.	Please abide by the RFP requirement	Clarification
263	27		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	Request bank to limit additional order to maximum of 25% of the original BOQ	Please abide by the RFP requirement	No change

264			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.	SIEM solution is always designed for Peak. However, with continuous peaks, the hardware utlisation may spike up. Hence require the clause to modified to be "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 6 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.	Please abide by the FP requirement	No Change
265	61		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:	The current timeline are too short considering the size of deployment. we request bank to increase the time lines to 52 weeks from the date of PO	Please abide by the RFP requirement	No change

266	70		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,	Requestbank to add the below clause: Liquidated damages shall be levied only on account of reasons attributable to bidder	Please abide by the RFP requirement	No change
267	24		The proposed solution must be selfcontained solution to provide the ease of adding functionalities such as UEBA, Threat hunting, Automation & Orchestration etc. Solution should use centralized Data Lake instead of traditional DB approach to avoid performance degradation during threat hunting	a)When you mention avoiding a "traditional database," are you specifically excluding any solutions with relational databases? b)Do you expect the SOC platform to be Kubernetes-native with microservices that can scale independently, or is containerized deployment on virtual machines acceptable?	Please abide by the RFP requirement	Clarification

268	78		The Bidder should have implemented or managed SOC with on-premises SIEM solution with minimum 1,00,000 Events Per Second (EPS) or 3.4TB / Day in at least one SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/NSE/SEBI in India during last 5 years. *(SCB – with minimum 1000 Branches in India): 1 implementation or managed : 60 marks, further additional implementation or managed : 20 marks each	Request bank to incorporate the below changes in the criterias to ensure wider participation: The Bidder should have implemented or managed SOC with on-premises SIEM solution with minimum 1,00,000 Events Per Second (EPS) or 3.4TB / Day in at least one SCHEDULED COMMERCIAL BANK (SCB)*/ RBI/ NPCI/ BSE/ NSE/ SEBI/ IFTAS/ Central Govt./State Govt./Enterprise in India during last 5 years. *(SCB – with minimum 1000 Branches in India):	Please abide by the RFP requirement	No change

				1 implementation or managed : 60 marks, further additional implementation or managed : 40 marks each		

269	79		The Bidder should have implemented or managed any on-premises SOAR solution in at least one SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/NSE/SEBI in India during last 5 years. *(SCB – with minimum 1000 Branches in India) 1 implementation : 35 marks, additional implementations : 15 marks each	Request bank to incorporate the below changes in the criterias: The Bidder should have implemented or managed any onpremises SOAR solution in at least one SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/NSE/SEBI/IFTAS/Central Govt./State Govt./Enterprise in India during last 5 years. *(SCB – with minimum 1000 Branches in India) 1 implementation : 35 marks, additional implementations : 15 marks each	Please abide by the RFP requirement	No change

270			The Bidder should have implemented or managed any on-premises UEBA solution with minimum 20,000 users in at least one SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/NSE/SEBI in India during last 5 years. *(SCB – with minimum 1000 Branches in India) 1 implementation : 25 marks, additional implementations : 15 marks each	Request bank to incorporate below changes in the evaluation criterias: The Bidder should have implemented or managed any onpremises UEBA solution with minimum 20,000 users/Unilimited user in at least one SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/NSE/SEBI/IFTAS/Central govt./State govt/Enterprise in India during last 5 years. *(SCB – with minimum 1000 Branches in India) 1 implementation : 25 marks, additional implementations : 15 marks each	Please abide by the FP requirement	No change
271	32		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 this do you need WORM/immutable storage with retention lock for archived logs ?	Please abide by the RFP requirement	Clarification
272	102		If the proposed solution has data replication functionalities, the same has to be achieved without relying on other thirdparty replication technologies on the operating system or storage level.	Data Replication consists of rules,alerts, use cases, reports etc. Logs are not considered here as they require storage based replication. Kindly confirm.	Please abide by the RFP requirement	No Change

