****

**भारतीय लघु उद्योग विकास बैंक**

**Small Industries Development Bank of India**

**साईबर सुरक्षा परिचालन केंद्र के कार्यान्वयन एबं प्रबंधन के लिए आर एफ़ पी**

RFP FOR IMPLEMENTATION AND MANAGEMENT OF

CYBER SECURITY OPERATIONS CENTER (CSOC)

**Tender no: 400/2019/1434/BYO/ITV**

**Critical Information Sheet**/ महत्वपूर्ण सूचना पत्र

|  |  |
| --- | --- |
| Date of issue of RFP*/ आरएफपी जारी करने की तारीख* | February 22nd 2019 |
| Last date for seeking clarifications for pre-bid meeting **/ पूर्व-बोली बैठक के लिए स्पष्टीकरण मांगने की अंतिम तिथि** | March 01st 2019 3:00 PM |
| E-mail ID for sending pre-bid queries / पूर्व-बोली प्रश्न भेजने के लिए ई-मेल आईडी | As mentioned in Contact details of SIDBI officials below |
| Pre Bid meeting/ **पूर्व-बोली बैठक** | March 06th 2019 3:00 PM |
| Pre Bid meeting location/ **पूर्व-बोली बैठक का स्थान** | Small Industries Development Bank of India,  Swavalamban Bhavan,  Bandra Kurla Complex, Bandra [East],  Mumbai 400 051 |
| Responses to Pre-Bid Queries by Bank / बैंक द्वारा पूर्व-बोली प्रश्नों का जवाब | Within 7 working days of the pre bid meeting |
| Last date for submission of bids/ **बोली जमा करने की अंतिम तिथि** | March 22nd 2019 3:00 PM |
| Place for submission of bids/ **बोली जमा करने का पता** | SIDBI Chennai Office  Overseas Towers, 756-L, Anna Salai, Chennai - 600002, Tamil Nadu |
| Cost of RFP*/ आरएफपी की लागत* | Rs 5,000/- |
| Earnest Money Deposit (EMD*)/ बयाना जमा राशि* | Rs 23,50,000/- |
| Date & Time of Opening of Technical Bid **/ बोली की न्यूनतम पात्रता व तकनीकी बोली खोलने की तिथि व समय** | March 22nd 2019 3:30 PM |
| Date & Time of Opening of Commercial Bid/ **वाणिज्यिक बोली खोलने की तिथि व समय** | Will be intimated to shortlisted vendors. |
| Contact details of SIDBI officials/ **सिडबी अधिकारियों के संपर्क विवरण** | Sh. Sanjay Kumar Srivastava,  DGM(Systems)  044-66636005, [ssrivastav@sidbi.in](mailto:ssrivastav@sidbi.in)  Sh. Raghava Rachuri,  CISO & DGM(Systems)  044-66636050, raghava@sidbi.in  Sh. A V Syam Sundar,  AGM(Systems)  044-66636052, [avshyam@sidbi.in](mailto:avshyam@sidbi.in) |
| Independent External Monitor/ **स्वतंत्र बाहरी निगरानी** | Shri. Ashok Sinha, (IAS retd.),  13 Yayati, Sector-58A, Nerul (West),  Palm Beach Road,  Navi-Mumbai 400706,  Ph: 9821844044,  Mail id: [asinha51@gmail.com](mailto:asinha51@gmail.com) |
| Bid Validity/ **बोली के वैधता** | Nine Month from the last date of bid submission |

**Notice of Confidentiality:**

This document, its appendices, and all annexes, are the property of Small Industries Development Bank of India (SIDBI). Use of contents of document, its appendices, and all annexes is, provided to you for the sole purpose of responding to this Request for Proposal. It may not be otherwise copied, distributed or recorded on any medium, electronic or otherwise without SIDBI’s express written permissions.

**Important Clarifications**

Some terms have been used in the document interchangeably for the meaning as mentioned below:

1. “The Bank” means Small Industries Development Bank Of India (SIDBI);
2. ‘RFP’ means Request for Proposal for Implementation and Management of Cyber Security Operations Centre in SIDBI
3. ‘Bidder’ means a vendor submitting the proposal in response to RFP.
4. Managed Security Services Provider (MSSP), Bidder, System Integrator (SI), Recipient, Respondent and / or Vendor generally means “Respondent to the RFP document” unless context specifies otherwise provide
5. ‘Solution’ means setting up of Cyber Security Operation Centre in SIDBI.
6. “The Contract” means the agreement entered into between the Bank after the acceptance of the Bid, represented by its Head Office / Regional Offices and the Bidder, as recorded in the Contract Form signed by the parties, including all attachments and appendices thereto and all documents incorporated by reference therein;
7. “The Project Site” means Mumbai Office, Chennai Office and Bank’s Data Centers at Navi Mumbai and Chennai. The project team shall operate from Chennai Office and/or Mumbai Office. However, final decision on place of operation will be taken by the Bank as per requirement.
8. “The Contract Price” means the price payable to the Bidder under the Contract for the full and proper performance of its contractual obligations;
9. Cyber security is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. In a computing context, security includes both cyber security and physical security. Ensuring cyber security requires coordinated efforts through an information system. It includes collection of policies, security concepts, security safeguards, guidelines, risk management approaches, tools, training, best practices, assurance and technologies that can be used to protect cyber environment, organization and user’s assets. Organization and user’s assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications, systems, and the totality of transmitted and / or stored information in the cyber environment.
10. Cyber Security Operations Center (CSOC) , Security Operations Center (SOC) mean bidder providing services for Cyber Security Operations Center (CSOC)
11. SIEM means Security Incident and Event Management
12. DC means Bank’s Primary Data Centre at Mahape, Navi Mumbai
13. DR, DRS means Bank’s Disaster Recovery Centre (site) which currently is at Chennai Office and is likely to be co-located to Siruseri, Chennai shortly.
14. T & C means Terms and Conditions
15. BFSI indicates Banking, Financial institutions and Insurance excluding RRBs and Co-Operative Banks.

**Abbreviations**

| **Acronym** | **Description** |
| --- | --- |
| AMC | Annual Maintenance Contract |
| APT | Advanced Persistent Threat |
| BG | Bank Guarantee |
| CISA | Certified Information Systems Auditor |
| CISSP | Certified Information Systems Security Professional |
| CSOC | Cyber Security Operations Center |
| DC | Data Center |
| DR | Disaster Recovery |
| DRS | Disaster Recovery Site |
| EMD | Earnest Money Deposit |
| EPS | Events Per Second |
| ISMS | Information Security Management System |
| ITV | Information Technology Vertical |
| LA | Lead Auditor |
| LI | Lead Implementer |
| MSSP | Managed Security Services Provider |
| NAC | Network Access / Admission Control |
| NDA | Non-Disclosure Agreement |
| NIPS | Network Intrusion Prevention System |
| NPV | Net Present Value |
| PBG | Performance Bank Guarantee |
| PDC | Primary Data Center |
| PIM | Privilege Identity Management |
| RCB | Registered Certification Body |
| RFP | Request for Proposal |
| RiMV | Risk Management Vertical |
| SI | System Integrator |
| SIEM | Security Information & Event Management |
| SLA | Service Level Agreement |
| SPEC | Standard Performance Evaluation Corporation |
| VAPT | Vulnerability Assessment & Penetration Testing |
| WAF | Web Application Firewall |

**Table of Contents**

[1. Introduction and Disclaimer 13](#_Toc1471902)

[1.1. Preface 13](#_Toc1471903)

[1.2. Information Provided 13](#_Toc1471904)

[1.3. For Respondent only 13](#_Toc1471905)

[1.4. Disclaimer 14](#_Toc1471906)

[1.5. Costs to be borne by Respondents 14](#_Toc1471907)

[1.6. No Legal Relationship 14](#_Toc1471908)

[1.7. Recipient Obligation to Inform Itself 14](#_Toc1471909)

[1.8. Invitation of Offers 14](#_Toc1471910)

[1.9. Acceptance of Selection Process 15](#_Toc1471911)

[1.10. Errors and Omissions 15](#_Toc1471912)

[1.11. Acceptance of Terms 15](#_Toc1471913)

[1.12. Communication to Requests for Proposal 15](#_Toc1471914)

[1.13. Notification 16](#_Toc1471915)

[2. RFP Response 17](#_Toc1471916)

[2.1. General 17](#_Toc1471917)

[2.2. Language of Bid 18](#_Toc1471918)

[2.3. Bid Price 18](#_Toc1471919)

[2.4. Earnest Money Deposit (EMD) 18](#_Toc1471920)

[2.5. Conditional Bids 19](#_Toc1471921)

[2.6. Receiving of RFP Response 19](#_Toc1471922)

[2.7. Clarification of Bids 19](#_Toc1471923)

[2.8. Amendment to the bidding document 20](#_Toc1471924)

[2.9. Rules for Responding to the RFP 20](#_Toc1471925)

[2.10. Period of Validity of Bids 22](#_Toc1471926)

[2.11. Deadline for submission of Bids 22](#_Toc1471927)

[2.12. Late Bids 23](#_Toc1471928)

[2.13. Modification And / Or Withdrawal of Bids 23](#_Toc1471929)

[2.14. Requests for information 23](#_Toc1471930)

[2.15. Pre-Bid Meeting 24](#_Toc1471931)

[2.16. Opening of Technical Bids by the Bank 24](#_Toc1471932)

[2.17. Disqualification 24](#_Toc1471933)

[2.18. Selection process 25](#_Toc1471934)

[2.19. Details of Bids to be submitted 25](#_Toc1471935)

[2.20. Pre Contract Integrity Pact (IP) 27](#_Toc1471936)

[2.21. Important 28](#_Toc1471937)

[2.22. Responsibility of the Bidder 29](#_Toc1471938)

[3. About SIDBI and Purpose of RFP 31](#_Toc1471939)

[3.1. About SIDBI 31](#_Toc1471940)

[3.2. Objective 31](#_Toc1471941)

[3.3. Current Information Technology Setup 33](#_Toc1471942)

[4. Scope of Work 38](#_Toc1471943)

[4.1. Security Information and Event Management 38](#_Toc1471944)

[4.2. Privilege Identity Management (PIM) 42](#_Toc1471945)

[4.3. Anti-Advance Persistent Threat (APT) 42](#_Toc1471946)

[4.4. Firewall Analyzer 43](#_Toc1471947)

[4.5. Network Access Control (NAC) 43](#_Toc1471948)

[4.6. VAPT Information and Remediation Services 44](#_Toc1471949)

[4.7. Security/Threat Intelligence Services 45](#_Toc1471950)

[4.8. Other General Requirement 46](#_Toc1471951)

[4.8.1. Hardware, Software and Network Connectivity 46](#_Toc1471952)

[4.8.2. Training 47](#_Toc1471953)

[4.8.3. Implementation & Integration 48](#_Toc1471954)

[4.8.4. Reporting 51](#_Toc1471955)

[4.8.5. System Integration Testing (SIT) and User Acceptance Testing (UAT) 52](#_Toc1471956)

[4.8.6. Monitoring 52](#_Toc1471957)

[4.8.7. Continuous Improvement 55](#_Toc1471958)

[4.8.8. SLA Compliance 55](#_Toc1471959)

[4.8.9. Business continuity 55](#_Toc1471960)

[4.9. Period of Contract 55](#_Toc1471961)

[4.10. Implementation Phases and Timelines 56](#_Toc1471962)

[5. Evaluation Methodology 58](#_Toc1471963)

[5.1. Pre-Qualification Criteria 58](#_Toc1471964)

[5.2. Technical Evaluation 58](#_Toc1471965)

[5.3 Commercial Evaluation of the Bidders 62](#_Toc1471966)

[5.3.1 Arithmetic errors correction 62](#_Toc1471967)

[5.3.2 Issue of purchase order 63](#_Toc1471968)

[5.3.3 Execution of Agreement 63](#_Toc1471969)

[6. Terms and Conditions 64](#_Toc1471970)

[6.1. Bid Security & Performance Guarantee 64](#_Toc1471971)

[6.1.1. Bid Security / Earnest Money Deposit (EMD) 64](#_Toc1471972)

[6.1.2. Performance Bank Guarantee (PBG) 64](#_Toc1471973)

[6.2. Forfeiture of performance security 65](#_Toc1471974)

[6.3. Preliminary Examinations 66](#_Toc1471975)

[6.4. Use of Contract Documents and Information 66](#_Toc1471976)

[6.5. Rules for Evaluation of Responses 67](#_Toc1471977)

[6.6. Contacting the Bank 68](#_Toc1471978)

[6.7. Commercial Bid 68](#_Toc1471979)

[6.8. No Commitment to Accept Lowest or Any Offer 68](#_Toc1471980)

[6.9. Service Delivery 69](#_Toc1471981)

[6.10. Ownership of Delivered Services 69](#_Toc1471982)

[6.11. Addition / Deletion of qualified offerings 70](#_Toc1471983)

[6.12. Expenses 70](#_Toc1471984)

[6.13. Terms of Payment and Payment Milestones 70](#_Toc1471985)

[6.14. Taxes and Duties 72](#_Toc1471986)

[6.15. Execution of Agreement and NDA 73](#_Toc1471987)

[6.16. Period of Contract 73](#_Toc1471988)

[6.17. Termination 73](#_Toc1471989)

[6.18. Applicable laws 76](#_Toc1471990)

[6.19. Statutory & Regulatory Compliance 76](#_Toc1471991)

[6.20. No Employer-Employee Relationship 77](#_Toc1471992)

[6.21. Rights to Visit 77](#_Toc1471993)

[6.22. Audit 77](#_Toc1471994)

[6.23. IPR Infringement 78](#_Toc1471995)

[6.24. Indemnity 78](#_Toc1471996)

[6.25. Limitation of liabilities 80](#_Toc1471997)

[6.26. Confidentiality 80](#_Toc1471998)

[6.27. Corrupt and fraudulent practice 83](#_Toc1471999)

[6.28. Resolution of Disputes 83](#_Toc1472000)

[6.29. Grievances Redressal Mechanism 85](#_Toc1472001)

[6.30. Force Majeure 85](#_Toc1472002)

[6.31. Subcontracting 85](#_Toc1472003)

[6.32. Negligence 85](#_Toc1472004)

[6.33. Miscellaneous 86](#_Toc1472005)

[6.34. Delivery, Installation, Commissioning and Acceptance 87](#_Toc1472006)

[6.35. Responsibility for Completeness 87](#_Toc1472007)

[6.36. Change of name of the bidding company and line of business 88](#_Toc1472008)

[6.37. Governing Law and Jurisdiction 88](#_Toc1472009)

[6.38. No third party rights 88](#_Toc1472010)

[6.39. Representations and Warranties 89](#_Toc1472011)

[6.40. Vicarious Liability 90](#_Toc1472012)

[6.41. No Set-off, counter-claim and cross claims 90](#_Toc1472013)

[6.42. Governing Language 90](#_Toc1472014)

[6.43. Insurance 91](#_Toc1472015)

[6.44. Conflict of Interest 91](#_Toc1472016)

[6.45. Patent Rights 91](#_Toc1472017)

[6.46. Business Continuity 92](#_Toc1472018)

[6.47. Privacy and Security Safeguards 92](#_Toc1472019)

[6.48. GST law 93](#_Toc1472020)

[6.49. Non-Assignment 93](#_Toc1472021)

[6.50. Conflict of Terms 93](#_Toc1472022)

[6.51. Signing of Contract 93](#_Toc1472023)

[6.52. Tax Deduction at Source 94](#_Toc1472024)

[6.53. Acceptance 94](#_Toc1472025)

[7. Service Level Agreement & Liquidated Damages 95](#_Toc1472026)

[7.1. Liquidated damages for delay in Delivery and Installation of Hardware and Software 95](#_Toc1472027)

[7.2. Liquidated damages for not maintaining uptime 95](#_Toc1472028)

[7.3. SLAs & Liquidity Damages for CSOC Operations 98](#_Toc1472029)

[7.4. Waiver 101](#_Toc1472030)

[8. Annexure for Pre-Qualification Criteria 102](#_Toc1472031)

[Annexure 8.1 Covering Letter for Pre-Qualification Criteria 102](#_Toc1472032)

[Annexure 8.2 Pre-Qualification Criteria for Bidder 104](#_Toc1472033)

[Annexure 8.3 General Information about Bidder 110](#_Toc1472034)

[Annexure 8.4 Power of Attorney 113](#_Toc1472035)

[Annexure 8.5 Declarations 114](#_Toc1472036)

[Annexure 8.6 Bank Mandate Form 116](#_Toc1472037)

[Annexure 8.7 EMD / Bid Security Form 118](#_Toc1472038)

[Annexure 8.8 Manufacturer Authorisation Format 120](#_Toc1472039)

[Annexure 8.9 Undertaking of Authenticity 121](#_Toc1472040)

[Annexure 8.10 Pre-Contract Integrity Pact 123](#_Toc1472041)

[9. Annexure for Technical Bid 130](#_Toc1472042)

[**Annexure 9.1 Technical Bid** 130](#_Toc1472043)

[**Annexure 9.2 – Statement of Deviations** 133](#_Toc1472044)

[**Annexure 9.3 – Letter of Competence** 134](#_Toc1472045)

[**Annexure 9.4 – Letter of Conformity** 135](#_Toc1472046)

[10. Annexure for Commercial Bid 136](#_Toc1472047)

[**Annexure 10.1 – Commercial Bid – Covering Letter** 136](#_Toc1472048)

[**Annexure 10.2 – Commercial Bid Format** 137](#_Toc1472049)

[11. Annexure for Technical Specifications and Requirements 143](#_Toc1472050)

[**Annexure 11.1 Security Information and Event Management** 143](#_Toc1472051)

[**Annexure 11.2 Privilege Identity Management** 152](#_Toc1472052)

[**Annexure 11.3 Anti – Advanced Persistent Threat** 158](#_Toc1472053)

[**Annexure 11.4 Firewall Analyzer** 163](#_Toc1472054)

[**Annexure 11.5 Network Access Control (NAC)** 166](#_Toc1472055)

[**Annexure 11.6 Vulnerability Assessment and Penetration Testing Service** 168](#_Toc1472056)

[**Annexure 11.7 Indicative List of hardware / network / security devices** 170](#_Toc1472057)

[**Annexure 11.8 Resource Requirement Details** 171](#_Toc1472058)

[**Annexure 11.9 Non-disclosure Agreement** 175](#_Toc1472059)

[**Annexure 11.10 Performance Bank Guarantee** 177](#_Toc1472060)

[**Annexure 11.11 Technical Bill of Material** 180](#_Toc1472061)

[**Annexure 11.12 Undertaking Letter for GST Law** 181](#_Toc1472062)

[**Annexure 11.13 Undertaking for Central Minimum Wages Act & Labour Laws** 182](#_Toc1472063)

# **Introduction and Disclaimer**

# **Preface**

This Request for Proposal document (‘RFP document’ or RFP) has been prepared solely for the purpose to outsource the Implementation and Management of Cyber Security Operations Center (CSOC), which includes the Maintenance and Support for a period of three years and extendable for a further duration of maximum two years at the discretion of the Bank under THREE (3) Bid System viz.

1) Pre-qualification Criteria

2) Technical Bid &

3) Commercial Bid.

The RFP document is not a recommendation, offer or invitation to enter into a contract, agreement or any other arrangement, in respect of the services. The provision of the services is subject to observance of selection process and appropriate documentation being agreed between SIDBI and any successful Bidder as identified by SIDBI, after completion of the selection process as detailed in this document.

# **Information Provided**

The RFP document contains statements derived from information that is believed to be relevant at the date but does not purport to provide all of the information that may be necessary or desirable to enable an intending contracting party to determine whether or not to enter into a contract or arrangement with SIDBI. Neither SIDBI nor any of its employees, agents, contractors, or advisers gives any representation or warranty, express or implied, as to the accuracy or completeness of any information or statement given or made in this document. Neither SIDBI nor any of its employees, agents, contractors, or advisers has carried out or will carry out an independent audit or verification exercise in relation to the contents of any part of the document.

# **For Respondent only**

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

# **Disclaimer**

Subject to any law to the contrary, and to the maximum extent permitted by law, Bank and its directors, officers, employees, contractors, representatives, agents, and advisers disclaim all liability from any loss, claim, expense (including, without limitation, any legal fees, costs, charges, demands, actions, liabilities, expenses or disbursements incurred therein or incidental thereto) or damage, (whether foreseeable or not) (“Losses”) suffered by any person acting on or refraining from acting because of any presumptions or information (whether oral or written and whether express or implied), including forecasts, statements, estimates, or projections contained in this RFP document or conduct ancillary to it whether or not the Losses arise in connection with any ignorance, negligence, inattention, casualness, disregard, omission, default, lack of care, immature information, falsification or misrepresentation on the part of Bank or any of its directors, officers, employees, contractors, representatives, agents, or advisers.

# **Costs to be borne by Respondents**

All costs and expenses incurred by Respondents in any way associated with the development, preparation, and submission of responses, including but not limited to the attendance at meetings, discussions, demonstrations, etc. and providing any additional information required by SIDBI, will be borne entirely and exclusively by the Respondent.

# **No Legal Relationship**

No binding legal relationship will exist between any of the Respondents and SIDBI until execution of a contractual agreement.

# **Recipient Obligation to Inform Itself**

The Recipient must apply its own care and conduct its own investigation and analysis regarding any information contained in the RFP document and the meaning and impact of that information.

# **Invitation of Offers**

The issuance of RFP document is merely an invitation to offer and must not be construed as any agreement or contract or arrangement nor would it be construed as any investigation or review carried out by a Recipient.

# **Acceptance of Selection Process**

Each Recipient / Respondent having responded to this RFP acknowledges to have read, understood and accepted the selection & evaluation process mentioned in this RFP document. The Recipient / Respondent ceases to have any option to object against any of these processes at any stage subsequent to submission of its responses to this RFP.

# **Errors and Omissions**

Each Recipient should notify SIDBI of any error, fault, omission, or discrepancy found in this RFP document but not later than twelve days prior to the due date for lodgment of Response to RFP.

# **Acceptance of Terms**

Recipient will, by responding to SIDBI for RFP, be deemed to have accepted the terms of this RFP including Introduction and Disclaimer.

# **Communication to Requests for Proposal**

Recipients are required to direct all communications related to this RFP, through the Nominated Point of Contact person:

Contact : Sh. Sanjay Kumar Srivastava

Position : Deputy General Manager (Systems)

Email : ssrivastava@sidbi.in

Telephone : +91 – 44 - 66636005

Contact : Sh. Raghava Rachuri

Position : CISO & Deputy General Manager (Systems)

Email : raghava@sidbi.in

Telephone : +91 – 44 - 66636050

Contact : Sh. A V Syam Sundar

Position : Assistant General Manager (Systems)

Email : avshyam@sidbi.in

Telephone : +91 – 44 - 66636052

SIDBI may, in its absolute discretion, seek additional information or material from any Respondents after the RFP closes and all such information and material provided must be taken to form part of such Respondent’s response.

Respondents should provide details of their contact person, telephone, mobile, fax, email and full address(s) to ensure that replies to RFP could be conveyed promptly.

If SIDBI, in its absolute discretion, deems that the originator of the question will gain an advantage by a response to a question, then SIDBI reserves the right to communicate such response to all Respondents.

SIDBI may, in its absolute discretion, engage in discussion with any Respondent (or simultaneously with more than one Respondent) after the RFP closes to improve or clarify any response.

# **Notification**

SIDBI will notify all short-listed Respondents in writing or by email as soon as practicable about the outcome of their RFP. SIDBI is not obliged to provide any reasons for any such acceptance or rejection.

# **RFP Response**

# **General**

1. The Bidders are expected to examine all instructions, forms, terms and specifications in the bidding documents. Failure to furnish all information required by the bidding documents may result in the rejection of its bid and will be at the bidder's own risk.
2. Information provided in this RFP is organized in several sections to bring clarity and help the reader to understand quickly. However, Bidder must take into consideration each and every line of this RFP document as a whole while responding. Bidder must get the doubts clarified, if any, by SIDBI before submitting the responses. The bids submitted should be complete in all respect meeting all deliverables under the project. It will be sole responsibility of the selected bidder to deliver each and everything as per the scope of the project during the contracted period. SIDBI shall not be responsible in case of bidder’s failure to notice any information, any requirement is underestimated, not understood or any requirement is not interpreted in right direction during preparation / submitting the response or seeking clarification thereof / thereon, from SIDBI, within the stipulated time period.
3. Unless expressly overridden by the specific agreement to be entered into between the Bank and the successful Bidder, the RFP and any subsequent modifications/clarifications shall be the governing document for arrangement between the Bank and the Bidders.
4. SIDBI shall be under no obligation to accept the lowest or any other offer received in response to this RFP and shall be entitled to reject any or all offers. SIDBI reserves the right to make any changes in the terms and conditions of purchase. SIDBI will not be obliged to meet and have discussions with any Bidder, and / or to respond to any representations.
5. SIDBI reserves the right to extend the dates for submission of responses to this document with intimation on the bank’s website and CPP portal.
6. Unless agreed to specifically by the Bank in writing for any changes to the RFP issued, the Bidders’ responses would not be incorporated automatically in the RFP document.
7. The Bank reserves the right to modify/cancel/re-tender without assigning any reasons whatsoever. The Bank shall not incur any liability to the affected bidder(s) on account of such rejection. Bank shall not be obliged to inform the affected bidder(s) of the grounds for the Bank's decision for rejection / cancellation.
8. The scope of the proposal shall be on the basis of single point responsibility, completely covering the solutions and services specified under this RFP.
9. The Bidder shall promptly notify SIDBI of any event or conditions, which might delay the completion of implementation work in accordance with the approved schedule and the steps being taken to remedy such a situation.

# **Language of Bid**

The bid prepared by the Bidders as well as all correspondence and documents relating to the Bid exchanged by the Bidder and the Bank and supporting documents and printed literature should be written in English.

# **Bid Price**

1. Non-refundable Bid Price of Rs 5,000/- (Rs Five Thousand only) by way of Banker’s Cheque / Demand Draft / Pay Order drawn on a scheduled bank, favoring “Small Industries Development Bank of India”, payable at Chennai must be submitted along with RFP response. Any bid received without this shall be considered unresponsive and rejected.
2. The Bank may, at its discretion, reject any Bidder where the application money has not been furnished with the RFP response.

# **Earnest Money Deposit (EMD)**

All the responses must be accompanied by a refundable interest free security deposit of the amount indicated in critical information sheet which needs to be issued from a scheduled commercial bank. The EMD should be in the form of:

a) Demand Draft / Banker’s Cheque in favour of “Small Industries Development Bank of India” payable at Chennai **OR**

b) Bank guarantee (BG) from a Scheduled Commercial Bank valid for a period of nine (9) months from the tender issue dateand strictly in the format as prescribed in section 8.7

The EMD amount / BG of all unsuccessful bidders would be refunded immediately upon occurrence of any the following events, whichever is earlier:

* + 1. Issue of Letter of Intent / Purchase order to the successful bidder

OR

* + 1. Receipt of the signed contract and performance security from the successful bidder. OR
    2. The end of the bid validity period, including extended period (if any)

# **Conditional Bids**

Conditional bids shall not be accepted on any ground and shall be rejected straightway. If any clarification is required, the same should be obtained by the bidder from the Bank before submission of bids.

# **Receiving of RFP Response**

Receiving of RFP response will be recorded by SIDBI in a ‘Tender Receiving Register’ kept for the purpose upon receiving the RFP response. The submission of the response should be in the format outlined in this RFP and should be submitted preferably through hand delivery. If the submission to this RFP does not include all the documents and information required or is incomplete or submission is through Fax mode, the RFP is liable to be summarily rejected. All submissions, including any accompanying documents, will become the property of Bank. The Recipient shall be deemed to have licensed and granted all rights to the Bank to reproduce the whole or any portion of their submission for the purpose of evaluation and to disclose and/or use the contents of the submission as the basis for any resulting RFP process, notwithstanding any copyright or other intellectual property right of the Recipient that may subsist in the submission or accompanying documents.

# **Clarification of Bids**

1. The bidder or its official representative is invited to attend pre-bid meeting (date and venue mentioned in Bid Information Sheet) It would be the responsibility of the Bidders representatives to be present at the venue of the meeting. A maximum of two representatives will be allowed for each bidder to attend the pre-bid meeting.
2. Clarification sought by bidder should be made in writing (Letter/E-mail/FAX etc.) and submitted by the last date of seeking clarifications mentioned in the first page of this RFP. Bank has discretion to consider any other queries raised by the bidder’s representative during the pre-bid meeting.
3. The text of the clarifications asked (without identifying the source of enquiry) and the response given by the Bank, together with amendment to the bidding document, if any, will be posted on the website within 7 working days post the date of pre-bid meeting. No individual clarifications will be sent to the bidders. It would be responsibility of the bidder to check the website before final submission of bids.
4. During evaluation of Bids, the Bank, at its discretion, may ask the Bidders for clarifications of their Bids. The request for clarification and the response shall be in writing (Fax/e-Mail/letter), and no change in the price of substance of the Bid shall be sought, offered or permitted.
5. Bidder to submit point by point compliance to the technical compliance and it should be included in the Bid.
6. Bidder to quote for entire package on a single responsibility basis for the solution and services it proposes to offer under the contract.
7. The pre-bid queries should be shared by the bidder as per the below template in excel sheet only :

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **S. No.** | **Section Name** | **Page No.** | **Point as stated in RFP** | **Category:**  **Clarification / Deviation / Suggestion** | **Description** |
| 1 |  |  |  |  |  |
| 2 |  |  |  |  |  |
| 3 |  |  |  |  |  |
| 4 |  |  |  |  |  |
| 5 |  |  |  |  |  |

# **Amendment to the bidding document**

1. At any time prior to the deadline for submission of Bids, SIDBI may, for any reason, whether at its own initiative or in response to a clarification requested by prospective Bidder(s), modify the RFP by amendment and same will be placed on the bank’s website (www.sidbi.in) for information of all prospective Bidders.
2. The amendment will also be posted on Central Public Procurement Portal (CPPP) i.e. eprocure.gov.in.
3. All Bidders must ensure that such clarifications have been considered by them before submitting the bid. Bank will not have any responsibility in case some omission is done by any bidder.
4. In order to allow prospective Bidders reasonable time in which to take the amendment into account in preparing their Bids, the Bank, at its discretion, may extend the deadline for the submission of Bids.

# **Rules for Responding to the RFP**

1. The responses to the RFP would be deemed to be legal documents and will form part of the final contract. Bidders are required to attach a ‘Letter of Competence’ from an authorized signatory attesting their competence and the veracity of information provided in the responses. Unsigned responses would be treated as incomplete and are liable to be rejected. Format of letter is given in Annexure 9.3.
2. Bidders shall have the opportunity to clarify doubts pertaining to the RFP in order to clarify any issues they may have prior to finalizing their responses. All questions are to be submitted to the contact details mentioned at 1.12, and should be received by the point of contact not later than the date mentioned in the RFP document. Responses to inquiries and any other corrections and amendment will be made available on bank’s website and CPP portal. The Bidder, which posed the question, will remain anonymous.
3. Any part of the response either technical or commercial bid, submitted by the bidder cannot be withdrawn / modified after the last date for submission of the bids unless otherwise asked and specifically permitted by the bank.
4. SIDBI reserves the right to call for any additional information and also reserves the right to reject the proposal of any Bidder if in the opinion of SIDBI, the information furnished is incomplete or the Bidder does not qualify for the contract.
5. The bids will have to be signed on all pages of the bid by the authorized signatory. Unsigned bids would be treated as incomplete and would be rejected.
6. The Bidder must submit the response exactly in the formats mentioned in this RFP and same should be to the point. It must not provide any irrelevant additional information. All the credentials, claimed in the response, must be accompanied with necessary proof. SIDBI would be at discretion to reject the response of the bidder in case any part or whole of the response document is found to be partially or fully incomplete or confusing or misguiding or having irrelevant additional information.
7. By submitting a proposal, the Bidder agrees to promptly contract with SIDBI for work related to this RFP, awarded to the Bidder. Failure on the part of the awarded Bidder to execute a valid contract with SIDBI within stipulated time will relieve SIDBI of any obligation to the Bidder and forfeit the EMD.
8. Any additional or different terms and conditions proposed by the Bidder would be rejected unless expressly assented to in writing by SIDBI.
9. Responses received after the due date / time would be considered late and shall not be accepted or opened. Late received bids shall be returned un-opened within 02 weeks from the bid submission date.
10. SIDBI would not assume any expenses incurred by the Bidder in preparation of the response to this RFP and also would not return the bid to the Bidder.
11. SIDBI shall not be liable for costs incurred during any discussion on proposals or proposed contracts or for any work performed in connection therewith.
12. The offers containing erasures or alterations will not be considered. There should be no hand-written material, corrections or alterations in the offer. Technical details must be completely filled up. Correct technical information / description of the product being offered must be filled in. Filling up of the information using terms such as “OK”, “accepted”, “offered”, “noted”, “as given in brochure / manual” is not acceptable. SIDBI may treat proposals not adhering to these guidelines as unacceptable and thereby the proposal may be liable to be rejected.
13. Responses received become the property of SIDBI and will not be returned. Information provided by each Bidder will be held in confidence, and will be used for the sole purpose of evaluating a potential business relationship with the Bidder.
14. The Bidders shall adhere to the terms of this RFP document and shall not deviate from the same. If the Bidders have absolutely genuine issues only then should they provide their nature of non-compliance to the same in the format provided separately with this RFP. The Bank reserves its right to not to accept such deviations to the Tender terms, in its sole and absolute discretion, and shall not be obliged to furnish any reason for exercising such right.
15. All responses should be submitted in hard and soft copy in English only.
16. All commercials submitted as part of the bid to be quoted in Indian Rupees (INR).
17. All bid responses would be deemed to be irrevocable offers/proposals from the bidder and may be accepted by SIDBI to form part of final contract between SIDBI and the selected bidder.

# **Period of Validity of Bids**

1. Prices and other terms offered by Bidders must be firm for an acceptance period of nine (9) months from last date for submission of bids.
2. In exceptional circumstances the Bank may solicit the Bidders consent to an extension of the period of validity. The request and response thereto shall be made in writing.
3. Bank, however, reserves the right to call for fresh quotes at any time during the period, if considered necessary.

# **Deadline for submission of Bids**

1. The bids must be received by the Bank at the specified address not later than date mentioned in the beginning of this document.
2. In the event of the specified date for the submission of bids, being declared a holiday for the Bank, the bids will be received up to the appointed time on the next working day.
3. The Bank may, at its discretion, extend the deadline for submission of Bids by amending the Bid Documents, in which case, all rights and obligations of the Bank and Bidders previously subject to the deadline will thereafter be subject to the deadline as extended.

# **Late Bids**

Any bid received by the Bank after the deadline for submission of bids prescribed by the Bank may be rejected and returned unopened to the bidder.

# **Modification And / Or Withdrawal of Bids**

1. The Bidder may modify or withdraw its bid after the bid’s submission, provided that written notice of the modification including substitution or withdrawal of the bids is received by the Bank, prior to the deadline prescribed for submission of bids.
2. The Bid modification or withdrawal notice must be on bidder’s letterhead, signed by authorized signatory and sealed. A withdrawal notice may also be sent by Fax / E-mail and followed by a signed confirmation copy received by the Bank not later than the deadline for submission of bids.
3. No bid may be modified or withdrawn after the deadline for submission of bids.
4. Bank has the right to reject any or all bids received without assigning any reason whatsoever. Bank shall not be responsible for non-receipt / non-delivery of the bid documents due to any reason whatsoever.

# **Requests for information**

1. Recipients are required to direct all communications for any clarification related to this RFP, to the designated Bank officials and must communicate the same in writing by the time mentioned in ‘Critical Information’ section above. No query / clarification would be entertained over phone.
2. All queries relating to the RFP, technical or otherwise, must be in writing only and may be sent via email. The Bank will try to reply, without any obligation in respect thereof, every reasonable query raised by the Recipients in the manner specified. However, the Bank will not answer any communication reaching the bank later than the time stipulated for the purpose.
3. The Bank may in its absolute discretion seek, but under no obligation to seek, additional information or material from any Respondents after the RFP closes and all such information and material provided must be taken to form part of that Respondent’s response. Respondents should invariably provide details of their email address as responses to queries will be provided to all Respondents via email.
4. The Bank may in its sole and absolute discretion engage in discussion with any Respondent (or simultaneously with more than one Respondent) after the RFP closes to clarify any response.

# **Pre-Bid Meeting**

1. The Bank shall hold a pre-bid meeting on the date and time mentioned in the beginning of the RFP. Purpose of the meeting is to bring utmost clarity on the scope of work and terms of the RFP being floated. The Bidders are expected to use the platform to have all their queries answered. No query will be entertained after the pre-bid meeting.
2. It would be the responsibility of the Bidders to be present at the venue of the meeting.

# **Opening of Technical Bids by the Bank**

1. Bids, except commercial bids, received within stipulated time, shall be opened as per schedule given in the RFP.
2. On the scheduled date and time, bids will be opened by the Bank Committee in presence of Bidder representatives. It is the responsibility of the bidder’s representative to be present at the time, on the date and at the place specified in the tender document. The bidders’ representatives who are present shall sign the required documents evidencing their attendance and opening of bids in their presence.
3. If any of the bidders or all bidders who have submitted the tender and are not present during the specified date and time of opening, bank at its discretion will proceed further with opening of the technical bids in their absence.
4. The Bidder name, presence or absence of requisite EMD and such other details as the Bank, at its discretion may consider appropriate will be announced at the time of bid opening.
5. Bids that are not opened at Bid opening shall not be considered for further evaluation, irrespective of the circumstances. Withdrawn bids will be returned unopened to the Bidders.

# **Disqualification**

Any form of canvassing / lobbying / influence / query regarding short listing, status etc. will result in a disqualification.

# **Selection process**

Successful Bidder will be selected through three bids evaluation process:

1. Pre-Qualification Criteria for Bidder
2. Technical Bid
3. Commercial Bid

# **Details of Bids to be submitted**

1. Bidders are required to submit their responses in THREE envelopes, with contents of each as under:

|  |  |  |  |
| --- | --- | --- | --- |
| **Envelope #** | **Bid Content** | **Number of Copies** | **Label of Envelope** |
| 1 | **Pre-Qualification Criteria for Bidder**   1. Covering Letter for Pre-Qualification Criteria as per format prescribed in Annexure 8.1 2. Pre - Qualification Criteria for Bidder as per format prescribed in Annexure 8.2 3. General Information about the Bidder as per format prescribed in Annexure 8.3 4. Power of Attorney to be signed by authorized person as per format prescribed in Annexure 8.4 5. Declarations as per format prescribed in Annexure 8.5 6. Bank Mandate Form as per format prescribed in Annexure 8.6 7. EMD / Bid Security Form as per format prescribed in Annexure 8.7 8. Manufacturer Authorisation Form as per prescribed format in Annexure 8.8 9. Undertaking of Authenticity as per prescribed format in Annexure 8.9 10. Pre-Contract Integrity Pact as per format in Annexure 8.10 11. Masked Commercial bid as per format prescribed in Annexure 10.2 | Hardcopy-1 and  Softcopy-1 (USB) | Envelope-1  “Pre-Qualification Criteria for  Implementation & Management of Cyber Security Operations Center (CSOC)” |
| 2 | **Technical Bid**   1. Technical Bid as per format prescribed in Annexure 9.1 2. Statement of Deviations as per format prescribed in Annexure 9.2 3. Letter of Competence as per format prescribed in Annexure 9.3 4. Letter of Conformity as per format prescribed in Annexure 9.4 | Hardcopy-1 and  Softcopy-1 (USB) | Envelope 2  “Technical Bid for  Implementation & Management of Cyber Security Operations Center (CSOC)” |
|  | **Technical Specifications & Others**   1. Security Information & Event Management (SIEM) as per format prescribed in Annexure 11.1 2. Privilege Identity Management (PIM) as per format prescribed in Annexure 11.2 3. Anti - Advanced Persistent Threat as per format prescribed in Annexure 11.3 4. Firewall Analyzer as per format prescribed in Annexure 11.4 5. Network Access Control (NAC) as per format prescribed in Annexure 11.5 6. Vulnerability Assessment and Penetration Testing as per format prescribed in Annexure 11.6 7. Non-disclosure Agreement as per format prescribed in Annexure 11.9 8. Technical Bill of Material as per format prescribed in Annexure 11.11 9. Undertaking letter for GST Law as per format prescribed in Annexure 11.12 10. Undertaking for Central Minimum Wages Act & Labour Laws as per format prescribed in Annexure 11.13 | Hardcopy-1  Softcopy-1 (USB) | Envelope 2  “Technical Bid for  Implementation & Management of Cyber Security Operations Center (CSOC)” |
| 3 | **Commercial Bid**   1. Commercial bid covering letter as per format prescribed in Annexure 10.1 2. Commercial bid as per format prescribed in Annexure 10.2 | Hardcopy-1 and  Softcopy-1 (USB) | Envelope 3  “Commercial Bid for  Implementation & Management of Cyber Security Operations Center (CSOC)” |

1. Above mentioned three separately sealed sub-envelopes should be put together in another master sealed envelope super-scribing “Technical and Commercial Proposal for Implementation and Management of Cyber Security Operations Center (CSOC) Tender no: 400/2019/1434/BYO/ITV dated 22/02/2019”.
2. All the individual envelopes must be super-scribed with the following information as well:
   1. Name of the bidder, Contact Number and mail id.
   2. Bids should be enclosed with all relevant documentary proofs / certificates duly sealed and signed.
   3. Envelope 1, 2 and 3 should also contain softcopy in the form of USB of respective response documents.
   4. Masked commercial bids must be given with Pre - Qualification Criteria eligibility Bid, failing which bids shall be liable to be rejected. Masked fields should be mentioned as ‘Quoted’. Partial commercial bid shall not be accepted.

# **Pre Contract Integrity Pact (IP)**

1. IP is an agreement between the prospective vendors / bidders and the buyer committing the persons / officials of both the parties not to exercise any corrupt influence on any aspect of the contract.
2. The Pact essentially envisages an agreement between the prospective bidders and the Bank, committing the persons/officials of both sides, not to resort to any corrupt practices in any aspect/stage of the contract.
3. Only those bidders, who commit themselves to the above pact with the Bank, shall be considered eligible for participate in the bidding process.
4. Foreign Bidders to disclose the name and address of agents and representatives in India and Indian Bidders to disclose their foreign principles or associates.
5. Bidders to disclose the payments to be made by them to agents/brokers or any other intermediary. Bidders to disclose any transgressions with any other company that may impinge on the anti-corruption principle.
6. Integrity Pact in respect of this contract would be operative from the stage of invitation of the Bids till the final completion of the contract. Any violation of the same would entail disqualification of the bidders and exclusion from future business dealings.
7. The Integrity Pact Agreement submitted by the bidder during the Bid submission will automatically form the part of the Contract Agreement till the conclusion of the contract i.e. the final payment or the duration of the Warranty / Guarantee / AMC if contracted whichever is later.
8. Integrity Pact, in respect of a particular contract would be operative stage of invitation of bids till the final completion of the contract. Any violation of the same would entail disqualification of the bidders and exclusion from future business dealings.
9. Integrity pact shall be signed by the person who is authorized to sign the Bid.
10. The bidder has to submit signed Pre-Contract Integrity Pact (IP) as per the format at Annexure 8.10 on non-judicial stamp paper of requisite value (to be borne by the bidder) applicable at the place of its first execution after the issue of Purchase Order.
11. Non submission of IP along with pre-qualification envelope may lead to rejection of the bid.

# **Important**

Bidders must take the following points into consideration during preparation and submission of bids.

1. Relevant documents must be submitted as proof wherever necessary. All the pages must be sealed and signed by the authorized signatory of the respondent.
2. Faxed copies of any submission are not acceptable and will be rejected by the Bank.
3. Responses should be concise and to the point. Submission of irrelevant documents MUST be avoided.
4. If the bids do not contain all the information required or is incomplete, the proposal is liable to be rejected.
5. The RFP is hosted on SIDBI website <http://www.sidbi.in>, Central Public Procurement Portal (CPPP) at eprocure.gov.in. SIDBI reserves the right to change the dates mentioned above. Changes and clarification, if any, related to RFP will be posted on SIDBI website and CPPP. Bidders must have close watch on SIDBI website and CPPP during the intervening period before submitting response to RFP.
6. The bidder cannot quote for the project in part.
7. Each bidder shall submit only one proposal.
8. The bidder should submit bid on behalf of company they are representing and not in consortium or partnership with other vendors.

# **Responsibility of the Bidder**

By submitting a signed bid/response to this RFP the Bidder certifies that:

1. The Bidder has arrived at the prices in its bid without agreement with any other bidder of this RFP for the purpose of restricting competition.
2. The Selected bidder has to inform change in the management of the company, if any, to the Bank within 30 days from the date of such change during contract period.
3. The prices in the bid have not been disclosed and shall not be disclosed to any other bidder of this RFP.
4. The Bank will call for Audited Balance Sheet of the selected Bidder at any point of time during Contract period and the selected Bidder shall provide the same.
5. The selected bidder will provide access to the Bank or auditors/consultants engaged by / representing the Bank for inspection / audit of its CSOC operations for any compliance or regulatory requirements. The selected bidder will facilitate and provide additional support during all audits conducted by the bank as part of contract period.
6. No attempt by the Bidder to induce any other bidder to submit or not to submit a bid for restricting competition has occurred.
7. The selected bidder shall submit updated Escalation Matrix for the product/services on a Half-Yearly basis as at the end of 31st March and 30th September.
8. Each Bidder must indicate whether or not they have any actual or potential conflict of interest related to contracting services with SIDBI. In case such conflicts of interest do arise, the Bidder must indicate the manner in which such conflicts can be resolved.
9. The Bidder represents and acknowledges to the Bank that it possesses necessary experience, expertise and ability to undertake and fulfill its obligations, under all phases involved in the performance of the provisions of this RFP. The Bidder represents that all software and hardware to be supplied in response to this RFP shall meet the requirement of the solution proposed by the Bidder. The Bidder shall be required to independently arrive at a solution, which is suitable for the Bank, after taking into consideration the effort estimated for implementation of the same. If any services, functions or responsibilities not specifically described in this RFP are an inherent, necessary or customary part of the deliverables or services and are required for proper performance or provision of the deliverables or services in accordance with this RFP, they shall be deemed to be included within the scope of the deliverables or services, as if such services, functions or responsibilities were specifically required and described in this RFP and shall be provided by the Bidder at no additional cost to the Bank. The Bidder also acknowledges that the Bank relies on this statement of fact, therefore neither accepting responsibility for, nor relieving the Bidder of responsibility for the performance of all provisions and terms and conditions of this RFP, the Bank expects the Bidder to fulfill all the terms and conditions of this RFP.

# **About SIDBI and Purpose of RFP**

# **About SIDBI**

Small Industries Development Bank of India (SIDBI), set up on April 2, 1990 under an Act of Indian Parliament, acts as the Principal Financial Institution for the Promotion, Financing and Development of the Micro, Small and Medium Enterprise (MSME) sector and for Co-ordination of the functions of the institutions engaged in similar activities.

The business domain of SIDBI consists of Micro, Small and Medium Enterprises (MSMEs), which contribute significantly to the national economy in terms of production, employment and exports. MSME sector is an important pillar of Indian economy as it contributes greatly to the growth of Indian economy with a vast network of around 5.1 crore units, creating employment of about 11.7 crore, manufacturing more than 6,000 products, contributing about 45% to manufacturing output and about 40% of exports in terms of value, about 37% of GDP.

# **Objective**

The Bank has decided to build a Cyber - Security Operation Centre (CSOC) to monitor, assess and defend Bank‘s information systems in order to protect confidentiality, integrity and availability of the Bank’s data.

The proposed CSOC facility is to be equipped with set of tools such as Security Information and Event Management Tool (SIEM), Incident Management tool, Anti – Advanced Persistent Threat (APT), Privilege Identity Management (PIM), Network Access Control (NAC) and Firewall Analyzer given in detail under this RFP and Security Intelligence services for better security monitoring and response capabilities. Bank intends to implement Cyber-Security Operation Centre (CSOC) for information assets at Primary Data Center and DR site. Bank expect Service provider to provide full-fledged Services including but not limited to design, supply, implementation, configuration, customization, integration, monitor, manage, backup, documentation, training, warranty support, post warranty maintenance support, back to back arrangement with OEM and any other activities related to or connected to the Information Technology / Cyber security solutions, devices & technologies. The Bank has plans to co-locate the DR Site from third party Data Center at Chennai and the order has already been issued for the same. The bidder should continue provide security services for co-located DR setup in future.

The bidder is expected to do following but not limited to:

1. Design, implement, manage and monitor CSOC
2. Security Monitoring of attacks into/on/against Bank‘s IT assets
3. Manage security, configuration, availability, performance and fault management, advisory for the security devices and its software stipulated in scope.
4. Ensure Malware Scanning / Protection/ Presentation /Reporting as required by the Bank including total Anti-APT solution.
5. Provide proactive threat intelligence and threat hunting.
6. Vulnerability Assessment & Penetration Testing for critical devices/ servers /applications/solutions on quarterly basis / as and when required by the Bank and provide solution for closure.
7. Risk assessment and mitigation, protection, execution support for the Security solutions, devices, software and tools under the scope of CSOC.
8. Ensure adherences to Bank‘s Information Security Policy and Cyber Security Policy.
9. Ensure adequacy, appropriateness and concurrency of various policies as per the requirement of regulatory authorities and Government of India Security authorities, IT Act 2000 and subsequent amendments and guidelines in place.
10. Provide forensics support as per the requirement of Bank in case of any incident or as and when required.
11. Dashboard for reporting and SLA management.
12. The selected Bidder will be responsible for implementing CSOC at central location identified by Bank, i.e. DC site. Selected Bidder will also supply and install all required infrastructure for operations of the CSOC as per the broad objectives outlined in this section & detailed scope of RFP.
13. As proposed in this bid, the SIEM tool and other security solutions have to be implemented in the bank premises and the procured security solutions to be integrated with SIEM tool. The proposed CSOC service should cover security event correlation, monitoring, incident management and providing proactive security alert and remediation. The selected bidder will be playing responsible for implementation and management of CSOC for all the security solutions/tools as detailed in Section 4.
14. Contain the cyber security attacks and Forensic capability on need basis for specific incidents
15. Hardening of devices needs to be performed for new devices as part of implementation
16. Support all kind of audits during contract period
17. Ensure future integration with new applications and devices as part of CSOC operations during contract period.

# **Current Information Technology Setup**

* 1. **Data Centre and DR Site**

SIDBI has its Primary Data center at Mhape, Navi Mumbai and DR Site at Chennai. All the IT applications & services are hosted at Data center (including email, Internet access) and the same are accessed over MPLS VPN by all locations and offices. In the event of failure of Primary Data center, DR Site is activated.

If any bidder/vendor is not able to attend the pre-bid meeting, the required information with respect to the servers and network devices of Data Center and DR Site may be obtained in person on submission of an authorization letter.

* 1. **Present IT Infrastructure**

The Indicative List of hardware / network / security devices to be integrated with the security solutions offered under CSOC is furnished in Annexure 11.7.

* 1. **Wide Area Network**
* SIDBI has implemented complete managed IP MPLS VPN based WAN at all locations/offices. Complete managed services include supply of all network hardware (router, MUX, Modem etc.) on lease, configuration, troubleshooting, monitoring, maintenance, reporting etc.
* The primary connectivity is wired or wireless with backup on 3G, CDMA, RF etc. based on feasibility of service provider at the location.
* The MPLS VPN network architecture is HUB and spoke, with HUB locations being Datacenter and DR Site. The MPLS is end to end encrypted (IPSec). All locations can reach DC and DR simultaneously.
* Further, three service providers are contracted to build the network. The bandwidth at the locations varies from 256Kbps to 32Mbps and at aggregation points (DC and DR) the bandwidth available is 4/32/64Mbps. Bandwidth at the locations is upgraded based on business requirements.
* SIDBI also carries out additional monitoring, configuration and management of WAN, which is currently carried out by outsourced partner. For carrying out the same Bank has deployed Open View (HPOV), Network Node Manager (NNM).
  1. **Local Area Network**

SIDBI has implemented IP based, wired LAN at DC and DR. The LAN switches at DC and DR are L3 switch(s).

* 1. **Point to Point Link**

For online log shipment / replication from DC to DR, Bank has deployed point to point links / MPLS link of requisite bandwidth taken from two service providers. The links are terminated on L3 switches at DC and DR.

* 1. **External Networks**
* SIDBI also has connectivity with third party networks like INFINET, Reuters, and SWIFT etc. at both DC and DR.
* The networks are currently connected as separate LAN and integrated with DC & DR LAN.
  1. **Internet**
* Internet at SIDBI is centralized with gateway at Data center and DR and all locations access Internet over WAN with proxy authentication.
* Bank has procured Internet bandwidth from two service providers at both Mumbai and Chennai.
* The links are terminated on link load balancers.
* Web Gateway Security (WGS) appliance is installed at Data center and DR Site which acts as proxy server with content filtering, antimalware and antivirus software loaded on it. The WGS is integrated with AD.
  1. **Mail**
* SIDBI is currently using Microsoft Outlook for mailing. Outbound mails are sent from Microsoft Outlook to internal SMTP and then transferred directly over Internet. SIDBI has its external mail box hosted with the Third party. All inbound internet mails from external domains, are first received at hosted mail box, gets scanned for anti-spam, thereafter they are pushed to SMTP server of the Bank.
* SIDBI has also enabled employees to access internal mails while on move through handheld devices (mobiles, tablets) for which Notes Traveler tool is deployed.
  1. **SMS facility**

SIDBI also subscribed to SMS facility wherein information about the dues is sent to the customers.

* 1. **End Computing Devices**

SIDBI has provided most of the users with laptops and few desktops. The laptops/desktops are installed with office automation software (MS Office), antivirus and basic utilities (winzip, acrobat reader etc.), citrix client etc. The operating system on laptops / desktops is Windows 7 and above.

* 1. **Video Conferencing**
* SIDBI has deployed video conferencing solution at all locations/offices. The solution is a mix of hardware/software based. The core infrastructure consists of Polycom DMA, RSS, MCU, RPAD, PRI gateway, Resource manager with software clients and Radvision Scopia Elite MCU. Endpoints are all of Polycom.
* The video conferencing is carried over existing WAN (no separate network for VC is implemented), Internet and PRI lines.
  1. **Security**
* The Security architecture deployed at DC and DR is two layer firewall architecture i.e. internal and perimeter.
* On the perimeter firewall different zones are created for hosting various web based applications, Mail server, VC firewall traversal device etc.
* On the core firewall different zones are created for hosting various application servers,
* Network Intrusion Prevention System (NIPS) is implemented at the perimeter and Antivirus software is implemented on all servers.
  1. **Syslog Server**

Bank has deployed syslog server to gather the logs of key network and security devices.

* 1. **SSL VPN**

To enable staff and customers access applications over Internet, SIDBI has deployed SSL VPN appliance at both Data Center and DR Site.

* 1. **Antivirus and Operating System Patches**
* Enterprise edition Antivirus is deployed at datacenter and clients loaded on all the servers and end computing devices. The antivirus definitions are updated periodically from the antivirus server hosted at datacenter.
* Further, WSUS server is installed in the datacenter and windows patches are periodically updated from the same to the servers.
  1. **Branch/Office**

All the branches are connected over MPLS VPN to Datacenter and DR Site. The local LAN is connected directly to the router. There is no security device/ appliance installed in the branches.

* 1. **Authentication**

Currently, Bank has two factor namely biometric authentication and password.

* 1. **Website**

SIDBI has its website hosted with third party. Content management is also carried out by separate vendor.

* 1. **Web Servers**

SIDBI has hosted few web servers & web applications in its datacenter which are used by internal users and external users.

* 1. **Connectivity Architecture**

The network and security architecture at Data Center and DR Site will be provided to the bidders at the time of pre-bid meeting, if required. If any bidder / vendor is not able to attend the pre-bid meeting, the required information with respect to the network and security architecture at Data Center and DR Site of Data Center and DR Site may be obtained in person on submission of an authorization letter.

* 1. **Business Applications**
* The application development, maintenance and support is done in-house or outsourced on need basis. Most of the legacy applications have been developed (or ported to) in Oracle forms 6i (Client-Server mode) and are being used with oracle 10g database. Few applications have been developed on Java platform. SIDBI has also purchased and implemented software for some specific operations, which use different technology. Few applications are deployed using .NET. Also some software has been developed using IBM Domino.
* The architecture is client-server architecture with the business logic distributed in the client as well as in the database stored procedures and triggers.
* All the applications have been deployed centrally at the Data Center using Citrix XenApp and Web Servers. Applications are accessed over WAN using Citrix web client or Internet browser. The client machines need to have Citrix web client and J- Initiator (Java utility) installed to access the applications. Most of the application servers are configured in load balancing mode. There is sufficient level of clustering build at the application level for Citrix and Web Application servers as well. The central deployment of the applications allows for easy deployment of the new releases and patches. Application access over internet is enabled for selected applications for few customers and Bank’s officers (on need basis), using Access Gateway.

# **Scope of Work**

The Scope of work for Cyber-Security Operation Centre (CSOC ) including but not limited to design, supply, configuration, implementation, customization, integrations, monitor, manage, backup, documentation, training, warranty support, post warranty maintenance support and any other activities related to or connected to the IT security, Security solutions, devices and technologies.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Location & CSOC Solutions** | **SIEM** | **PIM** | **Anti – APT** | **Firewall Analyzer** | **NAC** |
| **DC Site** | Yes | Yes | Yes | Yes | Yes |
| **DR Site** | Log collection device only | Yes (DR Readiness) | Yes | No | Yes (DR Readiness) |

# **Security Information and Event Management**

The SIEM solution is required to collect logs from network devices, servers, application security logs, Anti-virus, Proxy server, access control system, Security solutions like Anti-APT, PIM, SSL VPN Gateway, Firewall Analyzer, NAC Tool, VA tool etc. In addition, the logs being generated by the solutions deployed as part of the CSOC implementation need to be collected by the SIEM. The bidder should perform the following as part of the SIEM.

1. **Solution Implementation:**
2. Implement the SIEM tool to collect logs from the identified devices / applications / databases etc.
3. Provide and/or develop parsing rules for standard/ non-standard logs respectively.
4. Implement correlation rules based on out-of-box functionality of the SIEM solution and also based on the use-cases defined.
5. Inbuilt incident management and ticketing tool to generate tickets for the alert events generated by the SIEM or Separate tool which have capabilities of seamless integration. The tool should have feature to populate the relevant incident details from the alerts into the ticketing tool.
6. Build custom interfaces/ Connector for Applications. To begin with Bank will start with integration of critical applications. Bidders can be asked for integrating further more applications if found critical and required by bank.
7. While, it is expected that connectors for all the standard applications and devices will be readily available with the Bidder and connector for mostly in-house/custom built applications will need to be developed. Bidder team deployed for CSOC operations will be expected to develop connector for the custom built applications specifically developed for SIDBI.
8. The SIEM should be able to collect logs from the devices/applications/databases etc. mentioned by bank as per the Annexure 11.7 including the solutions deployed as part of this RFP. It should be able to collect the logs from devices from geographically dispersed locations.
9. The bidder should quote for Two (2) 60” Inch+ LEDs which will be used to display the configured correlation alerts maintained at the CSOC.
10. In addition, the bidder should quote for Four (4) desktops with dual VGA cards/ dual monitors and a minimum of 8 GB RAM and 1 TB HDD for the CSOC monitoring team with 3 Years warranty.
11. The logs collected by the SIEM log collector should be replicated across primary Data Center and Disaster Recovery location. The bidder will be responsible for providing P2P link for the log replication collected by SIEM log collectors across primary DC site and DR site. The sizing and requirement of all such links will be the responsibility of bidder.
12. The bidder should provide SIEM license for 10000 EPS from day 1.
13. Selected Bidder will customize incident management / dashboard / reports for the Bank and will modify the same as per the changing requirement of the Bank.
14. Bidder will also supply all the necessary Switches / cables / connectors / hardware /software etc. for integration of the components supplied for CSOC. Bank will supply only the Rack space, power and a network point in the Server room.
15. **Storage**
16. The SIEM should be able to maintain 3 months of logs on-box. In addition, the bidder should provide for near line storage i.e. secondary storage for archiving logs for up to 9 months and offline storage for storage of logs for up to 6 years. Total 7 years log must be available. The bidder is responsible for sizing the storage adequately based on the sustained EPS of 5,000 with 50% overload at the peak usage, scalable up to sustained level of 10,000 EPS.
17. Offsite storage facility is also required for additional 6 years in Tape Library with minimum of LTO 6.
18. The bidder is responsible for automated online replication of logs from DC to DR for redundancy. The solution should be capable of automatically moving the logs from device to archival storage based on the ageing of the logs. The storage should have “Write Once Read Many (WORM)” / Encryption/ Index and Search/ Retention and Disposal functionality. The storage should have the option to support backup on tape library. For DC-DR replication, the solution should also have the capabilities to replicate the logs in real-time and should have configuration for scheduled replication whenever required.
19. For Tape Backup/SAN required Tape and other Hardware should be provided by Bidder. Bank will provide the storage safe only to keep the Tape. The bidder will be responsible for tape movement securely to the offsite storage site.
20. The expected storage requirements is for 7 years. The bidder is expected to size the storage as per the requirements mentioned.
21. The bidder will have to make the archival logs available within 24 hours and live logs in real time of a request made by the bank. This request for retrieval of archival logs would be considered as a Medium Priority incident. If the bidder fails to provide the required logs within 24 hours, then penalties applicable for Medium Priority incidents would be levied.
22. The solution should also be scalable to expand storage based on the peak EPS requirement of bank. The bidder is expected to provide all supporting infrastructure for management of the storage devices such as SAN switches, controllers etc. and these are to be provided at the time implementation supporting the maximum scalability as defined above.
23. **Log collection**

Logs from all the in-scope devices and additional devices integrated as part of contract period located at the geographically dispersed location should be collected. Bidder / Vendor 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. Only in case where remote log collection is not feasible, bidder / vendor should install agent on the servers and applications for collection of logs. Raw logs should be made available in case of legal requirement.

1. **Log correlation**

Collected Logs should be correlated according to various predefined criteria for generation of alert and identification of the incident. The correlation rules should be predefined and also user configurable. Correlation rules should be customized by the bidder on 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.

1. **Alert generation**

Solution should be capable to generate alerts, register and send/receive the same through message formats like SMTP, SMS, Syslog, and SNMP as per user configurable parameters.

1. **Event viewer / dashboard / reports / incident management**

SIEM Solution should provide web based facility to view security events and security posture of the Bank’s Network and register incidents. Solution should have drill down capability to view deep inside the attack and analyze the attack pattern. Dash board 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 ISO27001, IT Act and regulatory reports. Selected bidder will customize incident management / dashboard / reports for the Bank and will modify the same as per the changing requirement of the Bank.

1. **Incident management tool**
2. The principal goal of the incident management process is to identify anomalous activities in the environment, contain those events and restore normal service operation as quickly as possible and minimize adverse impact on business operations, thus facilitating continued service quality and availability.
3. Solution should be able to register any security event and generate trouble ticket.
4. Solution should provide complete life cycle management (work flow) of trouble tickets from incident generation till closure of the incident.
5. Solution should also provide a detailed process for managing incidents - describing each phases of the process – prepare, identify, contain, eradicate/remediate, recover and learn from the incidents responded to.
6. Solution should provide the logging facility to different levels of users to   
   monitor and manage the incidents generated for closure of the same as per the defined workflow.
7. Solution should be able to integrate with different tools such as SIEM tool, Vulnerability Management tool etc. Incident management should include escalation as per the escalation matrix. However, it is preferred that the SIEM should have an inbuilt integrated incident management tool.
8. Detected incidents - Upon receiving an incident record identified by the Bank, a Bidder's Security Engineer is assigned to proceed with incident diagnosis and troubleshooting.
9. Notifications - The Notification Matrix defines the Bank's contacts, the incident management process step (initial, diagnose, update and resolve), the method (telephone, mobile, SMS, email) and hours (business hours or after hours). The Notification Matrix shall be customizable as per configuration item.
10. Develop workflow for incident management tool and be responsible for end to end incident management lifecycle.

The detailed Technical Specifications are furnished in Annexure 11.1

# **Privilege Identity Management (PIM)**

SIDBI intends to implement a Privileged Identity Management solution to protect, monitor, detect, alert and respond to privilege account escalation activity.

* Bidder should deploy PIM solution for the identified devices/servers etc.
* Bidder should deploy PIM solution for the identified administrators/users.
* Bidder should integrate PIM solution with proposed SIEM solution
* Bidder should implement PIM solution with DR readiness in active passive mode

A privileged identity management technology needs to accommodate for the special needs of privileged accounts, including their provisioning and life cycle management, authentication, authorization, password management, auditing, and access controls.

The detailed Technical Specifications are furnished in Annexure 11.2

# **Anti-Advance Persistent Threat (APT)**

SIDBI intends to implement Anti - APT solution to protect its network from known, unknown and zero day malware.

1. Bidder should install and configure Anti - APT solution to protect against web and email attacks.
2. Bidder should suggest required changes to be done to integrate Anti - APT solution to integrate with existing infrastructure
3. Bidder should integrate Anti - APT solution with proposed SIEM solution.
4. This service will help Organization mitigate the website related risks on continuous basis. The service will include:
   * 24X7 malware scanning of incoming network traffic (website, e-mail, etc.)
   * Coordinate rapid response
   * Forensics analysis

Bidder should provide an online solution for malware scanning at the network and email gateway/server level. Bidder should bring the required tools, processes and methodologies. Bidder proposals should capture process & methodology to offer these services, tool description, sample service output (report formats), experience with similar environments.

The detailed Technical Specifications are furnished in Annexure 11.3

# **Firewall Analyzer**

SIDBI intends to have Firewall Analysis to analyze and optimize policies/configuration of its multiple firewalls currently installed at DC & DR.

* 1. Bidder should analyze firewall configuration/policies based on best practices
  2. Bidder should provide detailed reports of the analysis
  3. Bidder should provide recommendation to optimize firewall configuration/ policies
  4. Bidder should execute this service on monthly basis / whenever required due to changes in network / system configuration

Firewall Analyzer should deliver visibility and analysis of firewalls and complex network security policies across on premise. It should automate and simplify security operations including troubleshooting, auditing and risk analysis. Firewall Analyzer should help in optimizing the configuration of firewalls, routers, web proxies and related network infrastructure to ensure security and compliance.

The detailed Technical Specifications are furnished in Annexure 11.4.

# **Network Access Control (NAC)**

The Bank intends to procure a Network Access Control solution which is an automated security control platform to monitor and control access on the network—all devices, all operating systems, all applications, all users. The solution shall let employees and guests remain productive on the network while critical network resources and sensitive data remain protected. The solution shall be easy to install, manage, configure and upgrade.

1. Bidder should install and configure NAC solution such as only authorized and compliant devices to access and operate on Bank’s network.
2. Bidder should design NAC solution such that bank does not need to re-architecture of the network.
3. Bidder should consider both wired and wireless users for NAC implementation.
4. Bidder should perform any OS upgrade on the network switches if required.
5. Bidder should integrate NAC solution with proposed SIEM solution.
6. Bidder should implement NAC solution with DR readiness in active passive mode
7. NAC shall provide following:

* Visibility into user identities and device types
* Guest user self-enrollment
* Easy access to wired networks and WPA2 secure wireless (when implemented)
* Real-time policy assessment
* Dynamic role-based enforcement
* Guided Self-Remediation Process

1. The Bidder is required to design & size the NAC solution. Currently Bank has approximately 1600 devices including laptops, desktops etc. which needs to be covered in this solution. The Bank envisages the increase in the number of such devices to 2000 during the next 3 years. The bidders proposed solution shall be sized to meet the 3 year requirement.
2. The Bank has offices at around 80 locations in addition to the DC and DR. Each of these locations has one or two Cisco router(s) & one / more manageable switches. The switches are of heterogeneous make with majority of them being HP/Aruba. Further, Bank has placed order for implementation of SD-WAN based IP MPLS network. The routers at the locations will be replaced with SD-WAN CPEs. The proposed solution should be able to capture logs from the CPE’s installed at the locations. The Bidder’s proposed solution shall meet the Bank's requirement as described and should support heterogeneous environments till the end of contract period.
3. Regarding NAC integration, the bidder has to ensure implementation of solution at all offices of the Bank with the support of Bank's IT Facility Management support, However, for UAT acceptance of all the solutions, the acceptance would be based on mutually accepted criteria between Bank / Bank appointed Consultant and the bidder.

The detailed Technical Specifications are furnished in Annexure 11.5.

# **VAPT Information and Remediation Services**

SIDBI intends to have Vulnerability Assessment as a service for its critical devices installed at DC & DR and perform Penetration Testing for servers hosted over Internet.

1. Bidder should provide vulnerability assessment services for mentioned devices/servers.
2. Bidder should perform penetration testing for servers hosted over Internet
3. Bidder should provide detailed reports of the assessment
4. Bidder should execute this service on quarterly basis

The vendor should carry out Vulnerability Assessment and Penetration testing both internal and external using required software/technical tools for assessing bank’s network **on quarterly basis.** The Bidder is to bring his own VAPT tools for testing purpose and obtain required approval for conducting the same. The bidder should provider advisory-cum-remediation services for the Vulnerabilities/Risks detected. The broad scope of work is given below.

1. The provider shall conduct a detailed study of the existing vulnerability reports and also conduct internal VAPT tests, understanding the background IT infrastructure in the Bank.
2. Provide steps for fixing the vulnerabilities and/or suggest Bank’s team of compensating controls that needs to be implemented in order to remediate /circumvent the vulnerability.
3. Upon getting Bank team’s concurrence, proceed with production resolution.
4. In the case of application dependencies, the details shall be provided and compensating controls suggested, wherever possible.

The detailed Technical Specifications are furnished in Annexure 11.6.

# **Security/Threat Intelligence Services**

Bank intends to have a system for tracking of new and emerging threats & vulnerabilities affecting organization across the world so that bank can proactively protect against them.

Bidder should track and provide information on global security threats and help the Bank to mitigate the relevant risks on continuous and proactive basis.

The service will include:-

1. 24\*7\*365 - Continuous tracking of global threats and vulnerabilities to tackle evolving threats and vulnerabilities.
2. Provide trusted detailed reports on newly discovered malicious threats and malware in the wild.
3. Detail the threat with the information appropriate to the Bank such as:
4. The threat type
5. Risk involved
6. Systems affected
7. Technical description of the threat and exploit parameters.
8. Mitigation strategies and the recommendations for the Bank to prevent the threat from causing harm to the environment.
9. Infiltration of malicious hackers and other communities.
10. Monitoring of network activities and discern risks to the Bank environment.
11. Advisories to the Bank on relevant threats and vulnerabilities.
12. The intelligence content should be able to look at the goals of the threat actor, variants of the threat, current activities implicating the threat, the outcomes for the Bank if the threat is successful as well as provide defense against the threat.
13. Track mitigation against identified risk exposure.
14. Assists the Bank to ensure such threats and vulnerabilities are mitigated in the Bank’s systems and Provide from the short term plans to the very long term strategies.
15. Assist the Bank in taking relevant decisions Assessment of inherent and residual risk, preferably expressed as impact on business processes, rather than the underlying technology.
16. The intelligence content should focus more on technical attacks against infrastructure.
17. The bidder shall be able to provide Integrated Threat Intelligence Feeds from partners and communities (acceptable to the Bank) as well as from IB-CART, NCIIPC, CERT-IN, NPCI etc. and shall be able to take advantage of this knowledge to address the threat, preferably using automated tooling standard format such as STIX.

# **Other General Requirement**

# **Hardware, Software and Network Connectivity**

1. The bidder needs to provide all the hardware and software required as part of this RFP.
2. The sizing of the infrastructure as proposed by the bidder, should be certified by the OEM.
3. The bidder shall ensure that the hardware proposed does not reach end of life (EOL) and end of support (EOS) during the contract period of three years plus addition of two year post completion of the contract.
4. None of the tools/software/utilities/solutions proposed should be Open Source. Any bid submitted with Open Source tools/software/utilities/solutions will be rejected.
5. The bidder needs to propose only Veritas backup solution for backups.
6. The bidder will be given the rack space and connectivity between DC and DR by the bank, all other necessary hardware and peripherals are to be provided by the bidder. Details of such hardware has to be given in the Commercial and Technical Bid Annexures.
7. There should be three separate environments: Development, Test (UAT), and Production (DC-DR). The environments must be configured on a separate physical servers. The Development environment should have at least 20% and Test (UAT) environments should have at least 50% of the configuration of the Production environment quoted by the Bidder.
8. Bidder should consider sizing as part of integration of additional devices during the contract period. SIDBI will not be responsible to pay for any additional cost other than the cost mentioned in commercial bid.
9. The network connectivity between SIDBI offices, Data Centre site and Disaster Recovery Site will be provided by the bank. The bidder will be responsible for any other network connectivity required for CSOC operations and P2P link for replication of logs of SIEM collectors in DC and DR.