273	32		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	For archival retrieval, are standard protocols such as NFS, SMB acceptable ?	Please abide by the RFP requirement	Clarification
274	60		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	Can we get basic details of existing DCs like Tier , IT Load max KVA capacity per rack , Cabling Overlay , Underlay , Floor Loading capacity. This will be helpful in providing power, space requirement inline with existing DC facility.	Details will be shared with successful bidder	Clarification
275	36	V. Brand Protection Services including Dark Web Monitoring		Please share the number of domains and brands to be considered for brand monitoring.	Will be shared with successful bidder	Clarification

276	80		The Bidder should have integrated TIF solution with any on-premise SOC in at least one SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/NSE/SEBI in India during last 5 years. *(SCB – with minimum 1000 Branches in India): 1 implementation : 20 marks, additional implementations : 10 marks each	Request Bank to modify the clause as per below: The Bidder should have integrated TIF solution with any on-premise SOC in at least one SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/NSE/SEBI/Central Govt/State Govt/Enterprises in India during last 5 years. *(SCB – with minimum 1000 Branches in India): 1 implementation : 20 marks, additional implementations : 10 marks each	Please abide by the RFP requirement	No change

277	80		The Bidder should have provided services of Brand Protection in at least one SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/NSE/SEBI in India during last 5 years. *(SCB – with minimum 1000 Branches in India)	Request to modify the clause as per below: The Bidder should have provided services of Brand Protection in at least one SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/NSE/SEBI/Central Govt./State Govt/ Enterprise in India during last 5 years. *(SCB – with minimum 1000 Branches in India)	Please abide by the RFP requirement	No change
278	90	AMC/ATS PAYMENT TERMS	AMC/ATS amount payable would be paid quarterly in arrears at the end of each quarter	Request you to please make the AMC/ATS payments on Annual in advance on submission of the PBG of equal amount	Please abide by the RFP requirement	No change

279			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	Request to modify the clause as per below: Biddershall provide the maintenance (Warranty, AMC & ATS) for a period of five years from the date of GO-Live of the each product in the Bank	Please abide by the RFP requirement	No change

280	137		The proposed solution should support historical correlation and to search for matching historical data using new correlation rule.	Please specify period of hisotorical data for correlation so users can rerun past events and flows on historical data, so new rules can be tested more precisely	Please abide by the RFP requirement	Clarification
281	48	MANPOWER & REQUIREMENT DESIRED SKILLSET		Please specify no of minimum L1, L2 & L3 resources required per day during weekdays, weekends & Public holidays instead of mentioning minimum resource requirement per shift. Let Bidder decide the placement of resources to fulfil SOW and cross skilling of resources should be allowed.	L1, L2 and L3 engineers must work on 24x7x365 basis. Project Director must be present on working days. However, project director must be able available onsite in case of need on nonworking days and should be available on phone all the time.	Clarification

282	48	MANPOWER REQUIREMENT & DESIRED SKILLSET		Please specify no of minimum L1, L2 & L3 resources requirement at DC & DR.	Will be discussed with Successful bidder	Clarification

283	152,Pt 8	68. ANNEXURE 2: MINIMUM TECHNICAL SPECIFICATIONS	Platform should provide : Website Watermarking Website Defacement monitoring	Please explain what is required in Website Defacement Monitoring	Please abide by the RFP requirement	Clarification
284	154 Pt 16	68. ANNEXURE 2: MINIMUM TECHNICAL SPECIFICATIONS	Stolen / Compromised Login Credentials and Customer Account Information. - Exposure in 3rd Party Breaches	Our Recommendation:The platform must validate credentials associated with official emails or sensitive subdomains/URLs by performing successful login tests and delivering screenshots as evidence for verification.	Please abide by the RFP requirement	No change
285	131	SIEM Requirement Specifications (Mandatory Specifications)	The solution must ensure that if data ingested is not parsed then with the new parser old data ingested should also be parsed without need to re-ingest data in the SIEM throughout the minimum retention period of online 180 days and 365 days of archival.	(The Search based approach adds more hardware footprint and takes time for detection. While real time co-relation will mitigate the risk of delays in detection capability.Most leading vendors licensing is flat model and doesn't charge extra for peak eps consumptions and doesn't charge based on search and for some vendors licensing is based on search / ingestion hence such clauses included.) Clause To be modified SIEM Clause 8- The solution must ensure that if data ingested is not parsed then the old data should be	Please abide by the RFP requirement	No change