# **Training**

1. **Pre-Implementation:** Provide training to the bank personnel/ SOC team on the product architecture, functionality and the design for each solution under the scope of this RFP.
2. **Post Implementation:** Provide hands-on training to the bank personnel/ SOC team on SIEM operations, alert monitoring, policy configuration for all solutions etc.
3. The bidder and OEM are required to provide training jointly as per the below table for people nominated by the bank for each solution specified in the scope of work.
4. The bidder and OEM are required to provide ad-hoc trainings to the bank staff, to acquaint them with the latest features and functionalities of the solutions for minimum of one day. Bank has the right to exercise this training option at its discretion. The cost of this training would need to be quoted in the Commercial Bid by the bidder in the pre-defined field.
5. The bidder is required to provide all trainees with detailed training material and 2 additional copies to the bank for each solution as per the scope of work of the bank. This training material should cover installation, operation, integration, maintenance, troubleshooting and other necessary areas for each solution.
6. All out of pocket expenses related to training shall be borne by the selected bidder.
7. The bidder may utilize the OEM resources in case the bidder does not have adequately experienced resources for providing training.

|  |  |  |
| --- | --- | --- |
| **Solution** | **Training Time** | |
| **Pre-Implementation (Days)** | **Post-Implementation (Days)** |
| SIEM | 3 | 5 |
| Anti-APT | 1 | 2 |
| PIM | 1 | 2 |
| Firewall Analyzer | 1 | 1 |
| NAC | 1 | 1 |
| VAPT Information and Remediation Services | 1 | 1 |
| Security/Threat Intelligence Services | 1 | 1 |

# **Implementation & Integration**

The implementation should cover the technical features as mentioned in Annexure 11.1 to 11.6.

1. Implementation should comply with the SIDBI Information Security Policy, SIDBI Cyber Security Policy and RBI Guidelines such as Cyber Security Guidelines, Gopal Krishna Committee guidelines, Localization of Payment Storage guidelines etc. and as specified from time to time.
2. The solution, service, hardware, software and storage services would be provided by the bidder. The Bank will provide facilities to host the devices and office arrangement for the personnel.
3. A comprehensive strategy should be provided by the Bidder on implementing the end to end CSOC solution within 7 days of issuance of Purchase Order (PO).
4. Once the purchase order (PO) is issued, the successful bidder is required to review the bank environment and specify any additional requirements that the banks may need to provide for the implementation of the solution.
5. Bidder has to develop the project plan, get it approved by the Bank and then implement the project based on timelines agreed.
6. The bidder is responsible to ensure that the CSOC solutions and operations comply with industry leading standards (such as ISO 27001, ISO 22301, PCI DSS, Privacy Laws and Regulations etc.) and any applicable laws and regulations such as RBI Guidelines during the contract period.
7. A comprehensive onsite warranty for a period of 3 years and additional AMC cost for 4th and 5th year shall be there on all the Hardware and Software supplied to/purchased by the Bank.
8. The bidders needs to provide warranty for entire 3 years at the start of contract period and warranty period will commence from the acceptance date of phase-1 UAT signoff from Bank.
9. In addition, the bidder is responsible for impact assessment and modification of SOC operations at no extra cost, on account of any changes to applicable information security policies/ procedures / standards/ regulations. Bidder should consider sizing as part of integration of additional devices during the contract period. SIDBI will not be responsible to pay for any further hardware cost.
10. The bidder would be responsible for updates, patches, bug fixes, version upgrades for the entire infrastructure. SIDBI will not be responsible to pay for any additional cost required as part of additional capacity required.
11. The Bidder should provide the latest version of the Solution. The bidder would be responsible for replacing the out-of-support, out-of-service, end-of-life, undersized, infrastructure elements at no extra cost to the bank during the contract period. Replacement to be done before 15 days from due of date of the product/service.
12. The support for all the solutions proposed should be provided for the contract period. Whereas free upgrade should be provided for all solutions if the end of life occurs within the period of contract with bank. The Updates/ Upgrades for medium and low should be implemented within 3 months of release of the same. For critical and high upgrades / updates, implementation to be implemented within 1 months of release.
13. All the solutions supplied as part of this RFP should be supplied with Enterprise wide License. The licenses should be perpetual from the first day with no dependence on payment quoted in the commercial bid and Bank wants the licenses to continue to be an integral asset of the Bank in perpetuity.
14. Integrate each solution with SIEM solution to provide a single view of events generated.
15. Bidder is responsible for developing and implementing the security configuration hardening of all the devices and software that are procured for Security Operations centre. Also, they have to periodically review the guidelines and configure as and when required.
16. Any interfaces required with existing applications/ infrastructure within the bank should be developed by the bidder for successful implementation of the CSOC as per the defined scope of bank.
17. Bidder shall be responsible for timely compliance of all Device level audit (DLA) and Vulnerability Assessment (VA) audit observations as and when shared by the bank.
18. In case the CSOC on-going operations are part of scope for a particular bank, the bidder is responsible for integrating any additional logs that the bank may wish to monitor with the SIEM solution at no additional cost to the bank.
19. The primary responsibility of integration of new solutions with implemented SIEM lies with the Bidder selected through this RFP.
20. Development and implementation of processes for management and operation of the CSOC including (but not limited to) the following processes:
    1. Configuration and Change Management
    2. Incident and Escalation management processes
    3. Daily standard operating procedures
    4. Training procedures and material
    5. Reporting metrics and continuous improvement procedures
    6. Data retention and disposal procedures
    7. BCP and DR plan and procedures for CSOC
    8. Security Patch management procedure
21. Implement necessary security measures for ensuring the information and cyber security of the proposed CSOC. This should also be in line with RBI Guidelines.
22. Develop Escalation Matrix in order to handle Information and cyber Security Incidents efficiently.
23. Provide necessary documentation including Standard Operating Procedures (SOPs), user manuals, SRS document, Design document, Architecture diagram, etc. for the operation, integration, customization, and training of each of the solutions in scope.
24. The Bidder would be responsible for installation, testing, commissioning, configuring, warranty and maintenance of the system. The bidder will also provide necessary support and coordination for conducting BCP/DR drill and testing as per SIDBI BCM and IT security policy.
25. In case a device goes down at DC, the operation and function being performed by the device should be taken over by a corresponding device at DR site and vice versa.
26. OEM would be responsible for all technical support to maintain the required uptime through the Bidder. Initial installation, configuration and integration should be done by the OEM, through the Bidder. The Bidder would be the single point of contact. The Bidder should have necessary agreement with the OEM for all the required onsite support for entire project period. Bidder should have back-to-back support with OEM during the total contract period for necessary support. OEM should review and certify the successful implementation.
27. All the tools supplied as part of this RFP should be supplied with Enterprise wide License and the licenses should be perpetual from the first day with no dependence on payment. 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, 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.
28. Bidder shall provide list of licenses to be procured, also maintain the inventory database of all the licenses and the updates installed. Also, the licenses should be in the name of Bank.
29. The period of support coverage would be for the entire contract period.
30. Bidder should provide utilization details that can affect the existing IT infrastructure.
31. Adherence to agreed Service Level Agreements (SLA) and periodic monitoring and reporting of the same to the bank through a portal.
32. The bidder needs to ensure that CSOC solution can integrate with the IT System and applications using standard methods/ protocols/ message formats for capturing logs, alerts and for monitoring purposes. No changes should be proposed to SIDBI in existing applications and system by bidder.
33. CSOC setup / infrastructure may be subjected to audit from Bank and/or third party and/or regulatory body. It shall be responsibility of the Bidder to co-operate and provide necessary information and support to the auditors. The Bidder must ensure that the audit observations are closed on top priority and to the satisfaction of the Bank, regulator and its appointed auditors. Extreme care should be taken by the Bidder to ensure that the observations do not get repeated in subsequent audits. Such non-compliance by Bidder shall attract penalty.
34. CSOC set up should assure the compliance to the Indian regulatory requirements, ISO27001 standards and also international regulations and laws where bank has its presence. The bidder is expected to study the regulations and comply with them as and when mandated.

# **Reporting**

1. The bidder should provide periodic reports to the Bank as per the following requirements:
   * 1. Daily Reports: Critical reports should be submitted by 11:00 AM
     2. Weekly Reports: By 11:00 AM, Monday
     3. Monthly Reports: 3rd working day of each month
2. The following list captures a few of the reports which will be provided by the selected Bidder once on boarded. The bidder is expected to detail every report which it will provide to the Bank related to the services and activities performed by it in the CSOC:
   * 1. Solution design documents for each solution designed for the Bank’s environment
     2. Implementation guide for the solutions implemented at the Bank’s premises
     3. Operations guide for all the solutions managed by the Bidder
     4. Incident management playbook which will govern the process followed for handling of incidents as per the defined incident types and the severity
     5. Weekly and monthly incident tracker and statistics capturing detailed information on the incident identified, its severity, the response by the team, the time taken from identification till closure of the incident and other relevant information
     6. Periodic reporting and status tracking / capturing the details of the log sources reporting to the SIEM manager
     7. Periodic reports capturing the incidents notified by the SIEM solution
     8. Periodic reports capturing the malwares detected and / or prevented by the anti-malware solution.
     9. Periodic reports capturing the phishing attempts detected and / or prevented by the anti-phishing solution.

# **System Integration Testing (SIT) and User Acceptance Testing (UAT)**

1. There will be a User Acceptance Testing by the Bank for the tools deployed and CSOC operations.
2. The Bank shall commence the User Acceptance Testing as and when each and every solution and services are made ready by the Bidder and a formal confirmation that the system is ready for UAT is submitted to the bank. The results thereafter will be jointly analyzed by all concerned parties.
3. UAT will cover acceptance testing of all the product/services, integration with CSOC tools (Primarily SIEM) and integration of CSOC with all targeted devices/systems.
4. The Bidder is expected to make all necessary modifications to CSOC solution including customizations, interfaces, appliances, software etc., if there are performance issues and errors identified by the Bank. These deviations/ discrepancies/ errors observed will have to be resolved by the Bidder immediately.
5. Complete acceptance has to adhere to the stipulated time lines.
6. The Bank will accept the solution on satisfactory completion of the above inspection. The contract tenure for the Solution will commence after acceptance of the solution by the Bank.
7. In case of discrepancy in facilities /services provided, the Bank reserves the right to cancel the entire contract.

# **Monitoring**

The bidder is required to provide the resource count for the operations of the CSOC as a part of the response to this RFP and specify the same in the Annexure 11.8 Resource Requirement Details. The bidder should monitor CSOC activities and events from each solution and devices already present in the bank’s environment on a 12\*6 basis (8 am to 8 pm) basis and suggest/ take appropriate action on an on-going basis.

|  |  |
| --- | --- |
| **Type** | **Role** |
|
| L1 | * Event monitoring & alert/Incident tracking; regular solution administration. * Fine tuning of the false positive events * Categorization of requests into functional clarification and provision of workaround * Bug identification/change requests to be logged and reported for further processing * Provide telephonic and / or electronic mechanisms for problem reporting requests as well as for service and status updates * Preparation of incident reports |
| L2 | * Provide continuous onsite support for the implementation of CSOC solution and support for integrating any applications to be interfaced with SIEM solution in future. * Troubleshoot at various levels in the CSOC Solution implementation * Resolve the call within stipulated timeframe as defined in Service Level Agreement * Coordinate with the L1 & L3 team for resolution and provide necessary information as may be required by the team to resolve the issues. Escalate the unresolved calls as per escalation matrix * Provide the timeframe for providing a solution of resolution of the escalated calls and automatically log calls during escalation * Prepare a root cause analysis document with the resolutions provided for major issues such as production issues, service disruptions or downtime, delayed response times, data/ table corruptions, system performance issues (high utilization levels) etc. * Perform the application audit on a quarterly basis or as mutually agreed with the bank and rectify any corruption in the software * Ensure patch releases are ported to the production environment with no business disruption or business losses * Support periodic BCP/DR drills * Routing the events through the backup system in case the primary system fails * Providing bank with daily hardware utilization reports and alerting BANK in case of any performance issues or hardware upgradation requirements * Preparation of incident reports and periodic reporting of critical incidents to management team of bank |
| L3 | * Resolve the call within the stipulated timeframe as defined under the service level agreements * Communicate the status of the call to the Bank and accordingly update the status, resolution or workaround and date of resolution * Prepare a root cause analysis document for issues referred to L3 support and provide to the Bank along with the resolution * Liaise with the L2 support personnel for the call information and resolution. * Perform version upgrades/migration as per the version release plan of OEM and agreed by the Bank. * Provide training to the Bank’s team on CSOC solution and new version functionalities |
| DC Operator (System Administrator) | * Managing and administrating entire infrastructure (server, storage, network devices, etc.) of CSOC operations at DC Site, Navi Mumbai |

* Bank reserves the right to conduct interviews of the proposed team members for CSOC operations.
* The CSOC operations and monitoring will be carried out from Chennai location during the contract period. However, bidder needs to deploy one dedicated resource at DC site, Navi Mumbai.
* L3 resource should assist Bank in governance of security event monitoring and incident/alert tracking and assist bank to comply compliance with RBI Guidelines and Indian Cyber Regulations.
* L3 resource should be present onsite for monitoring and operational activities and should act as team leader.
* In case of absence of a lower level resource, a higher level resource should perform the job of the absentee but the payment will be made as per the payment structure of lower level resource only.
* If any resource is absent, standby resources should be available. Bank may reject such manpower if Bank is not satisfied with his/her performance and payment will be made to bidder as per actual manpower support provided subject to adherence to SLA conditions.
* In case of resource replacement, bidder shall ensure proper Knowledge Transfer (KT) / handover is provided to new resource.
* Per Man Day Charges (to accommodate deduction on account of absence) = Charges per Man Year/ (12 x No. of working days in a Month).

# **Continuous Improvement**

1. Improve the policies configured on an on-going basis to reduce the occurrence of false positives.
2. Periodic health check should be carried out on-site, by the OEM every year to ensure the quality of implementation and operations.
3. Bidder shall curtail the closure time for incidents and events, also ensure the periodic check-up reviews for the same.
4. Bidder needs to update all solutions and Cyber Security Operations Centre (CSOC) based on any new regulations and RBI guidelines

# **SLA Compliance**

The bidder shall ensure compliance with SLAs as defined in the section 7 of RFP.

# **Business continuity**

The bidder is responsible for defining a DR/ BCP plan for the CSOC operations and also ensure that periodic tests are conducted as per the testing calendar agreed with the bank.

# **Period of Contract**

1. Bidder is required to provide the services for a period of 3 years extendable for a further duration of maximum two years at the discretion of the Bank on the same terms and conditions.
2. Post completion of the contract/ or in the event of early termination, the bidder is expected to provide support for transition of the services to the nominated members of the bank (or) to a third party nominated by the bank for a period of 6 months.
3. The Bidder is required to provide the warranty / AMC services at Bank’s DC / DR and other locations for which tools are procured or where tools are deployed, directly or through their OEM representatives at all locations for bank.
4. The bidders are expected to provide technical and commercial proposals in accordance with the terms and conditions contained herein. Evaluation criteria, evaluation of the responses to the RFP and subsequent selection of the successful bidder shall be as per the process defined in this RFP. Their decision shall be final and no correspondence about the decision shall be entertained.
5. In case of termination of contract / end of contract period, bidder has to provide extended services, with the rates mentioned as of last year. This extension of services to be provided till procurement of next solution / till 1 year, with same terms and conditions.
6. If any support is required after the contract w.r.t. to logs, the bidder has to provide the same.
7. Bidder shall provide transition support, which amongst other shall include provision of logs, rules, technical architecture of solution as deployed, detailed description of the processes, etc. as part of the transition to subsequent bidder or bank on completion or on termination of contract. The support will be for a period of 6 months.

# **Implementation Phases and Timelines**

All hardware and software components supplied under the scope must be implemented as per project timeline. Implementation of various solutions will be done in phased manner as per following details:

* 1. **Phase 1 -** Implementation of SIEM and integration of SIEM with other security tools (PIM, NAC, Firewall Analyzer and Anti-APT) and UAT signoff as per UAT signoff criteria. **The UAT signoff criteria will be defined as:**

1. NAC: Integration of NAC on around 100 end user devices.
2. PIM: Integration of 50 servers (all privilege users) with PIM
3. Firewall Analyzer: Integration of 10 firewalls with Firewall Analyzer
4. Anti-APT: Integration of web proxy server and email server with Anti-APT
   1. **Phase 2 –** Integration of Bank's remaining in-scope devices with SIEM and other security tools.

The project signoff for SIEM, PIM and NAC will be given post integration of 95% of total devices/users mentioned in Annexure 11.7. However, the bidder is responsible for integration of all devices/users.

|  |  |  |
| --- | --- | --- |
| **Stage** | **Activity** | **Time Period for Completion** |
| 1 | * 1. Submission of Detailed Project Plan   2. Placing of order with OEMs for supply of hardware, software security tools/solutions   3. Placing of order for connectivity link (if any) | 2 weeks from acceptance of PO |
| 2 | * 1. Preparation for CSOC setup and implementation of required processes.   2. Commissioning of link | 3 weeks from acceptance of PO |
| 3 | Pre-Implementation Training for the Bank Team | 4 weeks from acceptance of PO |
| 4 | Delivery of CSOC Hardware / Software and licenses and resources | 4 - 6 weeks from acceptance of PO |
| 5 | Deployment of CSOC Resources at Bank’s premises | 6 weeks from acceptance of PO |
| 6 | Installation & Configuration of SIEM and other Security Tools / Solutions | 8 weeks from acceptance of PO |
| 7 | Integration of SIEM with other Security Tools / Solutions under CSOC | 11 weeks from acceptance of PO |
| 8 | User Acceptance Test (UAT) and making the CSOC operational | 14 weeks from acceptance of PO |

The entire project needs to be completed as per the time schedules mentioned above. The selected bidder should nominate a Project Manager immediately on acceptance of the order, who shall be the single point of contact for the project. However, for escalation purpose, the escalation matrix to be provided. The Project Manager nominated by the bidder should have prior experience of 5 years in implementing similar project and should have at least one out of the following certification: ISO 27001 LA / ISO 27001 LI / CISA / CISSP / CISM / PMP. The Project Manager should not be changed without the consent/approval of the bank and should not be changed frequently as this affect the implementation of the project. Project Kick-Off meeting should happen within 7 days from the date of acceptance of purchase order. The Bidder shall submit a Weekly progress report to the Bank on the progress in installation / commissioning of the solution as per format, which will be made available to the selected bidder.

# **Evaluation Methodology**

The objective of this evaluation methodology is to facilitate the selection of one successful bidder fulfilling selection criteria and providing professional services at optimal cost.

The selected bidder will be entrusted with end-to-end responsibility of management of Implementation and Management of Cyber Security Operations Center (CSOC) for the period of three (03) years which can be extended for a further duration of maximum two years at the discretion of the Bank.

# **Pre-Qualification Criteria**

1. Only those Bidders who fulfil the Pre-Qualification Criteria for Bidder as mentioned in Annexure 8.2 are eligible to submit response to this RFP.
2. The Bidder is required to provide factually correct responses to the RFP. Adequate justification for the response (including the technical and other requirements) should be provided as part of the response. In case the Bank finds any response to be inadequate, the Bank has the right to ask for additional explanation/ justification. In the event of any discrepancy in the response submitted by the Bidder, the Bank reserves the right to disqualify/ blacklist the Bidder and the OEM.
3. The Bank reserves the right to change or relax the eligibility criteria to ensure inclusivity.
4. The Bank reserves the right to verify/evaluate the claims made by the Bidder independently. Any deliberate misrepresentation will entail rejection of the offer.

# **Technical Evaluation**

1. Only those Bidders who qualify as per the Pre-Qualification Criteria of Bidder (Annexure 8.2) will be considered for further Evaluation. Bids which do not qualify will not be considered for further evaluation.
2. The Technical Evaluation shall be performed first to identify the list of technically qualified Bidders as per the Technical Evaluation criteria defined in the RFP. Each Bidder shall be assigned a technical score (T).
3. Commercial Bid will be opened only for those Bidders who score minimum of 80% in Technical Evaluation (RSTech)
4. In case during Technical Evaluation, if less than three bidders fails to score 80% marks (RSTech), SIDBI reserves the right to shortlist maximum three bidders subject to 75% marks (RSTech). The decision of the Bank in this regard shall be final.
5. The technical offer submitted by the Bidders shall be evaluated as per various parameters mentioned below:

|  |  |  |
| --- | --- | --- |
| **S. No.** | **Technical Evaluation Parameters** | **Weightage** |
| A | Technical Requirements as per Annexure 11.1 to Annexure 11.6 | 60% |
| B | Demo of proposed solutions for use cases and Presentation covering Approach, Methodology, Timelines and Proposed Team for Implementation | 10% |
| C | Client Feedback | 15% |
| D | Number of employees having certifications such as ISO 27001 LA / ISO 27001 LI / CISA / CISSP / CISM | 15% |
| **Total** | | 100 |

1. **Scoring for Technical Requirement (TR)**
2. The proposed solution is expected to comply with the all requirements as mentioned in the Annexure 11.1 to 11.6 Technical Requirements.
3. The Bidder should use Bidder’s ‘Compliance’ column to provide the appropriate response for all the requirements mentioned in Annexure 11.1 to 11.6.
4. The Bidder can use the ‘Remarks’ column to provide an explanation as to how the requirement would be met by their solutions and also provide sufficient documents supporting the same such as product manual, datasheets, independent product review reports.
5. The Bidder needs to submit an undertaking / self-declaration stating their compliance to the features and requirements as mentioned in Annexure 8.5.
6. The bidders are expected to comply at least 90% of the technical requirements for technical evaluation.
7. The bidders will be allocated marks as per the following:
8. Technical requirements in Annexure 11.1 to 11.6 are categorized into High Priority (PH) requirements and Low Priority (PL) Requirements.
9. High Priority (PH): 2 marks will be awarded for compliance of each High Priority requirement. All proposed solutions are expected to obtain at least 90% of the maximum score for the High Priority requirements. In the event the Bidder scores less than the minimum qualification criteria, the bid shall be disqualified and will not be considered for commercial evaluation.
10. Low Priority (PL) Requirements: 1 mark will be awarded for compliance of each Low Priority requirement for each solution.

|  |  |  |  |
| --- | --- | --- | --- |
| **Technical Requirements** | **Number of High Priority (PH)** | **Number of Low Priority (PL)** | **Maximum Possible Score [(PH \*2) + (PL \*1)]** |
| Anti-APT | 72 | 0 | 144 |
| Firewall Analyzer | 32 | 1 | 65 |
| NAC | 27 | 3 | 57 |
| PIM | 93 | 4 | 190 |
| SIEM | 133 | 7 | 273 |
| VAPT | 30 | 3 | 63 |
| Total (TR) | | | 792 |

**Weighted TR = [(Bidder TR Score) / (Total TR)] \* 60**

1. **Scoring for Demo and Presentation Exercise (TD)**
2. Use cases for the CSOC solution similar to those mentioned in Annexure 11.1 to 11.6 will be tested and verified in the Demo. The date of the Demo and Bidder presentation, timelines, the final list of use cases, and locations for testing will be shared with all qualified Bidders.
3. The Demo and presentation would be rated by the Bank and scores would be assigned to each demo and presentation.
4. The bidder can demonstrate the use cases for proposed solutions either in live environment or through WebEx simulated own sandbox / test environment.
5. The qualified Bidders shall be invited to the Bank to deliver a demo and presentation for maximum of 120 minutes on the solutions that are proposed.
6. Score for the demo and presentation exercise will be awarded to the bidder as per the following:
   * + Proposed Architecture for CSOC
     + Approach for implementation for all solutions and services
     + Proposed Project Plan
     + Resources and Team Structure
     + Demonstration of use cases
   1. Maximum of 50 marks will be awarded to the bidder for demo of the proposed solutions and presentation exercise
   2. The total marks gained by the bidder will get normalized to the score of 10.

**Weighted TD = [(Bidder TD Score) / (Maximum TD score=50)] \* 10**

1. **Scoring for Client Feedback (TF)**
2. The Bidders are requested to fill detailed information on past implementations / engagements for all the solutions as per below format.

|  |  |
| --- | --- |
| **Organization Name** |  |
| **Contact Details** | Name:  Designation:  Mobile:  Email: |
| **Implemented Solution (Name & Version Details)** |  |
| **Implementation Scope** |  |
| **Implementation Timelines (months from PO release date)** |  |

1. The details provided should be verifiable.
2. The Bidders should provide documentary evidence highlighting the details of the past experience specified by the Bidder in the response.
3. Score for the feedback exercise will be awarded as per the following:
   1. The bidder will be awarded a maximum of 10 marks for each feedback.
   2. The score will be awarded as per following:

|  |  |  |  |
| --- | --- | --- | --- |
| **Parameters** | **Maximum Score** | **Client Feedback 1** | **Client Feedback 2** |
| Scope of Implementation | 2 |  |  |
| Quality of Resources | 2 |  |  |
| OEM Support and Customization | 2 |  |  |
| Implementation Timelines | 2 |  |  |
| Any breach in SLA | 2 |  |  |
| Total | |  |  |

1. The total marks gained by the bidder will get normalized to the score of 15.

**Weighted TF = [(Score of Client Feedback 1 + Score of Client Feedback 2)/20]\*15**

1. **Scoring for Resources having required Certification (TC)**
   1. The bidder is required to provide certifications of employees on permanent payroll having ISO 27001 LI/LA or CISA or CISSP or CISM.
   2. Resources with multiple certificates shall be counted once only.
   3. The bidder will be awarded a maximum of 15 marks as per the following:

|  |  |  |
| --- | --- | --- |
| S. No. | Parameter | Marks |
| 1 | Minimum of 10 employees | 5 |
| 2 | More than 10 and less than or equal to 20 employees | 10 |
| 3 | More than 20 employees | 15 |

1. **Final Calculation of Technical Score (T)**
   1. The total technical score of the bidder will be calculated as following:

**Technical Score (T) = TR + TD + TF + TC**

* 1. Relative Technical Score (RSTech) for each bidder will be calculated as follows

**RSTech = (T/ THigh) \* 100**

Where:

RSTech = Relative score obtained by the bidder

T = Technical score obtained by the bidder

THigh = Highest Technical score secured among the bidders

# **Commercial Evaluation of the Bidders**

1. The Bidders are required to submit Commercial Bid as per Annexure 10.
2. Commercial bids quoted in any other currency than Indian Rupees (INR) will be disqualified.
3. The Bidders are required to submit mask Commercial Bid Format as per Annexure 10.2 as part of Technical Proposal.
4. The commercial evaluation will be done on the “Total Cost” as defined in Annexure 10.2 – Commercial Bid Format.
5. Bids quoting unrealistic prices for any of the components of this RFP, including but not limited to the AMC and Resource cost, will be rejected at the discretion of the Bank.
6. The Commercial Bid shall be opened post the Technical Evaluation. The bids will be opened only for the technically qualified Bidders in presence of the Bank officials and representatives of technically qualified bidder’s.
7. The bidder with lowest Total Cost will be declared as L1 and successful bidder, subject to corrections in arithmetic errors.

# **Arithmetic errors correction**

Arithmetic errors, if any, in the price break-up format will be rectified on the following basis:

1. If there is discrepancy between the unit price and the total price, which is obtained by multiplying the unit price with quantity, the unit price shall prevail and the total price shall be corrected unless it is a lower figure.
2. If there is discrepancy in the unit price quoted in figures and words, the unit price, in figures or in words, as the case may be, which corresponds to the total bid price for the item shall be taken as correct.
3. If the bidder has not worked out the total bid price or the total bid price does not correspond to the unit price quoted either in words or figures, the unit price quoted in words shall be taken as correct.
4. If the unit price quoted by the bidder in figures and in words are equivalent but the total bid price of the item has NOT been worked out correctly, the unit price quoted by the bidder shall be taken as correct.
5. The bidders, for whom arithmetic corrections are warranted / required, must accept the arithmetic corrections in writing / mail, within a specified date and time as may be decided by the Bank, or their bid will be rejected.

# **Issue of purchase order**

Purchase Order (PO) will be issued to the successful bidder. The bidder has to accept the PO within 07 days from the date of issue of the PO accepting the terms & conditions. The bidder has to deliver, install and implement the CSOC as per time lines given in the Project schedule and implementation (section 4.10).

# **Execution of Agreement**

1. Within 21 days from the date of acceptance of the Order, the selected bidder shall sign a stamped “Agreement” with the Bank as per the format to be provided by the Bank.
2. The Agreement shall include all terms, conditions and specifications of RFP and also the Bill of Material meeting all requirements of the project and Price, as agreed finally after Bid evaluation and negotiation. The Agreement shall be executed in English language in one original, the Bank receiving the duly signed Original and the selected Bidder receiving the photocopy. The Agreement shall be valid till all contractual obligations are fulfilled.

# **Terms and Conditions**

# **6.1. Bid Security & Performance Guarantee**

# **Bid Security / Earnest Money Deposit (EMD)**

1. All the responses must be accompanied by a refundable interest free security deposit of amount as mentioned in Critical Information Sheet of RFP in form of Demand Draft / Pay Order OR Bank guarantee issued by a scheduled commercial bank.
2. Demand Draft / Pay order should be in favor of “Small Industries Development Bank of India” payable at Chennai or in the form of Performance Security. The Demand Draft / Pay Order should be of a Scheduled Commercial Bank only and will be accepted subject to the discretion of the Bank.
3. Format of EMD / Bid Security is prescribed in “Annexure 8.7 – EMD / Bid Security Form”.
4. Any bid received without EMD in proper form and manner shall be considered unresponsive and rejected.
5. The amount of Earnest money deposit (EMD) would be forfeited in the following scenarios:
   * 1. In case the Bidder withdraws the bid prior to validity period of the bid for any reason whatsoever;
     2. Bidder makes any statement or encloses any form which turns out to be false / incorrect at any time prior to signing of the contract.
     3. In case the successful Bidder fails to accept and sign the contract as specified in this document within time stipulated by SIDBI for any reason whatsoever; or
     4. In case the successful Bidder fails to provide the Performance Bank guarantee within ONE month from the date of issue of Purchase Order by the Bank. Besides forfeiting the EMD, the Bank may ban the bidder from subsequent bidding for a period of not less than 3 years.
6. Successful bidder will be refunded the EMD amount only after submission of Performance Bank Guarantee as mentioned in Performance Bank Guarantee (PBG) section.
7. No interest will be paid on EMD.

# **Performance Bank Guarantee (PBG)**

1. The successful Bidder shall provide an unconditional and irrevocable performance bank guarantee in the form and manner provided by the Bank equivalent to 10% of the total contract value from a scheduled commercial bank. The performance guarantee will be valid till at least three months beyond the expiry of the contract period. The performance security is to be submitted within 21 days from the purchase order. The bidder will be required to provide an extension of Performance Bank Guarantee (PBG) covering the contract period within 21 days post the date of acceptance (as per section 6.16 of this RFP) by the Bank.
2. In the event of non-performance of obligation or failure to meet terms of this RFP / Contract, the Bank shall be entitled to invoke the performance guarantee without notice or right of demur to the Bidder. The guarantee should be from a scheduled commercial bank only.
3. In case of expiry of PBG prior to project completion, the bidder will be required to renew the PBG for further period as per plan. If the performance bank guarantee is not submitted within the time stipulated by SIDBI, the Bank reserves the right to cancel the order and forfeit the EMD.
4. The Performance Bank Guarantee would be returned to the successful Bidder after the expiry or termination of the contract plus 90 days on satisfaction of the Bank that there are no dues recoverable from the successful Bidder.
5. Notwithstanding anything to the contrary contained in the contract, SIDBI shall be at liberty to invoke the Performance Bank Guarantee in addition to other remedies available to it under the contract / order or otherwise if the Successful Bidder fails to fulfill any of the terms of contract / order or commits breach of any terms and conditions of the contract.
6. On faithful execution of contract in all respects, the Performance Guarantee of the Bidder shall be released by SIDBI.
7. If aggregated shortfall in achieving Service Level requirement exceeds 10% successively in two quarters or any three quarters in a financial year, SIDBI will inter-alias, be at liberty to invoke the performance guarantee in addition to other remedies available to it under the contract or otherwise.
8. Time shall be the essence of the contract / order, therefore, no extension of time is anticipated, but if untoward or extraordinary circumstances should arise beyond the control of the Bidder, which in the opinion of SIDBI should entitle the Bidder to a reasonable extension of time, such extension may be considered by SIDBI at its sole and absolute discretion, however such extension shall not operate to relieve the Bidder of any of its obligations. SIDBI shall not be liable for any extra financial commitment due to such extension of time. In case of any such extension, the Bidder would be required to extend the validity period of the performance guarantee accordingly.
9. The selected bidder shall be responsible for extending the validity date and claim period of the Bank guarantees as and when it is due or if required.

# **Forfeiture of performance security**

1. The Bank shall be at liberty to set off / adjust the proceeds of the performance guarantee towards the loss, if any, sustained due to the bidder’s failure to complete its obligations under the contract. This is without prejudice to the Bank’s right to proceed against the Bidder in the event of the security being not enough to fully cover the loss / damage.
2. In the event of non-performance of obligation or failure to meet terms of this RFP / Contract, the Bank shall be entitled to invoke the performance guarantee without notice or right of demur to the Bidder.

# **Preliminary Examinations**

1. The Bank will examine the Bids to determine whether they are complete, the documents have been properly signed, supporting papers / documents attached and the bids are generally in order.
2. The Bank may, at its sole discretion, waive any minor infirmity, nonconformity or irregularity in a Bid which does not constitute a material deviation, provided such a waiver does not prejudice or affect the relative ranking of any Bidder. However, no deviation will be allowed with respect to the scope of work and deliverables of the project as defined in the RFP.
3. Prior to the detailed evaluation, the Bank will determine the substantial responsiveness of each Bid to the Bidding document. For purposes of these Clauses, a substantially responsive Bid is one, which conforms to all the terms and conditions of the Bidding Document without material deviations. Deviations from or objections or reservations to critical provisions, such as those concerning Bid security, performance security, qualification criteria, insurance, Force Majeure etc. will be deemed to be a material deviation. The Bank's determination of a Bid's responsiveness is to be based on the contents of the Bid itself, without recourse to extrinsic evidence. The bank may, at its sole discretion, may reject the deviations submitted by the bidder.
4. If a Bid is not substantially responsive, it will be rejected by the Bank and may not subsequently be made responsive by the Bidder by correction of the nonconformity.
5. Bids without EMD / Bid security in the proper form and manner will be considered non-responsive and rejected.
6. The Bidder is expected to examine all instructions, forms, terms and specification in the Bidding Document. Failure to furnish all information required by the Bidding Document or to submit a Bid not substantially responsive to the Bidding Document in every respect will be at the Bidder's risk and may result in the rejection of its Bid.

# **Use of Contract Documents and Information**

1. The bidder shall not, without the Bank’s prior written consent, disclose the Contract, or any provision thereof, or any specification, plan, drawing, pattern, sample or information furnished by or on behalf of the Bank in connection with, to any person other than a person employed by the Bidder in the performance of the Contract. Disclosure to any such employed person shall be made in confidence and shall extend only as far as may be necessary for purposes of such performance.
2. The Bidder will treat as confidential all data and information about the Bank, obtained in the execution of his responsibilities, in strict confidence and will not reveal such information to any other party without the prior written approval of the Bank.

# **Rules for Evaluation of Responses**

1. All the responsive bids will be evaluated as per the procedure detailed in Chapter-5 Evaluation Methodology.
2. All the documentary proofs are to be submitted along with the bid in this regard.
3. To assist in the scrutiny, evaluation and comparison of responses / offers, SIDBI may, at its discretion, ask some or all Bidders for clarification of their offer. The request for such clarifications and the response will necessarily be in writing. SIDBI has the right to disqualify the Bidder whose clarification is not received by SIDBI by the stipulated time or is found not suitable to the proposed project.
4. SIDBI may appoint the services of an external consultant for evaluation of the bid proposal.
5. Bidders must not present any reference as credential for which it is not in a position to present the verifiable facts/documents because of any non-disclosure agreement with its other customer or any other reason whatsoever. SIDBI would not consider any statement as a credential if same cannot be verified as per its requirement for evaluation.
6. SIDBI may at its absolute discretion exclude or reject any proposal that in the reasonable opinion of SIDBI contains any false or misleading claims or statements. SIDBI shall not be liable to any person for excluding or rejecting any such proposal.
7. Bank may waive off any minor infirmity or nonconformity or irregularity in a bid, which does not constitute a material deviation, provided such a waiving, does not prejudice or affect the relative ranking of any bidder.
8. SIDBI reserves the right to reject any proposal in case same is found incomplete or not submitted in the specified format given in this RFP document. SIDBI would not give any clarification / explanation to the concerned bidder in case of such rejection.
9. SIDBI reserves the right to modify the evaluation process at any time during the Tender process (before submission of technical and commercial responses by the prospective bidder), without assigning any reason, whatsoever, and without any requirement of intimating the Bidders of any such change.
10. SIDBI will award the Contract to the successful Bidder whose bid has been determined to be substantially responsive and has been determined as the best bid, provided further that the Bidder is determined to be qualified to perform the contract satisfactorily. However, SIDBI shall not be bound to accept the best bid or any bid and reserves the right to accept any bid, either wholly or in part, as it may deem fit.

# **Contacting the Bank**

1. After opening of Bid to the time a communication in writing about its qualification or otherwise received from the Bank, bidder shall NOT contact the Bank on any matter relating to its Bid.
2. Any effort by the Bidder to influence the Bank in its decisions on Bid evaluation, Bid comparison may result in the rejection of the Bidder’s Bid.

# **Commercial Bid**

1. Currency – The Bidder is required to quote in Indian Rupees (‘INR’/ ‘Rs’). Bids in currencies other than INR may not be considered.
2. The commercial bid submitted by the bidder will be valid for the tenure of contract period.
3. Tax -The prices quoted would include all costs including applicable taxes like GST, custom duties, transportation, out of pocket expenses, lodging and boarding expenses, etc., that need to be incurred (at current rate). No additional cost whatsoever would be paid.
4. While any increase in the rates of applicable taxes or impact of new taxes subsequent to the submission of commercial bid shall be borne by SIDBI, any subsequent decrease in the rates of applicable taxes or impact of new taxes shall be passed on to SIDBI in its favor. This will remain applicable throughout the contract period.
5. It would be bidder’s responsibility to identify and factor cost of each and every commercial item mentioned in this RFP document during submission of commercial bids. In case of any such item is left out and noticed after completion of commercial evaluation, the selected bidder (Service Provider) has to provide the services at its own cost.
6. The Commercial Bid should be strictly as per format mentioned in the RFP. Consideration of commercial bids, not submitted as per requisite format, will be at the discretion of the bank.

# **No Commitment to Accept Lowest or Any Offer**

1. The Bank reserves its right to reject any or all the offers without assigning any reason thereof whatsoever.
2. The Bank will not be obliged to meet and have discussions with any bidder and / or to entertain any representations in this regard.
3. The bids received and accepted will be evaluated by the Bank to ascertain the best and lowest bid in the interest of the Bank. However, the Bank does not bind itself to accept the lowest or any Bid and reserves the right to reject any or all bids at any point of time prior to the order without assigning any reasons whatsoever. The bank reserves the right to re-tender.

# **Service Delivery**

1. Project is based on delivery of on-site services at SIDBI’s office premises as per defined ‘Service Level Agreement’ (SLA). Bidder is required to post certain number of resources under several categories on-site at SIDBI office as per its response to this RFP.
2. In addition to providing services as per service window defined in this RFP document, service provider is required to provide services on Saturdays / Sundays / Holidays in case of urgent requirement of the bank.
3. The Bidder would align its expertise from its respective backend technology practice/tower/vertical in its organization to attend any critical technical issue as and when required. These services would be in addition to the resources deployed on-site in SIDBI premises. It may be noted that SIDBI will allow remote access of its SIEM, security systems under the CSOC scope for attending to any technical problem through link for the bidder's through secure channels. However, no modification in systems and troubleshooting would be allowed to be carried out remotely and would be carried by onsite team.
4. Service provider must arrange for posting of staff members having requisite qualification, experience, skill-set etc. as mentioned in the RFP document.
5. Time is the essence of this RFP / Contract to be entered with the Successful Bidder, therefore, the Bidder must strictly adhere to the delivery schedule of the manpower and services identified in their proposal. Failure to do so will be considered as breach of the terms and conditions of the contract.
6. The Bidder undertakes to provide appropriate human as well as other resources required, to execute various tasks assigned as part of the project, from time to time.
7. SIDBI reserves the right to reduce resources anytime during the contract period without assigning any reason thereof, with a prior written notice of 30 days. Payment of such resources shall be made on pro-rata basis till the date of stopping.

# **Ownership of Delivered Services**

1. The selected Bidder, who will be awarded the contract, will hold ownership of its delivery of the services under the contract and be responsible for the services delivered. All the deliverables as per the scope of this RfP will become the property of the Bank.
2. SIDBI has the sole ownership of and the right to use, all data that may be in possession of the Bidder or its representative in the course of performing the services under the agreement that may be entered into. All documents, report, information, data etc. collected and prepared by Bidder in connection with the scope of work submitted to SIDBI will be property of the Bank. The Bidder shall not be entitled either directly or indirectly to make use of the documents, reports given by SIDBI for carrying out of any services with any third parties. Bidder shall not without the prior written consent of SIDBI be entitled to publish studies or descriptive article with or without illustrations or data in respect of or in connection with the performance of services.

# **Addition / Deletion of qualified offerings**

1. For this purpose, a Change Order Procedure will be followed. Bank may issue a change order in the event of actual or anticipated change(s) to the agreed scope of work, services, deliverables and schedules. The Bidder will have to prepare a change order reflecting the actual or anticipated change(s) including the impact on deliverables schedule. The Bidder will be liable to carry out such services as required by the Bank at mutually agreed terms and conditions.
2. The Bidder will have to agree that the price for incremental offering cannot exceed the original proposed cost. The Bank has the right to order as much as it wants at those rates.
3. As a method for reviewing Bidder services and Bank requirements, the Bank will sponsor regular reviews to allow an exchange of requirements and opportunities.

# **Expenses**

It may be noted that SIDBI will not pay any additional amount separately towards travelling expenses / boarding expenses / lodging expenses / conveyance expenses / out of pocket expenses or any other fees / charges.

# **Terms of Payment and Payment Milestones**

1. The payments for all software appliances, hardware delivered are released as per details in the table given below. The payments for services will be released on quarterly basis as arrears for all the implemented solutions and services.
2. All deliverables and Services to be provided as per requirements for proposed solution specified in the RFP.
3. The quoted price should include Implementation, Installation, configuration of in-scope Security Solutions and other activities as defined in the scope of the RFP. The cost should also include training and other requirements given in detailed in the RFP.
4. Warranty and AMC / ATS will include onsite support for all products, solutions, etc. quoted under this RFP including Hardware, Software, Database, etc.
5. Implementation cost shall also include implementation effort both by OEM & bidder. Bank will not pay any extra charge to OEM and / or BIDDER as implementation cost.
6. Bank will not pay any labour charges for transportation, installation of hardware items separately.
7. If the cost for any line item is indicated as zero then it will be assumed by the Bank that the said item is provided to the Bank without any cost.
8. The Bidder has to make sure all the arithmetical calculations are accurate. Bank will not be held responsible for any incorrect calculations however for the purpose of calculation Bank will take the corrected figures / cost.
9. The Bank will make the payment within 30 days subject to submission of invoices along with supporting documents / reports towards delivery of services. Applicable liquidity damages will be deducted to arrive at the payable for the month.
10. The payments will be released after deducting applicable TDS / LD / Penalty if any,
11. No escalation in price quoted is permitted for any reason whatsoever. Prices quoted must be firm till the completion of the contract period.
12. All the payments will be made by SIDBI, Mumbai electronically through RTGS / NEFT. Bidder to submit Bank Mandate Form (as per Annexure 8.6) along with cancelled Cheque in original before raising first invoice.
13. The Bidder must accept the payment terms proposed by the Bank. The financial bid 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 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.
14. The Price offered by the Bidder to the Bank must be in Indian Rupees and payments will be made to the Bidder in Indian Rupee only. The costs should be inclusive of duties, insurance, freight, charges of road permit and inclusive of all taxes. The cost will also include the training costs also.
15. Submission of Performance Bank Guarantee (PBG) is the prerequisite before making any payment.
16. The payment milestones are defined as below:

|  |  |  |
| --- | --- | --- |
| **Description** | **Payment Milestones** | |
| **Cost of Product including OEM warranty for 3 years (including CSOC Solution License, Hardware and Storage Cost, Other Software License Cost)** | 50% | Delivery and acceptance of the SIEM and CSOC solution License with Environment Setup after post-delivery verification, on submission of invoice with Proof of Delivery, Proof of Entitlement, Proof of Warranty / AMC / ATS |
| 20% | Post UAT signoff (Phase-1) |
| 30% | Post project signoff (Phase-2) |
| **CSOC Implementation and Integration Cost** | 100% | Successful installation, implementation and integration of SIEM and other CSOC solution and project signoff (Phase - 2) |
| **Training** | 40% | Pre-implementation training |
| 60% | Post-implementation Training |

1. Payment for the CSOC Services (VAPT and Threat Intelligence) cost for contract period as part of Operational Cost will be divided into equal quarterly installments and will be payable on submission of VAPT reports.
2. Payment for the CSOC monitoring & operations cost, P2P link for DC-DR replication as part of Operational Cost for contract period will be divided into equal quarterly installments and will be payable to the Bidder quarterly in arrears on submission of invoice and other supporting documents.

# **Taxes and Duties**

1. The bidder shall be entirely responsible for all applicable taxes, duties, levies, charges, license fees, road permits, etc. in connection with delivery of services at site including incidental services.
2. The bidder must also ensure that all applicable laws framed by the Central Government, State Government and Local Bodies, including payment of applicable minimum wages and all laws pertaining to contract employees / labor laws are complied with while providing services. The selected bidder may have to execute an indemnity bond in favor of the Bank in this regard.
3. Providing clarifications / particulars / documents etc. to the appropriate tax authorities for assessment of tax, compliance with labor and other laws, etc. will be the responsibility of the bidder at his cost.
4. Tax deduction at Source - Wherever the laws and regulations require deduction of such taxes at the source of payment, the Bank shall effect such deductions from the payment due to the Bidder. The remittance of amounts so deducted and issuance of certificate for such deductions shall be made by the Bank as per the laws and regulations in force. Nothing in the Contract shall relieve the Bidder from his responsibility to pay any tax that may be levied in India on income and profits made by the Bidder in respect of this contract.
5. While any increase in the rates of applicable taxes or impact of new taxes subsequent to the submission of commercial bid shall be borne by SIDBI, any subsequent decrease in the rates of applicable taxes or impact of new taxes shall be passed on to SIDBI in its favor. This will remain applicable throughout the contract period.
6. The price quoted by the bidder should be in Indian Rupee and should be inclusive of all local taxes, VAT, GST, service tax, duties, levies, transportation costs, back to back support with OEM during warranty / AMC, insurance costs, training costs, implementation charges etc., till the bid validity period.

# **Execution of Agreement and NDA**

1. The selected bidder should execute agreement with the Bank which will remain valid for at least 3 years extendable upto 5 years at the discretion of the Bank. The agreement would include all the terms and conditions of the services to be extended as detailed herein and as may be prescribed or recommended by the Bank which will include a Non-disclosure Agreement clause.
2. The agreement with Non-disclosure agreement clauses should be executed within 21 days from the date of purchase order.
3. The date of Purchase Order shall be treated as date of engagement and the time-line for completion of the assignment shall be worked out with reference to this date.

# **Period of Contract**

1. The contract shall commence on the acceptance date of all solutions under CSOC (Phase – 1 Signoff) and continue for a period of THREE years thereafter. The contract may be extended for a maximum period of two years (in total five years) on the same terms and conditions at discretion of the bank.
2. The contract can be extended to 4th & 5th year at the discretion of the Bank if required, based on the same terms and conditions. The cost for the fourth and fifth year will be re-negotiated at the end of three year contract period. Bidders are to ensure that all the solutions including hardware, software, services or any other tool supplied will be supported up to 5 years and operations will be carried out for five years.
3. Post completion of the contract / or in the event of early termination the bidder is expected to provide support for transition of the services to nominated members of the bank or to a third party nominated by the bank for a period of 6 months.

# **Termination**

* + 1. The various clause for termination are as under:

|  |  |  |
| --- | --- | --- |
| **S.N.** | **Details for Termination** | |
| **1** | **Termination for non-performance (not meeting SLA)** | |
| Bank may, without prejudice to any other remedy for breach of contract, by giving written notice of **30 days** to the bidder, terminate the contract in whole or part ( link / location and / or contract):   1. If the bidder fails to deliver any or all of the services within the period(s) specified in the contract or within any extension thereof granted by the Bank pursuant to conditions of contract OR 2. The Selected bidder breaches its obligations under the scope document or the subsequent agreement and if the breach is not cured within 30 days from the date of notice OR 3. Serious discrepancy or demonstrable deterioration in the quality of service expected during the implementation, rollout and subsequent maintenance process OR 4. There has been a breach of confidentiality or there is a cyber-security breach of nature detrimental to the interest of Bank. Decision of Bank in this connection shall be final and binding on the successful bidder. 5. The Selected bidder (i) has a winding up order made against it; or (ii) has a receiver appointed over all or substantial assets; or (iii) is or becomes unable to pay its debts as they become due; or (iv) enters into any arrangement or composition with or for the benefit of its creditors; or (v) passes a resolution for its voluntary winding up or dissolution or if it is dissolved.   The bank’s decision in this regard will be final. Bank will not bear any compensation for these exits as they are due to non-performance of service provider. | |
| **2** | **Termination for insolvency** | |
| Bank may at any time terminate the Contract by giving written notice of **30 days** to the bidder, if the bidder becomes bankrupt or otherwise insolvent. In this event termination will be without compensation to the bidder, provided that such termination will not prejudice or affect any right of action or remedy, which has occurred or will accrue thereafter to the Bank. | |
| **3** | **Termination for the convenience of bank** |
| The bank may, at any point during the currency of this contract may terminate the contract by giving **30 days** advance notice to the bidders without assigning whatsoever reason. In this event, termination will be without compensation to the Bidder, provided that such termination will not prejudice or affect any right of action or remedy, which has accrued or will accrue thereafter to the Bank. |

* + 1. The Selected bidder shall have right to terminate only in the event of winding up of the Bank.
    2. In the event of termination of the Contract due to any cause whatsoever, [whether consequent to the stipulated term of the Contract or otherwise], BANK shall be entitled to impose any such obligations and conditions and issue any clarifications as may be necessary to ensure an efficient transition and effective business continuity of the Service(s) which the selected Vendor shall be obliged to comply with and take all available steps to minimize loss resulting from that termination/breach, and further allow the next successor Vendor to take over the obligations of the erstwhile Vendor in relation to the execution/continued execution of the scope of the Contract.
    3. In the event that the termination of the Contract is due to the expiry of the term of the Contract and the Contract is not further extended by BANK, the Vendor herein shall be obliged to provide all such assistance to the next successor Bidder or any other person as may be required and as BANK may specify including training, where the successor(s) is a representative/personnel of BANK to enable the successor to adequately provide the Service(s) hereunder, even where such assistance is required to be rendered for a reasonable period that may extend beyond the term/earlier termination hereof.
    4. The termination hereof shall not affect any accrued right or liability of either Party nor affect the operation of the provisions of the Contract that are expressly or by implication intended to come into or continue in force on or after such termination.
    5. BANK reserves the right to recover any dues payable by the selected bidder from any amount outstanding to the credit of the selected bidder, including the pending bills and/or invoking the Bank guarantee under this contract
    6. The Bank shall make such prorated payment for services rendered by the selected bidder and accepted by the Bank at the sole discretion of the Bank in the event of clause of termination, provided that the selected bidder is in compliance with its obligations till such date. However, no payment for “costs incurred, or irrevocably committed to, up to the effective date of such termination” will be applicable to selected Bidder. There shall be no termination compensation payable to the selected bidder.
    7. Termination shall not absolve the liability of the Bank to make payments of undisputed amounts to the selected bidder for services rendered till the effective date of termination. Termination shall be without prejudice to any other rights or remedies a party may be entitled to hereunder or at law and shall not affect any accrued rights or liabilities or either party nor the coming into force or continuation in force of any provision Selected Bidder hereof which is expressly intended to come into force or continue in force on or after such termination.
    8. Nothing herein shall restrict the right of BANK to invoke the Performance Bank Guarantee and other guarantees, securities furnished, enforce the Letter of Indemnity and pursue such other rights and/or remedies that may be available to BANK under law or otherwise.
    9. The termination hereof shall not affect any accrued right or liability of either Party nor affect the operation of the provisions of the Contract that are expressly or by implication intended to come into or continue in force on or after such termination.
    10. Bidder will submit a declaration confirming knowledge transfer/handover and no-ownership of CSOC.

# **Applicable laws**

1. The Contract shall be interpreted in accordance with the laws prevalent in India.
2. Compliance with all applicable laws: The Bidder shall undertake to observe, adhere to, abide by, comply with and notify 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 Tender and shall indemnify, keep indemnified, hold harmless, defend and protect the Bank and its employees / officers / resource / personnel / representatives / agents from any failure or omission on its part to do so and against all claims or demands of liability and all consequences that may occur or arise for any default or failure on its part to conform or comply with the above and all other statutory obligations arising there from.
3. Compliance in obtaining approvals / permissions / licenses: The Bidder shall promptly and timely obtain all such consents, permissions, approvals, licenses, etc., as may be necessary or required for any of the purposes of this project or for the conduct of their own business under any applicable Law, Government Regulation / Guidelines and shall keep the same valid and in force during the term of the project, and in the event of any failure or omission to do so, shall indemnify, keep indemnified, hold harmless, defend, protect and fully compensate the Bank and its employees / officers / resource / personnel/ representatives / agents from and against all claims or demands of liability and all consequences that may occur or arise for any default or failure on its part to conform or comply with the above and all other statutory obligations arising therefrom and the Bank will give notice of any such claim or demand of liability within reasonable time to the bidder.

# **Statutory & Regulatory Compliance**

The bidder should ensure all statutory and regulatory compliance towards:

1. ESIC & EPFO – All bidders have to ensure that the resources deployed at SIDBI sites are compliant as per the guidelines of ESIC & EPFO. Please note that these are Government bodies, compliance to which is Mandatory.
2. Minimum Wages Act (MWA) – The bidder also has to ensure that they are compliant to the Minimum Wages Act for deployment of resources across SIDBI site. The bidder should follow all payout norms as per the MWA.
3. Any other Act / Statutory and regulatory compliances as applicable.

# **No Employer-Employee Relationship**

The selected bidder during the term of the contract and for a period of two year thereafter shall not without the express written consent of the Bank, directly or indirectly

1. Recruit, hire, appoint or engage or attempt to recruit, hire, appoint or engage or discuss employment with or otherwise utilize the services of any person who has been an employee or associate or engaged in any capacity, by the Bank in rendering the services in relation to the contract; or
2. Induce any person who shall have been an employee or associate of the Bank at any time to terminate his / her relationship with the Bank.
3. The selected Bidder or any of its holding/subsidiary/joint-venture/ affiliate/ group/ client companies or any of their employees/ officers/ staff/ personnel/ representatives/ agents shall not, under any circumstances, be deemed to have any employer-employee relationship with SIDBI or any of its employees/ officers/ staff/ representatives/personnel/agents. Staff deployed by the bidder shall never be deemed to be appointed by SIDBI nor shall they be under its service conditions.

# **Rights to Visit**

1. All records of the Bidder with respect to any matters covered by this Tender document/ subsequent order shall be made available to SIDBI or its designees at any time during normal business hours, as often as SIDBI deems necessary, to audit, examine, and make excerpts or transcripts of all relevant data.
2. SIDBI, including its regulatory authorities like RBI etc., reserves the right to verify, through their officials or such other persons as SIDBI may authorize, the progress of the project at the development /customization site of the Bidder or where the services are being rendered by the bidder.
3. The Bank and its authorized representatives, including regulator like Reserve Bank of India (RBI) shall have the right to visit any of the Bidder’s premises with prior notice to ensure that data provided by the Bank is not misused. The Bidder will have to cooperate with the authorized representative/s of the Bank and will have to provide all information/ documents required by the Bank. The visit shall be conducted during normal business hours and on normal working days after informing the bidder in advance.

# **Audit**

1. The bidder shall allow the Bank, its authorized personnel, its auditors (internal and external), authorized personnel from RBI / other regulatory & statutory authorities, and grant unrestricted right to inspect and audit its books and accounts, to provide copies of any audit or review reports and findings made on the service provider, directly related to the services including Hardware, Software provided to the Bank and CSOC operations under this RFP and the bidder shall extend all cooperation in this regard.
2. Audit under this clause shall be restricted to physical files related to this arrangement. Audit shall be conducted during normal business hours and on normal working days after informing the bidder in advance.
3. The bank will also carry out annual review of the contract to ascertain the financial stability of the bidder in addition to the performance and service reliability. The bidder is required to submit the audited balance sheet and CA certificate, etc.

# **IPR Infringement**

As part of this project bidder / service provider will use software / tool to deliver services. If the deliverables and use of any such software/tool used for such delivery, infringe the intellectual property rights of any third person, bidder / service provider shall be primarily liable to indemnify SIDBI to the extent of direct damages against all claims, demands, costs, charges, expenses, award, compensations etc. arising out of the proceedings initiated by third party for such infringement, subject to the condition that the claim relates to Software provided / used by Bidder / Service provider under this project.

# **Indemnity**

The Bidder/ successful 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 attorneys' 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:

1. Bank’s authorized / bona fide use of the Deliverables and /or the Services provided by Bidder under this RFP document; and/or
2. An act or omission of the Bidder, employees, agents, sub-contractors in the performance of the obligations of the Bidder under this RFP document; and/or
3. Claims made by employees or subcontractors or subcontractors’ employees, who are deployed by the Bidder, against the Bank; and/or
4. Breach of any of the term of this RFP document and/or of the agreement to be entered subsequent this RFP or breach of any representation or false representation or inaccurate statement or assurance or covenant or warranty by the successful Bidder under this RFP document and/or of the agreement to be entered subsequent this RFP; and/or
5. Any or all Deliverables or Services infringing any patent, trademarks, copyrights or such other Intellectual Property Rights; and/or
6. Breach of confidentiality obligations of the Bidder contained in this RFP document; and/or
7. Negligence, fraudulence activities or gross misconduct attributable to the bidder or its employees or sub-contractors; and/or
8. The use of unlicensed and illegal Software and/or allied components by the successful Bidder

The Bidder will have to at its own cost and expenses defend or settle any claim against the Bank that the Deliverables and Services delivered or provided under this RFP document infringe a patent, utility model, industrial design, copyright, trade secret, mask work or trade mark in the country where the Deliverables and Services are used, sold or received, provided the Bank:

1. Notifies the Bidder in writing; and
2. Cooperate with the bidder in the defense and settlement of the claims.

The Bidder shall not be liable for defects or non-conformance resulting from:

1. Software, hardware, interfacing not approved by Bidder; or
2. Unauthorized modification of Software or any individual product supplied under this RfP document, or Bank’s failure to comply with any mutually agreed environmental specifications.
3. Use of a Deliverable in an application or environment for which it was not designed or not contemplated under this Agreement;
4. Modification of a deliverable by anyone other than the bidder where the unmodified version of the deliverable would not be infringing.
5. Any loss of profits, revenue, contracts, or anticipated savings.
6. Any consequential or indirect loss or damage however caused, provided that the claims against customers, users and service providers of the Bank would be considered as a “direct” claim.

The bidder shall indemnify the Bank and be liable for any loss or damage suffered by the Bank due to malfunctioning of the system as supplied and installed by them. The total liability of the selected bidder shall not exceed the total cost of the order value.

Indemnity would be limited to court; tribunal or arbitrator awarded damages and shall exclude indirect, consequential and incidental damages. However indemnity would cover damages, loss or liabilities suffered by the Bank arising out of claims made by its customers and/or regulatory authorities.

The selected bidder is required to furnish a separate Deed of Indemnity (Format whereof to be supplied by the Bank) in Banks favor in this respect before or at the time of execution of the Service Level Agreement

# **Limitation of liabilities**

Save and except the liability under Section of ‘IPR Infringement’ in herein above, in no event shall either party be liable with respect to its obligations under or arising out of this agreement for consequential, exemplary, punitive, special, indirect or incidental damages, including, but not limited to, loss of data / programs or lost profits, loss of goodwill, work stoppage, computer failure, loss of work product or any and all other commercial damages or losses whether directly or indirectly caused, even if such party has been advised of the possibility of such damages. The aggregate liability of bidder / service provider, arising at any time shall not exceed the total contract value.

# **Confidentiality**

The bidder shall take all necessary precautions to ensure that all confidential information is treated as confidential and not disclosed or used other than for the purpose of project execution. Bidder shall suitably defend, indemnify Bank for any loss/damage suffered by Bank on account of and to the extent of any disclosure of the confidential information. The bidder shall furnish a Non-disclosure Agreement as given in Annexure 11.9.

1. No media release/public announcement or any other reference to the RFP or any program there under shall be made without the written consent of the Bank, by photographic, electronic or other means.
2. The RFP document is confidential and is not to be disclosed, reproduced, transmitted, or made available by the Recipient to any other person. Bank may update or revise the RFP document or any part of it. The Recipient acknowledges that any such revised or amended document is received subject to the same confidentiality undertaking. The Recipient will not disclose or discuss the contents of the RFP document with any officer, employee, consultant, director, agent, or other person associated or affiliated in any way with Bank or any of its customers or suppliers without the prior written consent of Bank.
3. This tender document contains information proprietary to the Bank. Each recipient is entrusted to maintain its confidentiality. It should be disclosed only to those employees involved in preparing the requested responses. The information contained in the tender document may not be reproduced in whole or in part without the express permission of the Bank. Disclosure of any such sensitive information to parties not involved in the supply of contracted services will be treated as breach of trust and could invite legal action. This will also mean termination of the contract and disqualification of the said Bidder.
4. “Confidential Information” means any and all information that is or has been received by the Bidder (“Receiving Party”) from the Bank (“Disclosing Party”) and that:
5. relates to the Disclosing Party; and
6. is designated by the Disclosing Party as being confidential or is disclosed in circumstances where the Receiving Party would reasonably understand that the disclosed information would be confidential or
7. is prepared or performed by or on behalf of the Disclosing Party by its employees, officers, directors, agents, representatives or consultants.
8. without limiting the generality of the foregoing, Confidential Information shall mean and include any information, data, analysis, compilations, notes, extracts, materials, reports, specifications or other documents or materials that may be shared by the Bank with the Bidder.
9. “Confidential Materials” shall mean all tangible materials containing Confidential Information, including, without limitation, written or printed documents whether machine or user readable.
10. The Receiving Party shall, at all times regard, preserve, maintain and keep as secret and confidential all Confidential Information and Confidential Materials of the Disclosing Party howsoever obtained and agrees that it shall not, without obtaining the written consent of the Disclosing Party:
11. Unless otherwise agreed herein, use any such Confidential Information and materials for its own benefit or the benefit of others or do anything prejudicial to the interests of the Disclosing Party or its customers or their projects.
12. In maintaining confidentiality hereunder the Receiving Party on receiving the confidential information and materials agrees and warrants that it shall:
    1. Take at least the same degree of care in safeguarding such Confidential Information and materials as it takes for its own confidential information of like importance and such degree of care shall be at least, that which is reasonably calculated to prevent such inadvertent disclosure;
    2. Keep the Confidential Information and Confidential Materials and any copies thereof secure and in such a way so as to prevent unauthorized access by any third party;
    3. Limit access to such Confidential Information and materials to those of its directors, partners, advisers, agents or employees who are directly involved in the consideration/evaluation of the Confidential Information and bind each of its directors, partners, advisers, agents or employees so involved to protect the Confidential Information and materials in the manner prescribed in this document; and
13. Upon discovery of any unauthorized disclosure or suspected unauthorized disclosure of Confidential Information, promptly inform the Disclosing Party of such disclosure in writing and immediately return to the Disclosing Party all such Information and materials, in whatsoever form, including any and all copies thereof.
14. The Receiving Party who receives the confidential information and materials agrees that on receipt of a written demand from the Disclosing Party:
    1. Immediately return all written Confidential Information, Confidential materials and all copies thereof provided to, or produced by it or its advisers, as the case may be, which is in Receiving Party’s possession or under its custody and control;
    2. To the extent practicable, immediately destroy all analyses, compilations, notes, studies, memoranda or other documents prepared by it or its advisers to the extent that the same contain, reflect or derive from Confidential Information relating to the Disclosing Party;
    3. So far as it is practicable to do so immediately expunge any Confidential Information relating to the Disclosing Party or its projects from any hardware or other device in its possession or under its custody and control; and
    4. To the extent practicable, immediately furnish a certificate signed by its director or other responsible representative confirming that to the best of his/her knowledge, information and belief, having made all proper enquiries the requirements of this paragraph have been fully complied with.
15. The restrictions in the preceding clause shall not apply to:
    1. Any information that is publicly available at the time of its disclosure or becomes publicly available following disclosure (other than as a result of disclosure by the Disclosing Party contrary to the terms of this document); or any information which is independently developed by the Receiving Party or acquired from a third party to the extent it is acquired with the valid right to disclose the same.
    2. Any disclosure required by law or by any court of competent jurisdiction, the rules and regulations of any recognized stock exchange or any enquiry or investigation by any governmental, statutory or regulatory body which is lawfully entitled to require any such disclosure provided that, so far as it is lawful and practical to do so prior to such disclosure, the Receiving Party shall promptly notify the Disclosing Party of such requirement with a view to providing the Disclosing Party an opportunity to obtain a protective order or to contest the disclosure or otherwise agree to the timing and content of such disclosure. The Confidential Information and materials and all copies thereof, in whatsoever form shall at all times remain the property of the Disclosing Party and its disclosure hereunder shall not confer on the Receiving Party any rights whatsoever beyond those contained in this document.
16. The confidentiality obligations shall survive the expiry or termination of the agreement between the Bidder and the Bank.

# **Corrupt and fraudulent practice**

As per Central Vigilance Commission (CVC) directives, it is required that Bidders / Suppliers / Contractors observe the highest standard of ethics during the execution of this RFP and subsequent contract(s). In this context, the bidders are requested to note the following:

1. “Corrupt Practice” means the offering, giving, receiving or soliciting of anything of value to influence the action of an official in the procurement process or in contract execution.
2. “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 bid submission) designed to establish bid prices at artificial non- competitive levels and to deprive the Bank of the benefits of free and open competition.
3. The Bank reserves the right to declare a bidder ineligible, either indefinitely or for a stated period of time, to be awarded a contract if at any time it determines that the bidder has engaged in corrupt or fraudulent practices in competing for or in executing the contract.
4. The decision of Bank in determining the above aspects will be final and binding on the all the Bidders. No Bidder shall contact through any means of communication the Bank or any of its employees on any matter relating to its Bid, from the time of Bid opening to the time the contract is awarded. If the bidder wishes to bring additional information to the notice of the Bank, it may do so in writing.
5. Any effort/attempt by a bidder to influence the Bank in its decision on bid evaluation, Bid comparison or contract award may result in rejection of the Bidder’s bid and/or blacklisting the Bidder. The Bidder agrees not to hire, solicit or accept solicitation either directly or through a third party from any of the employees of the Bank directly involved in this contract during the period of contract and one year thereafter, except as the parties may agree on the case to case basis.
6. The selected bidder shall ensure compliance of CVC guidelines issued or to be issued from time to time for selection of bidder.

# **Resolution of Disputes**

1. All disputes and differences of any kind whatsoever, arising out of or in connection with this Offer or in the discharge of any obligation arising under this Offer (whether during the course of execution of the order or after completion and whether beyond or after termination, abandonment or breach of the Agreement) shall be resolved amicably by the Bank and the bidder.
2. In case of failure to resolve the disputes and differences amicably, the matter may be referred by the Bank to a sole arbitrator, for adjudication thereof, to be appointed in the manner hereinafter provided.
   * 1. the Bank will send within thirty days of receipt of the notice, to the contractor a panel of three names of persons who shall be presently unconnected with the organization for which the work is executed. The Bidder shall on receipt of the names of aforesaid, select any one of the persons named to be appointed as a sole Arbitrator and communicate his name to the Bank within thirty days of receipt of the names. The Bank shall thereupon without any delay appoint the said person as the Sole Arbitrator. If the Bidder fails to communicate such selection as provided above within the period specified, the competent authority shall make the selection and appoint the selected person as the Sole Arbitrator.
     2. If the Banker fails to send to the Bidder the panel of three names as aforesaid within the period specified, the Bidder shall send to the Bank a panel of three names of persons who shall all be unconnected with either party. The Bank shall on receipt of the named as aforesaid select anyone of the person’s name and appoint him as the Sole Arbitrator. If the Bank fails to select the person and appoint him as the Sole Arbitrator within 30 days of receipt of the panel and inform the Bidder accordingly, the Bidder shall be entitled to appoint one of the persons from the panel as the Sole Arbitrator and communicate his name to the Bank.

If the Arbitrator so appointed is unable or unwilling to act or resigns his appointment or vacates his office due to any reason whatsoever another Sole Arbitrator shall be appointed as aforesaid. The provisions of the Indian Arbitration and Conciliation Act, 1996, shall govern the arbitration.

1. The Bidder shall continue to work under the Contract during the arbitration proceedings unless otherwise directed in writing by the Bank or unless the matter is such that the work cannot possibly be continued until the decision of the Arbitrator or the umpire, as the case may be, is obtained.
2. Arbitration proceedings shall be held at Lucknow, India, and the language of the arbitration proceedings and that of all documents and communications between the parties shall be English.
3. 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 bidder/prospective bidder from committing any violation or enforce the performance of the covenants, obligations and representations contained in this RFP. These injunctive remedies are cumulative and are in addition to any other rights and remedies the 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.
4. All disputes and controversies between Bank and Bidder shall be subject to the exclusive jurisdiction of the courts in Mumbai and the parties agree to submit themselves to the jurisdiction of such court as this RFP/contract agreement shall be governed by the laws of India.
5. Any notice given by one party to the other pursuant to this Contract shall be sent to the other party in writing or by fax and confirmed in writing to the other party’s specified address. The same has to be acknowledged by the receiver in writing.
6. A notice shall be effective when delivered or on the notice’s effective date, whichever is later.
7. No conflict between Bidder and SIDBI will cause cessation of services. Only by mutual consent the services will be withdrawn.

# **Grievances Redressal Mechanism**

Bank has a grievances redressal mechanism for its customers and designated grievances redressal officers. The bank would use the same mechanism to address the grievances, if any, of the customers related to the services being rendered within the ambit of this RFP.

# **Force Majeure**

1. Successful Bidder shall not be liable for forfeiture of its performance security, liquidated damages or termination for default, if and to the extent that it’s delay in performance or other failure to perform its obligations under the contract subsequent to this RFP is the result of an event of Force Majeure.
2. If a Force Majeure situation arises, the Bidder shall promptly notify the Bank in writing of such condition, the cause thereof and the change that is necessitated due to the conditions. Until and unless otherwise directed by the Bank in writing, the Bidder shall continue to perform its obligations under the Contract as far as is reasonably practical, and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event.
3. 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 SIDBI and the successful bidder shall hold consultations with each other in an endeavor to find a solution to the problem
4. In the event of the Force Majeure conditions continuing for a period of more than three months the parties shall discuss and arrive at a mutually acceptable arrangement.

# **Subcontracting**

1. The selected Bidder shall not subcontract or permit anyone other than its personnel or the OEM supplier to perform any of the work, service or other performance required of the bidder under the contract without the prior written consent of the Bank.
2. If the Bank undergoes a merger, amalgamation, take-over, consolidation, reconstruction, change of ownership etc., this RFP shall be considered to be assigned to the new entity and such an act shall not affect the rights and obligations of the Bidder under this RFP.

# **Negligence**

1. In connection with the work or contravenes the provisions of General Terms, if the selected bidder neglects to execute the work with due diligence or expedition or refuses or neglects to comply with any reasonable order given to him in writing by the Bank, in such eventuality, the Bank may after giving notice in writing to the selected bidder calling upon him to make good the failure, neglect or contravention complained of, within such times as may be deemed reasonable and in default of the said notice, the Bank shall have the right to cancel the Contract holding the selected bidder liable for the damages that the Bank may sustain in this behalf. Thereafter, the Bank may make good the failure at the risk and cost of the selected bidder.
2. The below mentioned situations will also be treated as an act of negligence by the Bidder.
   1. In case of any damage of Bank’s property during execution of the work is attributable to the bidder, bidder has to replace the damaged property at his own cost.
   2. The selected Bidder shall take all steps to ensure safety of bidder’s and the bank’s personnel during execution of the contract and also be liable for any consequences due to omission or act of the selected bidder.

# **Miscellaneous**

1. Bidder is expected to peruse all instructions, forms, terms and specifications in this RFP and its Annexures.
2. SIDBI shall not be held liable for additional costs incurred during any discussion on contracts or for any work performed in connection therewith.
3. The offers containing erasures or alterations will not be considered. There should be no hand-written material, corrections or alterations in the offer. Technical details must be completely filled up. SIDBI may treat proposals not adhering to these guidelines as unacceptable and thereby the proposal may be liable to be rejected.
4. Bidder shall promptly notify SIDBI of any event or conditions, which might delay the completion of project in accordance with the approved schedule and the steps being taken to remedy such a situation.
5. Bidder shall indemnify, protect and save SIDBI against all claims, losses, costs, damages, expenses, action suits and other proceedings, resulting directly or indirectly from an act or omission of Bidder, its employees, its agents, in the performance of the services provided by contract, infringement of any patent, trademarks, copyrights etc. or such other statutory infringements in respect of all components provided by Bidder as part of the delivery to fulfill the scope of this project.
6. Any publicity by Bidder in which the name of SIDBI is to be used should be done only with the explicit written permission of SIDBI.
7. Bidder is obliged to give sufficient support to SIDBI’s staff, work closely with SIDBI’s staff, act within its own authority, and abide by directives issued by SIDBI that are consistent with the terms of the order. Bidder is responsible for managing the activities of its personnel, and will hold itself responsible for any misdemeanors.
8. SIDBI reserves the exclusive right to make any amendments/ changes to or cancel any of the above actions or any other action related to this RFP.
9. Personnel engaged by the bidder for performance of its obligations under the work, shall, for all purpose, including applicability of law and welfare enactments, be the employee / staff of the bidder and they shall have no claim to be appointed in the services of the Bank. Bidder shall take suitable measures for them in this regard.