				parsed with new parser, without need to re-ingest data, from outside of SIEM Platform & Archival storage and should not be manual process, throughout the data retention period of online 180 days and 365 days of archival		

286	138	SIEM Requirement Specifications (General Specifications) Fields, Schema and Log Parsing	The solution must support viewing data in different formats or schemas without reconsumption, re-indexing, redundant storage. Historical data also should be viewed as per new format or schema without re-consumption or without additional storage utilization.	(The Search based approach adds more hardware footprint and takes time for detection. While real time co-relation will mitigate the risk of delays in detection capability.Most leading vendors licensing is flat model and doesn't charge extra for peak eps consumptions and doesn't charge based on search. for some vendors licensing is based on search / ingestion hence such clauses included.) Clause TO BE MODIFIED :The solution must support viewing data in different formats or schemas without re-consumption, ~~reindexing~~, redundant storage.	Please abide by the RFP requirement	No change

				Historical data also should be viewed as per new format or schema without re-consumption or without additional storage utilization.		
287	138	SIEM Requirement Specifications (General Specifications) Fields, Schema and Log Parsing	Old data should be parsed with new parser without re-consumption or re-indexing the data. Any additional license or storage should not be consumed because of parsing through new parser.	Clause To be modified. Old data should be parsed with new parser without re consumption ~~or re-indexing~~ of addl license or storage	Please abide by the RFP requirement	No change
288	74	19 - INTEGRITY PACT		Request deletion of the Fall clause since the scope of work, contract term and terms &conditions varies from customer to customer	Please abide by the RFP requirement	No Change

289	93	24 - Order Cancellation		We request the Bank to: 1) Provide a cure period so that Bidder can fix any issues. 2) Use Liquidated Damages as the sole remedy for any performance related issue.	Please abide by the RFP requirement	No Change
290	105	39 - Intellectu Property Rights		Request deletion of this clause as its not applicable.	Please abide by the RFP requirement	No Change
291	107	41 - Termination		Bidder proposes the following to be added: (a) Bidder shall have the right to suspend the services if there are any default in payment by Bank. (b) In the event of such termination of this RFP/Agreement by Bank for its convenience, Bank shall pay early termination charges as determined by the Bidder.	Please abide by the RFP requirement	No Change
292	112	47 - of Violation Terms		We propose that the Liability should be capped to 12months amount paid to Bidder under the relevant PO giving rise to the liability.	Please abide by the RFP requirement	No Change

293	94	26 - Indemnity		Bidder should not be liable for any "indirect" claims, kindly remove such claims from Indemnity	Please abide by the RFP requirement	Clarification

294	95	26 - Indemnity		Request to delete clause ‘26". We are already providing LDs, claiming Indemnity is penalizing us twice for the same default. We suggest that clause for indemnity be kept mutual. We further suggest Indemnity clause to be framed as under that either party to indemnify each other for the following: 1. For third party IPR infringement claims Provided that the indemnification obligations shall be subject to following :- a) Immediate notice to be sent bythe Indemnified party. b) Control of the defence of theclaim by the indemnifying party. c) Assistance by the indemnifiedparty in the defence at the expense of the indemnifying party. In no event shall either party be liable to the other for any indirect, incidental, special, consequential, exemplary or punitive damages including, but not limited to, damages for lost revenue, lost profits, loss of goodwill, loss of data, technology, equipment or types of damages	Please abide by the RFP requirement	No Change

				whatsoever, whether or not caused by any acts of omission or commission and regardless whether such party has		

				been informed of the possibility or the likelihood of such damages. Maximum liability of either party be limited to annual contract value. However, liability under indemnity should be capped.		