# **Delivery, Installation, Commissioning and Acceptance**

1. Bank shall provide the address and contact details for delivery of Solution while placing the order.
2. Delivery of all solution including hardware should be as per the schedule given in 4.6.11 from the date of receipt of the Purchase Order. Please note that no extra charges will be paid for transport to those locations.
3. Necessary insurance of the goods supplied by the bidder for the damage, theft etc. till the delivery and installation at the delivery locations.
4. The successful bidder should ensure complete installation, configuration and commissioning of the delivered solution including deployment of Hardware and complete all the works specified in the Annexures for Technical Specifications
5. If the Bidder lacks the expertise for a particular in-scope (except SIEM) tool then the OEM can provide implementation service and support for its own solution only on behalf of the Bidder without any extra cost to Bank or the Bidder will be held accountable for OEM‘s inaction and penalty charges would be levied as per the SLA terms to Bidder.
6. The Bank will conduct acceptance test before accepting each solution supplied under this project. In the acceptance test, the solution should be completely operational, the solution should comply with its respective technical specification, and the solution should integrate with the applicable devices / systems available with the Bank. The Bank may engage the services of the external consultant to conduct the User Acceptance Test.
7. The Installation will be deemed as incomplete if the solution is not operational or not acceptable to the Bank after acceptance testing / examination. The installation will be accepted only after complete commissioning of all solutions covered under this RFP. The date of commencement of contract will be the date when the Bank accepts all solutions covered under this RFP. The contract tenure for the solutions covered under this RFP will commence after acceptance by the Bank.

# **Responsibility for Completeness**

1. The bidder shall ensure that the Solution provided [Hardware / Software / Appliance etc.] meets all the technical and functional requirements as envisaged in the scope of the RFP.
2. The bidder shall deliver, install the equipment and port the software, and arrange for user level demo at bidder’s cost as per accepted time schedules. The bidder is liable for penalties levied by Bank for any deviation in this regard. The bidder shall provide for all drivers/software required to install, customize and test the system without any further charge, expense and cost to Bank.
3. All tools, testing instruments, as required during all operations such as transport, installation, testing, commissioning maintenance during contract period, shall be provided by the Bidder at no extra cost to the Bank for completing the scope of work as per this RFP.
4. The bidder shall supply along with each item all the related documents, Software Licenses and Other Items without any additional cost. The documents shall be in English. These will include but not restricted to User Manual, Operation Manual, Other Software and Drivers etc.
5. The bidder should guarantee that the hardware items delivered to the Bank are brand new, including all components. In the case of software, the bidder should guarantee that the software supplied to the Bank includes all patches, updates etc., and the same are licensed and legally obtained. All hardware and software must be supplied with their original and complete printed documentation.
6. The Bidder shall be responsible for any discrepancies, errors and omissions or other information submitted by him irrespective of whether these have been approved, reviewed or otherwise accepted by the bank or not. The bidder shall take all corrective measures arising out of discrepancies, error and omission other information as mentioned above within the time schedule and without extra cost to the Bank.

# **Change of name of the bidding company and line of business**

Normally, the Order will be placed on the successful bidder as per the details given in this document. But, if there is any change in name/address/constitution of the bidding Firm/Company at any time from the date of bid document, the same shall be informed by the bidders to the Bank immediately. This shall be supported with necessary documentary proof or Court orders, if any. Further, if the bidding Firm/Company is undergoing any re-organization/restructuring/merger/ demerger and on account such a change the Firm/Company is no longer performing the original line of business, the same shall be informed to the Bank. There shall not be any delay in this regard. The decision of the Bank to place orders or otherwise under such situation shall rest with the Bank and the decision of the Bank is final.

# **Governing Law and Jurisdiction**

The RFP and agreement that may be entered into pursuant thereto will be governed by and construed and enforced in accordance with the laws of India and the same shall be subject to the exclusive jurisdiction of the courts in Lucknow, India.

# **No third party rights**

No provision of the RFP the agreement that may be entered into is intended to, or shall, confer any rights on a third party beneficiary or other rights or remedies upon any person other than the parties hereto; nor impose any obligations on the part of the parties to the agreement towards any third parties.

# **Representations and Warranties**

In order to induce SIDBI to enter into the agreement, the Bidder shall be deemed to have represented and warranted as follows:

1. That the Bidder is a company which has meets the requisite eligibility qualifications mentioned in RFP, and it has power and the authority to enter into agreement and provide the services and implementation of platform, sought by SIDBI.
2. That the Bidder is not involved in any major litigation, potential, threatened and existing, that may have an impact of affecting or compromising the performance and delivery of services, systems.
3. That the representations made by the Bidder in its bid shall be deemed to continue to remain true and the bidder continues to fulfill the requirements as are necessary for executing the duties, obligations and responsibilities as laid down in the RfP, unless SIDBI in writing specifies to the contrary, the Bidder shall be bound by all the terms of the bid.
4. That the Bidder has the professional skills, personnel and resources / authorizations that are necessary for providing services as are necessary to perform its obligations under the bid and the agreement.
5. That the Bidder shall ensure that all assets including but not limited to software, licenses, databases, documents, etc. developed, procured, deployed and created during the term of the agreement are duly maintained and suitably updated, upgraded, replaced or substituted with regard to contemporary and statutory requirements.
6. That the Bidder shall procure all the necessary permissions, adequate approvals and licenses for use of various software and any copyrighted process / product free from all claims, titles, interests and liens thereon and shall keep SIDBI, its directors, officers, employees, representatives, consultants and agents indemnified in relation thereto.
7. That all the representations and warranties as have been made by the Bidder with respect to its bid and agreement are true and correct, and shall continue to remain true and correct throughout the term thereof.
8. That the execution of the services herein is and shall be in accordance and in compliance with all applicable laws as amended from time to time and the regulatory framework governing the same.
9. That there are no legal proceedings pending or threatened against Bidder or its team which adversely affect/may affect performance under this agreement; and no inquiries or investigations have been threatened, commenced or pending against the Bidder or its team members by any statutory or regulatory or investigative agencies.
10. That the Bidder has the corporate power to execute, deliver and perform the terms and provisions of the agreement and has taken all necessary corporate actions, consents and approvals to authorize the execution, delivery and performance by it of the agreement.
11. That neither the execution and delivery by the Bidder of the agreement nor the Bidder’s compliance with or performance of the terms and provisions of the agreement (i) will contravene any provision of any applicable law or any order, writ, injunction or decree of any court or governmental authority binding on the Bidder, (ii) will conflict or be inconsistent with or result in any breach of any of the terms, covenants, conditions or provisions of, or constitute a default under any agreement, contract or instrument to which the Bidder is a party or by which it or any of its property or assets is bound or to which it may be subject or (iii) will violate any provision of the Memorandum and Articles of Association of the Bidder.

# **Vicarious Liability**

The selected bidder shall be the principal employer of the employees, agents, contractors, sub-contractors etc., engaged by the selected bidder and shall be vicariously liable for all the acts, deeds, matters or things, whether the same is within the scope of power or outside the scope of power, vested under the contract. No right of any employment in the Bank shall accrue or arise, by virtue of engagement of employees, agents, contractors, subcontractors etc. by the selected bidder, for any assignment under the contract. All remuneration, claims, wages dues etc. of such employees, agents, contractors, sub-contractors etc. of the bidder shall be paid by the selected bidder alone and the Bank shall not have any direct or indirect liability or obligation, to pay any charges, claims or wages of any of the selected bidder’s employees, agents, contractors, subcontractors etc. The selected bidder shall agree to hold the Bank, its successors, assigns and administrators fully indemnified, and harmless against loss or liability, claims, actions or proceedings, if any, whatsoever nature that may arise or caused to the Bank through the action of selected bidder’s employees, agents, contractors, subcontractors etc.

# **No Set-off, counter-claim and cross claims**

In case the Vendor/ Bidder has any other business relationship with SIDBI, no right of set-off, counter-claim and cross-claim and or otherwise will be available under this Contract/Agreement to the Vendor/ Bidder for any payments receivable under and in accordance with that business.

# **Governing Language**

* 1. The Contract shall be written in English. All correspondence and other documents pertaining to the Contract, which are exchanged by the parties, shall be written in English.
  2. The technical documentation involving detailed instruction for operation and maintenance, users' Manual etc. is to be delivered with every unit of the equipment supplied. The language of the documentation should be English.

# **Insurance**

* 1. The Bidder is responsible for acquiring insurance for all components, equipment and software. The goods supplied under the Contract shall be fully insured.
  2. The insurance shall cover “All Risks” (fire, burglary, natural calamities such as Earth quake, floods, power fluctuations etc.) till the end of contract period. If the vendor fails to obtain insurance cover and any loss or damage occur, the vendor will have to replace the items with new ones without any cost to the Bank.
  3. Where the Supplier is required under the Contract to transport the Goods to a specified place of destination within India, transport to such place of destination in India, including insurance and storage, as shall be specified in the Contract, shall be arranged by the Supplier
  4. Should any loss or damage occur, the Bidder shall
     1. Initiate and pursue claim till settlement, and
     2. Promptly make arrangements for replacement of any damaged item/s irrespective of settlement of claim by the underwriters

# **Conflict of Interest**

1. The service provider shall disclose to the Bank in writing, all actual and potential conflicts of interest that exists, arises or may arise in the course of performing the obligation(s) as soon as it becomes aware of that conflict
2. If a bidder submits bid on behalf of the OEM, the same bidder shall not submit a bid on behalf of another OEM for same item / product.
3. Either the bidder on behalf of the OEM or the OEM itself can bid but both cannot bid simultaneously for the same make model of the item under procurement.

# **Patent Rights**

In the event of any claim asserted by a third party of infringement of copyright, patent, trademark, industrial design rights, etc. arising from the use of the Goods or any part thereof in India or abroad, the Supplier shall act expeditiously to extinguish such claim. If the Supplier fails to comply and the Bank is required to pay compensation to a third party resulting from such infringement, the Supplier shall be responsible for the compensation including all expenses, court costs and lawyer fees. The Bank will give notice to the Supplier of such claim, if it is made, without delay

The Bank will give notice to the supplier of any such claim without delay, provide reasonable assistance to the Supplier in disposing of the claim, and shall at no time admit to any liability for or express any intent to settle the claim.

# **Business Continuity**

The bidder agrees for the following continuity arrangements to ensure the business continuity of the Bank:

1. In the event of this agreement comes to end on account of termination or by the expiry of the term/renewed term of the agreement or otherwise, the bidder shall render all reasonable assistance and help to the Bank and to any new service provider engaged by the Bank, for the smooth switch over and continuity of the services.
2. In the event of failure of the bidder to render the service, without prejudice to any other right the Bank shall have as per this agreement, the bank at its sole discretion may make alternate arrangements for getting the services from any other source. And if the bank gives a prior notice to the service provider before availing such service from any other alternative source, the service provider shall be liable to reimburse the expenses, if any incurred by the bank in availing such services from the alternative source.

# **Privacy and Security Safeguards**

1. SIDBI has the sole ownership of and the right to use, all data that may be in possession of the Successful bidder/Service provider or its representative in the course of performing the services under the agreement/contract that may be entered into. All documents, report, information, data etc. collected and prepared by bidder in connection with the scope of work submitted to SIDBI will be property of the Bank. The bidder shall not be entitled either directly or indirectly to make use of the documents, reports given by SIDBI for carrying out of any services with any third parties. Successful Bidder shall not without the prior written consent of SIDBI be entitled to publish studies or descriptive article with or without illustrations or data in respect of or in connection with the performance of services.
2. The bidder shall not publish or disclose in any manner, without the Banks prior written consent, the details of any security safeguards designed, developed or implemented by the bidder under this contract or existing at any Bank location. The bidder shall develop procedures and implementation plans to ensure that IT resources leaving the control of the bank (removed for repair, replaced or upgraded) are cleared of all Bank data and software. The bidder shall also ensure that all subcontractors (if permitted in contract) who are involved in providing such security safeguards or part of it shall not publish or disclose in any manner, without the Banks prior written consent, the details of any security safeguards designed, developed or implemented by the bidder under this contract or existing at any Bank location

# **GST law**

The bidder has to submit an Undertaking Letter for GST Law as per Annexure – 11.12, mentioning its compliance with all applicable GST Laws including GST Acts, Rules, Regulations, Procedures, Circulars & Instructions there under applicable in India from time to time and to ensure that such compliance is done.

# **Non-Assignment**

Neither the subject matter of the contract nor any right arising out of the contract shall be transferred, assigned or delegated to any third party by Vendor without prior written consent of the Bank.

# **Conflict 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 in this RFP. 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.

# **Signing of Contract**

1. The selected bidder has to sign a contract with the Bank as per the terms and conditions of the RFP on a non-judicial stamp-paper of appropriate value. This initial contract will be called as the Master Service Agreement (MSA) which will act as the comprehensive contract document between the Bank and the service provider for all purpose/conditions related to the RFP. The MSA will be the permanent reference & the contract document (with subsequent modifications, if any). The modifications to the MSA during the period of contract will be mutually agreed and will be accommodated in the form of addendum/schedules to the MSA since procedural aspects, services etc. will be continuously evolving.
2. The agreement shall include all terms and conditions, specifications of RfP and also the Bill of Material and price as agreed finally after Bid evaluation and negotiation. The agreement shall be executed in English language in one original, the Bank receiving the duly signed original and selected service provider receiving the photocopy. The contract agreement shall be valid till all the contractual obligations are fulfilled.
3. On behalf of the Bank, MSA will be signed by the Officials of IT Vertical at Mumbai.

# **Tax Deduction at Source**

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

# **Acceptance**

1. The acceptance / performance test will be performed after completion of installation and commissioning of all the services at respective location. Complete hardware and Software as specified in the tender must have been supplied & installed properly by the Bidder prior to acceptance of the same.
2. The acceptance test will be conducted by the Bank, their consultant or other such person nominated by the Bank at its option. The Bidder will be responsible for setting up and running the acceptance test without any extra cost to the Bank.
3. The Installation will be deemed as incomplete if any component of the hardware / software / links are not delivered or are delivered but not installed and / or not operational or not acceptable to the Bank after acceptance testing/ examination. In such an event, the supply and installation will be termed as incomplete and system(s) will not be accepted and the warranty period will not commence. The installation will be accepted only after complete commissioning of hardware.
4. In the event of hardware /software / links failing to pass the acceptance test, a period not exceeding one week will be given to rectify the defects and clear the acceptance test, failing which the Bank reserves the right to get the corresponding component replaced by the Bidder at no extra cost to the Bank or to cancel the order and recall all the payments made to the bidder by the bank along with interest.
5. Successful conduct and conclusion of the acceptance tests for the installed components shall also be the sole responsibility and at the cost of the Bidder. During acceptance testing the bidder has to demonstrate all the features of the respective hardware items.
6. The Bank ’s right to inspect, test and, where necessary, reject the Goods after the Goods’ arrival at destination shall in no way be limited or waived by reason of the Goods having previously been inspected, tested and passed by the Bank or its representative prior to the shipment of the goods.

# **Service Level Agreement & Liquidated Damages**

Liquidated damages clause is defined as follows for different purposes. All of them are independent of each other and several and cumulative and not exclusive of each other.

1. Bank reserves the right to adjust the Liquidity damages (LD), if any, against any amount payable to the bidder or will be adjusted against the PBG.
2. Liquidated damages would not be applicable for delay due to reasons attributable to the Bank and Force Majeure. However, it is responsibility of the selected bidder to prove that the delay is attributed to the Bank or Force Majeure.
3. However the Liquidated damages to be recovered under above clauses shall be restricted & capped to 10% of the total value of the order for each year independently during the contract period.

# **Liquidated damages for delay in Delivery and Installation of Hardware and Software**

1. The bidder is expected to procure and install all the security solutions as per the timelines mentioned in Implementation Timelines (section 4.10).
2. In case, if there is delay in delivery of the hardware & software, installation of the security solutions and associated hardware, software and software licenses, as given in commercial bid, beyond the schedule given in Section 4.10 from date of issue of PO, then LD at the rate of 1% per week of the cost quoted against each of respective item as mentioned in Commercial Bid for items not delivered will be levied per week or part thereof (on pro rata basis for the no. of days) and deducted against bills submitted.
3. The integration of all the security solutions with SIEM should be completed within a period as mentioned in the section 4.10 from the date of issue of PO. In case of delay in integration beyond three months, LD at the rate of 1% per month of the cost quoted against SIEM as mentioned in Commercial Bid will be levied per month for the no of days of delay (on pro rata basis for the no. of days) and deducted against bills submitted.
4. Liquidated Damages for non-performance: If the specifications of the RFP are not met by the bidder during various tests, the bidder shall rectify or replace the same at bidders cost to comply with the specifications immediately to ensure the committed uptime, failing which the Bank reserves its right to reject the items.

# **Liquidated damages for not maintaining uptime**

1. The bidder shall guarantee 24x7 availability with monthly uptime of 99% for the all the solutions under this project during the period of the Contract.
2. The "Uptime" is, for calculation purposes, equals to the Total contracted hours in a quarter less the Downtime. The "Downtime" is the time between the Time of Failure and Time of Restoration within the contracted hours. "Failure" is the condition that renders the Bank unable to perform any of the defined functions. "Restoration" is the condition when the selected bidder demonstrates that the solution is in working order and the Bank acknowledges the same.
3. If the Bidder is not able to attend the troubleshooting calls on solution 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 Bidder shall provide the Monthly uptime reports during the warranty period and AMC period, if contracted.
4. The Downtime calculated shall not include any failure due to bank, third party and Force Majeure.
5. The percentage uptime is calculated on monthly basis as follows:

(Total contracted hours in a quarter – Downtime hours within contracted hours) \*100

Total contracted hours in a quarter

1. If the bidder fails to maintain the guaranteed uptime, LD based on Level of availability of uptime will be deducted as under:

|  |  |  |  |
| --- | --- | --- | --- |
| **S. No.** | **Service Area** | **Uptime % calculated on quarterly basis** | **Liquidated Damages (LD)** |
| 1 | CSOC Operations Failure including any device (hardware / software) failure resulting in failure of CSOC operations | 99% and above | NA |
| 97% to 99% | 1% of Total CSOC Monitoring and Operations cost for each failure |
| 95% to 96.99% | 5% of Total CSOC Monitoring and Operations cost for each failure |
| Less than 95% | 10% of Total CSOC Monitoring and Operations cost for each failure |
| 2 | Individual Security / Device solution (Hardware / Software) Failure (including Incident Management Tool, SAN, backup tape solution). SIEM failure will be considered as total failure and liquidated damage will be as per the point 1. | 99% and above | NA |
| 97% to 99% | 10% of Notional AMC charges for each failure |
| 95% to 96.99% | 20% of Notional AMC charges for each failure |
| Less than 95% | 50% of Notional AMC charges for each failure |

1. For hardware / software items whether under AMC or under warranty, notional AMC / License fee shall be calculated at 10% of the asset value or their actual AMC cost quoted after expiry of warranty period, whichever is higher, will be considered for the purpose of calculating LD.
2. For repeat failure, same or higher LD will be charged depending upon the delay in rectification of the problem.
3. LD will be calculated on Quarterly basis and deducted against the Quarterly payments.
4. In case of CSOC operations failure, the LD will be charged for both CSOC Operations failure and individual security solution/device failure.
5. In the case of failure of P2P Link, the proportionate cost of the no. of day’s service not available will be deducted.
6. For the L1, L2 and L3 resources for the leave of absence: - Each on-site resource shall be granted a maximum up to 01 (One) day leave per month. However, substitute should be provided. LD will be levied for any absence for which no substitute is arranged by the Service Provider as per defined in the below table. The LD charges will be in addition to the pro rata charges for the resources for their days of absence.

|  |  |
| --- | --- |
| Resource Category | Liquidated Damages beyond leave of absence |
| Support Resources | * L1 Resource - Rs.2000/- per day maximum Rs.10000/- per month * L2 Resource - Rs.2500/- per day maximum Rs.15000/- per month * L3 Resource - Rs 3000/- per day maximum Rs 20000/- per month |

1. The Bank reserves right to recover / adjust the LD from any dues pending to the bidder.
2. However, the maximum LD levied shall not be more than the 10% of total value of the order per quarter.
3. If quarterly uptime of CSOC operations is less than 95%, the Bank shall levy LD as above and shall have full right to issue notice & seek explanation under this RFP. The above LD shall be deducted from any payments due to the bidder.

# **SLAs & Liquidity Damages for CSOC Operations**

|  |  |  |  |
| --- | --- | --- | --- |
| **S. No** | **Service Area** | **Service Level** | **Liquidated Damages** |
| 1 | Monitoring, Analysis & Incident Reporting | * 24x7 monitoring and reporting of all in-scope devices * Categorization of events into  Critical, High, Medium and Low priority shall be carried out in consultation with the selected bidder during the contracting period. * All Critical, High and Medium priority events should be logged as incident tickets and responded as per SLA. * Events along with action plan/ mitigation steps should be alerted to designated bank personnel as per the below SLA:   1) Critical events within 15 minutes of the event identification.  2) High priority events within 30 minutes of the event identification.  3) Medium and Low priority events within 60 minutes of the event identification. | * Critical Events: -   10% of quarterly CSOC Monitoring and Operations cost   * High Priority Events: -   5% of quarterly CSOC Monitoring and Operations cost   * Medium/Low Priority Events: -   3% of the quarterly CSOC Monitoring and Operations cost   * Low Priority/ Operational Events need to be logged  and maintained for reference.   An incident ticket need not be raised for such incidents. However, these need to be included in the daily reports. |
| 2. | Incident Resolution | For the devices/ solutions managed and administrated by the bidder  1. Critical incidents within 60 minutes of the event Identification.  2. High priority incidents within 90 minutes of the event identification.  3. Medium priority incidents within 120 minutes of the event identification. | Critical Incidents:  10% of quarterly CSOC Monitoring and Operations cost  High Incidents:  5% of quarterly CSOC Monitoring and Operations cost  Medium Priority Incidents:  3% of quarterly CSOC Monitoring and Operations cost  Low Priority/ operational incidents need to be logged and maintained for reference. These need to be included in the daily reports |
| 3. | Reports and  Dashboard | Daily Reports:  Critical reports should be submitted on a daily basis by 11:00 AM  Weekly Reports:  By 11:00 AM, Monday  Monthly Reports:  3rd working day of each month | 1) Delay in reporting for daily report for more than 2 hours shall incur a liquidated damage of Rs. 100/- per hour, maximum of Rs. 1000/- per day  2) Delay in reporting by more than 2 days for both weekly and monthly reports shall incur a LD of Rs. 1500/- per day, maximum of Rs. 4500/- per month |
| 4. | Vulnerability  Assessment | The bidder is expected conduct Vulnerably Assessments by using existing tools (Beyond Trust Retina CS, NESSUS, Nipper)  1) To be conducted for identified devices once every month based on a calendar documented in coordination with the bank to ensure that business operations are not impacted  2) Ad-hoc scan to be conducted for the new devices as and when required by the bank.  3) To identify new device in DC, DR and near DR and add the same to the network vulnerability management tool | 1. If the monthly periodic scan is not conducted for more than 35 days in any system/devices will incur Rs. 100 per system/device. 2. Delay in performing ad - hoc VA scan and providing report by more than 24 hours shall incur Rs. 500 per instance. 3. Delay in adding new devices (in DC, DR and Near DR) for more than 24 hours after reporting will incur Rs. 500 per instance. |
| 5 | VAPT advisory &  remediation  services | The bidder is expected to provide advisory-cum-remediation services for VAPT comments generated by internal and external vulnerability assessment and penetration testing.  Provide steps for fixing the vulnerabilities and/or suggest Bank’s team of compensating controls that needs to be implemented in order to circumvent the vulnerability Implement the resolution in Bank’s test setup. Upon getting Bank team’s concurrence, proceed with production resolution. In the case of application dependencies, the details shall be provided and compensating controls suggested, wherever possible | 1. Delay in providing steps for fixing the critical vulnerabilities within 3 working days after reporting will incur Rs. 100 per vulnerability.  2. Delay in providing steps for fixing the medium vulnerabilities within 7 working days after reporting will incur Rs. 300 per vulnerability  3. Delay in providing steps for fixing the low vulnerabilities within 30 working days after reporting will incur Rs.500 per vulnerability  4. Delay in implementing the  resolution in banks test setup for more than 5 days after getting approval from bank will incur Rs. 500 per instance. |
| 6 | Periodic Reviews | The bidder is expected to improve the operations on an on-going basis.  The bidder is expected to provide a quarterly report of the new improvements suggested, action plans, and the status of these improvements to the bank. The CSOC project sponsor or  location delegate from the bidder is expected to conduct a quarterly  review meeting with participating bank officials resulting in a report covering details about current CSOC SLAs, status of operations, key threats and new threats identified, issues and challenges etc. | Quarterly meeting for next three years to be conducted on the 25th (tentatively) of each month during the operations  phase.  A delay of more than Five days will incur a LD of 1% of quarterly CSOC Monitoring and Operations cost for that quarter |
| 7 | Security Intelligence Services | Advisories within 12 hours of new global threats & vulnerabilities disclosures. | A delay of more than Five days will incur a LD of 1% of quarterly CSOC Services cost for that quarter |
| 8 | New Patches | New patches are applied within three months of them becoming generally available to all related technologies supplied by the bidder. | A delay of more than Five days will incur a LD of 10% of quarterly CSOC Monitoring and Operations cost for that quarter. |
| 9. | Security Device Management and Administration | Bidder is expected to provide this service 24/7 basis. Management and administration of all security devices / solutions supplied under CSOC. | 1. For more than 4 hours delay (after the banks confirmation) for rule modification OR for wrong rule modification in any of the security devices / solutions will incur a LD of 10% of quarterly CSOC Monitoring and Operations cost for that quarter. |
| 10 | Optional Components | Bidder is expected to provide the optional components if required for future implementation / integration of all security devices / solutions supplied under CSOC. | For more than 4 weeks delay for implementation, the bidder will incur a LD of 1% of quarterly CSOC Monitoring and Operations cost for that quarter. |

1. All the above LDs are independent of each other and are applicable separately and concurrently.
2. LD is not applicable for the reasons attributable to the Bank and Force Majeure.

# **Waiver**

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

# **Annexure for Pre-Qualification Criteria**

# **Annexure 8.1 Covering Letter for Pre-Qualification Criteria**

*(To be submitted on bidder’s company letter head)*

Place: \_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_

To,

General Manager [ITV]

Small Industries Development Bank of India

SIDBI Tower,

15, Ashok Marg,

Lucknow,

Uttar Pradesh - 226001

Dear Sir,

IMPLEMENTATION AND MANAGEMENT OF CYBER SECURITY OPERATIONS CENTER (CSOC)

1. We, the undersigned, offer to submit our bid in response and accordance with your tender \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ dated \_\_\_\_\_\_\_\_\_\_\_\_\_ having examined the tender document including all Annexures carefully, hereby submitting our proposal along with all the requisite EMD, tender fee and other documents as desired by the Bank.
2. Further, we agree to abide by all the terms and conditions as mentioned herein the tender document. We agree to abide by this offer till nine (9) months from the date of last day for submission of offer (Bid).
3. If our offer is accepted we undertake to deploy Resources for Implementation and Management of Cyber Security Operations Centre (CSOC) for a period of three years starting from the acceptance date by the Bank.
4. If our offer is accepted we undertake to provide on-site comprehensive service support and warranty for three years for the hardware / software supplied as per the above referred RFP, post sign off of Phase-1.
5. We undertake that, in competing for (and, if the award is made to us, in executing) the above contract, we will strictly observe the laws against fraud and corruption in force in India namely “Prevention of Corruption Act 1988”.
6. We have also noted that SIDBI reserves the right to consider/ reject any or all bids without assigning any reason thereof.
7. We understand that the Bank is not bound to accept any proposal it receives.

Yours sincerely,

Authorized Signatories

Name: \_\_\_\_\_\_\_\_\_\_\_\_

Designation: \_\_\_\_\_\_\_\_\_\_\_\_

Name of Organisation: \_\_\_\_\_\_\_\_\_\_\_\_

Company Seal: \_\_\_\_\_\_\_\_\_\_\_\_

# **Annexure 8.2** **Pre-Qualification Criteria for Bidder**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S.No.** | **Pre-Qualification Criteria** | **Document Support** | **Compliance (Yes/No)** | **Page No. of Response** |
| 1 | The Bidder should be a registered company in India for a period of minimum 5 years as on 31.12.2018 | Certificate of Incorporation |  |  |
| 2 | The proposed bidder should have presence in India and should be able to support project in India (Mumbai and Chennai) during the contract period. | An undertaking letter to be enclosed by the Bidder confirming the same and provide its Head office address as per Annexure 8.5 |  |  |
| 3 | The bidder should be involved in providing SOC/ CSOC in India for a minimum of three years as on 31.12.2018 | PO copy or client’s certificate substantiating the engagement which is 3 years or older. |  |  |
| 4 | The bidder should have atleast 200 crores turnover per year in the past 03 years (2015-16, 2016-17 and 2017-18) from their India Operations | Audited balance sheets and certificate from CA to be submitted. |  |  |
| 5 | The bidder should have earned net profit during any two of the last three financial years (i.e. 2015-16, 2016-17 and 2017-18) from their India operations. | Audited balance sheets and certificate from CA to be submitted. |  |  |
| 5 | The Bidder should not have been blacklisted by any Government authority or Public sector Undertaking (PSU) as on date of submission of the tender, otherwise the bid will not be considered. | An undertaking (on their letter head) in this regard should be enclosed by the Bidder on behalf of the directors/partners.  Self-declaration in section 8.4 and 8.5 to be submitted by POA. |  |  |
| 6 | The Bidder must have implemented / under implementation of Security Operations Center (SOC) / Cyber Security Operations Centre (CSOC) in at least 2 BFSI customers in India having project cost of 5 crores and above  The project cost for these implementations should be as below:  one project cost should be 15 crores and above **and**  one project cost of 5 crore and above  Note: BFSI institutions for this purpose indicates Banking, Financial institution and Insurance excluding RRBs and Co-Operative Banks. | A PO copy along with a self-declaration on the letter head of the organization submitting the reference jointly signed by the authorized signatory provided it includes the following with no exceptions as per the below format:   |  |  |  | | --- | --- | --- | | Parameters | Project A (15 crore and above) | Project B  (5 crore and above) | | Organization Name |  |  | | Contact Details |  |  | | Implemented Scope |  |  | | Project cost in Rupees |  |  | |  |  |
| 7 | The bidder should have implemented SIEM in the BFSI institutions  **and**  any Two of the following solution should be implemented in the above-mentioned institutions:   1. Anti-Advanced Persistent Threat Management (APT) 2. Privilege Identity Management (PIM) 3. Firewall Analyzer 4. Network Access Control (NAC) | A PO copy along with a self-declaration on the letter head of the organization submitting the reference jointly signed by the authorized signatory provided it includes the following with no exceptions:   |  |  | | --- | --- | | Parameters | Project Details | | Organization Name |  | | Contact Details |  | | SIEM Implementation (Yes/No) |  | | Implemented Solutions | i. | | ii. | |  |  |
| 8 | The bidder should have a minimum of 10 individuals with minimum two years of experience in implementation and management of Security Operations Center or Cyber Security Operations Centre or both. All resources must be on the payroll of the bidder. | Resume / CV for each of these members  Self-declaration to this effect on company's letter head signed by authorized signatory of the Bidder. |  |  |
| 9 | The Bidder should be ISO 27001 Certified | Certification copy required |  |  |
| 10 | The bidder should not submit more than one bid for self or through all its associates / subsidiaries / sister concerns / parties etc. | An undertaking letter to be enclosed by the Bidder confirming the same. |  |  |
| 11 | The bidder should submit Pre-contract Integrity Pact as part of pre-qualification criteria bid | On Non judicial stamp paper to be submitted as per format Annexure 8.10 |  |  |
| 12 | The Bidder should not be existing Service provider providing services for Network Management (NOC) / Facility Management / Data Centre Services / Data Centre Management for SIDBI to avoid conflict of interest. | An undertaking letter to be enclosed by the Bidder confirming the same. |  |  |
| 13 | The proposed OEM solutions for this implementation should have been implemented / under implementation in minimum of one BFSI organizations in India | * Enclosed copies of reference letter provided by clients where solution is implemented. The details are to be submitted   (or)   * PO supporting all references provided.   (and)   * Client references along with contact details. |  |  |
| 14 | The bidder company should not be owned or controlled by any Director, employee (or  Relatives) of SIDBI. | Self-declaration to this effect on company's  letter head signed by company’s authorized  Signatory with Company seal. |  |  |

**I certify that the above mentioned information and the relevant annexure and enclosures are true and correct**

Date

Place

Authorized Signatories

Name: \_\_\_\_\_\_\_\_\_\_\_\_

Designation: \_\_\_\_\_\_\_\_\_\_\_\_

Name of Organisation: \_\_\_\_\_\_\_\_\_\_\_\_

Company Seal: \_\_\_\_\_\_\_\_\_\_\_\_

**Note**

* Bidder response should be complete with all relevant documents attached.
* Documentary proof, sealed and signed by authorized signatory, must be submitted
* Details of clients and relevant contact details are mandatory. Bidders may take necessary approval of the clients in advance before submission of related information. SIDBI will not make any separate request for submission of such information.
* SIDBI will contact the bidder referenced customer for verifications of facts, the bidder to ensure that the customer is intimated. Further in case SIDBI feels to visit the site, the bidder to take necessary approvals for the same. SIDBI will not make any separate request to the bidders customers.
* Proposal of the bidders are liable to be rejected in case of incomplete information or wrong information or non-submission of documentary proof.

# **Annexure 8.3 General Information about Bidder**

|  |  |  |
| --- | --- | --- |
| **S.No.** | **Description** | **Bidder Response** |
| 1 | Name of the bidder company  (Registered name of the bidding Company) |  |
| 2 | Details of Incorporation of the Company | Date:  Ref. No. |
| 3 | Type of Company  [Government/PSU/Pub. Ltd / Pvt. Ltd / Partnership / proprietary] |  |
| Registration No. and date of registration.  Copy of Registration Certificate to be enclosed (Yes / No) |  |
| 4 | Website of Company |  |
| 5 | Address of Registered Office with contact numbers |  |
| 6 | Address for Correspondence with contact number (if different from above). |  |
| 7 | PAN Number (Copy of PAN to be enclosed) |  |
| 8 | Sales Tax Registration No. (Copy of Sales Tax certificate to be enclosed) |  |
| 9 | GST / Service Tax Registration No. (Copy of GST / Service Tax certificate to be enclosed) |  |
| 10 | Contact Details of Bidder’s authorized signatories to make commitments to SIDBI | Name:  Designation:  Mobile:  Email: |
| **11** | **Financials (for last three years)** |  |
| 11.A | Annual Turnover | 2015-16:  2016-17:  2017-18: |
| 11.B | Net Profit | 2015-16:  2016-17:  2017-18: |
| 11.C | CA certificate attached for A and B above |  |
| 11.D | 1. Audited balance sheet and  2. P/L account attached. |  |
| **12** | **EMD Details** |  |
| 12.A | DD / Pay Order / Bank Guarantee |  |
| 12.B | Number |  |
| 12.C | Date of Issue |  |
| 12.D | Issuing Bank |  |
| 12.E | Amount (Rs) |  |
| **13** | **Tender Form Cost Details** |  |
| 13.A | DD / Pay Order / Bank Guarantee |  |
| 13.B | Number |  |
| 13.C | Date of Issue |  |
| 13.D | Issuing Bank |  |
| 13.E | Amount (Rs) |  |
| **14** | **MSME Status** |  |
| 14.A | Company does not qualify the status of MSE. |  |
| 14.B | Company does qualify the MSE status. |  |
| 14.C | SC/ST |  |
| 14.D | MSE registration certificate or a certificate from Chartered Accountant attached. (Yes/No) |  |
| **15** | **Bank Details** |  |
| 15.A | Bank Name |  |
| 15.B | Branch Name |  |
| 15.C | Branch / IFSC Code |  |
| 15.D | Account Type ( Saving / Current / Cash Credit ) |  |
| 15.E | Account Number ( Please attach a cancelled cheque of your bank for ensuring accuracy of the bank name, branch name, branch / IFSC code and Account Number) |  |

Authorized Signatories

Name: \_\_\_\_\_\_\_\_\_\_\_\_

Designation: \_\_\_\_\_\_\_\_\_\_\_\_

Name of Organisation: \_\_\_\_\_\_\_\_\_\_\_\_

Company Seal: \_\_\_\_\_\_\_\_\_\_\_\_

# **Annexure 8.4 Power of Attorney**

*(To be executed on a non-judicial stamped paper of requisite value based on place of execution)*

BY THIS POWER OF ATTORNEY executed on \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, 2019, We \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, a Company incorporated under the Companies Act, 1956, having its Registered Office at \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (hereinafter referred to as “the Company”) doth hereby nominate, constitute and appoint <Name>, <Employee no.>, < Designation> of the Company, as its duly constituted Attorney, in the name and on behalf of the Company to do and execute any or all of the following acts, deeds, matters and things, namely :-

* Execute and submit on behalf of the Company a Proposal and other papers / documents with ‘Small Industries Development Bank of India’ (“SIDBI”) relating to ‘Request for proposal No. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ For "Implementation and Management of Cyber Security Operations Centre (CSOC)" and to attend meetings and hold discussions on behalf of the Company with SIDBI in this regard.

THE COMPANY DOTH hereby agree to ratify and confirm all whatsoever the attorney shall lawfully do or cause to be done under or by virtue of these presents including anything done after revocation hereof but prior to actual or express notice thereof being received by the person or persons for the time being dealing with the attorney hereunder.

IN WITNESS WHEREOF, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ has caused these presents to be executed by \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ on the day, month and year mentioned hereinabove.

For and on behalf of the Board of Directors of

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

I Accept

\_\_\_\_\_\_\_\_\_\_\_\_ (Signature)

(Name, Title and Address of the Attorney)

# **Annexure 8.5 Declarations**

*(To be submitted on bidders company letter head)*

Date: \_\_\_\_\_\_\_\_\_

To

General Manager [ITV]

Small Industries Development Bank of India

SIDBI Tower,

15, Ashok Marg,

Lucknow,

Uttar Pradesh - 226001

Dear Sir,

IMPLEMENTATION AND MANAGEMENT OF CYBER SECURITY OPERATIONS CENTER (CSOC)

I have carefully gone through the Terms & Conditions contained in the RFP No. \_\_\_\_\_\_\_\_\_\_\_ regarding selection of the bidder for a period of three years.

We hereby declare the following:

* Our company has not been debarred/ black listed by any Public Sector Bank, RBI, IBA or any other Government / Semi Government organizations in India during last 05 years.
* Neither the Company nor our Partners/Promoters/Directors are defaulters to any Financial Institution.
* Our company have minimum of 10 resources with minimum two years of experience in implementation and management of Security Operations Center on our payroll.
* Our company is directly participating in this RFP with only one bid and not participating through our subsidiaries, associates or related parties.
* Our company has presence in India and we will be able to support project in India (Mumbai and Chennai) during contract period.
* The proposed OEM has presence in India and we will be able to support project in India (Mumbai and Chennai) during contract period.
* We further declare that we are eligible and competent as per the Pre-Qualification Criteria given by the bank and the information submitted by the company in Annexure 8.2 & 8.3 are true and correct and also we would be able to perform this contract as per RFP document.
* We further declare that the compliance provided for specifications and features of solutions as per technical requirements in Annexure 11 are true and correct.
* We further declare that we are not existing Service provider providing services for Network Management (NOC) / Facility Management / Data Centre Services / Data Centre Management for SIDBI to avoid conflict of interest.
* We also undertake that, we are not involved in any legal case that may affect the solvency / existence of our firm or in any other way that may affect capability to provide the services for the contracted period.
* We declare that our company is not owned or controlled by any Director, employee (or Relatives) of SIDBI.

I further certify that I am competent officer in my company to make this declaration that our bid and its terms & conditions is binding on us and persons claiming through us and that you are not bound to accept a bid you receive.

Authorized Signatories

Name: \_\_\_\_\_\_\_\_\_\_\_\_

Designation: \_\_\_\_\_\_\_\_\_\_\_\_

Name of Organisation: \_\_\_\_\_\_\_\_\_\_\_\_

Company Seal: \_\_\_\_\_\_\_\_\_\_\_\_

# **Annexure 8.6 Bank Mandate Form**

*(To be submitted in duplicate)*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1 | Name of Borrower / Vendor / Supplier: | |  | |
| 2 | Address of the Borrower / Vendor / Supplier: | |  | |
| City |  | E – mail Id |  |
| Pin Code |  | Mobile No. |  |
|  | Phone No. with STD Code | | |  |
| 3 | Permanent Account Number | | |  |
| 4 | MSE Registration / CA Certificate | | |  |

5. Particulars of Bank Account

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Beneficiary Name |  | | | | |
| Bank Name |  | Branch Name | |  | |
| Branch Place |  | Branch City | |  | |
| PIN Code |  | Branch Code | |  | |
| MICR Number |  | | | | |
| Account Type (Saving / Current / Cash Credit) |  | | | | |
| Account Number (as appearing in Cheque Book) |  | | | | |
| (Code number appearing on the MICR1 cheque supplied by the Bank. Please attach a cancelled cheque of your bank for ensuring accuracy of the bank name, branch name & code and Account Number) | | | | | |
| IFSC Code2 | For RTGS Transfer |  | For NEFT Transfer | |  |

6. I hereby declare that the particulars given above are correct and complete. If any transaction is delayed or not effected for reasons of incomplete or incorrect information, I shall not hold SIDBI / IDBI Bank responsible. I also undertake to advise any change in the particulars of my account to facilitate updations of records for purpose of credit of amount through RBI RTGS/NEFT.

Place: \_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_\_

Signature of party / Authorized Signatory

…………………………………………………………………………………………………………………………..

Certified that particulars furnished above are correct as per our records.

Bank’s stamp:

Date:

Signature of Authorized Official from the Bank

# **Annexure 8.7 EMD / Bid Security Form**

*(Sample Format – To be executed on a non-judicial stamped paper of requisite value)*

To: SMALL INDUSTRIES DEVELOPMENT BANK OF INDIA

WHEREAS …………………………………………………….. (Name of Vendor) (Hereinafter called the ‘the Vendor”) has undertaken, in pursuance of Request for Proposal (RFP) No. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ For Implementation and Management of Cyber Security Operations Center (Herein after called the ‘the RFP”) to you.

AND WHEREAS, it has been stipulated by you in the said RFP that the Vendor shall furnish you with a Bank Guarantee from a commercial Bank for the sum specified therein, as security for compliance with the Vendor’s performance obligations in accordance with the RFP.

AND WHEREAS we ----------------Bank having its registered office at ----- and inter alia a branch office situated at ------- have agreed to give a performance guarantee in lieu of EMD of Rs --------- (Rupees ------------------ only) on behalf of the Vendor.

We ------------------- Bank further undertake not to revoke and make ineffective the guarantee during its currency except with the previous consent of the buyer in writing.

We ------ Bank do hereby unconditionally and irrevocably undertake to pay to SIDBI without any demur or protest, merely on demand from SIDBI, an amount not exceeding Rs. ---------- (--------- only).by reason of any breach of the terms of the RFP dated ---- by vendor. We hereby agree that the decision of the SIDBI regarding breach of the terms of the RFP shall be final, conclusive and binding

WE do hereby guarantee and undertake to pay forthwith on demand to SIDBI a sum not exceeding Rs……………/-. (Rupees ………………………….. …only) (amount of the Guarantee in words and figures) and we undertake to pay you upon your first written demand declaring the Vendor to be in default under the RFP and without cavil or argument, any sum or sums within the limit of Rs……………/-. (Rupees …………………………..… only) (Amount of guarantee) as aforesaid, without your needing to prove or to show grounds or reasons for your demand or the sum specified therein.

Our obligation to make payment under this Guarantee shall be a primary, independent and absolute obligation and we shall not be entitled to delay or withhold payment for any reason. Our obligations hereunder shall not be affected by any act, omission, matter or thing which but for this provision might operate to release or otherwise exonerate us from our obligations hereunder in whole or in part, including and whether or not known to us or you:

1. Any time or waiver granted to the vendor;
2. The taking, variation, compromise, renewal or release of or refusal or neglect to perfect or enforce any rights, remedies or securities against the vendor;
3. Any Variation of or amendment to the RFP or any other document or security so that references to the Contract in this Guarantee shall include each such Variation and amendment;
4. Any unenforceability, invalidity or frustration of any obligation of the VENDOR or any other person under the RFP or any other document or security waiver by you of any of the terms provisions conditions obligations UNDER RFP or any failure to make demand upon or take action against the VENDOR;
5. Any other fact, circumstance, provision of statute or rule of law which might, were our liability to be secondary rather than primary, entitle us to be released in whole or in part from our undertaking; and;
6. Any change in constitution of the vendor;
7. Any petition for the winding up of the VENDOR has been admitted and a liquidator or provisional liquidator has been appointed or an order of bankruptcy or an order for the winding up or dissolution of the vendor has been made by a Court of competent jurisdiction;

The written demand referred to in paragraph above shall be deemed to be sufficiently served on us if you deliver to us at the address as set out in paragraph 3.

This guarantee is valid until the \_\_\_\_\_\_\_ day of \_\_\_\_\_\_. And a claim in writing is required to be presented to us within Claim Period i.e. six months from the date of expiry of the Guarantee i.e. on or before \_\_\_\_\_\_\_\_\_ or else all your rights will be forfeited and we shall be relieved of and discharged from all our liabilities mentioned hereinabove.

Signature and Seal of Guarantors (Vendor’s Bank)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_

Address: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# **Annexure 8.8 Manufacturer Authorisation Format**

*(To be submitted on OEM’s letter head for each of the products quoted)*

Ref: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_

To

General Manager [ITV]

Small Industries Development Bank of India

SIDBI Tower,

15, Ashok Marg,

Lucknow,

Uttar Pradesh - 226001

Manufacturer Authorisation for Request for Proposal (RFP) No. 400/2019/1434/BYO/ITV dated 22/02/2019 for Implementation and Management of Cyber Security Operations Center

We *<OEM Name>* having our registered office at *<OEM Address>* are an established and reputed manufacturer of *<hardware details>* do hereby authorise M/s\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (Name and address of the Partner) to offer their quotation, negotiate and conclude the contract with you against the above invitation for tender offer.

We hereby extend our full guarantee and warranty as per terms and conditions of the tender and the contract for the solution, products/equipment and services offered against this invitation for tender offer by the above firm and will extend technical support and updates / upgrades if contracted by the bidder.

We also confirm that we will ensure all product upgrades (including management software upgrades and new product feature releases) are provided by M/s ……..for all the products quoted for and supplied to the bank during the product warranty and AMC period.

<OEM Name>

<Authorized Signatory>

Name: \_\_\_\_\_\_\_\_\_\_\_\_

Designation: \_\_\_\_\_\_\_\_\_\_\_\_

Name of Organisation: \_\_\_\_\_\_\_\_\_\_\_\_

Company Seal: \_\_\_\_\_\_\_\_\_\_\_\_

Note: This letter of authority should be on the letterhead of the OEM and should be signed by a person competent and having the power of attorney to bind the manufacturer. It should be included by the bidder in its bid.

# **Annexure 8.9 Undertaking of Authenticity**

*(To be signed by authorized signatory of the Bidder)*

Ref: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_

To

General Manager [ITV]

Small Industries Development Bank of India

SIDBI Tower,

15, Ashok Marg,

Lucknow,

Uttar Pradesh - 226001

Undertaking of Authenticity

With reference to the hardware items (as mentioned in the Commercial Bid) quoted to you vide our quotation No.:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ dated \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ in response to your tender no. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, we hereby undertake that all the components / parts / assembly / software used in the hardware items shall be original / new from respective OEMs of the products and that no refurbished / duplicate / second hand components / parts / assembly / software are being used or shall be used.

We also undertake that in respect of licensed operating system if asked for by you in the purchase order, the same shall be supplied along with the authorised license certificate and also that it shall be sourced from the authorised source.

Should you require, we hereby undertake to produce the certificate from our OEM supplier in support of above undertaking at the time of delivery/installation. It will be our responsibility to produce such letters from our OEM supplier’s at the time of delivery or within a reasonable time.

In case of default and we are unable to comply with above at the time of delivery or during installation for the IT hardware / software already billed, we agree to take back the same, if already supplied and return the money if any paid to us by you in this regard.

We (Bidder name) also take full responsibility of both parts & service SLA as per the content even if there is any defect by our authorised service centre / reseller / BIDDER etc.

Signature of Authorised Signatory

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Designation: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Place: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Phone & E-mail: \_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name of the Organisation: \_\_\_\_\_\_\_\_\_\_\_\_

# **Annexure 8.10 Pre-Contract Integrity Pact**

*(To be submitted by bidders on non-judicial stamp paper of Rs.100/-)*

**1. General**

This pre-bid-pre-contract Agreement (hereinafter called the Integrity Pact) is made at \_\_\_\_\_\_\_\_\_ place\_\_\_ on ---- day of the month of -----, 2019 between Small Industries Development Bank of India, having its registered Head Office at 15, Ashok Marg, Lucknow – 226001 and inter alia, its Corporate Office at MSME Development Centre, C-11, G-Block, Bandra-Kurla Complex, Bandra(E), Mumbai 400051 (hereinafter called the “BUYER”/SIDBI, which expression shall mean and include, unless the context otherwise requires, its successors and assigns) of the First Part and M/s --- represented by Shri ----, Chief Executive Officer (hereinafter called the “BIDDER/Seller” which expression shall mean and include, unless the context otherwise requires, his successors and permitted assigns) of the Second Part.

WHEREAS the BUYER proposes to shortlist vendor for carrying out Implementation and Management of Cyber Security Operations Center (CSOC) (Tender \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_) and the BIDDER/Seller is willing to offer/has offered the services and

WHEREAS the BIDDER is a private company/public company, constituted in accordance with the relevant law in the matter and the BUYER is a corporation set up under an Act of Parliament

NOW, THEREFORE,

To avoid all forms of corruption by following a system that is fair, transparent and free from any influence /prejudiced dealing prior to, during and subsequent to the currency of the contract to be entered into with a view to :-

* Enabling the BUYER to obtain the desired said stores / equipment / services at a competitive price in conformity with the defined specifications by avoiding the high cost and the distortionary impact of corruption on public procurement and
* Enabling BIDDERs to abstain from bribing or indulging in any corrupt practice in order to secure the contract by providing assurance to them that their competitors will also abstain from bribing and other corrupt practices and the BUYER will commit to prevent corruption in any form by its officials by following transparent procedures.

The parties hereto hereby agree to enter into this integrity Pact and agree as follows:

**2. Commitments of the BUYER**

* 1. The BUYER undertakes that no official of the BUYER, connected directly or indirectly with the contract, will demand, take a promise for or accept, directly or through intermediaries, any bribe, consideration, gift, reward, favour or any material or immaterial benefit or any other advantage from the BIDDER, either for themselves or for any person, organization or third party related to the contract in exchange for an advantage in the bidding process, bid evaluation, contracting or implementation process related to the contract.
  2. The BUYER will during the pre-contract stage, treat all BIDDERs alike, and will provide to all BIDDERs the same information and will not provide any such information to any particular BIDDER which could afford an advantage to that particular BIDDER in comparison to other BIDDERs.
  3. All the officials of the BUYER will report to the appropriate Government office any attempted or completed breaches of the above commitments as well as any substantial suspicion of such a breach.
  4. In case any such preceding misconduct on the part of such official(s) is reported by the BIDDER to the BUYER with full and verifiable facts and the same is prima facia found to be correct by the BUYER, necessary disciplinary proceedings, or any other action as deemed fit, including criminal proceedings may be initiated by the BUYER and during such a period shall be debarred from further dealings related to the contract process. In such a case while an enquiry is being conducted by the BUYER the proceedings under the contract would not be stalled.

**3. Commitments of BIDDERs**

The BIDDER commits itself to take all measures necessary to prevent corrupt practices, unfair means and illegal activities during any stage of its bid or during any pre-contract or post-contact stage in order to secure the contract or in furtherance to secure it and in particular commit itself to the following: -

* 1. The BIDDER will not offer, directly or through intermediaries, any bribe, gift, consideration, reward, favour, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any officials of the BUYER, connected directly or indirectly with bidding process, or to any person, organization or third party related to the contract in exchange for any advantage in the bidding, evaluation, contracting and implementation of the contract.
  2. The BIDDER further undertakes that it has not given, offered or promised to give, directly or indirectly any bribe , gift, consideration, reward, favour, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of the BUYER or otherwise in procuring the Contract or forbearing to do or having done any act in relation to the obtaining or execution of the contract or any other contract with the Government for showing or forbearing to show favour or disfavour to any person in relation to the contract or any other contract with the Government.
  3. BIDDERs shall disclose the name and address of agents and representatives and Indian BIDDERs shall disclose their foreign principals or associates.
  4. BIDDERs shall disclose the payments to be made by them to agents/brokers or any other intermediary, in connection with this bid/contract.
  5. The BIDDER further confirms and declares to the BUYER that the BIDDER is the original manufacture / integrator / authorized government sponsored export entity of the defence stores and has not engaged any individual or firm or company whether Indian or foreign to intercede, facilitate or any way to recommend to the BUYER or any of its functionaries, whether officially or unofficially to the award of the contract to the BIDDER or has any amount been paid, promised or intended to be paid to any such individual, firm or company in respect of any such intercession, facilitation or recommendation.
  6. The BIDDER, either while presenting the bid or during pre-contract negotiations or before signing the contract, shall disclose any payments he has made, is committed to or intends to make to officials of the BUYER or their family members, agents, brokers or any other intermediaries in connection with contract and the details of services agree upon for such payments.
  7. The BIDDER will not collude with other parties interested in the contract to impair the transparency, fairness and progress of the bidding process, bid evaluation, contracting and implementation of the contract.
  8. The BIDDER will not accept any advantage in exchange for any corrupt practice, unfair means and illegal activities.
  9. The BIDDER shall not use improperly, for purposes of competition or personal gain or pass on the others, any information provided by the BUYER as part of the business relationship, regarding plans, technical proposals and business details, including information contained in any electronic data carrier. The BIDDER also undertakes to exercise due and adequate care lest any such information is divulged.
  10. BIDDER commits to refrain from giving any complaint directly or through any other manner without supporting it with full and verifiable facts.
  11. The BIDDER shall not instigate or cause to instigate any third person to commit any of the actions mentioned above.
  12. If the BIDDER or any employee of the BIDDER or any person acting on behalf of the BIDDER, either directly or indirectly, is a relative to any of the officers of the BUYER or alternatively, if any relative of the officer of the BUYER has financial interest/stake in the BIDDER’s firm, the same shall be disclosed by the BIDDER at the time of filling of tender. The term ‘relative’ for this purpose would be as defined in Section 2 (77) of the Companies Act, 2013.
  13. The BIDDER shall not lend to or borrow any money from or enter into any monetary dealings or transactions, directly or indirectly, with any employee of the BUYER.

**4. Previous Transgression**

* 1. The BIDDER declares that no previous transgression occurred in the last three years immediately before signing of this integrity Pact, with any other company in any country in respect of any corrupt practices envisaged hereunder or with any Public Sector Enterprise in India or any Government Department in India that could justify BIDDER’s exclusion from the tender process.
  2. The BIDDER agrees that if it makes incorrect statement on this subject, BIDDER can be disqualified from the tender process or the contract, if already awarded, can be terminated for such reason.

**5. Earnest Money (Security Deposit)**

* 1. While submitting commercial bid, the BIDDER shall deposit an amount Rs 23,50,000/- as Earnest Money/Security Deposit, with the BUYER through any of the following instrument.
  2. Bank Draft or a Pay Order in favour of Small Industries Bank of India, Payable at Mumbai.
  3. A confirmed guarantee by an Indian Nationalised Bank, promising payment of the guaranteed sum to the BUYER immediately on demand without any demur whatsoever and without seeking any reasons whatsoever. The demand for payment by the BUYER shall be treated as conclusive proof of payment.
  4. Earnest Money/Security Deposit shall be valid till the date of bid validity as mentioned in the RFP.
  5. In case of the successful BIDDER a clause would also be incorporated in the Article pertaining to Performance Bond in the Purchase Contract that the provision of Sanctions for Violation shall be applicable for forfeiture of Performance Bond in case of a decision by the BUYER to forfeit the same without assigning any reason for imposing sanction for violation of this Pact.
  6. No interest shall be payable by the BUYER to the BIDDER on Earnest Money/Security Deposit for the period of its currency.

**6. Sanctions for Violations**

* 1. Any breach of the aforesaid provision by the BIDDER or any one employed by it or acting on its behalf (whether with or without the knowledge of the BIDDER) shall entitle the BUYER to take all or any one of the following actions, wherever required :-
     + - 1. To immediately call off the pre contract negations without assigning any reason or giving any compensation to the BIDDER. However, the proceedings with other BIDDER(s) would continue
         2. The Earnest Money Deposit (in pre-contract stage) and /or Security Deposit/Performance Bond) (after the contract is signed) shall stand forfeited either fully or partially, as decided by the BUYER and the BUYER shall not be required to assign any reason therefore.
         3. To immediately cancel the contract, if already signed, without giving any compensation to the BIDDER
         4. To recover all sums already paid by the BUYER, and in case of Indian BIDDER with interest thereon at 2% higher than the prevailing Prime Lending Rate of State Bank of India. If any outstanding payment is due to the bidder from the buyer in connection with any other contract for any other stores, such outstanding payment could also be utilized to recover the aforesaid sum and interest.
         5. To encash the advance bank guarantee and performance bond/warranty bond, if furnished by the BIDDER, in order to recover the payments, already made by the BUYER along with interest.
         6. To cancel all or any other Contracts with the BIDDER, the BIDDER shall be liable to pay compensation for any loss or damage to the BUYER resulting from such cancellation/rescission and the BUYER shall be entitled to deduct the amount so payable from the money(s) due to the BIDDER
         7. To debar the BIDDER from participating in future bidding processes of the buyer or its associates or subsidiaries for minimum period of five years, which may be further extended at the discretion of the BUYER.
         8. To recover all sums paid in violation of this Pact by BIDDER(s) to any middleman or agent or broker with a view to securing the contract.
         9. In cases where irrevocable Letters of Credit have been received in respect of any contract signed by the BUYER with BIDDER, the same shall not be opened.
         10. Forfeiture of Performance Bond in case of decision by the BUYER to forfeit the same without assigning any reason for imposing sanction for violation of this Pact.
  2. The BUYER will be entitled to take all or any of the actions mentioned at para 6.1(i) to (x) of this Pact also on the commission by the BIDDER or any one employed by it or acting on its behalf (whether with or without the knowledge of the BIDDER), of an offence as defied in Chapter IX of the Indian Penal code, 1860 or Prevention of Corruption Act, 1988 or any other statute enacted for prevention of corruption.
  3. The decision of the BUYER to the effect that a breach of the provision of this Pact has been committed by the BIDDER shall be final and conclusive on the BIDDER. However, the BIDDER can approach the independent Monitor(s) appointed for the purposes of this Pact.

**7. Fall Clause**

The BIDDER undertakes that it has not supplied/is not supplying similar products /systems or subsystems at a price lower than that offered in the present bid in respect of any other Ministry/Department of the Government of India or PSU and if it is found at any stage that similar product/systems or sub systems was supplied by the BIDDER to any other Ministry/Department of the Government of India or a PSU 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 to the BUYER, if the contract has already been concluded.

**8. Independent Monitors**

* 1. The BUYER is in the process of appointing Independent Monitors (hereinafter referred to as Monitors) for this Pact in consultation with the Central Vigilance Commission.
  2. The task of the Monitors shall be to review independently and objectively, whether and to what extent the parties comply with the obligations under this Pact.
  3. The Monitors shall not be subject to instruction by the representatives of the parties and perform their functions neutrally and independently.
  4. Both the parties accept that the Monitors have the right to access all the documents relating to the project/procurement, including minutes of meetings.
  5. As soon as the Monitor notices or has reason to believe, a violation of the Pact, he will so inform the Authority designated by the BUYER
  6. The BIDDER(s) accepts that the Monitor has the right to access without restriction to all Project documentation of the BUYER including that provided by the BIDDER. The BIDDER will also grant the Monitor, upon his request and demonstration of a valid interest, unrestricted and unconditional access to his project documents. The same is applicable to Subcontractors. The Monitor shall be under contractual obligation to treat the information and documents of the BIDDER/Subcontractor(s) with confidentiality
  7. The BUYER 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 parties. The parties will offer to the Monitor the option to participate in such meetings

8.8 The Monitor will submit a written report to the designed Authority of the BUYER within 8 to 10 weeks from the date of reference or intimation to him by the BUYER/BIDDER and should the occasion arise, submit proposals for correcting problematic situations.

**9. Facilitation of Investigation**

In case of any allegation of violation of any provision of this Pact or payment of commission, the BUYER or its agencies shall be entitled to examine all the documents including the Books of Accounts of the BIDDER and the BIDDER shall provide necessary information and documents in English and shall extend all possible help for the purpose of such examination.

**10. Law and Place of Jurisdiction**

This Pact is subject to Indian Law. The place of performance and jurisdiction is the seat of the BUYER.

**11. Other Legal Actions**

The action stipulated in this integrity Pact are without prejudice to any other legal action that may follow in accordance with the provisions of the extant law in force relating to any civil or criminal proceedings.

**12. Validity**

* 1. The validity of this Integrity Pact shall be from date of its signing and extend upto 5 years or the complete execution of the contract to the satisfaction of both the BUYER and the BIDDER/Seller, including warranty period, whichever is later in case BIDDER is unsuccessful, this integrity Pact shall expire after six months from the date of the signing of the contract.
  2. Should one or several provisions of the Pact turn out to be invalid, the remainder of this Pact shall remain valid. In this case, the parties will strive to come to an agreement to their original intentions.

12.3 The parties hereby sign this integrity Pact, at \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ on \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

BUYER BIDDER

Name of Officer: \_\_\_\_\_\_\_\_\_\_\_\_\_ Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Designation: \_\_\_\_\_\_\_\_\_\_\_\_ Chief Executive Officer

SIDBI

Witness Witness

1. \_\_\_\_\_\_\_\_\_\_\_\_\_ 1. \_\_\_\_\_\_\_\_\_\_\_\_\_\_

2. \_\_\_\_\_\_\_\_\_\_\_\_\_ 2. \_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Annexure for Technical Bid

**Annexure 9.1 Technical Bid**

**1. Firm’s Profile**

|  |  |  |
| --- | --- | --- |
| **Sr No** | **Particulars** | **Response** |
| 1 | Name of the Company / Firm |  |
| 2 | Address |  |
| 3 | Brief description of the nature of the business and profile of the company with particular reference to SOC / CSOC/ IT Managed Security Services |  |
| 4 | Year of commencement of services (copy of commencement certificate may be enclosed) and number of years in this service industry. |  |
| 5 | Solutions Proposed by Bidder:   |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | | **Security Solution** | **SIEM** | **Anti-APT** | **PIM** | **NAC** | **Firewall Analyser** | **VAPT Services** | **Threat Intelligence Services** | | Solution proposed for SIDBI |  |  |  |  |  |  |  | | List of implementations carried out by bidder for proposed solution |  |  |  |  |  |  |  | | Name and address of OEM in India |  |  |  |  |  |  |  | | End of Life (EoL) or End of support (EoS) |  |  |  |  |  |  |  | | No of trained engineers available with the bidder |  |  |  |  |  |  |  | | Whether IPV6 compliant (Yes/No)? |  |  |  |  |  |  |  | | Whether  MAF is  submitted  (Yes/No)? |  |  |  |  |  |  |  |   1. The technical specifications mentioned in the Annexures 11.1 to 11.6 should be in accordance with the proposed solution for the Bank.  2. The EOL / EOS of each solution should cover the CSOC project timeline of the Bank. If End of Life (EoL) or End of support (EoS) date announced by the OEM, the bidder will be responsible for replacing / upgrading the solution. In case such date is not announced, it should be supported for minimum five years.  3. At least one trained engineer for each solution should be available with the Bidder. | |
| 6 | SOC / CSOC implementation carried out by the bidder for BFSI Customers having project cost of 5 crore and above | |  |  |  |  | | --- | --- | --- | --- | | Name of the customer and Contact Details of the reference provided | Project cost in Rupees | Implementation period | Should attach copies of work order | |  |  |  |  | |  |  |  |  | |  |  |  |  | |
| 7 | List of employees having certifications such as ISO 27001 LA/ ISO 27001 LI / CISA / CISSP / CISM (Certificates and CVs to be attached) | Self-declaration on company letter head |
| 8 | Project Team composition and role of the members for the proposed assignment.  (Project Manager will have minimum 5 years of experience in implementing similar project) | Project Manager :   |  |  | | --- | --- | | Team Member | Role | |  |  | |  |  | |
| 9 | Single Point of contact for RFP: | Name:  Designation:  Contact Details: |
| 10 | Project Schedule and implementation given in Section 4.10 is acceptable (Yes/No) |  |

Note: The relevant support documents should be attached without which the offer is liable for rejection.

Authorized Signatories

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Designation: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name of the Organization \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Company Seal:

**Annexure 9.2 – Statement of Deviations**

RfP No. 400/2019/1434/BYO/ITV dated 22/02/2019

(To be submitted on Bidders Company letter head)

Bidder is required to provide details of all deviations, comments and observations or suggestions in the following format with seal and signature. It also needs to provide a reference of the page number, state the clarification point as stated in tender document and the comment/ suggestion/ deviation that you propose as shown below.

SIDBI may at its sole discretion accept or reject all or any of the deviations, however it may be noted that the acceptance or rejection of any deviation by SIDBI will not entitle the bidder to submit a revised commercial bid. Clarifications given in Pre-bid will not be further entertained.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sr. No.** | **Page Number** | **Section Number** | **Clarification point as stated in the tender document** | **Comment/ Suggestion/ Deviation** |
| 1. |  |  |  |  |
| 2. |  |  |  |  |
| 3. |  |  |  |  |
| 4 |  |  |  |  |
| 5 |  |  |  |  |
| 6 |  |  |  |  |

Authorized Signatories

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Designation: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name of the Organization \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Company Seal:

**Annexure 9.3 – Letter of Competence**

RfP No. 400/2019/1434/BYO/ITV dated 22/02/2019

*(Sample Format – To be executed on a non-judicial stamped paper of Rs.100/-)*

This is to certify that we [Insert name of Bidder], address...............................................are fully competent and eligible to undertake and successfully deliver the scope of services mentioned in the above RfP. This recommendation is being made after fully understanding the objectives of the project and requirements of providing services as mentioned in the captioned RfP.

We also certify that all the information given by in response to this RfP is true and correct and also confirm that our company is eligible to perform this contract and whatever our company filed in response to the Pre-Qualification Criteria is true and correct.

Authorized Signatories

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Designation: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name of the Organization \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Company Seal:

**Annexure 9.4 – Letter of Conformity**

(To be submitted on Bidders Company letter head)

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

To

General Manager [ITV]

Small Industries Development Bank of India

SIDBI Tower,

15, Ashok Marg,

Lucknow,

Uttar Pradesh - 226001

Dear Sir,

Letter of Conformity

RfP No. 400/2019/1434/BYO/ITV dated 22/02/2019

We, the undersigned bidders, having read and examined along with terms and conditions the aforesaid RfP document on "Implementation and Management of Cyber Security Operations Center (CSOC)", issued by SIDBI and hereinafter referred as ‘Bank’ do hereby covenant, warrant and confirm as follows:

We hereby agree to comply with all the terms and conditions / stipulations as contained in the RFP and the related addendums and other documents including the changes made to the original tender documents issued by the Bank, provided however that only the list of deviations furnished by us in Annexure 9.2 of the main RfP document which are explicitly clarified by the Bank and communicated to us in writing, shall form a valid and binding part of the aforesaid RFP document. 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 and persons claiming through us.

We also here by confirm that our prices as specified in our Commercial Bid are as per the Payment terms specified in the Tender document.

Authorized Signatories

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Designation: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name of the Organization \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Company Seal:

# Annexure for Commercial Bid

**Annexure 10.1 – Commercial Bid – Covering Letter**

(To be submitted on Bidders Company letter head)

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

To

General Manager [ITV]

Small Industries Development Bank of India

SIDBI Tower,

15, Ashok Marg,

Lucknow,

Uttar Pradesh - 226001

Dear Sir,

Commercial Bid – Covering Letter

RfP No. 400/2019/1434/BYO/ITV dated 22/02/2019

I, the undersigned, offer to provide services for the above-mentioned project, in accordance with your RfP No. Tender \_\_\_\_\_\_\_\_\_\_dated \_\_\_\_\_\_\_\_\_\_\_ on “Implementation and Management of Cyber Security Operations Center (CSOC)” and our proposal (Technical and Commercial Proposals) dated [Date]. The Total fee is inclusive of all taxes, duties, charges and levies (as applicable and payable under the local laws) that we might incur and there will be no additional charges whatsoever. We will abide by the payment terms as mentioned in the aforesaid RfP.

Our commercial proposal shall be binding upon us, subject to the modifications resulting from contract discussions, up to expiration of the validity period of the proposal, i.e., [Insert date]

Authorized Signatories

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Designation: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name of the Organization \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Company Seal:

**Annexure 10.2 – Commercial Bid Format**

RfP No. 400/2019/1434/BYO/ITV dated 22/02/2019

Commercial Bid for Implementation and Management of Cyber Security Operations Center (CSOC)

**Table 1: Cost of Product including OEM warranty for 3 years**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **S. No.** |  | **Description** | **Cost including warranty of 3 years [in INR]** | | | |
| **Price (excluding taxes) [in INR]** | **GST Rate** | **GST Amount [in INR]** | **Price (including taxes) [in INR]** |
| 1 | CSOC License Cost | SIEM (DC) |  |  |  |  |
| 2 | SIEM – Log Collector (DR) |  |  |  |  |
| 3 | PIM# |  |  |  |  |
| 4 | Anti-APT (DC) |  |  |  |  |
| 5 | Anti-APT (DR) |  |  |  |  |
| 6 | Firewall Analyzer (DC) |  |  |  |  |
| 7 | NAC# |  |  |  |  |
| 8 | CSOC Hardware and Storage Cost | 2 LED TV (60 Inch+) |  |  |  |  |
| 9 | 4 Desktops |  |  |  |  |
| 10 | Veritas Backup Solution |  |  |  |  |
| 11 | *< to be inserted by bidder >* |  |  |  |  |
| 12 | *< to be inserted by bidder >* |  |  |  |  |
| 13 | Other Software License Cost | *< to be inserted by bidder >* |  |  |  |  |
| 14 | *< to be inserted by bidder >* |  |  |  |  |
| 15 | *< to be inserted by bidder >* |  |  |  |  |
| 16 | *< to be inserted by bidder >* |  |  |  |  |
| **Total Cost of Product including OEM warranty for 3 years (including taxes)** | | | | | |  |

# - In case of switching over of business operations from Primary DC Site (Navi Mumbai) to DR Site (Chennai), NAC and PIM security solutions are required for managing privileged users and providing access to clients. Hence, the two tools are to be installed and kept in readiness at the DR Site. The server and other infrastructure, if any, required at DR site are to be provided by the bidder.

**Table 2: Operational Cost**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **S. No.** |  | **Description** | **Operational Cost for one year [in INR]\*\*** | | | |
| **Price (excluding taxes) [in INR]** | **GST Rate** | **GST Amount [in INR]** | **Price (including taxes) [in INR]** |
| 1 | CSOC Monitoring and Operations Cost | 4 L1 resource – Annual Cost |  |  |  |  |
| 2 | 1 L2 resource – Annual Cost |  |  |  |  |
| 3 | 1 L3 resource – Annual Cost |  |  |  |  |
| 4 | 1 Resource for DC Site, Navi Mumbai – Annual Cost |  |  |  |  |
| 5 | CSOC Services Cost | Vulnerability Assessment and Penetration Testing – Annual Cost |  |  |  |  |
| 6 | Threat Intelligence Services |  |  |  |  |
| 7 | P2P link for DC-DR Replication – Annual Cost | |  |  |  |  |
| **Total Operational Cost for One Year (including taxes)** | | | | | |  |

**\*\*** Bank will calculate NPV on the 2nd and 3rd year quoted as part of Annual Cost using the formulae below:

**Net Present Value of Current Year = Cost of Respective Year / (1 + Discount Rate in %) Year-1**

The discount rate to be considered for above would be **8.38% per annum**

**Table 3: CSOC Implementation, Integration and Training Cost**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **S. No.** | **Description** | **CSOC Implementation, Integration and Training Cost** | | | |
| **Price (excluding taxes) [in INR]** | **GST Rate** | **GST Amount [in INR]** | **Price (including taxes) [in INR]** |
| 1 | CSOC Implementation and Integration Cost |  |  |  |  |
| 2 | Pre – Implementation Training |  |  |  |  |
| 3 | Post – Implementation Training |  |  |  |  |
| **Total CSOC Implementation, Integration and Training Cost (including taxes)** | | | | |  |

**Table 4: Optional Cost**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Optional Cost** | | | | | | |
| **S. No.** |  | **Description** | **Price (excluding taxes) [in INR]** | **GST Rate** | **GST Amount [in INR]** | **Price (including taxes) [in INR]** |
| 1 | CSOC License Cost, CSOC Hardware and Storage Cost, Other Software Cost (for all items mentioned as part of Table -1 in Annexure 10.2)++ | AMC / ATS Annual Cost for SIEM (DC) |  |  |  |  |
| 2 | AMC / ATS Annual Cost for SIEM – Log Collector (DR) |  |  |  |  |
| 3 | AMC / ATS Annual Cost for PIM |  |  |  |  |
| 4 | AMC / ATS Annual Cost for Anti – APT (DC) |  |  |  |  |
| 5 | AMC / ATS Annual Cost for Anti – APT (DR) |  |  |  |  |
| 6 | AMC / ATS Annual Cost for Firewall Analyzer (DC) |  |  |  |  |
| 7 | AMC / ATS Annual Cost for NAC |  |  |  |  |
| 8 | AMC / ATS Annual Cost for 2 LED TV ( 60 Inch +) |  |  |  |  |
| 9 | AMC / ATS Annual Cost for 4 Desktops |  |  |  |  |
| 10 | AMC / ATS Annual Cost for Veritas Backup Solution |  |  |  |  |
| 11 | AMC / ATS Annual Cost for *<to be inserted by bidder> as mentioned in Table 1* |  |  |  |  |
| 12 | AMC / ATS Annual Cost for *<to be inserted by bidder> as mentioned in Table 1* |  |  |  |  |
| 13 | AMC / ATS Annual Cost for *<to be inserted by bidder> as mentioned in Table 1* |  |  |  |  |
| 14 | AMC / ATS Annual Cost for *<to be inserted by bidder> as mentioned in Table 1* |  |  |  |  |
| 15 | Other Operational Costs | Integration of 5 business applications with SIEM |  |  |  |  |
| 16 | Cost for VAPT for 5 devices / applications |  |  |  |  |
| 17 | Cost for developing 5 connector / parser |  |  |  |  |
| 18 | Transition cost for 2 months after contract period (Ended / Terminated) |  |  |  |  |
| 19 | SIEM for additional 500 EPS at DC |  |  |  |  |
| 20 | SIEM – Log Collector (DR) for additional 500 EPS |  |  |  |  |
| **Total Optional Cost (including taxes)** | | | | | |  |

++ Bank will multiply the cost by 2 to arrive at cost for two years and will consider the multiplied cost for commercial evaluation.