295		26	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.	We request the Bank to exclude any liability towards Financial Loss as this is a service Agreement.	Please abide by the RFP requirement	No Change
296		26 - (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.	Bank to confirm if there would be any advance payment, if not then there should be no refund applicable. Hence we request to delete this provision.	Please abide by the RFP requirement	No Change

297	101	34 - SUCCESSFUL BIDDER'S LIABILITY	The Bidders 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 Bidders liability in case of claims against the Bank resulting from wilful misconduct or gross negligence of the 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 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. Subject to any law to contrary, and to the maximum extent permitted by law neither party shall be liable to other for any remote and indirect loss or damages arising out of this tender and subsequent agreement or services provided." This limitation shall not apply to third-party claims arising from: Intellectual Property (IP) Infringement Indemnity: The Bidder's liability for any claim or damages arising from infringement or alleged infringement of third-party intellectual property rights shall not be subject to the above limitation.	We request the Bank to make this clasue mutual. Further, we request to include the below: In no event shall either party be liable to the other for any indirect, incidental, special, consequential, exemplary or punitive damages including, but not limited to, damages for lost revenue, lost profits, loss of goodwill, loss of data, technology, equipment or types of damages whatsoever, whether or not caused by any acts of omission or commission and regardless whether such party has been informed of the possibility or the likelihood of such damages. Maximum liability of either party be limited to 12months amount paid to Bidder under the relevant PO giving rise to the liability.	Please abide by the RFP requirement	No Change

			Bodily Injury, Death, and Property Damage: The Bidder shall be fully liable for any bodily			

			injury (including death) or damage to real property or tangible property caused by the Bidder's negligence, fraud, or misrepresentation, or that of its employees, representatives, or subcontractors.			

298	104	38 - 38. LIMITATION OF LIABILITY	Bidder's aggregate liability under the contract shall be limited to a maximum of the contract value. For the purpose of this section, the contract value at any given point of time means the aggregate value of the purchase orders placed by the Bank on the Bidder that gave rise to the claim, under this Request for Proposal (RFP). This limitation shall not apply to third-party claims arising from: Intellectual Property (IP) Infringement Indemnity: The Bidder's liability for any claim or damages arising from infringement or alleged infringement of thirdparty intellectual property rights shall not be subject to the above limitation. Bodily Injury, Death, and Property Damage: The Bidder shall be fully liable for any bodily injury (including death) or damage to real property or tangible property caused by the Bidder's negligence, fraud, or misrepresentation, or that of its employees, representatives, or subcontractors. Indirect, Consequential, Incidental, or Special Damages: Notwithstanding the above, the SP shall be liable for any indirect, consequential, incidental, or special damages arising under this agreement or purchase order. These types of damages may include, but are not limited to, lost profits, loss of business opportunities, loss of use, or other similar damages, even if the Bidder has been advised of the possibility of such damages. Liability for Subcontractor Practices: The Service Provider shall be contractually liable for the performance of its subcontractors	There are 2 Limitation of liability clauses, this one and Bidder's liability (mentioned above). Which section will prevail? We request the Bank to make this clasue mutual. Further, we request toreplace the current clause with the below the below: In no event shall either party be liable to the other for any indirect, incidental, special, consequential, exemplary or punitive damages including, but not limited to, damages for lost revenue, lost profits, loss of goodwill, loss of data, technology, equipment or types of damages whatsoever, whether or not caused by any acts of omission or commission and regardless whether such party has been informed of the possibility or the likelihood of such damages. Maximum liability of either party be limited to 12months amount paid to Bidder under the relevant PO giving rise to the liability.	Due to typo error the clause is repeated and hence kindly ignore the clause	Clarification

			and must ensure that its subcontractors adhere to the same level of risk management practices as required by the Bank.			

			This includes ensuring that subcontractors meet the agreed-upon standards of performance, compliance, and quality.			

299	70	15. LIQUIDATED DAMAGE :	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.	We kindly request Bank to modify as per below to restrict LD max Cap of 5% . 15. LIQUIDATED DAMAGE : 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 5% 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.	Please abide by the RFP requirement	No Change

300	87	23. PAYMENT TERMS :	Payment Terms Hardware: 40% on delivery 50% on installation & acceptance 10% after 3 months of successful operation Software Licenses: 30% on delivery 50% on implementation & acceptance 10% after migration & DR drill 10% after 3 months post go-live Implementation & Migration: 70% on completion 10% after fine-tuning & go-live 20% after 3 months of stable operations AMC/ATS: Paid quarterly in arrears post warranty. Subscription: Yearly in advance from 2nd year; 1st year after go-live. FMS Charges: Quarterly in arrears based on actual deployed resources.	We kindly request bank to modify payment terms as per below 23. PAYMENT TERMS : Payment Terms Hardware: 70% on delivery 20% on installation & acceptance 10% after 3 months of successful operation Software Licenses: 70% on delivery 20% on implementation & acceptance 5% after migration & DR drill 5% after 3 months post go-live Implementation & Migration: 70% on completion 10% after fine-tuning & go-live 20% after 3 months of stable operations AMC/ATS: Paid Yealy in advance post warranty. Subscription: Yearly in advance from 2nd year; 1st year after golive. FMS Charges: Quarterly in Advance based on actual deployed resources.	Please abide by the RFP requirement	No change

301	63	12.1 SERVICE LEVEL AGREEMENTS (SLA)	The overall SLA penalty cap is 10% of the total contract value.	We request Bank to modify the overall SLA penalty cap is 5% of the total contract value.	Please abide by the RFP requirement	No change

302	13	Eligibility Criteria (11)	The Bidder should have implemented or managed on- premise SIEM solution and currently in use with minimum 1,00,000 Events Per Second (EPS) or 3.4TB / Day in at least ONE Scheduled Commercial Bank (SCB)*/RBI/NPCI/BSE/NSE/ SEBI in India during last 5 years.	The clause, in its current form, is restrictive in nature. Relaxation of the experience criteria will enable participation of other technically competent bidders, thereby fostering healthy competition. This, in turn, is expected to result in more competitive commercial bids and better value for the organization. Further, permitting experience in similar or equivalent technologies across other sectors will ensure that bidders possessing the requisite technical capabilities are not excluded solely due to differences in sectoral exposure, terminology, or nomenclature. The Bidder should have implemented or managed on-premise SIEM solution and currently in use with minimum 1,00,000 Events Per Second (EPS) or 3.4TB / Day in at least ONE Scheduled Commercial Bank (SCB)* /RBI /NPCI /BSE /NSE /SEBI or Telecom/PSU's/Govt of India	Please abide by the RFP requirement	No change

				having similar nature with the scope of work in India during last 7 years.		

303	13	Eligibility Criteria (12)	The Bidder should have implemented or managed on- premise SOAR solution in at least ONE Scheduled Commercial Bank (SCB)*/RBI/NPCI/BSE/NSE/SEBI/ in India during last 5 years	The clause, in its current form, is restrictive in nature. Relaxation of the experience criteria will enable participation of other technically competent bidders, thereby fostering healthy competition. This, in turn, is expected to result in more competitive commercial bids and better value for the organization. Further, permitting experience in similar or equivalent technologies across other sectors will ensure that bidders possessing the requisite technical capabilities are not excluded solely due to differences in sectoral exposure, terminology, or nomenclature. The Bidder should have implemented or managed on-premise SOAR solution in at least ONE Scheduled Commercial Bank (SCB)* /RBI /NPCI /BSE /NSE /SEBI or Telecom/PSU's/Govt of India having similar nature with the scope of work in India during last 7 years.	Please abide by the RFP requirement	No change

304	13	Eligibility Criteria (13)	The Bidder should have implemented or managed on-premise UEBA solution in at least ONE Scheduled Commercial Bank (SCB)*/RBI/NPCI/BSE/NSE/SEBI/ in India during last 5 years	The clause, in its current form, is restrictive in nature. Relaxation of the experience criteria will enable participation of other technically competent bidders, thereby fostering healthy competition. This, in turn, is expected to result in more competitive commercial bids and better value for the organization. Further, permitting experience in similar or equivalent technologies across other sectors will ensure that bidders possessing the requisite technical capabilities are not excluded solely due to differences in sectoral exposure, terminology, or nomenclature. The Bidder should have implemented or managed on-premise UEBA solution in at least ONE Scheduled Commercial Bank (SCB)* /RBI /NPCI /BSE /NSE /SEBI or Telecom/PSU's/Govt of India having similar nature with the scope of work in India during last 7 years.	Please abide by the RFP requirement	No change

305	13	Section 2 Eligibility Criteria, Point No. 11	The Bidder should have premise implemented or managed on SIEM solution and currently in use with minimum 1,00,000 Events Per Second (EPS) or 3.4TB / Day in at least ONE Scheduled Commercial Bank (SCB)*/RBI/NPCI/BSE/NSE/ SEBI in India during last 5 years *(SCB – with minimum 1000 Branches in India)	Request you to please reduce the criteria for minimum number of EPS from 100000 to 70000	Please abide by the RFP requirement	No change
306	78	Section – 1 – Experience Criteria Point 1 to 6		Request you to please reduce the criteria for number of branches from 1000 to 500	Please abide by the RFP requirement	No change
307	185	Section – 83 – ANNEXURE 17: ELIGIBILITY CRITERIA COMPLIANCE Point 11 to 13		Request you to please reduce the criteria for number of branches from 1000 to 500	Please abide by the RFP requirement	No change

308	Page 185	Point 11, 83. ANNEXURE 17: ELIGIBILITY CRITERIA COMPLIANCE		Request to Modify the clause as : The Bidder / wholly owned subsidiary company should have implemented or managed onpremise SIEM solution and currently in use with minimum 1,00,000 Events Per Second (EPS) or 3.4TB / Day in at least ONE Govt./ PSU Scheduled Commercial Bank (SCB)*/RBI/NPCI/BSE/NSE/ SEBI in India during last 5 years *(SCB – with minimum 1000 Branches in India)	Please abide by the RFP requirement	No change
309	Page 185	Point 12, 83. ANNEXURE 17: ELIGIBILITY CRITERIA COMPLIANCE		Request to Modify the clause as : The Bidder / wholly owned subsidiary company should have implemented or managed onpremise SOAR solution in at least ONE Govt./ PSU Scheduled Commercial Bank (SCB)*/RBI/NPCI/BSE/NSE/ SEBI in India during last 5 years *(SCB – with minimum 1000 Branches in India)	Please abide by the RFP requirement	No change

310	Page 185	Point 13, 83. ANNEXURE 17: ELIGIBILITY CRITERIA COMPLIANCE		Request to Modify the clause as : The Bidder / wholly owned subsidiary company should have implemented or managed onpremise UEBA solution in at least ONE Govt./ PSU Scheduled Commercial Bank (SCB)*/RBI/NPCI/BSE/NSE/ SEBI in India during last 5 years	Please abide by the RFP requirement	No change
				*(SCB – with minimum 1000 Branches in India)		
311	Page 186	Point 14, 83. ANNEXURE 17: ELIGIBILITY CRITERIA COMPLIANCE		Kindly consider HR Undertaking only instead of certifications.	Please abide by the RFP requirement	No change

312	Page 78	Point 1, Section – 1 – Experience Criteria		Request to modify the clause as: The Bidder/ bidder's wholly owned subsidiary should have implemented or managed SOC with on-premises SIEM solution during last 5 years. Atleast one implementation should be with minimum 1,00,000 Events Per Second (EPS) or 3.4TB / Day in at least one Govt./ PSU/ SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/NSE/SEBI in India during last 5 years. *(SCB – with minimum 1000 Branches in India)	Please abide by the RFP requirement	No change

313	Page 78	Point 2, Section – 1 – Experience Criteria		Request to modify the clause as: The Bidder/ bidder's wholly owned subsidiary should have implemented or managed SOC with any on-premises SIEM solution with minimum 1,00,000 Events Per Second (EPS) or 3.4TB / Day in at least one Govt./ PSU/ SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/NSE/SEBI in India during last 5 years. *(SCB – with minimum 1000 Branches in India)	Please abide by the RFP requirement	No change
314	Page 79	Point 3, Section – 1 – Experience Criteria		Request to modify the clause as: The Bidder/ bidder's wholly owned subsidiary should have implemented or managed any onpremises SOAR solution in at least one Govt./ PSU/ SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/NSE/SEBI in India during last 5 years. *(SCB – with minimum 1000 Branches in India)	Please abide by the RFP requirement	No change

315	Page 79	Point 4, Section – 1 – Experience Criteria		Request to modify the clause as: The Bidder/ bidder'swholly owned subsidiary should have implemented or managed any onpremises UEBA solutionwith in at least one Govt./PSU/ SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/NS E/SEBI in India during last 5 years. *(SCB – with minimum 1000 Branches in India)	Please abide by the RFP requirement	No change
316	Page 80	Point 5, Section – 1 – Experience Criteria		Request to modify the clause as: The Bidder/ bidder's wholly owned subsidiary should have integrated TIF solution with any on-premise SOC in at least one Govt./PSU/ SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/NS E/SEBI in India during last 5 years. *(SCB – with minimum 1000 Branches in India)	Please abide by the RFP requirement	No change

317	Page 80	Point 6, Section – 1 – Experience Criteria		Request to modify the clause as: The Bidder/ bidder's wholly owned subsidiary should have provided services of Brand Protection in at least one Govt./PSU/ SCHEDULED COMMERCIAL BANK (SCB)*/RBI/NPCI/BSE/NSE/SEBI in India during last 5 years. *(SCB – with minimum 1000 Branches in India)	Please abide by the RFP requirement	No change
318	Page 80	Point 6, Section – 1 – Experience Criteria		It will not be possible to provide Certificates of so many employees. Hence request to consider HR declaration with details of Employees and certifications.	Please abide by the RFP requirement	No change

Corrigendum 2 - 09/02/2026

Amendments

Sr No	Original RFP Page #	RFP Clause No.	RFP Clause	Amended Clause
1	131	SIEM Requirement Specifications (Mandatory Specifications) Sr no. 8	The solution must ensure that if data ingested is not parsed then with the new parser old data ingested should also be parsed without need to re-ingest data in the SIEM throughout the minimum retention period of online 180 days and 365 days of archival.	The solution must ensure that if data ingested is not parsed then the old data should be parsed with new parser, **without need to re-ingest data, from outside of SIEM Platform & Archival storage and should not be manual process, throughout the data retention period of** online 180 days and 365 days of archival
2	26	25. Data Retentions Requirements:	6 Months data should be available online and should be stored in highest speed of storage. Another 12 months data should be in **warm** node that can be accessible through the application. Beyond that till contract period, Data should be in Archival node	6 Months data should be available online and should be stored in highest speed of storage. Another 12 months data should be in **warm or offline** node that can be accessible through the application. Beyond that till contract period, Data should be in Archival node
3	145	UEBA Requirement Specifications (Mandatory Specifications) Sr no. 2	The UEBA must create a **heuristic** baseline of user activity by analyzing behavior, so it must perform multidimensional baselining, enabling the modeling of a broad set of user behaviors. Baselines are used to detect anomalous behavior via machine learning and other statistical analysis techniques.	The UEBA must create **heuristic or advanced** baseline of user activity by analyzing behavior, so it must perform multidimensional baselining, enabling the modeling of a broad set of user behaviors. Baselines are used to detect anomalous behavior via machine learning and other statistical analysis techniques.