Date: Signature of Authorized Signatory

Place: Name of Authorized Signatory

Designation

Name of the Organization

Company Seal

Note:

1. Once NPV is calculated (wherever applicable) for 2nd and 3rd year, NPV cost of 2nd and 3rd year will be added to the 1st year cost.
2. **To arrive at L1 bidder, Bank will arrive at the total cost for commercial evaluation as below:**

|  |  |  |
| --- | --- | --- |
| **Total Cost for Commercial Evaluation** | | |
| **S.No** | **Description** | **Amount (in INR)** |
| **1** | Total Cost of Product including OEM warranty for 3 years (including taxes) as per Table - 1 |  |
| **2** | Total Operational Cost for first Year (including taxes) as per Table - 2 + Total Operational Cost for Second Year after NPV calculation by bank (including taxes) + Total Operational Cost for Third Year after NPV calculation by bank (including taxes) |  |
| **3** | Total CSOC Implementation, Integration and Training Cost (including taxes) as per Table – 3 |  |
| **4** | Total Operational Cost for fourth Year (including taxes) + Total Operational Cost for fifth Year (including taxes) |  |
| **5** | Total Optional Cost for CSOC License Cost, CSOC Hardware and Storage Cost, Other Software Cost (including taxes) as per Table – 4 for two years |  |
| **6** | Total Optional Cost for Other Operational Costs (including taxes) as per Table – 4 |  |
| **Total Cost (Sum of S.No 1+2+3+4+5+6 as per the above table)** | |  |

The total cost arrived will be considered for evaluation of L1 bidder. However, the purchase order issued to the bidder will be on actual cost quoted by the bidder.

1. The price mentioned as part of operational cost (Table -2) will be considered the same for fourth and fifth year and if any additional resources (L1/ L2 / L3 / DC) are required during the contract period. For any additional requirements, the cost for any line items as part of operational cost (Table - 2) will be calculated on pro rata basis by the bank throughout the contract period depending on the number of resources required and time period deployed.
2. The optional cost (Table – 4) quoted by the bidder will be valid for five years and the cost will be calculated on pro rata basis by the bank throughout the contract period.
3. During the transition period, the bank will only pay cost quoted as part of transition cost under the Optional Cost.
4. The prices must be entered strictly as per the tabular format illustrated above. All fields mentioned as part of commercial bid needs to be filled up by the bidder. No separate price structure should be detailed. No separate format will be accepted.
5. If the cost for any line item is indicated as zero then it will be assumed by the Bank that the said item is provided to the Bank without any cost.
6. Masked commercial bids must be submitted with technical bid. If bidder has inserted and quoted for any component against *<to be provided by bidder>*, the details of same should be clearly indicated in the masked commercial bid.
7. Conditional commercial bids would not be considered

# **Annexure for Technical Specifications and Requirements**

**Annexure 11.1 Security Information and Event Management**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Requirement Description** | **Priority - High (H) / Low (L)** | **Compliance (Y/N)** | **Bidder Remarks (if any)** |
| 1 | The proposed solution should be an appliance with a clear physical or logical separation of the collection module, logging module and correlation module. It should support log collection, correlation and alerts for the number of devices mentioned in scope. | H |  |  |
| 2 | The proposed solution should be able to conduct agent less collection of logs except for those which cannot publish native audit logs | H |  |  |
| 3 | The proposed solution should be in Leaders/Challengers as per Gartner Magic quadrant OR Leaders/Strong performers as per Forrester Wave in the latest/current report | H |  |  |
| 4 | The proposed solution should integrate with other security solutions, such as IPS/IDS, Proxy, Anti-virus etc. | H |  |  |
| 5 | The proposed solution should ensure the integrity of the information collected. | H |  |  |
| 6 | Initial EPS requirement is for 5000. However, the appliance should be scalable up to 10000 EPS and the same appliance should support minimum 20,000 EPS | H |  |  |
| 7 | The proposed solution should have available connectors to support the standard devices / applications, wherever required the vendor should develop customized connectors for all standard devices at no extra cost | H |  |  |
| 8 | The proposed solution should have the capability to identify / remember frequently used queries and provide means for optimization of queries. | H |  |  |
| **Log Management** | | | | |
| 9 | The Appliance shall have additional storage for managing and storing logs from various devices. Storage should provide minimum 3 months online and 9 months offline. Bidder should provision for log storage for 7 years. The proposed system should support SAN, NAS and DAS for adding external storage as and when required. The bidder is expected to size the storage as per the requirements mentioned in this RFP. The bidder‘s response should include the calculations/ logic used to arrive at the sizing. It is to be noted that proposed hardware should be based on RAID 5 and have minimum 10000 Disk RPM. The storage solution should have adequate redundancy for handling disk failures. | H |  |  |
| 10 | All logs should be Authenticated (time-stamped), encrypted OR transmitted over a secure encrypted channel and compressed before / after transmission to be clarified with respect to encrypted channel and before and after compression. | H |  |  |
| 11 | The proposed solution should be able to continue to collect log data during database backup, de-fragmentation and other management scenarios, without any disruption to service. | H |  |  |
| 12 | The proposed solution should support log collection from all operating systems and their versions including but not limited to Windows, AIX, Unix, Linux, Solaris servers etc. | H |  |  |
| 13 | In case the connectivity with SIEM management system is lost, the collector should be able to store the data in its own repository. The retention, deletion, synchronization with SIEM database should be automatic but it should be possible to control the same manually. | H |  |  |
| 14 | The proposed solution shall allow bandwidth management, rate limiting, at the log collector level. | H |  |  |
| 15 | The proposed solution should ensure that the overall load on the network bandwidth at DC, WAN level is minimal | L |  |  |
| 16 | The proposed solution should provide time based store and forward feature at each log collection point | H |  |  |
| 17 | The proposed solution should have the capability to compress the logs by at least 70 % for storage optimization. | H |  |  |
| 18 | It should be possible to store the event data in its original format in the central log storage | H |  |  |
| 19 | Traceability of logs shall be maintained from the date of generation to the date of purging. | H |  |  |
| 20 | The proposed system should be able to capture all details in raw log, events and alerts and normalize them into a standard format for easy comprehension. | H |  |  |
| 21 | It should be feasible to extract raw logs from the SIEM and transfer to other systems as and when required. | H |  |  |
| 22 | The proposed should support the following log collection protocols at a minimum: Syslog over UDP / TCP, Syslog NG, SDEE, SNMP Version 2 & 3, ODBC, FTP, Windows Event Logging Protocol, Opsec,Netflow | H |  |  |
| 23 | The proposed solution should supports preservation of raw and normalized data. | H |  |  |
| 24 | The SIEM tool should maintain the audit trail for the management activities of individual users accessing and using the application and reports being accessed. | H |  |  |
| 25 | The proposed solution should have facility for log co-relation and / or investigation, incident management etc. with a search / drill down facility to search the collected raw log data for specific events or data. | H |  |  |
| 26 | The proposed solution should support industry log collection methods such as syslog, WMI, JDBC, SNMP, Checkpoint LEA, etc. | H |  |  |
| **Log taxonomy & Categorization** | | | | |
| 27 | The proposed solution should be able to capture critical fields of information in the original event data, logs and alert messages and normalize / parse them into a common standard event schema for further analysis, troubleshooting and other data processing needs. | H |  |  |
| 28 | The proposed solution should support correlation of events from multiple vendor devices, appliances and applications enabling analysis. | H |  |  |
| 29 | The proposed solution should collect log & support forensics with added context and threat Intelligence and provide complete visibility through packet inspection and analysis. | H |  |  |
| 30 | The proposed solution should provide summary of log stoppage alerts and automatic suppression of alerts. | H |  |  |
| 31 | The proposed solution must allow the creation of an unlimited number of new correlation rules, as well as the customization of existing rules. | H |  |  |
| **SIEM -CORRELATION AND ALERTING** | | | | |
| 32 | The proposed solution should provide alerting based on observed security threats from monitored devices. | H |  |  |
| 33 | The solution should be able to parse and correlate multi line logs | H |  |  |
| 34 | The proposed solution should support weighted alerts to allow prioritization of alerts. Weights should be assignable based on multiple characteristics such as asset type, protocol, application, etc. | H |  |  |
| 35 | The proposed solution should provide the ability to transmit alerts using multiple protocols and mechanisms to other solutions such as SMTP, Incident Management etc. | H |  |  |
| 36 | The proposed solution should provide UI based wizard and capabilities to minimize false positives and fine tuning of correlation rules. | H |  |  |
| 37 | The proposed solution should integrate with security and threat intelligence feeds data feeds (i.e. geographic mapping, known botnet channels, known hostile networks, etc.) for the purpose of correlating internal activity with external threats. These data feeds should be updated automatically by the solution. | H |  |  |
| 38 | The solution should have capability to import the vulnerability information from scanning and assessment tools on real time basis and correlate them for all possible implications. | L |  |  |
| 39 | Solution should be able to perform the following correlations (but not limited to): Rule based, Vulnerability based, Statistical based, Historical based etc. | H |  |  |
| 40 | The system/solution should have the ability to correlate all the fields in a log | H |  |  |
| 41 | Ability to gather information on real time threats and zero day attacks issued by anti-virus or IDS/ IPS vendors or audit logs and add this information as intelligence feed in to the SIEM solution via patches or live feeds | H |  |  |
| 42 | The solution should allow a wizard based interface for rule creation. The solution should support logical operations and nested rules for creation of complex rules | H |  |  |
| 43 | The central correlation engine database should be updated with real time security intelligence updates from OEM | H |  |  |
| 44 | The proposed solution should be able to integrate with physical access control systems. | L |  |  |
| 45 | The proposed system should have the correlation capability. The system should be updated with customizable correlation rules based on new identified attack patterns and threats. It must be possible to create Customized co-relation rules. | H |  |  |
| 46 | The proposed solution should have out of the box rules for IDS/IPS, firewalls routers, switches, VPN devices, antivirus, operating systems, databases and standard applications etc. | H |  |  |
| **Event Filtering & Analysis** | | | | |
| 47 | The proposed solution should provide the ability to aggregate an analyze events based on a user specified filter. | H |  |  |
| 48 | The proposed solution should provide more advanced event drill down when required for forensic analysis. | H |  |  |
| 49 | The system should identify the originating system and user details while capturing event data. | H |  |  |
| 50 | It should be possible to automatically create incidents, raise tickets and track their closure with respective alerts to the supporting/ help desk personnel | H |  |  |
| 51 | The event should reach the CSOC monitoring team within 1 minute of the log being captured | L |  |  |
| 52 | Pre-defined / custom parsers are available for parsing logs for the following applications: Finacle, Flexcube and Bancs | H |  |  |
| 53 | The solution should offer a means of escalating alerts between various users of the solution, such that if alerts are not acknowledged in a predetermined timeframe, that alert is escalated to ensure it is investigated. i.e. system should allow escalation matrix to be configured and tickets need to be escalated as per the configuration. | H |  |  |
| 54 | The proposed Solution should be able to filter the captured packets based on layer-2 to layer-7 header information. The solution should also provide ability to reconstruct data payload. | H |  |  |
| 55 | The solution must have the ability to capture network traffic and import PCAP files. | H |  |  |
| 56 | Solution should be able to provide asset details such as Asset owner, location, events & incidents, vulnerabilities and issue mitigation tracking mapped to individual assets/users | H |  |  |
| **SIEM Workflow** | | | | |
| 57 | The proposed solution should support ticketing/help desk systems that security operations staff may use to guide their work. | H |  |  |
| 58 | The proposed solution should provide a mechanism to track security incidents across a wide range of relevant attributes (i.e. IP addresses, usernames, MAC address, log source, correlation rules, user defined, etc.). | H |  |  |
| **Administration & Configuration** | | | | |
| 59 | The proposed solution should provide central management of all components and administrative functions from a single web based user interface. | H |  |  |
| 60 | The proposed solution should support auto-discovery of assets/hosts on the network by leveraging both passive network activity data as well as other data sources that feed the SIEM Solution (e.g. logs) | H |  |  |
| **Dashboard & Reporting** | | | | |
| 61 | The dashboard should be in the form of a unified portal that can show correlated alerts/ events from multiple disparate sources such as security devices, network devices, enterprise management systems, servers, applications, databases, etc. | H |  |  |
| 62 | Events should be presented in a manner that is independent of device specific syntax and easy to understand for all users | H |  |  |
| 63 | The dashboard should show the status of all the tools deployed as part of the SOC, including availability, bandwidth consumed, system resources consumed (including database usage) | H |  |  |
| 64 | It should be possible to categorize events while archiving for example , events for network devices, antivirus, servers etc. | H |  |  |
| 65 | Any failures of the event collection infrastructure must be detected and operations personnel must be notified as per SLA. The device Health monitoring must include the ability to validate that original event sources are still sending events | H |  |  |
| 66 | The proposed system should have out-of-the-box reports for supported devices and compliance standards for the supported devices. The reports should include standard security analysis reports and graphs. Any newer reports published by the product OEM should be made available for use at no extra license, it is expected that newer reports published are provided on a monthly basis for use within the Bank. | H |  |  |
| 67 | The proposed system should have the capability to provide detailed analysis of security incidents occurred and recorded by the system. | H |  |  |
| 68 | The bidder shall customize reporting and security dashboards for Bank as and when required by Banks Security Team and shall have provision to sort/search as per requirement such as IP based, host based, etc. | H |  |  |
| 69 | The solution should generate the following reports (but not restricted to): User activity reports, Configuration change reports, Incident tracking report, Attack source reports etc. In addition, the solution should have a reporting writing tool for development of any ad-hoc reports. | H |  |  |
| 70 | The Dashboard design for the solution should be editable on an ad hoc basis as per the individual user need | L |  |  |
| 71 | The system should display all real time events. The solution should have drill down functionality to view individual events from the dashboard | H |  |  |
| 72 | The solution should allow applying filters and sorting to query results. | H |  |  |
| 73 | The bidder shall be responsible for all performance related activities like system/database tuning etc. to ensure the guaranteed EPS performance for both correlation and collection of raw logs. | H |  |  |
| 74 | The solution should allow creating and saving of ad hoc log queries on archived and retained logs. These queries should be able to use standard syntax such as wildcards and regular expressions. | H |  |  |
| 75 | The solution should allow for qualification of security events and incidents for reporting purpose. The solution should be able to generate periodic reports (weekly, monthly basis) for such qualified security events/ incidents. | H |  |  |
| 76 | Should generate e-mail and SMS notifications for all critical/high risk alerts triggered from SIEM | H |  |  |
| 77 | The solution should allow users to initiate and track alert related mitigation action items. The portal should allow reports to be generated on pending mitigation activities | H |  |  |
| 78 | Solution should provide knowledge base and best practices for various security vulnerabilities | H |  |  |
| 79 | Dashboard should display asset list and capture details including name, location, owner, value, business unit, IP address, platform details | H |  |  |
| 80 | Dashboard should capture the security status of assets and highlight risk level for each asset. This should be used to capture security status of bank, status of different business units within the bank, status of key locations etc. | H |  |  |
| 81 | Dashboard should support reporting for consolidated relevant compliance across all major standards and regulatory requirements. This includes ISO 27001, RBI regulations, IT ACT, PCI DSS standards etc. The solution should include compliance reports for standard - ISO 27001. The solution should also generate reports for these standards. | H |  |  |
| 82 | Dashboard should support different views relevant for different stake holders including top management, operations team, Information Security Department | H |  |  |
| 83 | Dashboard should support export of data to multiple formats including CSV, XML, PDF, formats | H |  |  |
| 84 | Dashboard views should be customizable as per user rights and access to individual components of the application. | H |  |  |
| 85 | Administrators should be able to view correlated events, packet level event details, real-time raw logs and historical events through the dashboard. | H |  |  |
| 86 | Senior Management should be able to view compliance to SLA for all CSOC operations | H |  |  |
| 87 | The system should permit setting up geographical maps/images on real time dashboards to identify impacted areas and sources of alerts. | L |  |  |
| 88 | The tool should provide flexible dashboard interface customized to user preferences allowing the examination of a specific event or a holistic view of the systems within the enterprise. All the dashboards for SIEM monitoring should be completely customizable and shall have the feature for restricted access depending on user / group based. Dashboard should be hosted in Bank's premises. | H |  |  |
| 89 | The solution should allow creation of various dash boards for various purposes and user levels. Dashboard creation tool/wizard should be part of the solution | H |  |  |
| 90 | The proposed solution shall include reports for, but not limited to the devices mentioned in Implementation for the listed devices in Annexure 11.7 | L |  |  |
| 91 | Solution should have the ability to perform free text searches for events, incidents, rules and other parameters. | H |  |  |
| **Availability** | | | | |
| 92 | The SI should prepare a DR plan for switch over in case the DC operations are down | H |  |  |
| 93 | The solution should have high availability feature built in. There should be an automated switch over to secondary collector in case of failure on the primary collector. No performance degradation is permissible even in case of collector failure. | H |  |  |
| **Storage** | | | | |
| 94 | The bidder should provide for adequate storage to meet the EPS and retention requirements of the bank. Bidder shall be responsible for upgrade of the storage to meet the bank's requirements as above at no additional cost. The SI should provide adequate justification for the storage size proposed as part of the response. | H |  |  |
| 95 | The platform should provide tiered storage for the online, archival, and backup and restoration of event log information. | H |  |  |
| 96 | The Tier I and II storage should have the capability to authenticate logs on the basis of time, integrity and Origin | H |  |  |
| 97 | The storage solution should have the capability to encrypt/hash the logs in storage | H |  |  |
| 98 | System should have capacity to maintain the logs for 90 days on Tier I storage and older logs should be archived on Tier II storage and Tier 3 storage | H |  |  |
| 99 | Solution should be capable of retrieving the archived logs for analysis, correlation and reporting purpose automatically for any past time duration selected. | H |  |  |
| 100 | Should be able to part and filter logs before storage on the basis of type of logs; date etc | H |  |  |
| 101 | Solution should be capable to replicate logs in Synchronous / Asynchronous mode. | H |  |  |
| 102 | It should be possible to define purging and retention rules for log storage. | H |  |  |
| 103 | The solution should come with built-in functionality for archiving data. | H |  |  |
| **Scalability** | | | | |
| 104 | The solution should be scalable as per bank roadmap for expansion | H |  |  |
| 105 | Solution should support integration with big data storage configuration such as Hadoop etc. | H |  |  |
| 106 | The solution should support creation of incident management workflows to track incident from creation to closure, provide reports on pending incidents, permit upload of related evidences such as screenshots etc. | H |  |  |
| 107 | The system should receive feeds from a threat intelligence repository maintained by the OEM which consists of inputs from various threat sources and security devices across the globe. | H |  |  |
| **Integration** | | | | |
| 108 | Integrate with DLP solutions to identify misuse of sensitive information | H |  |  |
| 109 | Integrate with PIM and other Directory solution to relate security events to user activities | H |  |  |
| 110 | Integration with Vulnerability Assessment tools to identify security events | H |  |  |
| 111 | Integrate with GRC solution to capture compliance against security policies | H |  |  |
| 112 | Integrate with existing helpdesk/ incident management tools | H |  |  |
| 113 | Should be able to integrate with bank's existing backup solution for performing backup of the SIEM. | H |  |  |
| 114 | Should be able to integrate with Core Banking solution, RTGS/NEFT etc. and address the use cases mentioned in the RFP at a minimum. | H |  |  |
| 115 | Connector Development tool/SDK availability for developing collection mechanism for home-grown or any other unsupported applications | H |  |  |
| **Operational Requirements** | | | | |
| 116 | The proposed solution should have an automated/scheduled backup of logs and recovery process of backup media. | H |  |  |
| 117 | All the updates and upgrades to SIEM reports should be included with the solution | H |  |  |
| 118 | The successful bidder shall submit quarterly reports of the events encountered to the engineer-in-charge. The successful bidder shall also submit quarterly reports of equipment performance indicating equipment and disk space utilization. | H |  |  |
| 119 | SIEM tool should be running 24\*7\*365 for monitoring of the devices/ servers | H |  |  |
| 120 | The SIEM tool should maintain the audit trail for the management activities of individual users accessing and using the application and reports being accessed. | H |  |  |
| 121 | The offered solution should allow integration of log data information into watch list for monitoring in existing correlation rules. Ex- a suspicious IP can be added to blacklisted IP address in a correlation rule watching all outgoing/incoming connections through firewall | H |  |  |
| 122 | The proposed solution should be IPv6 compliant | H |  |  |
| 123 | The vendor should have a local depot in India for support for faster replacements. | H |  |  |
| **Platform/Hardware/Software** | | | | |
| 124 | The platform of the offered product should be supplied as a complete Solution including hardware and software. It should include all licensed software components necessary for correlation of logs for the devices including, but not limited to the list given in annexure for the functioning of the offered solution e.g. database licenses, reporting tools, customization tools etc. | H |  |  |
| 125 | In case any hardware or additional support required for ticketing tool, the same will be provided by bidder as part of delivery | H |  |  |
| **Location Independence** | | | | |
| 126 | The offered solution should be able to collect, correlate and analyze logs from various devices located at different locations of SIDBI, without any additional cost implication on SIDBI. The locations covered are Data Center, Navi Mumbai and DR Chennai. However it must be possible to include devices located at other locations of SIDBI without any significant changes in implementation. | H |  |  |
| **Log Storage Format** | | | | |
| 127 | The offered solution should store all logs in raw format as sent by the above devices. These raw logs should be time stamped and compressed before being written to the storage. The logs should be maintained in tamper proof condition and shall have proper integrity mechanisms to be in place for log security. | H |  |  |
| **Log Parsing** | | | | |
| 128 | Any Log parsing activities should not alter the raw log in any format. | H |  |  |
| **Log Retention Period** | | | | |
| 129 | The proposed system must provide support for defining different retention periods for different devices | H |  |  |
| **Notification** | | | | |
| 130 | The system must provide target device notification if target device is down or no longer sending/ receiving events. | H |  |  |
| **Tamper Logging** | | | | |
| 131 | The data archival should be configured to store information in tamper proof format and should comply with all the relevant regulations. The solution should prevent tampering of any type of logs and log any attempts to tamper logs. | H |  |  |
| 132 | Once the log is written to the storage it should not be modifiable. It should have proper mechanisms to prevent log tampering. | H |  |  |
| **Incident Management and Ticketing Tool** | | | | |
| 133 | The solution should have incident management and/or integrate with incident management tool to generate automated tickets for the alert events generated by the SIEM and other proposed tools. | H |  |  |
| 134 | The solution should provide complete life cycle management of tickets from incident generation till closure of the incident. The solution should have capability to structure rule based work flow and calendar/ event based alerting capability. | H |  |  |
| 135 | The tool should facilitate time/ event based automated escalation of tickets as per the escalation matrix defined by the Bank | H |  |  |
| 136 | The tool should be web based online portal available over desktop | H |  |  |
| 137 | Apart from CSOC team, the incident management tool access also needs to be provided to individual asset/application owners of Bank to enable them to track and close events/incidents pertaining to their section/department. | H |  |  |
| 138 | Bidder needs to provide ticketing tool for at-least 50 users | H |  |  |
| 139 | Access also needs to be provided to Bank‘s CISO and other identified individuals for monitoring purpose. | H |  |  |
| **Vulnerability Updates** | | | | |
| 140 | The offered solution should include vulnerability details with updates from a known vulnerability database like NVD (National Vulnerability Database) or similar databases. | H |  |  |

**Annexure 11.2 Privilege Identity Management**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Requirement Description** | **Priority - High (H) / Low (L)** | **Compliance (Y/N)** | **Bidder Remarks (if any)** |
| **Single Sign-on and Authentication Models** | | | | |
| 1 | The solution should be able to create seamless single sign-on for various technologies such as Operating Systems, Databases, Network and Security Devices. | H |  |  |
| 2 | The solution should have a Generic Target System Connectors to enable one to use this connector for non-standard devices etc. | H |  |  |
| 3 | The solution should be agent less, So no agent will be deploy on target devices. | H |  |  |
| 4 | The solution should support direct connections to windows, SSH, databases and other managed devices without having to use a jump server. | H |  |  |
| 5 | The solution should have an inbuilt dual factor authentication for soft token, mobile OTP etc. Also it should have an inbuilt authentication for Bio-Metrics without having to acquire another biometric authentication server. | H |  |  |
| 6 | The solution should be able to integrate with enterprise authentication methods e.g. multiple 3rd party authentication methods including LDAP, RADIUS and a built-in authentication mechanism | H |  |  |
| 7 | The solution should also provide local authentication and all the security features as per best standards. | H |  |  |
| 8 | The solution should support an application integration framework for web based as well as .exe based applications. There should be strong out of the box support including ease of integration with any third party connectors. | H |  |  |
| 9 | The solution should provide multi-tenancy feature whereby the entire operations can be carried out within a tenant or line of business. | H |  |  |
| 10 | The solution should provide multi-domain feature whereby the entire operations can operate in an distributed environment | H |  |  |
| 11 | The solution should be able to handle multi-location architecture or distributed architecture with seamless integration at the User Level. For example: Multiple datacenter may have multiple secondary installations but the primary installation will also simultaneously work for all users and all locations | H |  |  |
| **Shared Account Password Management** | | | | |
| 12 | The solution should set password options every x days, months, years and compliance options via the use of a policy | H |  |  |
| 13 | The solution should have ability to create exception policies for selected systems, applications and devices | H |  |  |
| 14 | The solution should enable an administrator to define different password formation rules for target accounts on different target systems and supports the full character set that can be used for passwords on each target system. | H |  |  |
| 15 | The solution should have flexibility that allows exclusivity for password retrieval or multiple users checking out the same password for the same device in the same time period. | H |  |  |
| 16 | All locally stored target-account passwords should be encrypted using AES or similar encryption with at least 256 bit keys. | H |  |  |
| 17 | The solution should have the ability to reconcile passwords manually upon demand. | H |  |  |
| 18 | The solution should allow secure printing of passwords in Pin Mailers. Lifecycle of printing and labeling of envelopes should be part of the module. | H |  |  |
| 19 | The solution should be able to control re-prints with adequate authorization. | H |  |  |
| 20 | The proposed solution should restrict the solution administrators from accessing or viewing passwords or approve password requests. | H |  |  |
| 21 | The solution should have the capability to seamlessly change the passwords for the large number of desktops. It should be able to handle floating IPs. | H |  |  |
| **Access Control** | | | | |
| 22 | The solution should be able to restrict usage of critical commands over a SSH based console based on any combination of target account, group or target system and end-user. | H |  |  |
| 23 | The solution should restrict privileged activities on a windows server (e.g. host to host jumps, cmd / telnet access, application access, tab restrictions) from session initiated with PIM. | H |  |  |
| 24 | The solution should be able to restrict usage of critical commands on command line through SSH clients on any combination of target account, group or target system and end-user. | H |  |  |
| 25 | The solution should be able to restrict usage of critical commands on tables for database access through SSH, SQL+ (client/), front-end database utilities on any combination of target account, group or target system and end-user. | H |  |  |
| 26 | The solution should provide for inbuilt database management utility to enable granular control on database access for Sql, my Sql, DB2, Oracle etc. | H |  |  |
| 27 | The solution should have workflow control built-in for critical administrative functions over SSH including databases (example user creation, password change etc.) and should be able to request for approval on the fly for those commands which are critical. | H |  |  |
| 28 | The solution should provide for a script manager to help in access controlling scripts and allow to run the scripts on multiple devices at the same time. | H |  |  |
| 29 | The solution should be able to define critical commands for alerting & monitoring purpose and also ensure user confirmation (YES or NO) for critical commands over SSH. | H |  |  |
| **Privileged Session Management and Log Management** | | | | |
| 30 | The solution should be able to support a session recording on any session initiated via PIM solution including servers, network devices, databases and virtualized environments. | H |  |  |
| 31 | The solution should be able to log commands for all commands fired over SSH Session and for database access through ssh, sql+ | H |  |  |
| 32 | The solution should be able to log / search text commands for all sessions of database even through the third party utilities | H |  |  |
| 33 | The solution should be able to log / search text commands for all sessions on RDP | H |  |  |
| 34 | All logs created by the solution should be tamper proof and should have legal hold | H |  |  |
| 35 | The solution should log all administrator and end-user activity, including successful and failed access attempts and associated session data (date, time, IP address. Machine address, BIOS No and so on). The solution can generate — on-demand or according to an administrator-defined schedule — reports showing user activity filtered by an administrator, end user or user group. | H |  |  |
| 36 | The solution should have capability to restrict access to different reports by administrator, group or role. | H |  |  |
| 37 | The solution should generate reports in at least the following formats: HTML, CSV and PDF | H |  |  |
| 38 | The solution should be able to define critical commands for alerting & monitoring purpose through SMS or Email alerts | H |  |  |
| 39 | The solution should provide separate logs for commands and session recordings. Session recordings should be available in image/ video based formats | L |  |  |
| 40 | The session recording should be SMART to help jump to the right session through the text logs | L |  |  |
| 41 | Secure and tamper-proof storage for audit records, policies, entitlements, privileged credentials, recordings etc. | H |  |  |
| 42 | The proposed solution shall allow a blacklist of SQL commands that will be excluded from audit records during the session recording. All other commands will be included. | H |  |  |
| **PIM Security** | | | | |
| 43 | The proposed solution should use minimum FIPS 140-2 validated cryptography for all data encryption. | H |  |  |
| 44 | The proposed solution should be TLS 1.2 and SHA-2 compliant for PCI-DSS compliance | H |  |  |
| 45 | All communication between system components, including components residing on the same server should be encrypted. | H |  |  |
| 46 | All communication between the client PC and the target server should be completely encrypted using secured gateway. (Example: a telnet session is encrypted from the client PC through the secured gateway) | H |  |  |
| 47 | The Administrator user cannot see the data (passwords) that are controlled by the solution. | H |  |  |
| 48 | The solution should secure master data, records, entitlement, policy data and other credentials in tamper proof storage container. | H |  |  |
| **PIM Administration** | | | | |
| 49 | The solution should have central administration web based console for unified administration. | H |  |  |
| 50 | The tool uses Active Directory/LDAP as an identity store for administrators and end users. | H |  |  |
| 51 | Administrative configurations (e.g. configuration of user matrix) shall be accessible via a separate client where client access is controlled by IP address. | H |  |  |
| 52 | Important configuration changes in the solutions (example changes to masters) should be based on at least 5 level workflow approval process and logged accordingly | H |  |  |
| 53 | Segregation of Duties - The Administrator user cannot view the data (passwords) that are controlled by other teams/working groups (UNIX, Oracle etc.). | H |  |  |
| 54 | The solution should provide for self-service portal for users and devices for ease of on boarding both users and devices. | H |  |  |
| 55 | All administrative task should be done LOB wise i.e. Line of Business Wise | L |  |  |
| **Administration, Management, Encryption & Solution Security** | | | | |
| 56 | The solution architecture should be highly scalable both vertically as well as horizontally. | H |  |  |
| 57 | The proposed solution shall provide multi-tier architecture where the database and application level is separated. | H |  |  |
| 58 | The solution should work at the network layer instead through a jump server. This will have achieve large number of sessions. | H |  |  |
| 59 | The proposed solution shall provide scalability where it is not limited by the hardware. Also the solution shall provide modular design for capacity planning and scalability metrics. | H |  |  |
| 60 | The proposed solution shall have the ability to support multiple mirrored systems at offsite Disaster Recovery Facilities across different data center locations. | H |  |  |
| 61 | The proposed solution shall have built-in options for backup or integration with existing backup solutions | H |  |  |
| 62 | The proposed solution shall handle loss of connectivity to the centralized password management solution automatically. | H |  |  |
| 63 | The proposed solution shall not require any network topology changes in order to ensure all privileged sessions are controlled by the solution. | H |  |  |
| 64 | The proposed solution shall support distributed network architecture where different segments need to be supported from a central location. | H |  |  |
| 65 | The proposed solution shall support both client based (in the case where browser is not available) as well as browser based administration | H |  |  |
| 66 | The proposed solution should be 100% agentless that includes password storage, password management and session recording features. | H |  |  |
| 67 | The solution must support parallel execution of password resets for multiple concurrent requests. | H |  |  |
| 68 | The solution if required should be available to install on a virtual sever | H |  |  |
| 69 | The system should be highly available (24x7x365) and redundant from a hardware failure, application failure, data failure, and or catastrophic failure. | H |  |  |
| 70 | The solution should have an ability to have direct connection to target device as well as using secured gateway channel. | H |  |  |
| **Out of Box Integration** | | | | |
| 71 | The solution should have an ability to integrate with enterprise authentication methods e.g. multiple 3rd party authentication methods including AD, LDAP, Windows SSO, PKI, RADIUS and a built-in authentication mechanism. | H |  |  |
| 72 | The solution should have an ability to integrate with Bio-Metric Solutions | H |  |  |
| **Application Password Management** | | | | |
| 73 | The solution should have an ability to eliminate, manage and protect privileged credentials in applications, scripts, configuration files etc. | H |  |  |
| 74 | The solution should be able to authenticate and trust the application requesting the privileged password based on various authentication methods | H |  |  |
| 75 | Application Servers Support - The solution should support removing static hard coded passwords from Data Sources in Application Servers. | H |  |  |
| **Auto Discovery of Privilege Accounts** | | | | |
| 76 | The solution should be able to perform auto discovery of privileged accounts on target systems and perform two way reconciliation. | H |  |  |
| 77 | The solution should have an ability to quickly identify all non-built-in local administrator accounts in your environment (flag possible 'backdoor' accounts) | H |  |  |
| 78 | The solution should have an ability to quickly identify private and public SSH keys, including orphaned SSH keys, on Unix/Linux machines, extracts key related data and ascertain the status of each key | H |  |  |
| **Notification Engine** | | | | |
| 79 | The solution should have capability to provide alerts and notification for critical PIM events over SMS & Email | H |  |  |
| 80 | The solution should have capability to provide alerts and notification for all administration/configuration activities over SMS & Email | H |  |  |
| 81 | Customizable notification for command executed on SSH and Telnet based devices | H |  |  |
| 82 | Customizable notification for command/Process executed on Windows | H |  |  |
| 83 | Notification on target being access on criteria like Line of Business or Groups | H |  |  |
| **Solution Workflow** | | | | |
| 84 | The solution should have inbuilt workflow to manage | H |  |  |
| 85 | Electronic Approval based Password Retrieval | H |  |  |
| 86 | The solution should support Onetime access / Time Based / Permanent Access | H |  |  |
| 87 | 5 level approval workflow with E-mail and SMS notification with delegation rules | H |  |  |
| 88 | Ability to provide for delegation at all levels in the workflow | H |  |  |
| 89 | Mobile device support - ability to send a request to access a password, approve the request and retrieve the password, all from a hand-held mobile device e.g. smart phones | L |  |  |
| 90 | Supports a workflow approval process that is flexible to assign multiple level of approvers based on product or model (i.e. require 2 or more approvals before access is allowed). | H |  |  |
| 91 | Supports a workflow approval process that requires approvers to be in sequence before final approval is granted. | H |  |  |
| 92 | Ability to log workflow processes and/or have the ability to be reported or audited. | H |  |  |
| **Dashboard & Reporting & Built-in Ticketing system** | | | | |
| 93 | Dashboard Capabilities should include real-time view of activities performed by the administrators | H |  |  |
| 94 | The solution should have ability to report on all system administrative changes performed by PIM Administrators with relevant auditable records | H |  |  |
| 95 | Proposed solution should have its own built in ticketing systems | H |  |  |
| 96 | The vendor should have a local depot in India for support for faster replacements**.** | H |  |  |
| 97 | Copy of credential information to be kept at DR location which will be used in case of any disaster at DC. Bidder can plan additional resources etc. at DR for this requirement. | H |  |  |

**Annexure 11.3 Anti – Advanced Persistent Threat**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Requirement Description** | **Priority - High (H) / Low (L)** | **Compliance (Y/N)** | **Vendor Remarks (if any)** |
| 1 | The proposed solution should have breach detection rate of more than 99% as per NSS lab Breach Detection Systems test report & the test report should be submitted | H |  |  |
| 2 | The Proposed solution should not have been disqualified for false compliance, incorrect RFP submission of the required specs in any other Government/ PSU's in past. | H |  |  |
| 3 | The proposed solution should be able to inspect multi-protocol sessions to detect and flag suspicious activity including file downloads through the web, mail attachments and internal infections. It should not have any port based restrictions and should support all ports. | H |  |  |
| 4 | The proposed solution should be able to detect and prevent the persistent threats which come through executable files, PDF files , Flash files, RTF files and/or other objects without relying upon any external box solution like Firewall / NGFW / IPS/NGIPS/Web Proxy | H |  |  |
| 5 | The proposed Solution should have throughput of 2 GBPS, have the ability to support both inline and out-of-band detection and should cause limited interruption to the current network environment. The Bank reserves the option of using deployment as Inline or out-of-band. | H |  |  |
| 6 | The proposed solution should have event detection capabilities that should include malware type, severity, source and destination of attack and the history of the movement of the malware in the network. | H |  |  |
| 7 | The proposed Solution should be deployed on premise along with on premise sandbox capability. Sensitive data (such as files) should not be sent outside the network except metadata. | H |  |  |
| 8 | The proposed solution have a capability to store the complete file (if the file is identified as malware or its current state cannot be determined) and its associated artefacts. | H |  |  |
| 9 | The proposed solution should be able to store packet captures (PCAP) of all Malicious communications detected by sandbox. | H |  |  |
| 10 | The proposed solution should be able to support XFF (X-Forwarded-For) to identify the IP Address of a host in a proxy environment. | H |  |  |
| 11 | The proposed solution should be able to integrate with its own threat intelligence portal for further investigation, understanding and remediation of an attack. | H |  |  |
| 12 | The Proposed solution should be able to support up to 5 network segments on a single appliance to give visibility into WAN, DMZ, Server Farm, Wi-Fi network, MPLS links etc. simultaneously. | H |  |  |
| 13 | The Proposed solution should be able to detect and block communications to known command and control servers, detect reputation of URL being accessed. | H |  |  |
| 14 | The proposed solution should be able to identify and help understand the severity and stage of each attack. | H |  |  |
| 15 | The proposed solution should have built in capabilities to add exceptions for detections & have capabilities to configure files, IP, URLs and Domains to Black list or white list. | H |  |  |
| 16 | The Proposed solution must provide a web service interface/API for customer to customize integration. | H |  |  |
| 17 | The Proposed solution should provide correlated threat data such as: IP addresses, DNS domain names, URLs, Filenames, Process names, Windows Registry entries, File hashes, Malware detections and Malware families through a portal. | H |  |  |
| 18 | The proposed solution should support SIEM integration using varied methods like open standards/API/Syslog/CEF/LEEF etc. | H |  |  |
| 19 | The proposed solution should be deployed to protect Bank‘s IT Infrastructure from threat originating/coming from E- mail and Web. | H |  |  |
| 20 | The proposed solution should have capability of horizontal scalability. | H |  |  |
| 21 | The proposed Solution should be address HTTP,HTTPS,SMTP,SMTP CIFS, FTP and other protocols | H |  |  |
| **Architecture/Design - Operations** | | | | |
| 22 | The proposed solution should support maximum number of protocols on Single Sandbox appliance. | H |  |  |
| 23 | The proposed solution should have an option to deploy in 'fail open' mode in any case of any device failure | H |  |  |
| **Performance** | | | | |
| 24 | Solution should have a provision of 10G interfaces on Appliance proposed for Data ports. | H |  |  |
| **Technology - Security Effectiveness** | | | | |
| 25 | The proposed solution should have a combination of static and dynamic analysis techniques to unmask cleverly disguised malware. | H |  |  |
| 26 | The proposed solution should have ability to block all outbound call-back communication initiated by the internal clients (infected) or also within SandBox environment. | H |  |  |
| 27 | The proposed solution should be able to give User notification over Email, Web and support customization of User Notification page | H |  |  |
| 28 | The proposed solution should be able to retrieve original files by providing justification and delivery incase original file is clean | H |  |  |
| **Endpoint Detection and Response** | | | | |
| 29 | The proposed solution should be able to provide customizable sandbox to match customer's endpoint environments, Sandbox must supports multiple operating systems for both 32-bits and 64-bits OS, Should Support multiple version of Windows and must have the ability to simulate the entire threat behavior | H |  |  |
| 30 | The proposed solution should have provision to identify entry point of malware. | H |  |  |
| 31 | The proposed solution should have grayware detection capabilities and should detect network Attacks and Exploits. | H |  |  |
| 32 | Solution must be capable of performing multiple file format analysis which includes but not limited to the following: LNK, Microsoft objects, pdf, exe files, compressed files, .chm, .swf, .jpg, .dll, .sys, .com and .hwp | H |  |  |
| 33 | The proposed solution must provide the capability to export network packet files and encrypted suspicious files for further investigation. | H |  |  |
| 34 | The proposed solution have the capability to perform tracking and analysis of virus downloads and suspicious files. | H |  |  |
| 35 | The proposed solution should have capabilities to scan inside archives. | H |  |  |
| 36 | The Proposed solution should have capabilities to detect Malwares and Spywares on windows and non-windows platforms and have capabilities to detect Mac, Linux and mobile malwares. | H |  |  |
| 37 | The proposed solution should have option to configure unrestricted Internet for sandboxes. Solution should be able to detect known malwares/threats based on various engines before sending suspicious files to Sandbox for analysis. | H |  |  |
| 38 | The proposed solution must be able to quarantine/clean infected files once it is determined to be malicious. | H |  |  |
| 39 | Solution must have the capability to analyze large files and Must be able to support minimum 100MB file size. | H |  |  |
| 40 | The proposed solution should have an automated Incident analysis function that provides a comprehensive view of attack flow, root cause, business impact, and entry point to enable accelerated remediation | H |  |  |
| 41 | The proposed solution should support forensics analysis of malicious files. | H |  |  |
| 42 | The proposed solution should not require users to specify the operating system and application used during the analysis. The solution proposed should offer the necessary intelligence to provide the right environment to draw out the malware behavior based on the file telemetry information. | H |  |  |
| 43 | The proposed solution should have capabilities to configure separate notifications to the administrator or individuals based on specific events like, Sandbox detection, Black List and license events etc. | H |  |  |
| 44 | The proposed solution should be able to correlate local APT attacks with Global historical APT attacks. | H |  |  |
| 45 | The proposed solution should have usable storage of 2 TB and support at least 6 Ethernet Interfaces | H |  |  |
| 46 | The Proposed solution for Email Anti-APT should be deployable in inline mode as MTA. | H |  |  |
| 47 | The proposed solution should detect and analyze the URL which is pointed from a file or the mail body and subject. Known bad URLs should be detected by the engines without sending it to sandbox. | H |  |  |
| 48 | The Proposed solution should be able to Deliver the email message to the recipient after replacing the suspicious attachments with a text file and tag the email message subject with a string to notify the recipient. Solution should also be able to pass and tag the email message | H |  |  |
| 49 | The Proposed Email Anti-APT solution should have detailed dashboards for Attack Sources, High-Risk Messages, Detected Messages, Top Attack Sources, Quarantined Messages, Delivery Queue, Hardware Status, sandbox Queue, Suspicious Objects from Sandbox, Email Messages with Advanced Threats, | H |  |  |
| 50 | The Proposed solution should be able to Identify suspicious embedded object in document file like OLE, Macro extraction, Shell code & exploit matching. | H |  |  |
| 51 | The proposed solution should be able to detect and take action if file has suspicious attributes like True-file type & Naming trick. | H |  |  |
| 52 | The proposed solution should be able to detect and take action if file has suspicious attributes like True-file type & Naming trick. | H |  |  |
| 53 | The proposed solution should Block and hold file from spreading across all endpoints i.e. prevent lateral movement | H |  |  |
| **Management & Reporting** | | | | |
| 54 | The solution should support CLI, and must be administered through a web based console using SSH/HTTPS. Should support AAA for role based administration | H |  |  |
| 55 | The proposed solution should have feasibility to receive Threat feeds/Updates from OEM cloud. | H |  |  |
| 56 | The proposed solution should have an intuitive Dashboard that offers real time threat visibility and attack characteristics. | H |  |  |
| 57 | The proposed solution should provide reports with (but not limited to) HTML/CSV/PDF formats. | H |  |  |
| 58 | The proposed solution should be able to schedule reports and also provide the flexibility to generate on-demand reports in daily/weekly/monthly/yearly or specific range (by day and time). | H |  |  |
| 59 | The proposed solution should support logging of important parameters like Source IP, Destination IP, ports, protocol, Domain, time stamp etc. of the attacks sessions. | H |  |  |
| 60 | The proposed solution should have the flexibility to provide customizable dashboard. | H |  |  |
| 61 | The proposed solution should have the option to provide Investigative dashboard that is capable of displaying graphical data that is based on link-graph, geo-map, chart, tree-map / pivot table. | H |  |  |
| 62 | The proposed solution should be able to provide in-depth reporting including the level of risk, sandbox assessment, and network activity analysis. | H |  |  |
| 63 | The proposed solution must be able to provide intelligence portal for malware information, threat profile, source, destination, &user where applicable. | H |  |  |
| 64 | The Proposed solution should be able to generate out of box reports to highlight Infections, C&C behaviour, Lateral Movement. | H |  |  |
| 65 | The proposed solution shall support Local Password & Radius for authentication schemes | H |  |  |
| 66 | The proposed Sandbox shall also be capable of analysing URLs. | H |  |  |
| 67 | The vendor should have a local depot in India for support for faster replacements. | H |  |  |
| 68 | Solution should address known/unknown malwares using multi layered security methodology and should not be only dependent on Sandboxing. | H |  |  |
| 69 | Solution should have an option of file scrubbing within seconds like removing macros, java scripts, embedded objects from Microsoft office and Adobe PDF and deliver malware free document to user. | H |  |  |
| 70 | In case of non-availability of proposed APT solution at DC, production should not be impacted. | H |  |  |
| 71 | The proposed solution should support exporting of analysis results such as C&C server IP and malicious domain listing. | H |  |  |
| 72 | The Proposed solution should be able to provide details of files with very low prevalence, Footprint (Identification of system, IP's and user machines) of a given file and provide detailed file execution report for all sandbox detections. | H |  |  |

**Annexure 11.4 Firewall Analyzer**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Requirement Description** | **Priority - High (H) / Low (L)** | **Compliance (Y/N)** | **Bidder Remarks (if any)** |
| 1 | The proposed solution should support all the major Firewall and devices such as Juniper, Cisco, PaloAlto, Checkpoint, Forcepoint, and Fortinet. | H |  |  |
| 2 | Proposed solution should conduct risk analysis by analyzing all possible traffic passing through the Firewalls | H |  |  |
| 3 | Proposed solution should have risk identification capability for the traffic passing from non-secured to secured Zones enforcing strong network segmentation | H |  |  |
| 4 | The proposed solution should support application based Risk analysis for Next Generation Firewalls | H |  |  |
| 5 | The proposed solution should provide below auto-completed compliance/Audit reports for both Individual and for group of firewalls – PCI DSS V3.2 ISO 27001 SOX J-SOX NERC Basel II | H |  |  |
| 6 | The proposed solution should provide information on – Unused Rules Disabled rules Time-inactive rules Duplicate object and services Rules without logging Rules with non-compliant comments Rules about to expire | H |  |  |
| 7 | The proposed solution should provide information on Rule Reordering - with Actionable reordering recommendation and also the expected improvements after reordering the rules | H |  |  |
| 8 | The proposed solution should provide information on both un-attached and unused objects | H |  |  |
| 9 | The proposed solution should specifically suggest consolidation of Firewall rule sets for optimizing the rules for better manageability, audit and performance | H |  |  |
| 10 | The proposed solution should allow opening a Change Request for removing the Unused Rules and Covered rules directly from the analysis report for ease of operations. The removal of these rules should also be automatic irrespective of the firewall brand in case bank decides to procure change management module as well from the same OEM in near future. | H |  |  |
| 11 | The proposed solution should generate enterprise-wide interactive network map based on the routing information and topology of the added devices | H |  |  |
| 12 | The proposed solution should provide information on Tightening the overly permissive rules. For example it should identify exact ports/IP’s getting used under “ANY” under any of the Policy/ACL | H |  |  |
| 13 | Firewall analysis report should present Objects' content of Host, Host Group, IP range, Service & Service Object when exporting the Policies to PDF for better visibility and easy troubleshooting | H |  |  |
| 14 | The proposed solution should have a change management capability and should support Bulk change request submission through Excel file | H |  |  |
| 15 | The proposed solution should Auto-detect, and respond to FW Change Requests where the traffic is already allowed based on source, destination and service details | H |  |  |
| 16 | The proposed solution should Allow change planning through a simulation of traffic path and find all the rules in all the firewalls that block requested traffic | H |  |  |
| 17 | The proposed solution should automatically compute and push policies on Cisco IOS Routers | H |  |  |
| 18 | FW change management solution should automatically identify the business impact of the Change Request and assess the risk per the built in best practices database | H |  |  |
| 19 | The proposed solution should automatically detect violations of regulatory requirements introduced by Change Request before implementing on the Firewalls. | H |  |  |
| 20 | FW change management solution should automatically create the work-order in the FW's native format and suggest the optimal way to define the policies - For eg - modification of the existing policies instead of creating a new policy to the required traffic | L |  |  |
| 21 | The proposed solution should be able to automatically push the policies on Checkpoint gateway via Checkpoint management server, Palo-Alto Device group via Panorama & on Fortimanager for Fortinet devices. | H |  |  |
| 22 | The solution should be able to automatically create the CLI recommendation and centrally push policies on Cisco FWSM, PIX, ASA devices and on Juniper SRX devices as well. | H |  |  |
| 23 | The proposed solution should have out of the box workflows including but not limited to: Rule Removal, Service Object Change Rule Modification Rule Re-certification Drop Traffic Parallel Approval | H |  |  |
| 24 | Solution should allow user to set a traffic workflow which runs automatically from submission to resolution i.e. Planning, risk assessment, recommending changes, implementation and validation, all stages be performed automatically without any human intervention to help bank to enhance service delivery | H |  |  |
| 25 | Proposed solution should have in built workflow to populate the organization specific security policies to new devices i.e. enables bulk updating of tens or hundreds of rules using a single change request during the Firewall Migration Process | H |  |  |
| 26 | The Proposed solution should have a scalability factor to discover and map the business applications and the associated logical connectivity with the underlying security policies. It should also be able to build the application flows based on the Firewall policies if required. | H |  |  |
| 27 | Solution should identify Blocked and allowed flows from an application perspective to enable application team to collaborate with the operations team. | H |  |  |
| 28 | Solution should present Firewalls/Routers that intercepts the application flow | H |  |  |
| 29 | The proposed solution should have a provision of decommissioning of business application. The decommissioning process should be fully automated and the rules should be removed automatically from the Firewalls only for that application which needs to be decommissioned. The system should also identify those rules which cannot be removed as those could be linked to other applications. | H |  |  |
| 30 | The proposed solution should be application centric and have a provision for server migration process. The process should be fully automated and should specify the inline applications and their logical connectivity which requires changes. The proposed system should even provision the necessary rules on the FW's automatically. | H |  |  |
| 31 | The solution should provide an ability to verify the impact on business applications if the inline FW is down or a specific policy on the FW is blocking the application traffic. | H |  |  |
| 32 | The proposed solution should have a capability to map the Firewall configuration risks with the inline business applications. It should present the risks in the overall application context. | H |  |  |
| 33 | The vendor should have a local depot in India for support for faster replacements**.** | H |  |  |

**Annexure 11.5 Network Access Control (NAC)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Requirement Description** | **Priority - High (H) / Low (L)** | **Compliance (Y/N)** | **Bidder Remarks (if any)** |
| 1 | The solution should support continuous detection of devices attempting to connect to the network. | H |  |  |
| 2 | The solution should gather the following data before an endpoint has access to network:   1. Device type, 2. Operating system 3. User identity, 4. Operating system 5. Patch status 6. Anti-virus status, 7. Host firewall status, 8. Known/Unknown device status, 9. Past policy compliance and threat history, 10. Wired/Wireless connection, 11. Windows registry settings | H |  |  |
| 3 | The solution should have a registration process for the external devices to access internal network and maintain guest access. | H |  |  |
| 4 | The solution should not allow infection of already quarantined elements by other quarantined elements | H |  |  |
| 5 | The solution should support quarantine mechanism performed both at Layer 2 and Layer 3 | H |  |  |
| 6 | The solution should detect handheld devices with platforms such as iPhone/iPad, Blackberry, Android, Windows and Nokia Symbian etc. | H |  |  |
| 7 | The solution should detect devices without IP addresses, such as stealthy packet capture devices designed to steal sensitive data. | H |  |  |
| 8 | The solution should be able to integrate with existing directory services/ identity and access management system for Role-based access facility. | H |  |  |
| 9 | The solution should be able to report violations based on bank's defined device baseline to the SIEM. For example all endpoints should be in compliance with Bank's antivirus policy, should be properly patched and free of unauthorized software etc. | H |  |  |
| 10 | The solution should support existing standard-based authentication and directories such as 802.1x, Directory services, AAA mechanisms etc. | H |  |  |
| 11 | The solution should be able to link and identify iPads that are owned by the Bank, and block other iPads | L |  |  |
| 12 | The solution should support existing third party hardware/software such as Network switches, Wireless Access Points, VPN, Antivirus, Patch Management, Ticketing, SIEM, Vulnerability assessment scanners and MDM. | H |  |  |
| 13 | The solution should support out-of-band deployment. | H |  |  |
| 14 | The solution should support the following mechanisms for access control and policy validation:  VLAN Steering, DHCP, Anti ARP spoofing, Agent based enforcement, Mac Authentication etc. | H |  |  |
| 15 | The solution should capture audit logs that contain the following but not limited to user name , IP, roles , groups, compliance status of endpoint etc. | H |  |  |
| 16 | The solution should be able to detect through periodic monitoring if endpoint security configurations are modified after obtaining access to the network and identify users who have violated in the past. | H |  |  |
| 17 | The solution should support alerting mechanism such as e-mail, SMS etc. | H |  |  |
| 18 | The solution should be able to control access to network as per time, location of user, mode of access, type of system used to access etc. | H |  |  |
| 19 | The solution should be able to detect endpoint Mac address, IP addresses, network resources devices, resources such as printers and scanners, network zones etc. through auto discovery. | H |  |  |
| 20 | The solution should be able to provide visibility to VPN users as well | H |  |  |
| 21 | The solution should be able to support virtualized environments. | H |  |  |
| 22 | The solution should support Microsoft NAP and Trusted Computing Group. | H |  |  |
| 23 | The solution should permit admin to define thresholds for threat levels received from the NAC | H |  |  |
| 24 | The proposed solution should provide scanning to discover and mitigate threats from infected endpoints and incorporate the indicators of compromise (IOC’s) the bank receives from time to time from external sources. | H |  |  |
| 25 | The solution should support non-disruptive, out-of-band deployment with built-in configuration wizards and customizable policy templates for rapid time-to-value. | H |  |  |
| 26 | In case of non-availability of proposed NAC solution, end users across all locations should be able to login to the network without any issues. | H |  |  |
| 27 | The solution should be able detect and manage hand held devices used for financial inclusion process | L |  |  |
| 28 | The solution should support both 802.1X and Non-802.1X Architecture. The support for Non-802.1X Architecture will allow early integration with Bank's existing network  infrastructure without the need of any hardware and software upgrades required for 802.1X deployments | H |  |  |
| 29 | The NAC solution should detect endpoint state changes (AV disabled, execution of an unauthorized application, etc.) and perform auto-remediation. | L |  |  |
| 30 | The NAC Solution should support agentless , agent base & Desolvable agent mode | H |  |  |

**Annexure 11.6 Vulnerability Assessment and Penetration Testing Service**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Requirement Description** | **Priority - High (H) / Low (L)** | **Compliance (Y/N)** | **Bidder Remarks (if any)** |
| **VAPT Service** | | | | |
| 1 | The proposed solution should perform a targeted scan (i.e. check for a specific set of vulnerabilities or IP Addresses). | H |  |  |
| 2 | The proposed solution should provide info on applications running on non-standard ports. | H |  |  |
| 3 | The proposed solution should be able to conduct vulnerability assessment for all operating systems and their versions including but not limited to: Windows, AIX, Unix, Linux, Solaris servers etc. | H |  |  |
| 4 | The proposed solution should scan workstation, servers, network and security equipment and other devices such as printers, mobiles, webcams, tablets etc. | H |  |  |
| 5 | The proposed solution should perform authenticated and unauthenticated scans | H |  |  |
| 6 | The proposed solution should scan application databases for vulnerabilities | H |  |  |
| 7 | The proposed solution should detect weak password for databases and point out accounts with simple, weak and shared passwords. | H |  |  |
| 8 | The proposed solution should identify out-of-date software versions, applicable patches and system upgrades. | H |  |  |
| 9 | The proposed solution should provide remediation information in the reports including links to patches etc. | H |  |  |
| 10 | The proposed solution should produce a report listing all applications on a host or network, regardless of whether the application is vulnerable or not | H |  |  |
| 11 | The proposed solution should generate report in line with RBI, PCI DSS and ISO 27001 Guidelines | H |  |  |
| 12 | The proposed solution should produce reports in the following formats: XLS, PDF, CSV, XML etc. | H |  |  |
| 13 | The proposed solution must be able to export scan data in format including but not limited to ARF, CSV, CyberScope XML, JDBC-Compliant Database, Simple, XML 1.0 and 2.0, SCAP XML, SQL Query Export and XCCDF. | H |  |  |
| 14 | The proposed solution must support reports to filter vulnerabilities by category and severity. | H |  |  |
| 15 | The proposed solution must support integration with external penetration testing platforms to perform automatic vulnerabilities exploitation without running any manual imports to confirm that vulnerabilities can be exploited. | L |  |  |
| 16 | The proposed solution must have ability to identify virtual devices that are in a suspended or off state. | H |  |  |
| 17 | The proposed solution must be able to create reports that identify the top 10 steps to reduce the risk of (a user defined) group of devices | L |  |  |
| 18 | The proposed solution must calculate risk for each detected vulnerability. Risk scoring must include CVSS scoring, asset exploitability, and susceptibility to malware kits. | H |  |  |
| 19 | The proposed solution must be able to distribute reports to external recipient at least in the form of email and support report scheduling capabilities. | H |  |  |
| 20 | The proposed solution must be able to automatically send reports when scans are completed. | H |  |  |
| 21 | Solution must be able to support installation on 64-bit Linux and Windows (64-bit). | H |  |  |
| 22 | Solution shall have latest updates (e.g. exploit module) as frequent as on a weekly basis. | H |  |  |
| 23 | Solution shall support offline activation and manual updates. | H |  |  |
| 24 | Solution must be able to run jobs or tasks (e.g. scan, exploit) on schedule. | H |  |  |
| 25 | Solution must support importing of scan result from external solutions including but not limited to Nexpose, Metasploit, Foundstone, Microsoft, nCircle, NetSparker, Nessus, Qualys, Burp, Acunetix, AppScan, Nmap, Retina, Amap, Critical Watch, IP Address List, Libpcap, Spiceworks and Core Impact. | H |  |  |
| 26 | Solution shall support dry runs to show the scan information in task log only. | L |  |  |
| 27 | Solution shall automatically select and apply exploit modules based on OS, service and vulnerability references. | H |  |  |
| 28 | Solution shall have at least 6 reliability levels of exploit codes for automated exploitation. | H |  |  |
| 29 | Solution shall support running individual exploit module manually from the user interface. | H |  |  |
| 30 | Solution shall support replay of exploitation tasks. | H |  |  |
| 31 | Solution shall support brute force testing on services including but not limited to AFP, SMB, Postgres, DB2, MySQL, MSSQL, HTTP, HTTPS, SSH, SSH PUBKEY, Telnet, FTP, POP3, VNC, SNMP, WinRM. | H |  |  |
| 32 | Solution must provide built-in standard reports and support customized report functionality. | H |  |  |
| 33 | Solution must support reports to be stored locally and sent to recipient by email after created. | H |  |  |

**Annexure 11.7 Indicative List of hardware / network / security devices**

**(To be integrated with the security solutions offered under CSOC)**

|  |  |  |
| --- | --- | --- |
| **S.No.** | **Devices** | **Total Number** |
|
| 1. | Number of devices to be integrated with SIEM | 300 |
| 2. | Number of devices to be integrated with NAC | 1600 |
| 3. | Number of devices to be integrated with PIM | 200 |
| 4. | Number of devices for Vulnerability Assessment | 100 |
| 5. | Number of devices for Penetration Testing | 50 |

Devices include hardware, software, appliance, applications, IP, endpoints etc.

The asset list given above in this section is an indicative list and the bidder is expected to take the details of the inventory at the time of project implementation. Further, bidder will assist the Bank in incorporating the newer hardware devices with all the tools.

**Annexure 11.8 Resource Requirement Details**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Type** | **Role** | **Experience** | | **Academics** | **Minimum Number of Resources (12\*6) 8 AM to 8 PM for 6 days** |
| **Total in IT (yrs)** | **IT Security (yrs.)** |
| L1 | * Event monitoring & alert/Incident tracking; regular solution administration. * Fine tuning of the false positive events * Categorization of requests into functional clarification and provision of workaround * Bug identification/change requests to be logged and reported for further processing * Provide telephonic and / or electronic mechanisms for problem reporting requests as well as for service and status updates * Preparation of incident reports | 2 yrs. (min.) | 1 year (min.) | BE/B.Tech  B.Sc. – IT or BCA | 4 (in 2 shifts) |
| L2 | * Provide continuous onsite support for the implementation of CSOC solution and support for integrating any applications to be interfaced with SIEM solution in future. * Troubleshoot at various levels in the CSOC Solution implementation * Resolve the call within stipulated timeframe as defined in Service Level Agreement * Coordinate with the L1 & L3 team for resolution and provide necessary information as may be required by the team to resolve the issues. Escalate the unresolved calls as per escalation matrix * Provide the timeframe for providing a solution of resolution of the escalated calls and automatically log calls during escalation * Prepare a root cause analysis document with the resolutions provided for major issues such as production issues, service disruptions or downtime, delayed response times, data/ table corruptions, system performance issues (high utilization levels) etc. * Perform the application audit on a quarterly basis or as mutually agreed with the bank and rectify any corruption in the software * Ensure patch releases are ported to the production environment with no business disruption or business losses * Support periodic BCP/DR drills * Routing the events through the backup system in case the primary system fails * Providing bank with daily hardware utilization reports and alerting BANK in case of any performance issues or hardware upgradation requirements * Preparation of incident reports and periodic reporting of critical incidents to management team of bank | 4 yrs. (min) | 3 years (min.) | BE/B.Tech/MCA/MSc. IT | 1 in general shifts |
| L3 | * Resolve the call within the stipulated timeframe as defined under the service level agreements * Communicate the status of the call to the Bank and accordingly update the status, resolution or workaround and date of resolution * Prepare a root cause analysis document for issues referred to L3 support and provide to the Bank along with the resolution * Liaise with the L2 support personnel for the call information and resolution. * Perform version upgrades/migration as per the version release plan of OEM and agreed by the Bank. * Provide training to the Bank’s team on CSOC solution and new version functionalities | 6 years (min.) | 5  (min 2 years on proposed CSOC solution) | BE/B.Tech/MCA/MSc.IT | 1 in general shift onsite |
| DC Operator (System Administrator) | * Managing and administrating entire infrastructure (server, storage, network devices, etc.) of CSOC operations at DC Site, Navi Mumbai | 4 yrs. (min) | 3 years (min.) | BE/B.Tech/MCA/MSc. IT | 1 in general shifts |

**Annexure 11.9 Non-disclosure Agreement**

(TO BE EXECUTED ON A NON-JUDICIAL STAMPED PAPER of requisite value based on place of execution)

WHEREAS, we, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, having Registered Office at \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, hereinafter referred to as the COMPANY, are agreeable to execute “Implementation and Management of Cyber Security Operations Center (CSOC)” as per scope defined in the Request for Proposal (RfP) No Tender\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ for Small Industries Development Bank of India, having its Head office at SIDBI Tower, 15 Ashok

Marg, Lucknow, 226001, and office at, MSME Development Centre, Plot No. C-11, G Block, Bandra Kurla Complex (BKC), Bandra (E), Mumbai - 400 051 (hereinafter referred to as the BANK) and WHEREAS, the COMPANY understands that the information regarding the Bank’s Infrastructure shared by the BANK in their Request for Proposal is confidential and/or proprietary to the BANK, and

WHEREAS, the COMPANY understands that in the course of submission of the offer for the said RfP and/or in the aftermath thereof, it may be necessary that the COMPANY may perform certain jobs/duties on the Bank’s properties and/or have access to certain plans, documents, approvals, data or information of the BANK;

NOW THEREFORE, in consideration of the foregoing, the COMPANY agrees to all of the following conditions, in order to induce the BANK to grant the COMPANY specific access to the BANK’s property/information:

The COMPANY will not publish or disclose to others, nor, use in any services that the COMPANY performs for others, any confidential or proprietary information belonging to the BANK, unless the COMPANY has first obtained the BANK’s written authorisation to do so;

The COMPANY agrees that information and other data shared by the BANK or, prepared or produced by the COMPANY for the purpose of submitting the offer to the BANK in response to the said RfP, will not be disclosed to during or subsequent to submission of the offer to the BANK, to anyone outside the BANK;

The COMPANY shall not, without the BANK’s written consent, disclose the contents of this Request for Proposal (Bid) or any provision thereof, or any specification, plan, pattern, sample or information (to be) furnished by or on behalf of the BANK in connection therewith, to any person(s) other than those employed/engaged by the COMPANY for the purpose of submitting the offer to the BANK and/or for the performance of the Contract in the aftermath. Disclosure to any employed/engaged person(s) shall be made in confidence and shall extend only so far as necessary for the purposes of such performance.

Yours Sincerely,

Signature of Authorised Signatory

Name of Authorized Signatory:

Designation:

Office Seal:

Date

Place

**Annexure 11.10 Performance Bank Guarantee**

*(To be executed on a non-judicial stamped paper of requisite value)*

KNOW ALL MEN BY THESE PRESENTS that in consideration of the Small Industries Development Bank of India (SIDBI), a Corporation constituted and established under the Small Industries Development Bank of India Act, 1989, and having its Head Office at SIDBI Tower, 15 Ashok Marg, Lucknow, 226001, and office at 3rd Floor, MSME Development Centre, Plot No. C-11, G Block, Bandra Kurla Complex (BKC), Bandra (E), Mumbai - 400 051 (hereinafter called the Corporation / Bank) having agreed to accept from M/s. ‘Vendor Name’ having its office at ‘Vendor’s Office Address’, (hereinafter called "the Vendor") an agreement of guarantee for Rs. \_\_\_\_\_\_\_ (Rupees \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ only), for the due fulfillment by the vendor of the terms and conditions of the Purchase order No. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ dated \_\_\_\_\_\_\_\_\_\_ made between the vendor and the Corporation for providing services for SIDBI’s ‘Project Details’ hereinafter called "the said Agreement”).

1. We, Bank (Bank Name and Details), do hereby undertake to indemnify and keep indemnified the Corporation to the extent of Rs. \_\_\_\_\_\_\_ (Rupees \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ only) against any loss or damage caused to or suffered by the Corporation during warranty period by reason of any breach by the Vendor of any of the terms and conditions contained in the said Agreement of which breach the opinion of the Corporation shall be final and conclusive.

2. And we Bank (Bank Name and Details), do hereby guarantee and undertake to pay forthwith on demand to the Corporation such sum not exceeding the said sum of Rs. \_\_\_\_\_\_\_ (Rupees \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ only) only as may be specified in such demand, in the event of the vendor failing or neglecting to execute fully efficiently and satisfactorily the order for implementation services for the ‘Project Details’ placed with it (the work tendered for by it) within the period stipulated in the said Agreement in accordance with the design, specification, terms and conditions contained or referred to in the said Agreement or in the event of the Vendor refusing or neglecting to maintain satisfactory operation of the equipment or work or to make good any defect therein notified by the Corporation to the vendor during the warranty period or otherwise to comply with and conform to the design, specification, terms and conditions contained or referred to the said Agreement.

3. We, Bank (Bank Name and Details), further agree that the guarantee herein contained shall remain in full force and effect during the period that would be taken for the performance of the said order as laid down in the said agreement including the "Warranty obligations" or till validity date of this guarantee i.e. upto \_\_\_\_\_\_\_\_, whichever is earlier and subject to the terms of the "the said Agreement” it shall continue to be enforceable for the breach of warranty conditions within warranty period and till all the defects notified by the Corporation to the vendor during the warranty period have been made good to the satisfaction of Corporation & the Corporation or its authorized representative certified that the terms and conditions of the said agreement have been fully and properly complied with by the vendor or till validity of this guarantee i.e \_\_\_\_\_\_\_\_\_, whichever is earlier.

4. We, Bank (Bank Name and Details), may extend the validity of Bank Guarantee at the request of the Vendor for further period or periods from time to time beyond its present validity period, but at our sole discretion.

5. The liability under this guarantee is restricted to Rupees \_\_\_\_\_\_\_\_/- only and will expire on \_\_\_\_\_\_\_\_\_ and unless a claim in writing is presented to us at Bank (Bank Name and Details) within 3 months from \_\_\_\_\_\_\_\_\_ , i.e. on or before \_\_\_\_\_\_\_\_\_, all your rights will be forfeited and we shall be relieved of and discharged from all our liabilities there-under.

6. The Guarantee herein contained shall not be determined or affected by Liquidation or winding up or insolvency or closure of the Vendor.

7. The executant has the power to issue this guarantee and executants on behalf of the Bank and hold full and valid Power of Attorney granted in their favour by the Bank authorizing them to execute this guarantee.

Notwithstanding anything contained here in above, our liability under this guarantee is restricted to Rs. \_\_\_\_\_\_\_ (Rupees \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ only). Our guarantee shall remain in force until \_\_\_\_\_\_\_\_. Our liability hereunder is conditional upon your lodging a demand or claim with Bank (Bank Name and Details) on or before \_\_\_\_\_\_\_\_\_. Unless a demand or claim is lodged with Bank (Bank Name and Details) within the aforesaid time, your rights under the guarantee shall be forfeited and we shall not be liable there under. This guarantee shall be governed by and construed in accordance with the laws of India. All claims under this guarantee will be made payable at Bank (Bank Name and Details). This Guarantee will be returned to the Bank when the purpose of the guarantee has been fulfilled or at its expiry, whichever is earlier.

We, Bank (Bank Name and Details) lastly undertake not to revoke this guarantee during its currency except with the previous consent of the Corporation in writing.

In witness where of we ...................... have set and subscribed our hand and seal this ........................day of .........................2019.

SIGNED, SEALED AND DELIVERED.

BY

AT

IN THE PRESENCE OF WITNESS:

1. Name..........................

Signature.....................

Designation..................

2. Name..........................

Signature.....................

Designation..................

**Annexure 11.11 Technical Bill of Material**

****

**Annexure 11.12 Undertaking Letter for GST Law**

*(To be submitted on bidder’s letterhead)*

To,

General Manager [ITV]

Small Industries Development Bank of India

SIDBI Tower,

15, Ashok Marg,

Lucknow,

Uttar Pradesh - 226001

Dear Sir,

**GST Law**

Further to our proposal dated ………………………………, in response to the Request for Proposal (Bank’s tender No. …………………………………. hereinafter referred to as “RFP”) issued by Bank, we hereby covenant, warrant and confirm as follows:

We, the bidder M/s ……………………………, hereby agree to comply with all applicable GST Laws including GST Acts, Rules, Regulations, Procedures, Circulars & Instructions thereunder applicable in India from time to time and to ensure that such compliance is done.

Authorized Signatories

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Designation: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Company Seal:

**Annexure 11.13 Undertaking for Central Minimum Wages Act & Labour Laws**

To,

General Manager [ITV]

Small Industries Development Bank of India

SIDBI Tower,

15, Ashok Marg,

Lucknow,

Uttar Pradesh - 226001

Dear Sir,

Further to our proposal dated ………………………………, in response to the Request for Proposal (Bank’s tender No. …………………………………. hereinafter referred to as **“RFP”**) issued by Bank, we hereby covenant, warrant and confirm as follows:

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

2. We ensure that the payment towards services is in consonance with the Central Minimum Wages Act & Labour Laws. We would comply with Governments rules and regulations like minimum wages act, Provident fund and ESIC facility standard for the employees / resources deployed by us on-site for the said project.

3. Proof of compliance and labour license are attached with herewith.

Authorized Signatories

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Designation: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Company Seal: