****

**भारतीय लघु उद्योग विकास बैंक**

**Small Industries Development Bank of India**

**RFP For Implementation and Management OF**

**Cyber Security Operations Center (CSOC)**

 **[RfP No. Tender 400/2018/1279/BYO/RiMV dated November 06 , 2017]**

|  |  |
| --- | --- |
| **Date of issue of RFP** | **NOVEMBER 06 , 2017** |
| **Last date for seeking clarifications for pre-bid meeting**  | **NOVEMBER 13, 2017 3:00PM** |
| **Pre Bid meeting** | **NOVEMBER 17, 2017 11:00am** |
| **Last date for submission of bids** | **DECEMBER 01, 2017 3:00PM** |
| **Cost of RFP** | **Rs 5,000/-** |
| **Earnest Money Deposit (EMD)** | **Rs 20,50,000/-** |
| **Date & Time of Opening of Minimum Eligibility bid &Technical bid** | **DECEMBER 01, 2017 4:00PM** |

**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**

1. **Some terms have been used in the document interchangeably for the meaning as mentioned below:“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 Vendor generally means “Respondent to the RFP document” unless context specifies otherwise**
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 Small industries Development Bank of India, Mumbai Office and DR site Chennai.**
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. **‘Successful Bidder’/ ‘H1 bidder’ means the Bidder who is found to be the highest scored bidder after conclusion of the bidding process, subject to compliance to all the Terms and Conditions of the RFP, etc.**
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 Data centre at BKC, Mumbai**
13. **DR, DRS means Bank’s Disaster Recovery centre (site) at Chennai**
14. **T & C means Terms and Conditions**
15. **BFSI means - Scheduled commercial banks in public or private sector / All India FIs / Insurance Companies.**

**Table of contents**

[**1. Introduction and Disclaimers 14**](#_Toc497679900)

[1.1. Preface 14](#_Toc497679901)

[1.2. Information Provided 14](#_Toc497679902)

[1.3. For Respondent only 14](#_Toc497679903)

[1.4. Disclaimer 14](#_Toc497679904)

[1.5. Costs to be borne by Respondents 15](#_Toc497679905)

[1.6. No Legal Relationship 15](#_Toc497679906)

[1.7. Recipient Obligation to Inform Itself 15](#_Toc497679907)

[1.8. Evaluation of Offers 15](#_Toc497679908)

[1.9. Acceptance of Selection Process 15](#_Toc497679909)

[1.10. Errors and Omissions 16](#_Toc497679910)

[1.11. Acceptance of Terms 16](#_Toc497679911)

[1.12. Requests for Proposal 16](#_Toc497679912)

[1.13. Notification 16](#_Toc497679913)

[**2. RfP Response 18**](#_Toc497679914)

[2.1. General 18](#_Toc497679915)

[2.2. Language of Bid 19](#_Toc497679916)

[2.3. Bid Price 19](#_Toc497679917)

[2.4. Earnest Money Deposit (EMD) 19](#_Toc497679918)

[2.5. Conditional Bids 19](#_Toc497679919)

[2.6. Receiving of RFP Response 19](#_Toc497679920)

[2.7. Clarification of Bids 20](#_Toc497679921)

[2.8. Amendment to the bidding document 20](#_Toc497679922)

[2.9. Rules for Responding to the RFP 21](#_Toc497679923)

[2.10. Period of Validity of Bids 22](#_Toc497679924)

[2.11. Deadline for submission of Bids 23](#_Toc497679925)

[2.12. Late Bids 23](#_Toc497679926)

[2.13. Modification And/ Or Withdrawal of Bids 23](#_Toc497679927)

[2.14. Requests for information 23](#_Toc497679928)

[2.15. Pre-Bid Meeting 24](#_Toc497679929)

[2.16. Opening of Technical Bids by the Bank 25](#_Toc497679930)

[2.17. Disqualification 25](#_Toc497679931)

[2.18. Selection process 25](#_Toc497679932)

[2.19. Details of Bids to be Submitted 26](#_Toc497679933)

[2.20. Pre Contract Integrity Pact (IP) 28](#_Toc497679934)

[2.21. Important 29](#_Toc497679935)

[2.22. Responsibility of the Bidder: 30](#_Toc497679936)

[**3. Background About SIDBI 32**](#_Toc497679937)

[3.1. About SIDBI 32](#_Toc497679938)

[3.2. Cyber Security 32](#_Toc497679939)

[3.3. Objective 32](#_Toc497679940)

[3.4. Current IT Setup 34](#_Toc497679941)

[**1. Data Centre and DR Site 34**](#_Toc497679942)

[**2. Present IT Infrastructure 34**](#_Toc497679943)

[**3. Details of Present Network and Security Infrastructure at DC and DR 34**](#_Toc497679944)

[**4. Purpose 39**](#_Toc497679945)

[4.1. CSOC Coverage: 39](#_Toc497679946)

[**5. Scope of Work 41**](#_Toc497679947)

[5.1. Introduction 41](#_Toc497679948)

[5.2. Security solutions / services to be integrated with SIEM 53](#_Toc497679949)

[5.3. Privilege Identity Management 59](#_Toc497679950)

[5.4. Anti APT (Advanced Persistent Threat) 59](#_Toc497679951)

[5.5. Firewall Analyser 60](#_Toc497679952)

[5.6. Network Access Control (NAC) 60](#_Toc497679953)

[5.7. VAPT Advisory & Remediation Services 62](#_Toc497679954)

[5.8. Security / Threat Intelligence Services 63](#_Toc497679955)

[5.9. Project Schedule and Implementation 64](#_Toc497679956)

[5.10. Training: 67](#_Toc497679957)

[**6. Evaluationmethodology 69**](#_Toc497679958)

[6.1. Evaluation process 69](#_Toc497679959)

[6.1.1. Objective 69](#_Toc497679960)

[6.1.2. Evaluation steps 69](#_Toc497679961)

[6.2. Preliminary Examinations 70](#_Toc497679962)

[6.3. Evaluation of Minimum Eligibility / Pre-Qualification Criteria 71](#_Toc497679963)

[6.4. Evaluation of Technical Bids 71](#_Toc497679964)

[**6.4.1 Technical Evaluation Criteria 72**](#_Toc497679965)

[**6.4.2 Marks for the Technical Specifications of the security solutions offered: 73**](#_Toc497679966)

[6.5. Evaluation of Commercial Bids 75](#_Toc497679967)

[6.6. Final Selection of the Eligible Bidder 76](#_Toc497679968)

[6.7. Arithmetic errors correction 76](#_Toc497679969)

[6.8. Issue of purchase order 77](#_Toc497679970)

[6.9. Execution of Agreement 77](#_Toc497679971)

[**7. Terms and Conditions 78**](#_Toc497679972)

[7.1. Bid Security & Performance Guarantee 78](#_Toc497679973)

[**1. Bid Security / Earnest Money Deposit (EMD) 78**](#_Toc497679974)

[**2. Performance Bank Guarantee (PBG) 79**](#_Toc497679975)

[7.2. Forfeiture of performance security 80](#_Toc497679976)

[7.3. Preliminary Examinations 80](#_Toc497679977)

[7.4. Use of Contract Documents and Information 81](#_Toc497679978)

[7.5. Rules for Evaluation of Responses 82](#_Toc497679979)

[7.6. Contacting the Bank 83](#_Toc497679980)

[7.7. Commercial Bid 83](#_Toc497679981)

[7.8. No Commitment to Accept Lowest or Any Offer 84](#_Toc497679982)

[7.9. Service Delivery 84](#_Toc497679983)

[7.10. Ownership of Delivered Services 85](#_Toc497679984)

[7.11. Addition / Deletion of qualified offerings 85](#_Toc497679985)

[7.12. Expenses 86](#_Toc497679986)

[7.13. Terms of Payment 86](#_Toc497679987)

[7.14. Taxes and Duties 90](#_Toc497679988)

[7.15. Execution of Agreement and NDA 91](#_Toc497679989)

[7.16. Period of Contract 91](#_Toc497679990)

[7.17. Termination 92](#_Toc497680012)

[7.18. Applicable laws 94](#_Toc497680013)

[7.19. Statutory & Regulatory Compliance 95](#_Toc497680014)

[7.20. No Employer-Employee Relationship 95](#_Toc497680015)

[7.21. Rights to Visit 95](#_Toc497680016)

[7.22. Audit 96](#_Toc497680017)

[7.23. IPR Infringement 96](#_Toc497680018)

[7.24. Indemnity 97](#_Toc497680019)

[7.25. Limitation of liabilities 98](#_Toc497680020)

[7.26. Confidentiality 99](#_Toc497680021)

[7.27. Corrupt and fraudulent practice 102](#_Toc497680022)

[7.28. Resolution of Disputes 103](#_Toc497680023)

[7.29. Grievances Redressal Mechanism 104](#_Toc497680024)

[7.30. Force Majeure 104](#_Toc497680025)

[7.31. Subcontracting 105](#_Toc497680026)

[7.32. Negligence 105](#_Toc497680027)

[7.33. Miscellaneous 106](#_Toc497680028)

[7.34. Delivery, Installation, Commissioning and Acceptance 107](#_Toc497680029)

[7.35. Responsibility for Completeness 108](#_Toc497680030)

[7.36. Change of name of the bidding company and line of business 109](#_Toc497680031)

[7.37. Governing Law and Jurisdiction 109](#_Toc497680032)

[7.38. No third party rights 109](#_Toc497680033)

[7.39. Representations and Warranties 109](#_Toc497680034)

[7.40. Vicarious Liability 111](#_Toc497680035)

[7.41. No Set-off, counter-claim and cross claims 111](#_Toc497680036)

[**8. Service Level Agreement & Liquidated Damages 112**](#_Toc497680037)

[8.1. Liquidated damages for delay in Delivery and Installation of Hardware and Software 112](#_Toc497680038)

[8.2. Liquidated damages for not maintaining uptime 113](#_Toc497680039)

[8.3. SLAs & Liquidity Damages for CSOC Operations 116](#_Toc497680040)

[8.4. Waiver 122](#_Toc497680041)

[**9. Annexure for Minimum Eligibility/Pre Qualification Criteria 124**](#_Toc497680042)

[Annexure A.1 – Eligibility Bid – Covering Letter 124](#_Toc497680043)

[Annexure A.2 –Minimum Eligibility/ Pre-Qualification Criteria 126](#_Toc497680044)

[Annexure A.3 – General Information about Bidder 129](#_Toc497680045)

[Annexure A.4 - Power of Attorney 132](#_Toc497680046)

[Annexure A.5 – Declaration regarding Clean Track Record 133](#_Toc497680047)

[Annexure A.6 – Bank Mandate Form 134](#_Toc497680048)

[Annexure A.7- EMD / Bid Security Form 136](#_Toc497680049)

[Annexure A.8 - Manufacturer Authorisation Format 138](#_Toc497680050)

[Annexure A.9 - Undertaking of Authenticity 139](#_Toc497680051)

[Annexure A.10– Pre-Contract Integrity Pact 140](#_Toc497680052)

[**10. Annexure for Technical Bid 146**](#_Toc497680053)

[Annexure B.1- Technical Bid 146](#_Toc497680054)

[Annexure B.2 – Statement of Deviations 149](#_Toc497680055)

[Annexure B.3 – Letter of Competence 150](#_Toc497680056)

[Annexure B.4 – Letter of Conformity 151](#_Toc497680057)

[**11. Annexure - Commercial Bid 152**](#_Toc497680058)

[Annexure C.1 – Commercial Bid – Covering Letter 152](#_Toc497680059)

[Annexure C.2 –Commercial Bid Format 153](#_Toc497680060)

[**12. Annexure for Technical Specifications & Others 157**](#_Toc497680061)

[Annexure D.1: Security Incident & Event Management (SIEM) 157](#_Toc497680064)

[Annexure D.2: Privilege Identity Management (PIM) 174](#_Toc497680065)

[Annexure D.3: Anti APT (Advanced Persistent Threat) 182](#_Toc497680066)

[Annexure D.4: Firewall Analyzer 188](#_Toc497680067)

[Annexure D.5: Network Access Control (NAC) 191](#_Toc497680068)

[Annexure D.6: VAPT Advisory & Remediation Services 194](#_Toc497680069)

[Annexure D.7: Indicative List of hardware / network / security devices 195](#_Toc497680070)

[Annexure D.8: Non-disclosure Agreement 196](#_Toc497680071)

[Annexure D.9: Performance Bank Guarantee 198](#_Toc497680072)

 **Abbreviations**

| **Acronym** |  **Description** |
| --- | --- |
| **AMC** | **Annual Maintenance Contract** |
| **APT** | **Advanced Persistent Threat** |
| **BFSI** | **Banking Financial Services & Insurance** |
| **BG** | **Bank Guarantee** |
| **CCIE** | **Cisco Certified Internetwork Expert** |
| **CEH** | **Certified Ethical Hacker** |
| **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** |
| **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 Incident & Event Management** |
| **SLA** | **Service Level Agreement** |
| **SPEC** | **Standard Performance Evaluation Corporation** |
| **TCO** | **Total Cost of Ownership** |
| **VAPT** | **Vulnerability Assessment & Penetration Test** |
| **WAF** | **Web Application Firewall** |

**Annexure Details**

| **Annexure(s)**  |
| --- |
| **(A) Annexure for Minimum Eligibility/Pre Qualification Criteria:** |
| **1.** | **Annexure A.1**  | **Eligibility Bid - Covering Letter** |
| **2.**  | **Annexure A.2** | **Minimum Eligibility / Pre-Qualification Bid** |
| **3.** | **Annexure A.3** | **General Information about Bidder** |
| **4.** | **Annexure A.4** | **Power of Attorney** |
| **5.** | **Annexure A.5** | **Declaration regarding Clean Track Record**  |
| **6.** | **Annexure A.6** | **Bank Mandate Form**  |
| **7.** | **Annexure A.7** | **EMD / Bid Security Form**  |
| **8.** | **Annexure A.8** | **Manufacturer's Authorisation Form** |
| **9.** | **Annexure A.9** | **Undertaking of Authenticity** |
| **10** | **AnnexureA.10** | **Pre-Contract Integrity Pact** |
| **(B) Annexure for Technical Bid:**  |
| **11.** | **Annexure B.1** | **Technical Bid** |
| **12.** | **Annexure B.2** | **Statement of Deviations** |
| **13.** | **Annexure B.3** | **Letter of Competence** |
| **14.** | **Annexure B.4** | **Letter of Conformity**  |
| **(C) Annexure for Commercial Bid:** |
| **15.** | **Annexure C.1** | **Commercial Bid Covering letter**  |
| **16.** | **Annexure C.2**  | **Commercial Bid** |
| **(D) Annexure for Technical Specifications & Others :** |
| **17.** | **Annexure D.1** | **Security Incident & Event Management (SIEM)** |
| **18.** | **Annexure D.2** | **Privilege Identity Management (PIM)**  |
| **19.** | **Annexure D.3** | **Anti-APT (Advanced Persistent Threat)**  |
| **20.** | **Annexure D.4** | **Firewall Analyzer** |
| **21.** | **Annexure D.5** | **Network Access Control (NAC)** |
| **22.** | **Annexure D.6** | **VAPT Advisory & Remediation Services** |
| **23.** | **Annexure D.7** | **Indicative List of hardware / network / security devices** |
| **24.** | **Annexure D.8** | **Non-disclosure Agreement** |
| **25.** | **Annexure D.9** | **Performance Bank Guarantee** |

**Critical Information / महत्वपूर्ण सूचना**

**(RfP No. 400/2018/1279/BYO/RiMV dated NOVEMBER 06, 2017)**

|  |  |  |  |
| --- | --- | --- | --- |
| **SNo.****क्र.सं.** | **Events / कार्यक्रम** | **Date/ तिथि** | **Time/ समय** |
| **1** | **Last date for seeking clarifications for pre-bid meeting/ पूर्व-बोली बैठक के लिए स्पष्टीकरण मांगने की अंतिम तिथि** | **नवम्बर 13, 2017****/ NOVEMBER 13, 2017** | **3:00pm** |
| **2** | **Pre Bid meeting (*no clarifications would be given after pre-bid meeting*)/ पूर्व-बोली बैठक के बाद कोई भी स्पष्टीकरण नहीं दिया जाएगा।** | **नवम्बर 17, 2017****/ NOVEMBER 17, 2017** | **11:00am** |
| **3** | **Last date for submission of bids / बोली जमा करने की अंतिम तिथि** | **दिसम्बर 01, 2017****/ DECEMBER 01, 2017** | **3:00pm** |
| **4** | **Address for Bid Submission/ बोली जमा करने का पता** | **सीआईएसओ एवं उप महाप्रबन्धक (सिस्टम्स) /****CISO & Deputy General Manager (Systems)****Small Industries Development Bank of India****3rd Floor, Information Technology Vertical****MSME Development Centre****Plot No. C-11, G Block, Bandra Kurla Complex****Bandra (E), Mumbai- 400 051****Phone: 022-67531100 / 67531243****Fax: 022-67531236** |
| **5** | **Date & Time of Opening of Minimum Eligibility bid &Technical bid/ बोली की न्यूनतम पात्रता व तकनीकी बोली खोलने की तिथि व समय** | **दिसम्बर 01, 2017****/ DECEMBER 01, 2017** | **4:00pm** |
| **6** | **Date and time of opening of commercial bids / वाणिज्यिक बोली खोलने की तिथि व समय** | **To be intimated at a later date****बाद की तिथि में सूचित किया जायेगा** |
| **7** | **Bid Validity/ बोली के वैधता** | **Six Month from the last date of bid submission.****बोली जमा करने की अंतिम तिथि से छह महीने तक|** |
| **8** | **Contact details of SIDBI officials****सिडबी अधिकारियों के संपर्क विवरण** | **1. राघवा राचूरी/Raghava Rachuri,****सीआईएसओ एवं उप महाप्रबन्धक (सिस्टम्स)****CISO & DGM(Systems)****022-67531243, raghava@sidbi.in****2. टी के लिन्सन / T K Linson****प्रबंधक(सिस्टम्स) / Manager(Systems)****022-67531362, tklinson@sidbi.in** |
| **9** | **स्वतंत्र बाहरी निगरानी Independent External Monitor** | **Shri. Ashok Sinha, (IAS retd.),** **13 Yayati, Sector-58A, Nerul (West),** **Palm Beach Road,****Navi-Mumbai 400706,** **Ph: 9821844044,** **Mail id: asinha51@gmail.com** |

# Introduction and Disclaimers

## Preface

**This Request for Proposal document (‘RFP document’ or RFP) has been prepared solely for the purpose of RfP is to Outsource the Implementation and Management of Cyber Security Operations Center, which includes the Maintenance and Support for a period of three years under THREE (3) Bid System viz. 1) Minimum Eligibility / 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.**

## Evaluation 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 accepts 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.**

## Requests for Proposal

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

**Contact : Raghava Rachuri**

**Position : CISO & Deputy General Manager (Systems)**

**Email : raghava@sidbi.in**

**Telephone : +91 - 22 - 67531243**

**Fax : +91 - 22 - 67531236**

**Contact : T K Linson**

**Position : Manager (Systems)**

**Email : tklinson@sidbi.in**

**Telephone : +91 - 22 - 67531362**

**Fax : +91 - 22 - 67531236**

**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 that Respondent’s response.**

**Respondents should provide details of their contact person, telephone, 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.**
3. **Unless expressly overridden by the specific agreement to be entered into between the Bank and the successful Bidder, the RFP 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 including those received late or incomplete offers without assigning any reason whatsoever. 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.**
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 rejection/cancellation.**
8. **The scope of the proposal shall be on the basis of single point responsibility, completely covering the 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 shall 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, favouring “Small Industries Development Bank of India”, payable at Mumbai 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. Details of the EMD are given in section 7.1.1.**

## 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 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.**
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. 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 services it proposes to offer under the contract.**

## 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 CPP portal.**
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 B.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, and should be received by the point of contact not later than the date mentioned in ‘Critical Information’ of this RfP document. Responses to inquiries and any other corrections and amendment will be made available on bank’s website. 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 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 authorised 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 any work 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 a different Bidder may be selected.**
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.**

## Period of Validity of Bids

1. **Prices and other terms offered by Bidders must be firm for an acceptance period of six (6) months from last date for submission of bids as mentioned in ‘Critical information’ sheet.**
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 ‘Critical Information’, given 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 will 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/email 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 ‘Critical Information’ section above. 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.**
3. **Clarification sought by bidder should be made in writing (Letter/E-mail etc) and submitted on or before the date as indicated in the ‘Critical Information' Section. Bank has discretion to consider any other queries raised by the bidder’s representative during the pre-bid meeting.**
4. ***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 Bank (***[***www.sidbi.in***](http://www.sidbi.in)***) website and Central Public Procurement Portal (CPPP) within 07 working days from the date of the pre-bid meeting*. It would be responsibility of the bidder to check the websites before final submission of bids.**
5. **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.**

## 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 ‘Critical information’ sheet.**
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

**The Bank's existing outsourced partners of Data Center management and Facility Management services are NOT Eligible to participate in this bidding.**

 **Successful Bidder will be selected through three bids evaluation process:**

 **[A].Minimum Eligibility / Pre Qualification Criteria**

 **[B]. Technical Bid**

 **[C]. 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 Contents** | **No. of Copies** | **Label of Envelope** |
| **I** | **Minimum Eligibility / Pre Qualification Criteria**1. **Minimum Eligibility Bid – Covering letter as per format prescribed in Annexure A.1**
2. **Minimum Eligibility / Pre - Qualification Bid as per format prescribed in Annexure A.2**
3. **General Information about the Bidder as per format prescribed in Annexure-A.3**
4. **Power of Attorney as per format prescribed in Annexure-A.4**
5. **Declaration regarding Clean Track Record as per format prescribed in Annexure-A.5**
6. **Bank Mandate Form as per format prescribed in Annexure-A.6**
7. **EMD/Bid Security Form as per format prescribed in Annexure-A.7**
8. **Manufacturer's Authorisation Form as per prescribed format in Annexure-A.8**
9. **Certificate of Authenticity as per prescribed format in Annexure-A.9**
10. **Pre-Contract Integrity Pact as per format in Annexure A.10**
11. **Masked Commercial bid as per format prescribed in Annexure C.2**
 | **Hardcopy – 2****A CD containing Editable Softcopy - 1** | **Envelope I****“Minimum Eligibility / Pre Qualification Criteria”****Implementation and Management of Cyber Security Operations Center (CSOC)****RfP No. Tender 400/2018/1279/BYO/RiMV dated November 06, 2017** |
| **II** | **TECHNICAL BID**1. **Technical Bid as per format prescribed in Annexure B.1**
2. **Statement of deviations as per format prescribed in Annexure B.2**
3. **Letter of Competence as per format prescribed in Annexure B.3**
4. **Letter of Conformity as per format prescribed in Annexure B.4**
 | **Hardcopy – 2****A CD containing Editable Softcopy - 1** | **Envelope II-A****“Technical Bid”****Implementation and Management of Cyber Security Operations Center (CSOC)****RfP No. Tender 400/2018/1279/BYO/RiMV dated November 06, 2017** |
| **Technical Specifications & Others**1. **Security Incident & Event Management (SIEM) as per format prescribed in Annexure D.1**
2. **Privilege Identity Management (PIM) as per format prescribed in Annexure D.2**
3. **Anti APT (Advanced Persistent Threat) as per format prescribed in Annexure D.3**
4. **Firewall Analyzer as per format prescribed in Annexure D.4**
5. **Network Access Control (NAC) as per format prescribed in Annexure D.5**
6. **VAPT Advisory & Remediation Services as per format prescribed in Annexure D.6**
7. **Indicative List of hardware / network / security devices as per format prescribed in Annexure D.7**
8. **Non-disclosure Agreement as per format prescribed in Annexure D.8**
 | **Hardcopy – 1****A CD containing Editable Softcopy – 1** | **Envelope II-B****“Technical Specifications & Others”****Implementation and Management of Cyber Security Operations Center (CSOC)****RfP No. Tender 400/2018/1279/BYO/RiMV dated November 06, 2017** |
| **III** | **COMMERCIAL BID**1. **Commercial bid covering letter as per format prescribed in Annexure C.1**
2. **Commercial bid as per format prescribed in Annexure C.2**
 | **Only Hardcopy – 1** | **Envelope III****“Commercial Bid”****Implementation and Management of Cyber Security Operations Center (CSOC)****RfP No. Tender 400/2018/1279/BYO/RiMV dated November 06, 2017** |

1. **Above mentioned three separately sealed sub-envelopes should be put together in another master sealed envelope super-scribing “Implementation and Management of Cyber Security Operations Center (CSOC) RfP No. Tender 400/2018/1279/BYO/RiMV dated November 06, 2017”.**
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 I, II-A, II-B should also contain softcopy in the form of DVD of respective response documents.**
		4. **Masked commercial bids must be given with Minimum Eligibility / 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 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 A.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.**

## 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**](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.**
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.**

**\*\*\*\*\*\*\***

# Background About SIDBI

## 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.**

## Cyber Security

 **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 throughout 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 the 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.**

## 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-APT, PIM, etc 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 Data Center/DR Site/Web servers from third party Data Centers in future and the bidder should continue provide security services for co-located Datacenter 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.**

 **The selected Bidder will be responsible for implementing CSOC at central location identified by Bank at Mumbai. 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.**

**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 vendor will be playing the role of Managed Security Services Provider (MSSP) of the bank as well as System Integrator(SI) for all the security solutions/tools as detailed in Section 5.**

## Current IT Setup

### Data Centre and DR Site

**SIDBI has its Primary Data center at 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.**

**The required information with respect to the servers and network devices at Data Center and DR Site will be provided to the bidders at the time of pre-bid meeting, if required. If any 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 authorisation letter.**

### Present IT Infrastructure

| **SrNo** | **Indicative list of servers and storage solutions** | **Make** | **Quantity** |
| --- | --- | --- | --- |
| **A.** | **Data Center** |
| **1** | **Rack servers (Intel based)** | **Dell / HPE / IBM / SUN** | **21** |
| **2** | **Blade servers (installed in a Chassis)** | **Dell / HPE** | **20** |
| **3** | **Hp-Ux Unix server** | **HPE** | **3** |
| **4** | **VC** | **Polycom / Radvision** | **7** |
| **5** | **SAN** | **Dell / HPE** | **2** |
| **6** | **SAN Switches** | **HPE** | **2** |
| **7** | **SAN Controller** | **HPE** | **1** |
| **8** | **Tape Library** | **SUN** | **1** |
| **9** | **Citrix Netscaler appliance** | **Citrix** | **1** |
| **B.** | **DR Site** |
| **1** | **Rack Servers(Intel based)** | **HPE/Huawei/Dell** | **16** |
| **2** | **Hp-Ux Unix server** | **HPE** | **1** |
| **3** | **SAN** | **HPE** | **1** |
| **4** | **SAN Switches** | **HPE** | **4** |
| **5** | **Citrix Netscaler appliance** | **Citrix** | **1** |

**The Indicative List of hardware / network / security devices to be integrated with the security solutions offered under CSOC is furnished in Annexure D.7.**

### Details of Present Network and Security Infrastructure at DC and DR

1. **Network Connectivity**
2. ***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 last mile is 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 8Mbps 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 HPOV, NNM.**
1. ***LAN***

**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 of requisite bandwidth taken from two service providers. The links are terminated on L3 switches at DC and DR.**

1. **The indicative list of hardware used at DC and DR is given in the Annexure D.7**
2. **External Networks**
* **SIDBI also has connectivity with third party networks like INFINET, Reuters, 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 Mumbai and single service provider at Chennai.**
* **At Mumbai 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.**
* **Bank is in the process of upgrading Internet connectivity at DR Site by addition of load balancer and multiple links**
1. **Mail**
* **SIDBI is currently using Lotus Domino for mailing. Outbound mails are sent from Domino 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**
2. **DataCenter and DR Site**
* **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 and end computing devices.**
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 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 authorisation 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.**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

# Purpose

 **In order to streamline comprehensive information security monitoring and compliance, the Bank proposes to implement and maintain Cyber Security Operations Center (CSOC) for its Information Technology setup, comprising critical infrastructure at DC, DR and other IT locations including third party Data centre hosting site which may come up in the future. The Bank has plans to co-locate the Data Center/DR Site/Web servers from third party Data Centers in future and the bidder should continue provide security services for co-located Datacenter setup in future. The Bank intends to issue this bid document to the bidders to participate in the competitive bidding for procurement, implementation and maintenance of Security Operation Centre, managing SIEM Solution and other security solutions/services as detailed below**

 **Bank has its Primary Data Center at Mumbai (currently at own premises) with DR site at Chennai (currently at own premises). Bank has implemented various applications at DC and DR in a centralized environment.**

## CSOC Coverage:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Sr No** | **Coverage** | **Correlation Engine** | **Log Storage Server** | **Log Collection Device** | **SIEM Management Console** |
| **1** | **DC, Mumbai** | **Yes**  | **Yes** | **Yes**  | **Yes** |
| **2** | **DR, Chennai** | **NA** | **NA** | **Cold standby (R1)** | **NA  (R2)** |

**R1- In case of switchover from primary to DR site in case of failure of Primary Data centre(PDC) at Mumbai, the log collection of the IT devices to be managed at DR site. However, CSOC operations will be resumes once primary site is up and made operational. Log collection device should have capacity to store minimum 3 days of logs locally at Chennai DR site. Relevant cold standby devices to be provided in DC. In case of switching over of business operations from PDC (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 DRSite or the provision should be there to override the controls of these two security tools so that operations are not affected. The server and other infrastructure, if any, required at DR site are to be provided by the vendor.**

**R2- During DR testing, SIEM management console has to be managed from Mumbai Data Centre (Primary) only by CSOC team. The log and security data from DR site are to be routed to CSOC centre at the primary site only and CSOC operations to be continued uninterrupted.**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

# Scope of Work

## Introduction

**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.**

**A. Scope of CSOC**

 **The Scope of work & specifications of CSOC based on which the SIEM (Security Information Event Management) and its complementing security technologies is to be implemented as follows.**

1. **Design, validate, implement & periodically review CSOC architecture (along with all the required solution as per scope of work).**
2. **Bidder is required to supply, install, configure, integrate, maintain and manage all Security tools/ solutions from onsite over the tenure of the contract.**
3. **Overall scope to ensure full coverage of monitoring & management aspects of various security solutions, devices, software, like Firewalls, Network Intrusion Prevention Systems, Host Intrusion Prevention Systems/SIEM/PIM and Networking devices and devices at the Data Center / DR Site identified by Bank.**
4. **Identify information security threats / vectors targeting Bank‘s environment and prevent impact or breach by implementing adequate security mechanisms.**
5. **Ensure that all aspects of Installation, de-installation, integration, Configuration, Re-configuration, relocation (within the identified locations by Bank), enhancements, updates, upgrades, bug fixes, problem analysis, performance analysis, backups, audits, on-site as well as off-site support for the proposed hardware/software required for delivering the Managed Security Support services.**
6. **Conduct the Risk Assessment activity for the devices under the scope of CSOC as per the Risk Management process of the Bank.**
7. **Monitor/Manage all types of make and models of the product range such as Bluecoat, Cisco, Checkpoint, Fortinet, IBM and any other standard Make launched/ introduced or required by Bank from time to time.**
8. **Reporting and logging of information security incidents through the use of appropriate ticketing tools. Track and monitor the closure of these information security incidents and Escalation of these incidents to appropriate teams/ individuals in the Bank.**
9. **CSOC should deliver and implement the services to Bank in compliance with RBI Working Group Report, Cyber Security Framework of RBI, ISO 27001 & other standards wherever applicable.**
10. **Ensure that the SIEM (Security Information and Event Management) manager & other solutions used in the CSOC are up to date in terms of product releases, version upgrades, patches and other service packs.**
11. **The service delivery (SLA Management) and periodic reporting should be done through Dashboard.**
12. **Bidder should perform Vulnerability Management for various IT assets such as critical devices/ servers / applications as per the requirement of Bank.**
13. **Provide forensic Support in case on any incident**
14. **Continual improvement of CSOC operations.**

**B. For the purpose of implementation, following should be noted:**

1. **The solution, racks, hardware, software storage, services, displaying units (LED TVs 48inch – 2Nos) and 4 desktops (Intel Core i5, 7th Gen with 16GB RAM, dedicated 2GB graphics and 1TB HDD) would be provided by the bidder. The Bank will provide facilities to host the devices and seating arrangement for the personnel. The above requirements are indicative and in case, if any other requirement from the Bank's side is to be provided, it has to be clearly specified by the bidder and the same to be agreed upon by the Bank.**
2. **Bidder should supply Products as specified, and Services which includes development, integration, management, maintenance, audit compliance, training and knowledge transfer in respect of CSOC as detailed in the subsequent sections.**
3. **Bidder should also provide complete services of CSOC Operations with top of the line capabilities in terms of CSOC Product, Solution, Process, Services, Resources, Support and management capabilities.**
4. **CSOC implementation plan recommended by Bidder should consider optimum utilization of tools, technologies, and services which are being procured as a part of this RFP.**
5. **A comprehensive strategy and Standard Operating Procedure (SOP) should be provided by the Bidder on implementing the end to end CSOC solution.**
6. **Bidder has to develop the project plan, get it approved from the Bank and then implement the project based on timelines given in the RFP.**
7. **Compliance of various audits like ISO 27001:2013, ISO 22301 etc., should be closed by the Bidder in the proposed solution.**
8. **Preparation of all documents related to deployment architecture, operation, maintenance including the Standard Operating Procedures (SOP) for all the underlying processes, roles and responsibilities of the personnel. Provide the complete set of Operation and System Manuals in 3 sets of Hardcopies as well as in Softcopies of all the systems/components provided as part of the CSOC implementations.**
9. **A comprehensive onsite warranty for a period of 1 year shall be there on all the Hardware and Software supplied to/purchased by the Bank. Warranty will commence from the acceptance/sign off date from Bank for SIEM/ each tool. The warranty also includes all software subscriptions (critical hot fixes, service packs, and major upgrades). The vendor has to take AMC/ATS after expiry of warranty for a period of 2 Years with back-to-back arrangement with Original Equipment Manufacturer (OEM). .**
10. **The bidder would be responsible for updates, patches, bug fixes, version upgrades for the entire infrastructure without any additional cost to the Bank during the contract period.**
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 entire contact period of 3 Years. Replacement to be done before due date of the product/service and the intimation to be given to Bank at least one month before in case of any of the above scenario.**
12. **The Bidder, in coordination with OEM do a gap analysis and submit a detailed study of the Bank‘s infrastructure and requirements relating to the CSOC solution, prepare a detailed plan document/ road map mentioning all the pre-requisites, time-frame of mile-stones/ achievements leading to the full operationalization of the solution vis-à-vis Bank‘s requirement. This exercise should not affect the normal day to day functionality of the Bank.**
13. **Selected Vendor would be responsible for all technical support to maintain the required uptime. Initial installation, configuration and integration should be done by the OEM only, through the Bidder. The Bidder would be the single point of contact. The Bidder should have necessary back-to-back agreement with the OEM for all the required onsite support for entire contract period.**
14. **RFP For Implementation and Management of Cyber Security Operation Center (CSOC) support with OEM during the total contract period for necessary support. Bidder would submit a letter by OEM issued to bidder in this regard.**
15. **If the Bidder / SI 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 / SI without any extra cost to Bank or the Bidder / SI will be held accountable for OEM‘s inaction and penalty charges would be levied as per the SLA terms to Bidder / SI.**
16. **Solution being provided should be scalable and user configurable to cater to the future requirement of the Bank.**
17. **Bidder will manage CSOC operations in consultation with the Bank‘s team. Bidder will deploy on-site resources on 12\*5 basis at Bank‘s premises to support CSOC operations. However offsite/ remote monitoring of SIEM tool, Incidents to be carried out 24\*7\*365.**
18. **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, 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.**
19. **Bidder shall provide list and details of licenses to be procured and also maintain the inventory database of all the licenses and the updates installed. All licenses should be in the name of SIDBI.**
20. **The period of product support coverage would be for 3 years from the date of sign off of all security solutions and services covered under this RFP and extendable to another maximum 2 years at same terms and conditions.**
21. **All phase installation/ configuration till sign-off would be done by the Bidder‘s engineers. However, for Designing and deployment validation, sign-off may be done by both OEM and Bidder‘s engineers. It will be the Bidder‘s responsibility to liaison with the OEM to provide full technical support to the satisfaction of the Bank for the complete tenure of agreement.**
22. **The bidder has to provide the documentation for the project including but not limited to references regarding scope, functional and operational requirements, resource requirements, project design/plan, product description, guidance for best practices, implementation guidelines, user acceptance test plan, operation manual, security implementation, training materials, evaluation scoreboards and matrices etc.**
23. **The bidder is expected to size the Hardware/appliance/storage as per the requirements mentioned in this RFP. The bidder‘s response should include the calculations/ logic used to arrive at the sizing. In case any further clarification related to sizing of hardware is required, Bidder can visit bank to meet authorized officials and sought clarification.**
24. **Bidder should provide utilization details that may affect the day to day normal functionality of existing IT infrastructure.**
25. **Adherence to agreed Service Level Agreements (SLA) and periodic monitoring and reporting of the same to the bank through a portal, which should be accessible to the Bank officials over Desktop and Laptop irrespective of platforms used.**
26. **Bidder should provide the detailed architecture of the solution being offered. The architecture to be deployed has to be approved by the Bank.**
27. **In case the systems are not able to send the logs to the collector device, system should be able to extract the logs stored in the temporary memory of the devices at that site.**
28. **If connectivity between log collection agents and logger is down then the Log collector agents should store the logs of at least 3 days and send them once connectivity is established.**
29. **Bidder will be responsible to store logs in industry standard solution and format.**
30. **SI needs to ensure that CSOC solution can integrate with the IT System using standard methods/ protocols/ message formats without affecting the existing functionality of Bank.**
31. **The configured correlation alerts and dashboards should be displayed on LED display maintained at the CSOC.**
32. **The bidder should arrange for required number of laptops/desktops with the required specifications for the onsite CSOC support team (minimum 4 nos).**
33. **Bidder should also quote for Backup solution including hardware software & licenses for taking Backup.**
34. **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.**
35. **C-SOC Vendor shall propose solution that should be capable of retrieving the archived logs for analysis, correlation, reporting and forensic purposes.**
36. **C-SOC Vendor shall propose solution that has the incident management / ticketing system workflow and solution shall support creating incident automatically based on the rules defined and tracking them.**
37. **C-SOC Vendor shall provide different dashboard and screens for different roles, provide online secured portal (web-based dashboard) for viewing real-time incidents / events, alerts, status of actions taken etc.**
	1. **Top Management (Company View).**
	2. **Department Heads (View to the data associated with their function group / business line).**
	3. **CISO (complete and detailed dashboard of Security posture of the organization set-up being monitored through this C-SOC).**
	4. **Network / Security Administrator / Auditor (for devices / equipment for which he/she is administrator).**
38. **CSOC Vendor shall provide required Hardware (Compute / Storage) for SIEM solution and other security tools implementation as per sizing and architecture required for this project.**
39. **C-SOC Vendor must ensure that once the logs are written to the disk/ database no one including SIEM or database / system administrator should be able to modify or delete the stored raw logs.**
40. **C-SOC Vendor must ensure that for each security incidents, solution should provide online and real time remediation guidance.**
41. **C-SOC Vendor must provide threat intelligence feed for identifying new global threats around the globe like DDoS, Malicious IP Addresses, Known C&C (Command and Control) hosts etc.**
42. **Proactively inform about potential security threats/vulnerabilities, new global security threats/ zero day attacks in circulation and suggest and implement suitable countermeasures to safeguard Bank‘s IT assets and customer data against such evolving threats / attacks along with the analysis.**
43. **Ensure SIEM Tool and other security systems are running 24x7x365 for monitoring of the devices / servers under scope and support for troubleshooting.**
44. **Service availability monitoring of devices / servers configured and submit a report in case of service non availability of the devices along with the status.**
45. **Provide assistance during cyber security drills / audits as and when conducted.**
46. **Alerting events / incidents and recommending remedial actions.**
47. **Daily report of critical and major events / incidents, correlation, analysis, recommendations and protection.**
48. **Monthly report summarizing the list of events / incidents reported correlation analysis, recommendations, status of actions and other security advisories. It should include the trend analysis comparing the present reporting cycle data with the previous reporting cycle data (Monthly and annually as what may be applicable).**
49. **CSOC Vendor should operationalize the C-SOC services for configured devices within 6 weeks from the date of delivery of hardware or installation of required hardware at respective site i.e. DC and DR.**
50. **CSOC Vendor should develop a Standard Operating Procedure (SOP) for alert management, incident management, forensics, report management, log storage and archiving, Business Continuity. SOP should also cover log monitoring tool management including configuration, agent deployments, backup and recovery.**
51. **C-SOC Vendor should provide knowledge transfer and training on the technology, functionality and operations of the CSOC.**

**C. Incidents and Problem Management**

**Under these services the bidder must provide the below mentioned activities as per SLA‘s asked for in this tender:**

1. **The bidder has to provide an incident management and integrate with ticketing tool to generate automated tickets for the alert events generated by the SIEM and other proposed tool.**
2. **The bidder will also provide a detailed process for managing incidents - describing each phases of the process – prepare, identify, contain, eradicate, recover and learn from the incidents responded to.**
3. **Develop response plan/ strategy which will describe the prioritization of incidents based on the organizational impact**
4. **Bidder should also develop/document Crisis Management Plan based upon various threat scenarios. Crisis management Plan should be tested on half yearly along with various stakeholders in Bank/Other relevant service providers. Crisis management plan should also be reviewed periodically or as and when required.**
5. **The incident management solution should be able to register any security event and generate tickets. 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.**
6. **The tool should facilitate time/ event based automated escalation of tickets as per the escalation matrix defined by the Bank.**
7. **Establishing process for identifying, preventing, detecting, analyzing & reporting all Information Security incidents as per the internal policies of the bank, this may revise time to time.**
8. **Investigating Information Security (IS) incidents through various modes like forensic evidence collection & preservation, log analysis etc.**
9. **Incident and problem Management, resolution, root cause analysis, and reporting within time limit as per the requirement of Bank.**
10. **Events handling of the events reported by security Solutions and devices such as log monitoring tool, Network Intrusion Prevention/Detection Systems, SIEM/PIM etc.**
11. **Troubleshooting the problem / issue reported in the context of security solutions & devices and coordinate with the respective vendor / supplier till the closure of the call. Trouble shooting should be performed within accepted time limit.**
12. **Virus alerts through e-Mail for the viruses, worm‘s activity observed at the security solutions and devices under the bidder scope. Subsequent activities of remediation & closure are the responsibility of Antivirus service provider. Bidder will track the status of the Trouble Ticket opened in this context.**

**D. Ticketing Tool**

**In order to facilitate effective reporting and logging of information security events/incidents, Bidder needs to provide ticketing tool as part of this RFP. Tool will be used to track and monitor the closure of various information security events/incidents and Escalation of these incidents to appropriate teams/ individuals in the Bank if required. Apart from CSOC team, the ticketing 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. Access also needs to be provided to Bank‘s CISO and other identified individuals for monitoring purpose. The tool should be web based online portal available over desktop. The tool should also be able to automatically send e-mails (with integration with Bank‘s mail / messaging solution) to users for escalations. Bidder needs to provide ticketing tool for at-least 50 users. Same should be reflected in Bill of Material. In case any hardware or additional support required for ticketing tool, the same will be provided by bidder as part of this RFP. Bank may also avail the ticketing tool for additional users on pro-rata basis as per price quoted in the Bill of Material during the contract period, if required**

**E. Storage:**

1. **The SIEM should be able to maintain minimum 3 months of logs online (in the appliance). In addition, the bidder should provide for near line storage i.e. secondary storage for archiving logs up to minimum 9 months in SAN and offline storage for storage of logs for minimum 6 years. Minimum Total 7 years log must be available. The bidder is responsible for sizing the storage adequately based on the sustained EPS of 5,000 and peak usage, scalable upto 10,000 EPS.**
2. **Storage for 7 years to be done on tape library, the minimum of LTO 6 to be provided with a facility to restore the logs for further review at any given point of time.**
3. **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 it after office hours.**
4. **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.**
5. **The expected storage requirements are of minimum 7 Years. The bidder is expected to size the storage as per the requirements mentioned in the section 3.4 (Current IT setup) and Annexure D.7. in this RFP. The bidder‘s response should include the calculations/ logic used to arrive at the sizing.**
6. **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 based on RAID 5 and have minimum 10000 Disk RPM.**
7. **For Tier-III Archival Storage of minimum 6 years, the SI could use Magnetic Tapes, which will be stored at the Bank‘s DC and DR premises respectively.**
8. **These magnetic tapes will be restored every three months by the System Integrator and signed by Bank officials.**
9. **The SI will have to make the logs available within 24 hours of a request made by Bank. This request for retrieval of logs would be considered as a Medium Priority incident. If the SI fails to provide the required logs within 24 hours, then penalties applicable for Medium Priority incidents would be levied.**
10. **All storage devices should include a minimum dual controller and should be of the following minimum specifications with respect to host connectivity:**

|  |  |  |
| --- | --- | --- |
| **Host connectivity** | **1GBE iSCSI****10GB iSCSI****8GB FC**  | **2 Ports/ Controller** **2 Ports/ Controller** **4 Ports/ Controller**  |
| **Archival storage Connectivity** | **Protocols to be supported: CIFS, NFS & HTTP.** |  |

 **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 switches (NAS/SAN), controllers etc. and these are to be provided at the time implementation supporting the maximum scalability as defined above.**

**F. Functional Principles:**

 **The Intent for implementing a CSOC at the Bank is covered in the below functional principles:**

1. **Detection of Information Security Threat & Prevention of Impact / Breach: The CSOC should be able to identify information security threats / vectors targeting bank’s environment and prevent impact or breach due to, these factors, through implementation of adequate security mechanisms.**
2. **Incident Management and Ticketing Tool: Reporting and logging of information security incidents through the use of appropriate ticketing tools. Track and monitor the closure of these information security incidents and Escalation of these incidents to appropriate teams/ individuals in the bank if required.**
3. **Continuous Improvement: Continuously improve CSOC operations.**
4. **Bidder has to provide all Technical Support till the end of contract period from the date of acceptance of the solution by the Bank. Technical support should be provided online/offsite on 24x7x365 basis. However, if the problem is not resolved through online/offsite, onsite support should be provided.**

**G. CSOC Operations and Responsibilities of the MSSP are as given below:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Item No** | **Item description** | **Service****Window****(Hours)** | **Responsibilities** | **Operating****Location** |
| **1** | **Technical****Coordinator****Service (R1)** | **12x5** | **Act as single point****contact, coordination,****SLA compliance, Reviews** | **Onsite /****Offsite** |
| **2** | **SIEM Management and Monitoring onsite** | **12x5** | **Security log and event****Monitoring , Call logging** **incident management and resolution** | **Onsite** |
| **3** | **SIEM Management and Monitoring****Service** | **24x7** | **Security log and event****Monitoring , Call logging** **incident management and resolution (This service is for holidays and after office hours which is not covered at Item No 2)** | **Offsite (R2)** |
| **4** | **Device Management** | **12X5** | **To update patches and configurations of CSOC hardware and software** | **Onsite** |
| **5** | **Analyst Service** | **24x7** | **Analyzing and Advising for incident management and resolution** | **Offsite (R2)** |
| **6** | **Help Desk** |  **24X7** |  **Call logging , monitoring** **and management** | **Onsite****/ Offsite (R2)** |

**R1- : May be extended to 6 days or 24 x 7 in future if and when required. Additional resources required for such support would be provided by the vendor on chargeable basis.Cost for such additional Resources, if requested, for L1 and L2 would be based on the cost as quoted in the commercial bid Annexure C.2 for such resources.**

**R2- : All offsite remote support from vendor location for the bank should be accessed through secure dedicated line or VPN connectivity. The support engineer should be able to provide support through remote desktop sharing/ viewing and for guiding the onsite support engineer for trouble shooting/expert advice/remediation services.**

**H. Resource Matrix**

|  |  |  |  |
| --- | --- | --- | --- |
| **Sr No** | **Resource Type** | **No of Resource required** | **Qualifications and Experience** |
| **1** | **L1 - Onsite Resource** | **2** | **BE/BTech/MCA with minimum 2 year Networking / Security experience or BCA / BSc with 4 year Networking / Security experience** |
| **2** | **L2 - Onsite Resource** | **1** | **BE/BTech/MCA with minimum 4 year experience out of which one year should be in SOC/CSOC or BCA / BSc with 6 year Networking / Security experience** |
| **3** | **Offsite 24x7 Monitoring Resources – L3 as and when required** | **-** |  **L3 should be senior level SOC expert.** |

## Security solutions / services to be integrated with SIEM

 **Cyber Security Operations Centre for security solutions/services to be implemented and integrated with SIEM are as given below:**

|  |  |  |
| --- | --- | --- |
| **Sr No** | **Scope of CSOC** | **Remarks** |
| **1** | **Security Incident & Event Management (SIEM)** | **Onsite** |
| **2** | **Privilege Identity Management (PIM)**  | **Onsite** |
| **3** | **Anti APT (Advanced Persistent Threat)**  | **Onsite** |
| **4** | **Firewall Analyser** | **Onsite** |
| **5** | **Network Access Control (NAC)** | **Onsite** |
| **6** | **VAPT Advisory & Remediation Services** | **Once in a quarter** |
| **7** | **Security / Threat Intelligence Services** | **Service on continuous basis** |

1. **Security Incident & Event Management (SIEM)**

 **(Pl. refer Annexure D.1)**

**Bidder shall offer a complete solution that shall include any hardware and software, all licenses, upgrades, updates, subscriptions required for meeting the requirement for correlating and analysis of events.**

**The bidder should offer the SIEM device with all requisite modules for collection of logs, monitoring and displaying of events on individual device or on correlation basis, to facilitate administrators to take proactive actions for prevention of security threats that might occur on network access devices.**

**The offered solution shall include toolkits/modules/utilities for integrating all required devices supported by the SIEM equipment without any additional cost implication to SIDBI.**

**The offered solution shall provide storage and correlation of logs from various devices in SIDBI network.**

**SIDBI intends to implement SIEM with a centralized dashboard to monitor various IT Security threats originating across the organization. The solution should provide a single dashboard with correlation of threats originating in the form of events across various network, security and system devices in the organization.**

1. **Deploy the SIEM for the in-scope infrastructure and security tools**
2. **Integration of log sources from various devices / servers / network devices/ security devices / applications with SIEM as part of implementation**
3. **SI should discuss, develop 10 use cases with Bank & Implement in project phase**
4. **SI should carry out fine tuning of use cases based on evolving requirement in ongoing operations phase**
5. **SI should develop parsers for 5 critical devices for logs in project phase**
6. **SI should develop parsers for non-standard logs in ongoing operations phase, SI team deputed onsite will be expected to develop parsers for non-standard logs required during ongoing operations phase**
7. **SI should generate 10 different reports and create a customized dashboard to provide an overview of security landscape of organization**
8. **SI should integrate the proposed SIEM with ticketing tool for automated ticket generation**
9. **Patch SIEM system as and when required in case new updates available.**

**The solution shall provide following functionality:**

* + - 1. **Log Collection**
			2. **Log Storage**
			3. **Event Co-relation**
			4. **Alerting**
1. **SIEM tool and related components**
2. **Initial EPS requirement is for 5000. However, the appliance should be scalable upto 10000 EPS with all components at the DC.**
3. **The SIEM should be able to maintain minimum 3 months of logs on-box. In addition, the bidder should provide for near line storage i.e. secondary SAN storage for archiving logs up to minimum 9 months and offline storage for storage of logs for minimum 6 years. Minimum Total 7 years log must be available. The storage requirement should be sized accordingly by the vendor.**
4. **Offsite storage facility is also required for additional 6 years in Tape Library with minimum of LTO 6.**
5. **The bidder has to provide monitoring of SIEM solution to be managed in 2 shifts, 5 days a week (except Saturday and Sunday) on site. The first shift person to review the previous night /Saturday/Sunday logs next morning thus covering 24 hours logs monitoring and review. Shifts timings to be decided mutually as per requirement/convenience. The tentative timings are in two shifts from 9 am to 5 pm and 12 pm to 8pm for the L1 resource. For the L2 resource, timings are from 10am to 6pm. The Bank at its discretion may opt for 3 shifts ( i.e. 24x 7) and on Saturday and Sunday also on site, if required in future. In that case, the bidder has to provide monitoring of SIEM solution to be managed in 3 shifts, 7 days a week.**
6. **However, the bidder has to provide monitoring & Security Analysis of the infrastructure through SIEM solution off-site on 24x7 basis.**
7. **Patch the SIEM systems as and when required in case new updates available.**
8. **Monitor all security incidents using SIEM solution deployed at DC and DR and integrated with various infrastructure devices and security solutions of bank. The solution should integrate with Network / Security / Servers / Applications / Database of Bank.**
9. **Log collection**

**Logs from all the in-scope devices located at the geographically dispersed location should be collected. 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, 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 aggregation and normalization**

**Logs collected from all the devices should be aggregated as per the user configured parameters. Logs from multiple disparate sources should be normalized in a common format for event analysis and correlation.**

1. **Log archival**

**Logs collected from all the devices should be stored in a non-tamperable format on the archival device in the compressed form. Collection of Logs and storage should comply with the Regulatory requirement and should maintain a chain of custody to provide the same in the court of law, in case the need arises. For correlation and report generation purpose, past 3 months log data should be available on-box. In addition, the bidder should provide for near line storage i.e. secondary SAN storage for archiving logs up to minimum 9 months. Logs prior to 12 month’s period should be stored on removable media. Solution being provided should be scalable and user configurable to cater to the future requirement of the Bank.**

**Retrieval of archived logs should not require any proprietary tools/protocol and should be retrievable using open standards/protocols or else the retrieval tool should be provided to the Bank at no extra cost.**

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 vendor/System Integrator 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 the same through message formats like SMTP, SMS, Syslog, 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 vendor 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, Database Activity Monitoring tool, Vulnerability Management tool etc. Incident management should include escalation as per the escalation matrix.**
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 customisable as per configuration item.**
10. **Integration with in-scope monitored devices**

**The vendor is responsible for integrating SIEM solution with the hardware items & security solutions. As the system integrator the vendor will also be responsible for integrating all in scope security solutions/devices with the SIEM solution for log monitoring, correlation and Bidder will be required to integrate all the devices supplied as part of this RFP.**

1. **Development of connectors for customized applications / devices**

**While it is expected that connectors for all the standard applications and devices will be readily available in the collector and Log management devices, connector not available for devices will need to be developed. It is the responsibility of the vendor to develop connector applications for such devices.**

1. **Proof of concept testing of SIEM and incident management tools.**

**Bank may at its discretion ask the Bidders to demonstrate Proof of Concept (POC) for the proposed solution to the Bank. Bank would like the selected Bidder to perform a proof of concept testing in the Bank’s environment with DC/DR cutover and meeting the Recovery Point (RPO) and Recovery time objective (RTO) of the proposed solution and demonstrate the SIEM solution capability for the following Use cases.**

1. **Use Cases for Firewall and IPS**
2. **Use Cases for Intranet Applications at server level**
3. **Use Cases for Email**
4. **Use Cases for RTGS / NEFT Transactions**

**The solution shall support the various Use Cases in order to provide log collection, event correlation, Alert Generation and escalation. Bank will have the right to reject the solution, if not satisfied with the proof of concept testing.**

**The detailed Technical Specifications are furnished in Annexure D.1.**

## Privilege Identity Management

**(Pl. refer Annexure D.2)**

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

* **SI should deploy PIM solution for the identified devices/servers etc.**
* **SI should deploy PIM solution for the identified administrators**
* **SI should integrate PIM solution with proposed SIEM solution**

**A privileged identity management technology needs to accommodate for the special needs of privileged accounts, including their provisioning and life cycle management,**[**authentication**](https://en.wikipedia.org/wiki/Authentication)**,**[**authorization**](https://en.wikipedia.org/wiki/Authorization)**,**[**password management**](https://en.wikipedia.org/wiki/Password_management)**, auditing, and access controls.**

**The detailed Technical Specifications are furnished in Annexure D.2.**

## Anti APT (Advanced Persistent Threat)

**(Pl. refer Annexure D.3)**

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

1. **SI should install and configure Anti-APT solution to protect against web and email attacks.**
2. **SI should suggest required changes to be done to integrate Anti-APT solution to integrate with existing infrastructure**
3. **SI 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-**
5. **24X7 malware scanning of critical websites**
6. **Coordinate rapid response**
7. **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 D.3.**

## Firewall Analyser

**(Pl. refer Annexure D.4)**

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

* **SI should analyze firewall configuration/policies based on best practices**
* **SI should provide detailed reports of the analysis**
* **SI should provide recommendation to optimize firewall configuration/ policies**
* **SI should execute this service on quarterly 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 D.4.**

## Network Access Control (NAC)

**(Pl. refer Annexure D.5)**

1. **The Bank intends to procure a Network Access Control solution which is an automated security control platform that can monitor and control everything 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.**
2. **SI should install and configure NAC solution such as only authorized and compliant devices to access and operate on Bank’s network.**
3. **SI should design NAC solution such that bank does not need to re-architecture of the network.**
4. **SI should consider both wired and wireless users for NAC implementation.**
5. **SI should perform any OS upgrade on the network switches if required.**
6. **SI should integrate NAC solution with proposed SIEM solution.**
7. **NAC shall provide following:**
8. **Visibility into user identities and device types**
9. **Guest user self-enrollment**
10. **Easy access to wired networks and WPA2 secure wireless (when implemented)**
11. **Real-time policy assessment**
12. **Dynamic role-based enforcement**
13. **Guided Self-Remediation Process**
14. **NAC solution deployed shall allow only authorized and compliant devices to access and operate on Bank’s network. The bidder shall design the NAC solution such that the Bank does not need re-architecture of the network or upgrade/ replacement of the network devices.**
15. **The Bidder is required to design & size the NAC solution. Currently Bank has approximately 1500 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 5 years. The bidders proposed solution shall be sized to meet the 5 year requirement.**
16. **The Bank has offices at around 90 locations in addition to the DC and DR. Each of these locations has one Cisco router & one / more manageable switches. The switches are of heterogeneous make with majority of them being HP/Aruba. Further, during the period of contract Bank may change to newer technology like SD-WAN, in which case the routers may not be present and equipment from other vendors would be installed. The Bidder’s proposed solution shall meet the Bank's requirement as described and should support heterogeneous environments till the end of contract period.**
17. **Regarding NAC integration, the vendor 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 Vendor.**

**The detailed Technical Specifications are furnished in Annexure D.5.**

## VAPT Advisory & Remediation Services

**(Pl. refer Annexure D.6)**

**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. **SI should provide vulnerability assessment services for mentioned devices/servers.**
2. **SI should perform penetration testing for servers hosted over Internet**
3. **SI should provide detailed reports of the assessment**
4. **SI 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 Vendor is to bring his own VAPT tools for testing purpose and obtain required approval for conducting the same. The vendor 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 D.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 defence 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.**

## Project Schedule and Implementation

|  |  |  |  |
| --- | --- | --- | --- |
| **# Stage** | **Activity** | **Duration in weeks** | **Time period for Completion** |
| **1** | **a. Submission of Detailed Project Plan.** **b. Placing of order with OEMs for supply of hardware, software security tools/solutions** **c. Placing of order for P2P link including network required hardware between Bank's CSOC and the Service Provider for remote monitoring.**  | **2** | **2 Weeks of issuing the Purchase order** |
| **2** | **Preparation for CSOC setup and implementation of required processes.****Commissioning of P2P link between MSSP and Bank.** | **2** | **4 Weeks of issuing the Purchase Order** |
| **3** | **Training for the Bank Team** | **1** | **5 Weeks of issuing the Purchase Order**  |
| **4** | **Delivery of CSOC Hardware / Software and licenses and resources**  | **-** | **6 Weeks of issuing the Purchase Order** |
| **5** | **Deployment of CSOC Resources at Bank’s premises**  | **-** | **6 Weeks of issuing the Purchase order** |
| **6** | **Installation & Configuration of SIEM and other Security Tools/Solutions (including DR log collection setup)** | **2** | **8 Weeks of issuing the Purchase Order** |
| **7** | **Integration of SIEM with other Security Tools/Solutions under CSOC and other devices (Network devices)**  | **$** | **14 weeks from issuing purchase order**  |
| **8** | **User Acceptance Test (UAT) (#) and making the CSOC operational**  | **2** | **16 weeks from issuing purchase order**  |

**$ - Activity should start in parallel after delivery of hardware/software**

**# - The Solution will be deemed accepted only when all the functionalities as per the Scope are provided, commissioned and accepted by the Bank or the Bank appointed Consultant. The UAT shall be signed off between the Bank and the Successful Bidder.**

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

**Phase I - All security solutions supplied under the CSOC scope, should be implemented and integrated within 14 weeks from date of PO. It will include all DC & DR infrastructures. P2P link between MSSP and Bank should be commissioned within 1 month of issuing purchase order for CSOC. Bidder need to specify any requirement from Bank's side for the P2P link.**

**Phase II –Bank's existing networking and security devices such as firewalls, IPSs, IDSs, Routers, Switches, proxies etc are to be integrated with SIEM.**

**The bidder shall perform the Project Management of CSOC implementation as detailed below**

| **Phase** | **Activities** | **Deliverables** |
| --- | --- | --- |
| **I**  | **Planning** | **Conduct Kick-off meeting*** **Identify project point(s) of contact**
* **Identify Bank resources required to assist in deployment, policy walkthrough, testing, and installation.**
* **Identify business requirements**
* **Identify technical requirements**
* **Project Planning**
* **Plan the schedule**
 | * **Project Plan and Gap Analysis**
 |
| **II**  | **Design** | * **Various OEM should be involved in this phase.**
* **Develop and/or review and validate solution design/architecture documents which will include:**
	+ **Solution overview and conceptual design**
	+ **Detailed design and connectivity parameters**
	+ **Create a User Acceptance Test Document**
 | * **Design & Architecture Document**
* **Prerequisite Document**
* **User Acceptance Test Plan**
 |
| **III**  | **Installation and Configuration**  | * **Deploy solution**
* **Complete implementation and configuration of each Security tools / solutions**
* **Complete Integration of Security tools / solutions with SIEM**
* **Documentation of installation and configuration**
 | * **Successful deployment solution**
* **Installation and Configuration Document**
* **Gap Assessment**
 |
| **IV**  | **Optimize** | * **Fine-tuning of solution**
* **Monitor and resolve issues**
* **Provide an information knowledge-transfer workshop**
 | * **Tuning policies.**
* **Resolution of deviations in policy**
* **Transfer of Information session**
 |
| **V**  | **Deployment Validation**  | * **This phase will comprise of deployment validation to be conducted by OEM.**
* **In case OEM is not satisfied with the installation and configuration of product, they will submit their recommendation in form of a report to the Bank accordingly.**
* **UAT and Acceptance**
 | * **Validation Report by OEM**
* **UAT report by the Bank appointed consultant**
 |
| **VI**  | **Monitoring, Management & Sustenance**  | * **Post- deployment bidder will manage & monitor proposed solution**
* **Facilitation & operation for all change management, upgradation, updates, etc during contract period**
 | * **Reports and Dashboards as per defined SLAs**
* **Go Live Operations**
 |

 **The entire project needs to be completed as per the time schedules mentioned above. The Bank and the selected bidder shall nominate a Project Manager each 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 in implementing similar project. The Project Manager should not be changed without the consent/approval of the bidder 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.**

## Training:

1. **The bidder shall arrange hands on training in two stages to 5 persons of the Bank at vendor’s location. Implementation training should be provided during project implementation of duration 2 to 3 days covering overall CSOC management. Training should be on the following areas: Knowledge Transfer of the Deployed Solution Architecture and Design, hardware, software, integration, and customization, policy installation, troubleshooting process, creation of policies/rules, generation of reports, and analysis of the reports, troubleshooting and familiarization of features and functionalities, alert monitoring and other aspects of the solution.**
2. **In the second stage, SIEM Training should be by faculty certified up to advance level with required practical experience and should provide courseware with adequate practical training. The training should be provided by the OEM/SI
employee and should be of five days, 8 hours a day.**
3. **Provide hands-on training on policy configuration, alert monitoring, Administration & Management of each component of the proposed solution.**
4. **Bidder shall provide comprehensive training manual, presentations, videos, lecture notes, hand-outs and other training documentation for all trainings.**
5. **A refresher training to be provided at periodic basis as and when required and it should be at least once in a year. The course duration will be of 2 days.**
6. **Project level higher training to CISO / Project Manager identified members of the Bank during the first year of implementation.**
7. **Bidder should submit broad course content along at the time of acceptance.**
8. **The Bidder shall also provide the administrative training of the NAC solution to the Bank personnel for 1 batch with 5 personnel in each batch.**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

# Evaluationmethodology

1. **The objective of this evaluation methodology is to facilitate the selection of one Service Provider (SP) fulfilling selection criteria and providing professional services at optimal cost. The successful bidder/service provider will be playing the role of both Managed Security Service Provider (MSSP) and System Integrator(SI).**
2. **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.**

## Evaluation process

## 6.1.1. Objective

1. **The objective of this evaluation methodology is to facilitate the selection of MSSP for implementing and managing the CSOC at optimal cost.**
2. **The project is based on CSOC implementation cost and CSOC Services Cost and the selected bidder has to deliver the goods and services as per scope of the project.**

## 6.1.2. Evaluation steps

1. **The Bank has adopted a three (3) bid processes in which the Bidder has to submit following bids in separate envelopes at the time of submission of bids as stipulated in this document.**

#### Minimum Eligibility / Pre-Qualification Criteria

#### Technical Bid

#### Commercial Bids

1. **The Bank shall evaluate first the ‘Minimum Eligibility/ Pre-Qualification Criteria’ bids and based on its evaluation, ‘Technical Bids’ shall be undertaken for evaluation at the second stage. ‘Commercial bids’ shall be opened for only the shortlisted bidders out of technical evaluation. The final selection will be done based on Techno-commercial evaluation.**
2. **Evaluation criteria proposed to be adopted will be Quality cum Cost Based System (QCBS) where Technical Bid Score will get a weightage of 70% and Commercial Bid Score a weightage of 30%.**
3. **The evaluation by the Bank will be undertaken by a Committee of officials or/and representatives formed by the Bank and its decision will be final.**

## 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.**
3. **Prior to the detailed evaluation, the Bank will determine the substantial responsiveness of each Bid to the Bidding document. For the purpose of this clause, a substantially responsive Bid is one, which conforms to all the essential and mandatory requirements and / or contains reservations with regard to the critical and essential terms and conditions of the Bidding Document without material deviations.**
4. **Deviations from or objections or reservations to critical provisions, such as those concerning Bid security, performance security, qualification criteria, Force Majeure etc. will be deemed to be a material deviation.**
5. **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 would also evaluate the Bids on technical and functional parameters including possible visit to inspect live site(s) of the bidder, witness demos, bidders presentation, verify functionalities / response times etc.**
6. **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.**
7. **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.**
8. **Bids without EMD / Bid security in the proper form and manner will be considered non-responsive and rejected.**
9. **The bidder should satisfy the pre-qualification criteria as specified in the tender.**

## Evaluation of Minimum Eligibility / Pre-Qualification Criteria

1. **Bids submitted by all the bidders would be evaluated for eligibility as mentioned in ‘Annexure A.2 Minimum Eligibility / Pre-Qualification Criteria’. Bids not complying with any of the Minimum Eligibility/ Pre-Qualification Criteria are liable to be rejected and will not be considered for further evaluation. Only those Bidders who fulfill the given criteria are eligible to respond to this RFP. The Technical Proposal will be evaluated only for those respondents who are fulfilling the ‘Minimum Eligibility/Pre-Qualification Criteria’ as detailed below.**
2. **Successful bids out of this stage would be considered for technical evaluation.**
3. **Bidders must submit the proof of all the credentials as required for evaluation of Minimum Eligibility/ Pre-Qualification Criteria. Claims of the bidders without verifiable facts will not be considered as credentials towards satisfying Minimum Eligibility/ Pre-Qualification Criteria.**
4. **The bidder is required to submit list of projects / references supported by any of the required documents as evidences of having relevant experience:**
5. **Copy of Work order (with commercial masked if required)/ agreement along with completion certificate for completed projects.**
6. **Relevant credential letters, supporting the claim, from the respective organization along with contact details of the organization.**

## Evaluation of Technical Bids

1. **The technical bids will be evaluated for determining the continued eligibility of the Bidder for Project and compliance of the bids with the necessary technical requirements and scope of work of this tender.**
2. **SIDBI may seek specific clarifications from any or all the Bidder(s) at this stage. All the clarifications received within the stipulated time shall be considered for evaluation. In case satisfactory clarifications are not received from the bidders within the stipulated time, the respective technical parameters would be treated as non-compliant and decision to qualify the bidder shall be accordingly taken by SIDBI.**
3. **Technical bids would be evaluated as follows:**

**6.4.1 Technical Evaluation Criteria**

| **Sr No** | **Criteria** | **Maximum Marks** | **Documents to be Submitted** |
| --- | --- | --- | --- |
| **A.** | **Credentials / Experience** |
| **1** | **The number of SOC/CSOC setup in India for BFSI**  **clients with Project Cost of minimum Rs 5 crores**  | **For each assignment - 05**  | **15** | **Should attach copies of work order marked as Annexure E-1.** |
| **2** | **The number of SOC/CSOC setup in India for other clients with Total Project Cost of minimum INR 5 crores.** | **For each assignment - 3 marks** | **9** | **Should attach copies of work order marked as Annexure E-2.** |
| **3** | **SIEM tool proposed should be in Leaders/Challengers as per Gartner Magic quadrant OR****Leaders/Strong performers as per Forrester Wave.** | **Leader Quadrant – 15 Marks**  **Challenger/Strong Quadrant – 10 Marks** **Zero marks if solution is not in Gartner leader/challenger or Forrester Wave Leaders/Strong quadrant** | **15** | **Should attach copies of proof marked as Annexure E-3.** |
| **4** | **Experience of the bidder in implementing SIEM solution offered to SIDBI ( i.e specific solution offered to the Bank under this project)** | **For each implementation - 5 marks** | **15** | **Should attach copies of work order marked as Annexure E-4.** |
| **5** | **Experience of the bidder in implementing PIM (can be of any OEM)** | **For each implementation - 2 marks** | **04** | **Should attach copies of work order marked as Annexure E-5.** |
| **6** | **Experience of the bidder in implementing Anti-APT (can be of any OEM)** | **For each implementation - 3 marks** | **06** | **Should attach copies of work order marked as Annexure E-6.** |
| **7** | **Experience of the bidder in implementing Firewall Analyzer (can be of any OEM)** | **For each implementation - 2 marks** | **04** | **Should attach copies of work order marked as Annexure E-7.** |
| **8** | **Experience of the bidder in implementing NAC (can be of any OEM)** | **For each implementation - 2 marks** | **04** | **Should attach copies of work order marked as Annexure E-8.** |
| **9** | **Experience of the bidder in VAPT** | **For each implementation - 2 marks** | **04** | **Should attach copies of work order marked as Annexure E-9.** |
| **10** | **Experience of the bidder in implementing Security / Threat Intelligence services** | **For each implementation - 2 marks** | **04** | **Should attach copies of work order marked as Annexure E-10.** |
|  | **Total marks (A)** | **80** |  |

**6.4.2 Marks for the Technical Specifications of the security solutions offered:**

|  |  |  |
| --- | --- | --- |
| **Sr No** | **Scope of CSOC** | **Maximum Marks** |
| **1** | **Security Incident & Event Management (SIEM)** | **50** |
| **2** | **Privilege Identity Management (PIM)** | **15** |
| **3** | **Anti APT (Advanced Persistent Threat)**  | **20** |
| **4** | **Firewall Analyser** | **20** |
| **5** | **Network Access Control (NAC)** | **15** |
|  | **Total marks (B)** | **120** |

 **Total Technical marks (A+B ) : 200**

1. **For the scope item SIEM and NAC, 2 marks will be awarded if the bidder is compliant with the requirement which is marked as essential and 1 mark will be given for the requirement marked as preferable. Zero marks will be awarded if no solution is provided against the requirement. For the other items in the scope, one marks will be awarded if the requirement is compliant with the requirement and 0 marks will be awarded if no solution is provided against the requirement. For all the tools, maximum marks for the technical specifications for each of the security solution will be scaled to the total no of specifications mentioned and marks obtained will be given on pro rata basis based on no of points complied by the vendor. For eg maximum marks for the technical specifications for SIEM tool is 50 for 110 parameters and if the vendor compliance is for 90 points, it would be 50X90/110 =40.1.**
2. **During Technical evaluation, the bidders who score >= 75% marks would be considered for commercial evaluation. In case, all the bidders fails to score more than 75% marks or less than three bidders obtain more than 75% marks, then in that case top three bidder will be considered for opening commercial bids provided marks obtained by them are more than 70%. The decision of the Bank in this regard shall be final. The evaluation process for short listing of bidder will be based on the evaluation matrix (6.4.1 and 6.4.2 ) given above.**
3. **The technical bid will be analyzed and evaluated, based on which the Relative Technical Score (RSTech) shall be assigned to each bid on the basis of parameters mentioned above.**
4. **Relative Technical Score (RSTech) for each bidder will be calculated as follows based on above parameters:**

|  |
| --- |
| **RSTech = T / T-High \* 100** |

**Where:**

|  |  |  |
| --- | --- | --- |
| **RSTech** | **=** | **Relative score obtained by the bidder** |
| **T** | **=** | **Technical score obtained by bidder** |
| **T-High** | **=** | **Highest Technical score secured among the Bidders**  |

## Evaluation of Commercial Bids

1. **In this phase, the Commercial Bids of the Bidders, who are found technically qualified in previous phase, will be taken for commercial evaluation.**
2. **The date for opening of commercial bids will be separately advised.**
3. **Relative Technical Score (RSTech) of the technically qualified bids would be announced before the representatives of the bidders and the commercial bids of those bidders would be opened for commercial evaluation.**
4. **Total Cost of Ownership (TCO) for 03 Years using Net Present Value (NPV) would be calculated as under:**

**TCO = NPV (CSOC Implementation cost) + NPV (CSOC Services cost for 3 years as mentioned in the commercial bid).**

**Net Present Value (NPV) of the yearly cost would be calculated using the Microsoft Excel Worksheet formulae, to arrive at the NPV for three years. The discount rate to be considered for above would be 8.5% per annum.**

|  |
| --- |
| **RSCom = CLow / C \* 100** |

1. **Relative Commercial Score (RSCom) for each vendor will be calculated as follows:**

 **Where:**

|  |  |  |
| --- | --- | --- |
| **RSCom** | **=** | **Relative score for Commercial Bid of the vendor** |
| **C** | **=** | **Commercial bid value of the bidder under consideration and is based TCO.** |
| **CLow** | **=** | **Lowest commercial bid value out of all the eligible commercial bids obtained and is based TCO.** |

## Final Selection of the Eligible Bidder

1. **Total Relative Score (RS) obtained by each eligible vendor will be calculated as follows:**

|  |
| --- |
| **RS = RSTech \* 0.7 + RSCom\* 0.3** |

1. **The eligible bidder “H1 Bidder” will be selected based on HIGHEST Relative Score (RS) thus obtained.**
2. **The vendor with the highest Relative Score (RS) will be selected for further discussion for finalizing contract / placing PO or LOI subject to satisfying all the terms and conditions defined in this RfP document.**

**Site Visit:**

 **Bank at its discretion may visit any or all reference sites (including CSOC Vendor) where bidder has implemented SOC, SOC centre of Bidder.**

**Note1: Marks provided by the Bank to the bidder shall be final. No objection/query/justification related to given marks from any bidder shall be entertained. Decision of Bank in this regard shall be final & binding.**

**Note 2: It is to be noted that Bank will only disclose final marks to technically qualified bidders.**

## 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 vendor 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 15 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 5.9).**

## Execution of Agreement

1. **Within 30 days from the date of acceptance of the Order, the selected bidder shall sign a stamped “Agreement” with the Bank at Mumbai 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

## 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 of Rs 20,50,000/- (Rs Twenty Lakh and Fifty Thousand only) in the form of Demand Draft / Pay Order OR Bank guarantee issued by a scheduled commercial bank.**
2. **Demand Draft / Pay order should be in favour of “Small Industries Development Bank of India” payable at Mumbai 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 A.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:**
6. **In case the Bidder withdraws the bid prior to validity period of the bid for any reason whatsoever;**
7. **Bidder makes any statement or encloses any form which turns out to be false / incorrect at any time prior to signing of the contract.**
8. **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**
9. **In case the successful Bidder fails to provide the Performance Bank guarantee within within ONE month from the date of issue of Purchase Order by the Bank or signing of the contract, whichever is earlier, for any reason whatsoever.**

**Besides forfeiting the EMD, the Bank may ban the bidder from subsequent bidding for a period of not less than 3 years.**

1. **The EMD amount / BG of all unsuccessful bidders would be refunded immediately upon occurrence of any the following events, whichever is earlier:**
2. **Receipt of the signed contract and performance security from the successful bidder. OR**
3. **The end of the bid validity period, including extended period (if any), OR**
4. **Issue of Letter of Intent / Purchase order to the successful bidder**
5. **Successful bidder will be refunded the EMD amount only after submission of Performance Bank Guarantee as mentioned in Performance Bank Guarantee (PBG) section.**
6. **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 ONE month from the date of issue of Purchase Order 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 BG prior to project completion, the bidder will be required to renew the BG 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.**
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.**
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- 6 - Bid 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. **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.**
3. **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 favour. This will remain applicable throughout the contract period.**
4. **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. However, if anything is missed out by SIDBI in the RfP document, SIDBI would bear the additional expenditure to avail the services at the rate mentioned in the commercial bids of the Service Provider for similar such item.**
5. **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 organisation 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 P2P link for the bidder's through secure channels. However, no modification in systems and trouble shooting 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

 **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.**

**SIDBI has the sole ownership of and the right to use, all data that may be in possession of the Vendor 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 Vendor in connection with the scope of work submitted to SIDBI will be property of the Bank. The Vendor 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. Vendor 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

 **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.**

 **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.**

 **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

**The standard payment terms are given below:**

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. **AMC / ATC 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 & SI. Bank will not pay any extra charge to OEM and/or SI 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. **Payment will be made quarterly on submission of invoices for CSOC Services Cost. The service provider will submit invoices at the end of the each quarter. 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. Vendor to submit Bank Mandate Form (as per Annexure A.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.**

**Payment Schedule**

**Submission of Performance Bank Guarantee (PBG) is the prerequisite before making any payment.**

| **Sr No** | **Deliverables** | **% of payment** | **STAGES (On completion of the activities)** |
| --- | --- | --- | --- |
| **1** | **Hardware / Appliance / Software / License**  | **50% of the goods delivered** | **1. Delivery and verification of the Hardware and software and on submission of invoice with Proof of Delivery.****2. Commissioning of P2P link by the vendor.** |
| **2** | **40% of the goods delivered** | **On individual Solution implementation and integration and Sign-off**  |
| **3** | **10% of the goods delivered** | **1. Submission of the Back to back warranty certificate from OEM valid for a period of 1 year from date of acceptance.** **2. Acceptance of all solutions by the Bank** |
| **4** | **Payment for Managed services** |  | **Payment will be made quarterly in arrears. The payment will begin after integration and acceptance of each of the solutions and will be based on the quarterly SLA reports submitted by the engaged vendor.** |
| **5** | **AMC/ATS** |  | **A comprehensive onsite warranty / support for a period of 1 year shall be there on all the Hardware and Software supplied to/purchased by the Bank. The vendor has to take AMC/ATS after expiry of warranty for a period of 2 Years. Warranty will commence from the acceptance/sign off date from Bank for SIEM/ each tool under CSOC.** |
| **6** | **General Conditions** |  | **There shall be no escalation in the prices once the prices are fixed and agreed by the Bank and the Bidder****No advance payment will be made prior to the start of the implementation.****All applicable taxes and duties will be deducted at source as per applicable laws.****Any penalties / liquidated damages imposed on the bidder for non-performance will be deducted from the payment as deemed necessary** |
| **7** | **Delivery, implementation and Roll out:** |  | **The Selected Bidder shall be responsible for delivery; implementation and rollout of all the solutions required under this RFP and also must agree to the timeline as specified above.****In the event of Bidder‘s failure to deliver and/or implement all required components of a fully functional system (pertaining to the scope of the project) within the stipulated time schedule or by the date extended by the Bank, unless such failure is due to reasons entirely attributable to the Bank, it will be a breach of contract. In such case, the Bank would be entitled to charge a penalty or will have the right to terminate the contract, as specified in this RFP.** |

## 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 / labour laws are complied with while providing services. The selected vendor may have to execute an indemnity bond in favour of the Bank in this regard.**
3. **Providing clarifications / particulars / documents etc. to the appropriate tax authorities for assessment of tax, compliance with labour and other laws, etc will be the responsibility of the vendor 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 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.**
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 favour. 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 three weeks 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 and continue for a period of THREE years thereafter. If so desired by SIDBI, contract may be extended for a maximum period of TWO more years (in total FIVE years) on the same terms and conditions.**
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 supplied will be supported up to 5 years.**
3.
4.
5.
6.
7. 1.
	2.
	3.
	4.
	5.
	6.
	7.
	8.
	9.
	10.
	11.
	12.
	13.
	14.
	15.
	16.

## Termination

1. **Bank shall have the option to terminate the contract, in whole or in part by giving the Successful Bidder / Service Provider at least 90 days’ prior notice in writing. Without prejudice to the generality of the foregoing, the Bank will be entitled to terminate the contract, if Bidder breaches any of its obligations set forth in this RFP and subsequent contract and**
	1. **Such breach is not cured within thirty (30) Working Days after Bank gives written notice; or**
	2. **If such breach is not of the type that could be cured within thirty (30) Working Days, failure by Bidder to provide Bank, within thirty (30) Working Days, with a reasonable plan to cure such breach, which is acceptable to the Bank.**
	3. **Delay in delivery beyond the 6 months period for delivery.**
	4. **Failure to meet SLA for 2 consecutive quarters**
	5. **Negligence**
2. **The successful Bidder shall not have any right to terminate the contract entered into subsequent to this RfP for convenience. However, without prejudice to the generality of the foregoing, the successful Bidder will be entitled to terminate the agreement entered into subsequent to this RfP, if:**
	1. **Bank materially breaches any of its obligations set forth in this Tender and subsequent Agreement; and**
	2. **Such breach is not cured within thirty (30) Working Days after Bidder gives written notice, or**
	3. **If such breach is not of the type that could be cured within thirty (30) Working Days, failure by Bank to provide Bidder, within thirty (30) Working Days, with a reasonable plan to cure such breach.**
3. **This Tender and subsequent Agreement shall be deemed to have been terminated by either Party one day prior to the happening of the following events of default:**
	1. **The other Party becomes unable to pay its debt as they fall due or otherwise enters into any composition or arrangement with or for the benefit of its creditors or any class thereof;**
	2. **A liquidator or a receiver is appointed over all or a substantial part of the undertaking, assets or revenues of the other Party and such appointment continues for a period of twenty one (21) days;**
	3. **The other Party is subject of an effective resolution for its winding up other than a voluntary winding up for the purpose of reconstruction or amalgamation upon terms previously approved in writing by the other Party; or**
	4. **The other Party becomes the subject of a court order for its winding up.**
4. **Either Party shall have the immediate right to terminate this Tender and subsequent contract upon written notice to the other Party in the event that such other Party ceases to be in operation or ceases to do business in India.**
5. **Immediately upon the date of expiration or termination of the Tender and subsequent Agreement, Bank shall have no further obligation to pay any fees for any periods commencing on or after such date.**

 **Without prejudice to the rights of the Parties, upon termination or expiry of this Tender and subsequent Agreement, Bank shall pay all the undisputed fees outstanding till the date of termination to the Service Provider of completion of the reverse transition period. The 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 security deposit, if any, under this contract.**

1. **Upon the termination or expiry of this Tender and subsequent Agreement:**
	1. **The rights granted to Bidder shall immediately terminate.**
	2. **Upon Bank’s request, with respect to, (i) any agreements for maintenance, services or other third-party services used by Bidder to provide the Services; and (ii) the assignable agreements, Bidder shall, use its reasonable commercial endeavours to assign such agreements to Bank and its designee(s) on commercially reasonable terms mutually acceptable to both Parties.**
	3. **Upon Bank’s request in writing, Bidder will be under an obligation to transfer to Bank or its designee(s) the Deliverables being used by Bidder to perform the Services free and clear of all liens, security interests, or other encumbrances at a value calculated as stated.**

## Applicable laws

 **The Contract shall be interpreted in accordance with the laws prevalent in India.**

1. **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.**
2. **Compliance in obtaining approvals / permissions / licenses: The Bidder shall promptly and timely obtain all such consents, permissions, approvals, licenses, etc., as may be necessary or required for any of the purposes of this project or for the conduct of their own business under any applicable Law, Government Regulation / Guidelines and shall keep the same valid and in force during the term of the project, and in the event of any failure or omission to do so, shall indemnify, keep indemnified, hold harmless, defend, protect and fully compensate the 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 :**

###### **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.**

###### **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.**

###### **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 years 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 utilise 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 vendor 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 authorise, 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 vendor shall allow the Bank, its authorised personnel, its auditors (internal and external), authorised 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 under this RFP and the vendor 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.**

## 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

1. **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, damages, expenses, action suits and other proceedings, resulting directly or indirectly from an act or omission of Bidder, its employees in the performance of the services provided by contract with respect to the infringement of any law pertaining to patent, trademarks, liabilities, claims, copyrights 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, or such other statutory infringements in respect of all solutions under CSOC supplied by the selected Bidder to 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 any subsequent agreement; and/or**
	2. **The breach, default or non-performance of undertakings, warranties, covenants or obligations by the bidder;**
	3. **An act or omission of the Bidder and its employees and the OEM in the performance of the obligations of the Bidder under this RfP document or any subsequent agreement; and/or**
	4. **Claims made by employees who are deployed by the Bidder, against the Bank; and / or**
	5. **Breach of any of the term of this RfP document and/or of the agreement to be entered subsequent to 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**
	6. **Negligence or gross misconduct attributable to the Bidder or its employees or sub-contractors.**
	7. **Any or all Deliverables or Services infringing any patent, trademarks, copyrights or such other Intellectual Property Rights; and / or**
	8. **Breach of confidentiality obligations of the Bidder contained in this RfP document; and / or**
	9. **The use of unlicensed and illegal Software and/or allied components by the successful Bidder.**
	10. **Any contravention or Noncompliance with any applicable laws, regulations, rules, statutory or legal requirements by the bidder;**
2. **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. **Cooperates with the Bidder in the defence and settlement of the claims.**
3. **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 Bidder where the unmodified version of the Deliverable would not be infringing.**

## 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

1. **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 an undertaking as given in Annexure D.8.**
2. **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.**

**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.**

**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.**

 **“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:**

1. **relates to the Disclosing Party; and**
2. **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**
3. **is prepared or performed by or on behalf of the Disclosing Party by its employees, officers, directors, agents, representatives or consultants.**
4. **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.**
5. **“Confidential Materials” shall mean all tangible materials containing Confidential Information, including, without limitation, written or printed documents whether machine or user readable.**
6. **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:**
7. **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.**
8. **In maintaining confidentiality hereunder the Receiving Party on receiving the confidential information and materials agrees and warrants that it shall:**
9. **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;**
10. **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;**
11. **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**

**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.**

1. **The Receiving Party who receives the confidential information and materials agrees that on receipt of a written demand from the Disclosing Party:**
2. **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;**
3. **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;**
4. **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**
5. **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.**
6. **The restrictions in the preceding clause shall not apply to:**
7. **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.**
8. **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.**
9. **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 vendor.**

## 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 to a sole arbitrator mutually agreed upon after issue of at least 30 days’ notice in writing to the other party clearly setting out there-in the specific disputes. In the event of absence of consensus about the single arbitrator, the dispute may be referred to joint arbitrators; one to be nominated by each party and the said arbitrators shall appoint a presiding arbitrator. The provisions of the Indian Arbitration and Conciliation Act, 1996, shall govern the arbitration.**
3. **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.**
4. **Arbitration proceedings shall be held at Mumbai, India, and the language of the arbitration proceedings and that of all documents and communications between the parties shall be English.**
5. **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.**
6. **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.**
7. **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.**
8. **A notice shall be effective when delivered or on the notice’s effective date, whichever is later.**
9. **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 its 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 endeavour 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

 **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 vendor under the contract without the prior written consent of the Bank.**

**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 Vendor under this RFP.**

## Negligence

**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.**

**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 misdemeanours.**
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 5.9 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 vendor for the damage, theft etc till the delivery 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 [D.1 till D.6].**
5. **If the Bidder / SI 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 / SI without any extra cost to Bank or the Bidder / SI will be held accountable for OEM‘s inaction and penalty charges would be levied as per the SLA terms to Bidder / SI.**
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, 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 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, 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 the 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 Mumbai, 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 Vendor shall be deemed to have represented and warranted as follows:**

**i. 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.**

**ii. 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 .**

**iii. 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.**

**iv. 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.**

**v. 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.**

**vi. 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.**

**vii. 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.**

**viii. 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.**

**ix. 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.**

**x. 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.**

**xi. 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 vendor shall be paid by the selected vendor 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.**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

# Service Level Agreement & Liquidated Damages

1. **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.**
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. **Bank reserves the right to adjust the Liquidity damages (LD)/penalty, if any, against any amount payable to the bidder or will be adjusted against the PBG.**
4. **However the penalty to be recovered under above clauses shall be restricted & capped to 10% of the total value of the order.**

## 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 project schedule and implementation (section 5.9).**
2. **In case, if there is delay in delivery of the hardware & software, installation of the security solutions and associated hardware, software and software licences, as given in commercial bid, beyond the schedule given in Section 5.9 from date of issue of PO, then penalty 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 as given in Section 5.2 with SIEM should be completed within a period as mentioned in the section 5.9 from the date of issue of PO. In case of delay in integration beyond six months, penalty 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. **Penalties/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 working due to closure of the office/non-availability of access to the solution, the response time/uptime will be taken from the opening of the office for the purpose of uptime calculation. The 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)**

**X100/Total contracted hours in a quarter**

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

| **Sr No** | **Service Area** | **Uptime % calculated on quarterly basis** | **Penalty** |
| --- | --- | --- | --- |
| **1** | **Device (Hardware / Software) Failure (including Incident Management Tool) of the complete CSOC operations or SIEM failure.** | **99% and above** | **NA** |
| **97% to 99%** | **1% of Total C-SOC Services Cost for each failure**  |
| **95% to 96.99%** | **5% of Total C-SOC Services Cost for each failure**  |
| **Less than 95%** | **10% of Total C-SOC Services 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 penalty will be as per the point 1.** | **99% and above** | **NA** |
| **97% to 99%** | **10% of Notional AMC charges for each failure *(Refer A below)*** |
| **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/free support, 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 penalty.**
		2. **For repeat failure, same or higher penalty will be charged depending upon the delay in rectification of the problem.**
		3. **Penalty will be calculated on Quarterly basis and deducted against the Quarterly payments.**
		4. **In the case of failure of P2P Link, the proportionate cost of the no days service not available will be deducted.**
		5. **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. Penalty will be levied for any absence for which no substitute is arranged by the Service Provider as per defined in the below table. The penalty charges will be in addition to the pro rata charges for the resources for their days of absence.**

|  |  |
| --- | --- |
| **Resource Category** | **Penalty beyond leave of absence** |
| **Support Resources** | * **Online L3 Resource - Rs 3000/- per day maximum Rs 20,000/- per month**
* **L2 Resource - Rs.2,000/- per day maximum Rs.10,000/- per month.**
* **L1 Resource - Rs.1500/- per day maximum Rs. 7,500/- per month.**
 |

* + 1. **The Bank reserves right to recover / adjust the penalties/LD from any dues pending to the vendor.**
		2. **However, The maximum penalty 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 penalty as above and shall have full right to issue notice & seek explanation under this RFP. The above penalty shall be deducted from any payments due to the bidder.**

## SLAs & Liquidity Damages for CSOC Operations

| **S.No** | **Service Area** | **Service Level** | **Penalty** |
| --- | --- | --- | --- |
| **1** | **Monitoring & Log Analysis Services** | **24x7 monitoring 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 priority events within 60 minutes of the event identification.** | **Critical Events: -****15% of quarterly CSOC Monitoring and Management charges****High Priority Events: - 10% of quarterly CSOC Monitoring and Management charges Medium Priority Events: - 5% of the quarterly CSOC Monitoring and Management charges 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 vendor****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 Management charges** **Medium Priority Incidents: 5% of quarterly CSOC Monitoring and Management charges****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 at 10.am everyday Weekly Reports: By 10:00 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 Penalty of 3% of quarterly CSOC Monitoring and Management charges** **2) Delay in reporting by more than 3 days for both weekly and monthly reports shall incur a penalty of 10% of quarterly CSOC Monitoring and Management charges** |
| **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.****1. 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. 100 per vulnerability****3. Delay in providing steps for fixing the low vulnerabilities within 30 working days after reporting will incur Rs. 100 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.** | **Anti Phishing Anti Malware and Anti trojan****Service, Anti- Rogue Mobile application****services along with taking down Phishing sites and Rogue mobile application.** | **The bidder is expected to provide this service on a 24/7 basis.****Incidents need to be logged and the resolution SLA is as per the incident resolution section**1. **Take down of malicious sites/ applications within 24 hours of identification if confirmed by the bank.**
2. **Daily report of new phishing sites/rouge applications, action taken, instances of reactivation etc to be shared with bank.**
 | **For a delay of 8 hours after confirmation from bank in takedown of sites/ applications, a penalty of 50% of the quarterly CSOC Monitoring and Management charges will be levied.****For a delay of more than one week in takedown of such sites/ applications a penalty of 100% of quarterly CSOC Monitoring and Management charges will be levied****For more than one month delay in takedown of such site/applications, the service shall be discontinued****In the event that a new site is identified which shares the same Home URL of a site already taken down; additional payment for the take down of such sites shall not be made.** **Re-occurrence within a month of a site already taken down by the bidder shall not be considered as a new site and no additional payment shall be made for the takedown of such a site.** |
| **7** | **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 penalty of 1% of quarterly CSOC Monitoring and Management charges for that quarter** |
| **8** | **Security Intelligence Services** | **Advisories within 12 hours of new global threats & vulnerabilities disclosures.** | **A delay of more than Five days will incur a penalty of 1% of quarterly CSOC Monitoring and Management charges for that quarter** |
| **9** | **New Patches** | **New patches are applied within three months of them becoming generally available to all related technologies supplied by the vendor.** | **A delay of more than Five days will incur a penalty of 15% of quarterly CSOC Monitoring and Management charges for that quarter.** |
| **10.** | **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 penalty of 10% of Notional AMC cost of the individual solution supplied under CSOC.**  |

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.**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**ANNEXURES**

# Annexure for Minimum Eligibility/Pre Qualification Criteria

**Annexure A.1 – Eligibility Bid – Covering Letter**

**(To be submitted on Bidders Company letter head)**

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

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

**The Chief General Manager,**

**Risk Management Vertical,**

**Small Industries Development Bank of India,**

**6th Floor, Risk Management Vertical,**

**MSME Development Centre,**

**Plot No. C-11, G Block**

**Bandra Kurla Complex (BKC), Bandra (E)**

**Mumbai - 400 051**

**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 No. Tender 400/2018/1279/BYO/RiMV dated November 06, 2017. 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 six (6) 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 Center (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 for the hardware / software supplied as per the above referred RFP, during warranty of 1 year and AMC of 2 years. The price quoted by us includes back to back 1 years warranty and 2 years AMC with OEM and support.**
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 the Organisation\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Company Seal:**

**Annexure A.2 –Minimum Eligibility/ Pre-Qualification Criteria**

**Tender No. 400/2018/1279/BYO/RiMV dated November 06, 2017**

| **Sr. No** | **Criteria** | **Documents to be submitted as a proof** | **Bidder Compliance (Yes / No)** | **Page No. of Response where proof is attached** |
| --- | --- | --- | --- | --- |
| **1** | **The bidder should be a registered company in India and should be in existence for a minimum period of Five years as on the date of RFP.** **The Bidder should be either a Government Organization/ PSU/ PSE/ limited Company or a partnership firm under Indian Laws or /and an autonomous Institution approved by GOI.** | **Proof, such as Registration/Incorporation Certificate is to be submitted.*** **Partnership firm: Certified copy of Partnership Deed.**
* **Limited Company: Certified copy of Certificate of Incorporation / Certificate of Commencement of Business.**
* **Reference of Act /Notification**
 |  |  |
| **2** | **The bidder should be currently in the business of providing CSOC/SOC/Managed Security Services including log monitoring & co-relation for minimum 100 devices to at least TWO national level customers / Government organisations in India in last four years. i.e 2013-14, 2014-15, 2015-16 and 2016-17.** | **a. Copy of Work order / agreement of the projects (ongoing or completed) to be provided as proof. The completion certificate for completed projects may also be furnished, if available.** **.****b. Contact details of the client references on letter-head signed by authorized signatory of the Bidder.****(*The references of the customers must be submitted with official contact details for verification. References which cannot be verified with provided contact details may not be considered as valid evidences.)*** |  |  |
| **3** | **The Bidder should have a minimum turnover of at least INR 150 Crore per annum in the last 3 financial years as on the date of submission of Bid.** | **Chartered Accountant (CA) certificate and Audited Balance Sheet and Profit & Loss accounts are to be submitted as a proof.** |  |  |
| **4** | **The Bidder should have made cash profit in at least 2 years out of last 3 financial years out of Indian Operations.** | **Chartered Accountant (CA) certificate and copies of last three years’ profit and Loss statement and balance sheet** |  |  |
| **5** | **The bidder must have minimum 10 IT Security professionals having degree higher or equivalent to Bachelor of Engineering (B.E.)/Bachelor of Technology (B.Tech)/MCA on their payroll with certification in CISA/CISSP/CISM or professional certification from any SIEM or any other relevant certification in the field of IT Security.**  | **Self declaration to this effect on company's letter head signed by authorized signatory of the Bidder along with names, qualifications and certifications of the resources (mention 10 only).** |  |  |
| **6** | **The Bidder should have registered office and their own SOC/CSOC setup in India.** | 1. **Details of Service Provider's SOC/CSOC setup :**
2. **Address in India-**
3. **Floor area in Sq ft**
4. **Total no of engineers**

**ii. Self declaration with address and contact details on letter-head signed by authorized signatory of the Bidder** |  |  |
| **7** | **The Bidder should be ISO 27001 Certified** | **Certification copy required** |  |  |
| **8** | **The bidder should not have been black-listed by any Public Financial Institutions, Public Sector Bank, RBI or IBA or any other Government agencies during the last 03 years.**  | **Provide self declaration as per Annexure A.5** |  |  |
| **10** | **Pre-contract Integrity Pact as per format Annexure A.10** | **On Non judicial stamp paper to be submitted** |  |  |

**BFSI: Scheduled commercial banks in public or private sector / All India FIs\* / Insurance Companies will be considered under BFSI.**

**\* NABARD, SIDBI, EXIM Bank, NHB and IFCI**

**Authorized Signatories**

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

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

**Name of the 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 A.3 – General Information about Bidder**

**Tender No. 400/2018/1279/BYO/RiMV dated November 06 , 2017**

| **S.N.** | **Description** | **Bidder’s 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** | **www.** |
| **5** | **Address of Registered Office with contact numbers.** |
| **A** | **Address**  |  |
| **B** | **Pin Code** |  |
| **C** | **Land Line No (with STD code)** |  |
| **D** | **Fax No. (with STD code)** |  |
| **6** | **Address for Correspondence (if different from above).** |
| **A** | **Address**  |  |
| **B** | **Pin Code** |  |
| **C** | **Land Line No (with STD code)** |  |
| **D** | **Fax No. (with STD code)** |  |
| **7** | **PAN No.**  |  |
| **Copy of PAN enclosed. (Yes/No)** |  |
| **8** | **Sales Tax Registration No.** |  |
| **Copy of Sales Tax certificate enclosed. (Yes/No)** |  |
| **9** | **GST / Service Tax Registration No.** |  |
| **Copy of GST / Service Tax certificate enclosed. (Yes/No)** |  |
| **10** | **Contact Details of Bidder’s authorized representative to make commitments to SIDBI.**  |
| **A** | **Name** |  |
| **B** | **Designation** |  |
| **C** | **Land Line No. (with STD code)** |  |
| **D** | **Mobile No.** |  |
| **E** | **Fax No. (with STD code)** |  |
| **F** | **Mail Id** |  |
| **11** | **Financials (for last three years)** |
| **Parameter** | **FY** | **Amount in lakh** |
| **A** | **Annual Turnover** | **2014 - 2015** |  |
| **2015 - 2016** |  |
| **2016 - 2017** |  |
| **B** | **Cash Profit** | **2014 - 2015** |  |
| **2015 - 2016** |  |
| **2016 - 2017** |  |
| **C** | **Net worth** | **2014 - 2015** |  |
| **2015 - 2016** |  |
| **2016 - 2017** |  |
| **D** | **CA certificate attached for A, B and C above.**  | **(Yes / No)** |
| **E** | 1. **Audited balance sheet and**
2. **P/L account attached.**
 | **(Yes/ No)** |
| **12** | **EMD Details** |
| **A** | **DD / Pay Order / Bank Guarantee** |  |
| **B** | **Number** |  |
| **C** | **Date of Issue** |  |
| **D** | **Issuing Bank** |  |
| **E** | **Amount (Rs)** |  |
| **13** | **Tender Form Cost Details** |
| **A** | **DD / Pay Order / Bank Guarantee** |  |
| **B** | **Number** |  |
| **C** | **Date of Issue** |  |
| **D** | **Issuing Bank** |  |
| **E** | **Amount (Rs)** |  |
| **14** | **MSME Status (Tick appropriate)**  |
| **A** | **Company does not qualify the status of MSE.**  |  |
| **B** | **Company does qualify the MSE status.**  |  |
| **C** | **SC/ST** |  |
| **D** | **MSE registration certificate or a certificate from Chartered Accountant attached. (Yes/No)**  |  |

**Authorized Signatories**

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

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

**Name of the Organisation\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

 **Company Seal:**

**Annexure A.4 - Power of Attorney**

 **RfP No. Tender 400/2018/1279/BYO/RiMV dated November 06, 2017**

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

**BY THIS POWER OF ATTORNEY executed on \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, 2017, 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 :-**

1. **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. Tender 400/2018/1279/BYO/RiMV dated November 06, 2017 for "Implementation and Management of Cyber Security Operations Center (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**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**WITNESS:**

**Signature of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Attested**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Annexure A.5 – Declaration regarding Clean Track Record**

**(To be submitted on Bidders Company letter head)**

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

**To**

**The Chief General Manager ,**

**Risk Management Vertical,**

**Small Industries Development Bank of India**

**MSME Development Center, 6th Floor**

**Risk Mabagement Vertical, Plot No.C-11, G Block**

**Bandra Kurla Complex, Bandra [East],**

**Mumbai 400 051**

**Dear Sir,**

**Declaration regarding Clean Track Record**

**Tender No. 400/2018/1279/BYO/RIMV dated November 06 , 2017**

**I have carefully gone through the Terms & Conditions contained in the RFP No. Tender 400/2018/1279/BYO/RIMV dated November 06, 2017 regarding selection of the vendor for a period of three years.**

**We hereby declare that 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 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.**

**We further declare that we are eligible and competent as per the Eligibility/ Pre-Qualification Criteria given by the bank and the information submitted by the company in Annexure A.2 & A.3 are true and correct and also we would be able to perform this contract as per RFP document.**

**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.**

**Authorized Signatories**

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

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

**Name of the Organisation\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Company Seal:**

**Annexure A.6 – Bank Mandate Form**

**(To be submitted in Duplicate)**

**Please fill in the information in CAPITAL LETTERS. Please TICK wherever it is applicable)**

1. **Name of Borrower / vendor / supplier: ­­­­­­­­­­­­­­­­­­­­­­­­­­­­\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**
2. **Vendor Code (if applicable):\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**
3. **Address of the Borrower / vendor / supplier:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

 **City Pin Code \_\_\_\_\_\_\_\_\_\_\_\_\_\_ E-mail id:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Phone No. with STD code:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Mobile:No.: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Permanent Account Number \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**MSME Registration / CA Certificate (if applicable):\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**3. Particulars of Bank account:**

|  |  |
| --- | --- |
| **Beneficiary Name** |  |
| **Bank Name** |  | **Branch Name** |  |
| **Branch Place** |  | **Branch City** |  |
| **PIN Code** |  | **Branch Code** |  |  |  |  |  |  |  |  |  |  |
| **MICR No.** |  |  |  |
| **Account type** |  **Saving** |  **Current** | **Cash Credit** |
| **Account No.** | **(As appearing in the 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** |  |

**4. Date from which the mandate should be effective :**

 **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 updation of records for purpose of credit of amount through RBI RTGS/NEFT.**

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

**Date : \_\_\_\_\_\_\_\_\_\_\_\_\_ Signature of: the 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 A.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. Tender 400/2018/1279/BYO/ITV dated November 06, 2017 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 situate 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 it’s 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 ie 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 A.8 - Manufacturer Authorisation Format**

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

**Ref: Date:**

**To**

**The Chief General Manager ,**

**Risk Management Vertical,**

**Small Industries Development Bank of India**

**MSME Development Center, 6th Floor**

**Risk Mabagement Vertical, Plot No.C-11, G Block**

**Bandra Kurla Complex, Bandra [East],**

**Mumbai 400 051**

**Dear Sir,**

 **Manufacturer Authorisation for**

**Request for Proposal (RFP) No. Tender 400/2018/1279/BYO/RiMV dated November 06, 2017 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>**

**<Authorised Signatory>**

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

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

**Name of the 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 A.9 - Undertaking of Authenticity**

**[to be signed by authority not lower than the Company Secretary of the Bidder ]**

**Ref: Date:**

**To**

**The Chief General Manager ,**

**Risk Management Vertical,**

**Small Industries Development Bank of India**

**MSME Development Center, 6th Floor**

**Risk Mabagement Vertical, Plot No.C-11, G Block**

**Bandra Kurla Complex, Bandra [East],**

**Mumbai 400 051**

**Dear Sir,**

**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. 400/2018/1279/BYO/ITV dated November 06, 2017, 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 (Vendor 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 / SI etc.**

|  |  |
| --- | --- |
| **Date** | **Signature of Authorised Signatory …** |
| **Place** | **Name of the Authorised Signatory …** |
|  | **Designation …** |
|  | **Phone & E-mail:** |
|  | **Name of the Organisation …** |

**Annexure A.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 -----, 2017 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 400/2018/1279/BYO/RIMV dated November 06, 2017) 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:**

1. **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.**
2. **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 disfavor 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.**

* 1. **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.**
1. **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.**
2. **Earnest Money (Security Deposit)**
	1. **While submitting commercial bid, the BIDDER shall deposit an amount Rs 20,50,000/- /- as Earnest Money/Security Deposit, with the BUYER through any of the following instrument.**
3. **Bank Draft or a Pay Order in favour of Small Industries Bank of India, Payable at Mumbai.**
4. **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.**
	1. **Earnest Money/Security Deposit shall be valid till the date of bid validity as mentioned in the RfP.**
	2. **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.**
	3. **No interest shall be payable by the BUYER to the BIDDER on Earnest Money/Security Deposit for the period of its currency.**
5. **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 :-**
6. **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**
7. **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.**
8. **To immediately cancel the contract, if already signed, without giving any compensation to the BIDDER**
9. **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.**
10. **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.**
11. **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**
12. **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.**
13. **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.**
14. **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.**
15. **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.**
	1. **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.**
	2. **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.**
16. **Fall Clause**
	1. **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.**
17. **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. **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.**
18. **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.**

1. **Law and Place of Jurisdiction**

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

1. **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.**

1. **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.**
2. **The parties hereby sign this integrity Pact, at \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ on \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**BUYER BIDDER**

**Name of the Officer**

**Designation CHIEF EXECUTIVE OFFICER**

**SIDBI**

**Witness Witness**

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

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

# Annexure for Technical Bid

**Annexure B.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 / 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**  | **SOC / CSOC implementation carried out by the bidder:-** |
| **a** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Name of the customer and Contact Details of the reference provided** | **Project cost in Rupees crores** | **Implementation period** | **Should attach copies of work order marked as Annexure E-1.** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**BFSI / Government sector customers****(BFSI Sector customers carries more weightage)** |
| **b** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Name of the customer and Contact Details of the reference provided**  | **Project cost in Rupees crores** | **Implementation period** | **Should attach copies of work order marked as Annexure E-2.** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Other Customers** |
| **6** | **a. Name of the SIEM tool proposed****b. Mention the ranking:**  **Gartner Magic quadrant Leaders/Challengers OR Forrester Wave Leaders/Strong performers****(Should attach proof of the same marked as Annexure E-3)** |  |
| **7** | **No of assignments in implementing SIEM solution offered to the Bank - (should attach copies of work order marked as Annexure E-4)** |  |
| **8** | **No of assignments in implementing PIM - (Should attach copies of work order marked as Annexure E-5)** |  |
| **9** | **No of assignments in implementing Ant-APT - (Should attach copies of work order marked as Annexure E-6)** |  |
| **10** | **No of assignments in implementing Firewall Analyzer - (Should attach copies of work order marked as Annexure E-7)** |  |
| **11** | **No of assignments in implementing NAC - (Should attach copies of work order marked as Annexure E-8)** |  |
| **12** | **No of assignments in implementing VAPT - (Should attach copies of work order marked as Annexure E-9)** |  |
| **13** | **No of assignments in implementing Security / Threat Intelligence Services - (Should attach copies of work order marked as Annexure E-10)** |  |
| **14** | **OEM Details**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Sr No** | **Security Solution requested by Bank** | **Security solution proposed for SIDBI CSOC** | **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** | **SIEM** |  |  |  |  |  |  |
| **2** | **PIM** |  |  |  |  |  |  |
| **3** | **Anti APT** |  |  |  |  |  |  |
| **4** | **Firewall Analyzer** |  |  |  |  |  |  |
| **5** | **NAC** |  |  |  |  |  |  |
| **1.The technical specifications mentioned in the Annexures D1 to D5 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.** **In case such date is not announced, it should be supported for minimum three years.****3. At least one trained engineer for each solution should be available with the Bidder.** |

 |
| **15** | **Project Team composition and role of the members for the proposed assignment.**  | **Project Lead :**

|  |  |
| --- | --- |
| **Team Member** | **Role** |
|  |  |
|  |  |

 |
| **16** | **Single Point of contact for RFP:** | **Name:** **Designation:****Contact Details:** |
| **17**  | **Project Schedule and implementation given in Section 5.9 is acceptable**  | **YES / NO** |
| **18** | **Number of banks / Financial Institutions to which this kind of services are being given. \***  | **Self declaration on company letter head, references from BFSI Sector customers carries more weightage.**  |

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

**Authorized Signatories**

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

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

**Name of the Organisation\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Company Seal:**

**Annexure B.2 – Statement of Deviations**

 **RfP No. Tender 400/2018/1279/BYO/RiMV dated November 06, 2017**

**(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.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S.N.** | **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 Organisation\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Company Seal:**

**Annexure B.3 – Letter of Competence**

 **RfP No. Tender 400/2018/1279/BYO/RiMV dated November 06, 2017**

 ***(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 Minimum Eligibility/ Pre-Qualification Criteria is true and correct.**

**Authorized Signatories**

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

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

**Name of the Organisation\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Company Seal:**

**Annexure B.4 – Letter of Conformity**

**(To be submitted on Bidders Company letter head)**

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

**To**

**The Chief General Manager [RiMV]**

**Small Industries Development Bank of India**

**MSME Development Center, 3rd Floor**

**Information Technology Vertical**

**Plot No.C-11, G Block**

**Bandra Kurla Complex**

**Bandra [East]**

**Mumbai 400 051**

**Dear Sir,**

**Letter of Conformity**

 **RfP No. Tender 400/2018/1279/BYO/RiMV dated November 06, 2017**

**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 B.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 Organisation\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Company Seal:**

# Annexure - Commercial Bid

**Annexure C.1 – Commercial Bid – Covering Letter**

**(To be submitted on Bidders Company letter head)**

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

**To**

**The Chief General Manager ,**

**Risk Management Vertical,**

**Small Industries Development Bank of India**

**MSME Development Center, 3rd Floor**

**Information Technology Vertical**

**Plot No.C-11, G Block**

**Bandra Kurla Complex**

**Bandra [East]**

**Mumbai 400 051**

**Dear Sir,**

**Commercial Bid – Covering Letter**

**Tender 400/2018/1279/BYO/RiMV dated November 06, 2017**

**I, the undersigned, offer to provide services for the above-mentioned project, in accordance with your RfP No. Tender 400/2018/1279/BYO/RiMV dated November 06, 2017 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 Organisation\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Company Seal:**

**Annexure C.2 –Commercial Bid Format**

**RfP No. Tender 400/2018/1279/BYO/RiMV dated November 06, 2017**

**RfP – for Implementation and Management of Cyber Security Operations Center (CSOC)**

**Table 1:- CSOC Implementation cost (Amount in Rupees)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S.N.** | **CSOC Implementation cost**  | **Cost for the hardware, software including 1 year warranty**  | **Cost of AMC for the hardware, software**  | **Total cost** |
| **2nd year** | **3rd year** |
| **1** | **SIEM** |  |  |  |  |
| **2** | **PIM (R1)** |  |  |  |  |
| **3** | **Anti APT** |  |  |  |  |
| **4** | **Firewall Analyser** |  |  |  |  |
| **5** | **NAC (R1)** |  |  |  |  |
| **6** | **Security / Threat Intelligence** |  |  |  |  |
| **7** | **Backup and Storage Solution (including SAN, controllers, Tape drive etc)** |  |  |  |  |
| **8** | **Other Infrastructure (including Server requirements, 2 TVs, 4 Desktops at DC and server requirement at DR site)** |  |  |  |  |
| **9** | **Total cost for the hardware, software and licenses including the storage solutions (X)** |  |  |  |  |
| **10** | **Taxes & Levies @\_\_\_\_ % (Y)** |  |  |  |  |
| **11** |  **Total for the CSOC implementation cost (A=X+Y)**  |  |  |  |  |

 **R1 - In case of switching over of business operations from PDC (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 DRSite. The server and other infrastructure, if any, required at DR site are to be provided by the vendor.**

**Table 2:- CSOC Services Cost (Amount in Rupees)**

|  |  |  |  |
| --- | --- | --- | --- |
| **S.N** | **CSOC Services Cost** | **Annual Cost** | **Total for 3 Years** |
| **Year – 1** | **Year – 2** | **Year – 3** |
| **1** | **CSOC Management services**  **(The consumables like backup tapes which will be provided by the vendor)** |  |  |  |  |
|  | **a. CSOC Monitoring and Management** |  |  |  |  |
|  | **b. Incident Management Tool** |  |  |  |  |
|  | **c. Backup and Storage services** |  |  |  |  |
|  | **d. Onsite CSOC Resources L1 Onsite Resource - 2 nos** |  |  |  |  |
|  | **e. Onsite CSOC Resources L2 Onsite Resource - 1 nos** |  |  |  |  |
|  | **f.Offsite 24x7 Monitoring Resources – L3** |  |  |  |  |
|  | **g. VAPT charges for 30 devices** |  |  |  |  |
| **2** | **P2P link including network hardware between Bank's CSOC and the Service Provider for remote monitoring**  |  |  |  |  |
| **Total [C]** |  |  |  |  |
| **Taxes & Levies @\_\_\_\_ % [D]** |  |  |  |  |
| **Total CSOC Services cost** **including taxes [B=C+D]** |  |  |  |  |

**Table 3:- Grand Total calculation (Amount in Rupees)**

|  |  |
| --- | --- |
| **Grand Total calculation** | **Cost for each requirement** |
| **CSOC Implementation cost (I)** |  |
| **Net Present Value (NPV) for the CSOC Services cost for 3 years (II)** |  |
|  **GRAND TOTAL (I + II)** |  |

**Note: Bidders are requested to note the following:**

1. **Cost should be inclusive of all taxes.**
2. **TDS will be deducted as per rules applicable.**
3. **The costs should include the training costs also.**
4. **Total Cost of Ownership (TCO) for 03 Years using Net Present Value (NPV) would be calculated as under:**
5. **Net Present Value (NPV) of the yearly cost of resources would be calculated using the Microsoft Excel Worksheet formulae, to arrive at the NPV for three years. The discount rate to be considered for above would be 8.5% per annum.**

**Table 4:- Optional Cost -Main for CSOC (Amount in Rupees)**

 **In the case of optional LI and L2 resources, if required by the Bank will be taken at the cost mentioned in the Table 2:- CSOC Services Cost.**

|  |  |
| --- | --- |
| **Item** | **Cost** **(inclusive of all taxes)** |
| **Cost of the parser for non standard logs and implementing and integrating with the SIEM.**  |  |
| **Optional cost of VAPT for one device** |  |

|  |  |
| --- | --- |
| **Date** | **Signature of Authorised Signatory …** |
| **Place** | **Name of the Authorised Signatory …** |
|  | **Designation …** |
|  | **Name of the Organisation …****Company Seal:** |

# Annexure for Technical Specifications & Others

1. 1.

**Annexure D.1: Security Incident & Event Management (SIEM)**

**Name of the Security tool / solution proposed:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**OEM details:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Whether MAF is submitted (Y/N):\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

| **SL. No.** | **SIEM - Requirement details** | **High Priority (H) Low Priority (L)** | **Compliance****Mention -****Yes / No / Deviation** | **Remarks****(Provide adequate reference to product manuals to substantiate how the product confirms to each requirement.****Mention deviations / workarounds if any)** |
| --- | --- | --- | --- | --- |
|  |  |
|  | **General** |  |  |  |
| **1** |  **The solution should be appliance based.**  | **H** |  |  |
| **2** | **It support log collection, correlation and alerts for the number of devices mentioned in scope.**  | **H** |  |  |
| **3** | **The 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** | **a. The solution should support log collection, correlation and alerts for the number of devices mentioned in scope.** | **H** |  |  |
| **b. The solution should be able to conduct agent less collection of logs except for those which cannot publish native audit logs** | **H** |  |  |
| **5** | **The solution should have connectors to support the listed devices / applications, wherever required the vendor should develop customized connectors for all standard devices at no extra cost** | **H** |  |  |
| **EPS Supported** |
| **6** | **Initial EPS requirement is for 5000. However, the appliance should be scalable up to 10000 EPS.** | **H** |  |  |
| **Log Storage** |
| **7** | **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 based on RAID 5 and have minimum 10000 Disk RPM. The storage solution should have adequate redundancy for handling disk failures.** | **H** |  |  |
| **Log Collection and Management** |
| **8** | **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** |  |  |
| **9** | **The 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** |  |  |
| **10** | **The 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** |  |  |
| **11** |  **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.** | **L** |  |  |
| **12** | **The solution shall allow bandwidth management, rate limiting, at the log collector level.**  | **L** |  |  |
| **13** | **The solution should ensure that the overall load on the network bandwidth at DC, WAN level is minimal** | **L** |  |  |
| **14** | **The solution should provide time based store and forward feature at each log collection point** | **H** |  |  |
| **15** | **The solution should have the capability to compress the logs by at least 70 % for storage optimization.** | **H** |  |  |
| **16** | **It should be possible to store the event data in its original format in the central log storage** | **L** |  |  |
| **17** |  **Traceability of logs shall be maintained from the date of generation to the date of purging.** | **L** |  |  |
| **18** | **The system shall be able to capture all details in raw log, events and alerts and normalize them into a standard format for easy comprehension.** | **H** |  |  |
| **19** | **It should be feasible to extract raw logs from the SIEM and transfer to other systems as and when required.** | **H** |  |  |
| **20** | **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** |  |  |
| **Correlation** |
| **21** | **SIEM must allow the creation of an unlimited number of new correlation rules** | **H** |  |  |
| **22** | **Solution should be able to perform the following correlations (but not limited to): Rule based, Vulnerability based, Statistical based, Historical based, Heuristics based, Behavioral based, Risk based etc.** | **H** |  |  |
| **23** | **The system/solution should have the ability to correlate all the fields in a log** | **H** |  |  |
| **24** | **The solution should be able to parse and correlate multi line logs** | **H** |  |  |
| **25** | **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** |  |  |
| **26** | **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** |  |  |
| **27** | **The central correlation engine database should be updated with real time security intelligence updates from OEM** | **H** |  |  |
| **Dashboard and Reporting** |
| **28** | **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** |  |  |
| **29** | **Events should be presented in a manner that is independent of device specific syntax and easy to understand for all users** | **H** |  |  |
| **30** | **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)**  | **L** |  |  |
| **31** | **It should be possible to categorize events while archiving for example , events for network devices, antivirus, servers etc.** | **L** |  |  |
| **32** | **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** |  |  |
| **33** | **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** |  |  |
| **34** | **The Dashboard design for the solution should be editable on an ad hoc basis as per the individual user need** | **L** |  |  |
| **35** | **The system should display all real time events. The solution should have drill down functionality to view individual events from the dashboard** | **H** |  |  |
| **36** | **The solution should allow applying filters and sorting to query results.** | **H** |  |  |
| **37** | **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** |  |  |
| **38** | **The solution should provide event playback for forensic analysis.**  | **L** |  |  |
| **39** | **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** |  |  |
| **40** | **Should provide summary of log stoppage alerts and automatic suppression of alerts.** | **H** |  |  |
| **41** | **Should generate e-mail and SMS notifications for all critical/high risk alerts triggered from SIEM**  | **H** |  |  |
| **42** | **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** |  |  |
| **43** | **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** |  |  |
| **44** | **Solution should provide knowledge base and best practices for various security vulnerabilities** | **L** |  |  |
| **45** | **Dashboard should display asset list and capture details including name, location, owner, value, business unit, IP address, platform details** | **H** |  |  |
| **46** | **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** |  |  |
| **47** | **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** | **H** |  |  |
| **48** | **Dashboard should support different views relevant for different stake holders including top management, operations team, Information Security Department** | **H** |  |  |
| **49** | **Dashboard should support export of data to multiple formats including CSV, XML, Excel, PDF formats etc** | **H** |  |  |
| **50** | **Dashboard views should be customizable as per user rights and access to individual components of the application.** | **H** |  |  |
| **51** | **Administrators should be able to view correlated events, packet level event details, real-time raw logs and historical events through the dashboard.** | **L** |  |  |
| **52** | **Senior Management should be able to view compliance to SLA for all CSOC operations** | **L** |  |  |
| **53** | **The system should permit setting up geographical maps/images on real time dashboards to identify impacted areas and sources of alerts.** | **L** |  |  |
| **54** | **The solution should have the capability to identify / remember frequently used queries and provide means for optimization of queries.** | **L** |  |  |
| **55** | **Solution should have the ability to perform free text searches for events, incidents, rules and other parameters.** | **L** |  |  |
| **56** | **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** |  |  |
| **Event and Incident Management** |
| **57** | **The system should identify the originating system and user details while capturing event data.** | **H** |  |  |
| **58** | **It should be possible to automatically create incidents, raise tickets and track their closure with respective alerts to the supporting/ help desk personnel** | **H** |  |  |
| **59** | **The event should reach the CSOC monitoring team within 1 minute of the log being captured** | **H** |  |  |
| **60** | **Pre-defined / custom parsers are available for parsing logs for the following applications:FinacleFlexcube Bancs** | **L** |  |  |
| **61** | **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** |  |  |
| **Storage** |
| **62** | **The vendor should provide for adequate storage to meet the EPS and retention requirements of the bank. SI 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** |  |  |
| **63** | **The solution should be able to store both normalized and RAW logs** | **H** |  |  |
| **64** | **The platform should provide tiered storage for the online, archival, and backup and restoration of event log information.** | **H** |  |  |
| **65** | **The Tier I and II storage should have the capability to authenticate logs on the basis of time, integrity and Origin** | **L** |  |  |
| **66** | **The storage solution should have the capability to encrypt/hash the logs in storage** | **H** |  |  |
| **67** | **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** |  |  |
| **68** | **Solution should be capable of retrieving the archived logs for analysis, correlation and reporting purpose automatically for any past time duration selected.** | **L** |  |  |
| **69** | **Should be able to part and filter logs before storage on the basis of type of logs; date etc** | **L** |  |  |
| **70** | **Solution should be capable to replicate logs in Synchronous as well as Asynchronous mode.** | **H** |  |  |
| **71** | **It should be possible to define purging and retention rules for log storage.** | **H** |  |  |
| **72** | **The solution should come with built-in functionality for archiving data.** | **L** |  |  |
| **Integration** |
| **73** | **Integrate with IPS, IDS, Firewall, Proxy, NAC etc. to identify network security issues** | **H** |  |  |
| **74** | **Integrate with DLP solutions to identify misuse of sensitive information** | **H** |  |  |
| **75** | **Integrate with PIM and other Directory solution to relate security events to user activities** | **H** |  |  |
| **76** | **Integration with Vulnerability Assessment tools to identify security events** | **H** |  |  |
| **77** | **Integrate with GRC solution to capture compliance against security policies** | **H** |  |  |
| **78** | **Should be able to integrate with physical access control systems.** | **L** |  |  |
| **79** | **Integrate with existing helpdesk/ incident management tools** | **H** |  |  |
| **80** | **Should be able to integrate with bank's existing backup solution for performing backup of the SIEM.** | **L** |  |  |
| **81** | **Should be able to integrate with Core Banking solution, RTGS/NEFT etc. and address the use cases mentioned in the RFP at a minimum.** | **L** |  |  |
| **82** | **Connector Development tool/SDK availability for developing collection mechanism for home-grown or any other unsupported applications** | **H** |  |  |
| **83** | **The system should have out of the box rules for listed IDS/IPS, firewalls routers, switches, VPN devices, antivirus, operating systems, Databases and standard applications etc.** | **H** |  |  |
| **Availability** |
| **84** | **The SI should prepare a DR plan for switch over in case the DC operations are down** | **H** |  |  |
| **85** | **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 ispermissible even in case of collector failure.** | **H** |  |  |
| **Scalability** |
| **86** | **The solution should be scalable as per bank roadmap for expansion** | **H** |  |  |
| **87** | **Solution should support integration with big data storage configuration such as Hadoop etc** | **L** |  |  |
| **88** | **The solution should support creation of incident management workflows to track incident from creation to closure, provide reports on pending incidents and permit upload of related evidences such as screenshots etc at the Incident management tool manually.** | **H** |  |  |
| **89** | **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.**  | **L** |  |  |
| **90** | **Solution should be preferably appliance based solution** | **L** |  |  |
| **Platform /Hardware /Software** |
| **91** | **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** |  |  |
| **Location Independence** |
| **92** | **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 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** |
| **93** | **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** |
| **94** | **Any Log parsing activities should not alter the raw log in any format.** | **H** |  |  |
| **Log retention Period** |
| **95** | **The proposed system must provide support for defining different retention periods for different devices** | **L** |  |  |
| **Notification** |
| **96** | **The system must provide target device notification if target device is down or no longer sending/ receiving events.** | **H** |  |  |
| **Tamper Proof Logging** |
| **97** | **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** |  |  |
| **98** | **Once the log is written to the storage it should not be modifiable. It should have proper mechanisms to prevent log tampering.** | **H** |  |  |
| **Co-relation Methods** |
| **99** | **The system should support the following types of correlation:****a) Rule-Based Correlation****b) Vulnerability Based Correlation****c) Statistical Based** | **H** |  |  |
| **Co-Relation Rules** |
| **100** | **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.** | **L** |  |  |
| **Standards Compliance** |
| **101** | **The solution should include compliance reports for standard - ISO 27001. The solution should also generate reports for these standards.** | **H** |  |  |
| **Updates and Upgrades** |
| **102** | **All the updates and upgrades to SIEM reports should be included with the solution** | **L** |  |  |
| **Vulnerability Updates** |
| **103** | **The offered solution should include vulnerability details with updates from a known vulnerability database like NVD (National Vulnerability Database) or similar databases.** | **H** |  |  |
| **Dashboard** |
| **104** | **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** |  |  |
| **Watch list** |
| **105** | **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** |  |  |
| **Audit Trail** |
| **106** | **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** |  |  |
| **Reporting** |
| **107** | **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.** | **L** |  |  |
| **108** | **The proposed system should have the capability to provide detailed analysis of security incidents occurred and recorded by the system.** | **H** |  |  |
| **109** | **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.** | **L** |  |  |
| **110** | **The offered solution shall include reports for, but not limited to the devices mentioned in Implementation for the listed devices in Annexure** | **L** |  |  |
| **111** | **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.** | **L** |  |  |
| **112** | **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** |  |  |
| **113** | **SIEM tool should be running 24\*7\*365 for monitoring of the devices/ servers** | **H** |  |  |
|  | **Incident Management and Ticketing Tool**  |  |  |  |
| **114** | **The bidder has to provide an incident management and integrate with ticketing tool to generate automated tickets for the alert events generated by the SIEM and other proposed tools.** | **H** |  |  |
| **115** | **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** |  |  |
| **116** | **The tool should facilitate time/ event based automated escalation of tickets as per the escalation matrix defined by the Bank** | **H** |  |  |
| **117** | **Bidder needs to provide ticketing tool like Remedy, Jira or Solar Winds as part of this RFP**  | **H** |  |  |
| **118** | **The tool should be web based online portal available over desktop**  | **H** |  |  |
| **119** | **Apart from CSOC team, the ticketing 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** |  |  |
| **120** | **Access also needs to be provided to Bank‘s CISO and other identified individuals for monitoring purpose.** | **H** |  |  |
| **121** | **Bidder needs to provide ticketing tool for at-least 50 users** | **H** |  |  |
| **122** | **In case any hardware or additional support required for ticketing tool, the same will be provided by bidder as part of delivery** | **H** |  |  |
| **123** | **The vendor should have a local depot in India for support for faster replacements.** | **H** |  |  |

**Annexure D.2: Privilege Identity Management (PIM)**

**Name of the Security tool / solution proposed:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**OEM details:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Whether MAF is submitted (Y/N):\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

| **A** | **PIM - Requirements** | **Compliance (Y/N)** | **Vendor comments if any** |
| --- | --- | --- | --- |
| **1** | **Single - Sign On and Authentication Models The solution should be able to create seamless single sign-on for various technologies such as Operating Systems, Databases, Network and Security Devices.** |  |  |
| **2** | **The solution should have a Generic Target System Connectors to enable one to uses this connector for non-standard devices etc** |  |  |
| **3** | **The solution should be agent less, So no agent will be deploy on target devices.** |  |  |
| **4** | **The solution should support direct connections to windows, ssh, databases and other managed devices without having to use a jump server.** |  |  |
| **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.** |  |  |
| **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** |  |  |
| **7** | **The solution should also provide local authentication and all the security features as per best standards.** |  |  |
| **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.** |  |  |
| **9** | **The solution should provide multi-tenancy feature whereby the entire operations can be carried out within a tenant or line of business.** |  |  |
| **10** | **The solution should provide multi-domain feature whereby the entire operations can operate in an distributed environment** |  |  |
| **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** |  |  |
| **12** | **The solution should be in Leaders/Challengers as per Gartner Magic quadrant OR****Leaders/Strong performers as per Forrester Wave in the latest/current report** |  |  |
| **13** | **The solution should be implemented in atleast five Banks apart from co -operative banks and Insurance** |  |  |
| **B** | **Shared Account Password Management** |  |  |
| **14** | **The solution should set password options every x days, months, years and compliance options via the use of a policy** |  |  |
| **15** | **Ability to create exception policies for selected systems, applications and devices** |  |  |
| **16** | **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.** |  |  |
| **17** | **Flexibility that allows exclusivity for password retrieval or multiple users checking out the same password for the same device in the same time period.** |  |  |
| **18** | **All locally stored target-account passwords should encrypted using AES or similar encryption with at least 256 bit keys.**  |  |  |
| **19** | **The solution should have the ability to reconcile passwords manually, upon demand** |  |  |
| **20** | **The tool allows secure printing of passwords in Pin Mailers. Lifecycle of printing and labeling of envelopes should be part of the module.**  |  |  |
| **21** | **The solution should be able to control re-prints with adequate authorization** |  |  |
| **22** | **The proposed solution should restrict the solution administrators from accessing or viewing passwords or approve password requests** |  |  |
| **23** | **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** |  |  |
| **C** | **Access Control** |  |  |
| **24** | **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.** |  |  |
| **25** | **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** |  |  |
| **26** | **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.** |  |  |
| **27** | **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.** |  |  |
| **28** | **The solution should provide for inbuilt database management utility to enable granular control on database access for Sql, my Sql, DB2, Oracle etc.** |  |  |
| **29** | **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.** |  |  |
| **30** | **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.**  |  |  |
| **31** | **System should be able to define critical commands for alerting & monitoring purpose and also ensure user confirmation (YES or NO) for critical commands over SSH.** |  |  |
| **D** | **Privileged Session Management and Log Management** |  |  |
| **32** | **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.**  |  |  |
| **33** | **The solution should be able to log commands for all commands fired over SSH Session and for database access through ssh, sql+**  |  |  |
| **34** | **The solution should be able to log/search text commands for all sessions of database even through the third party utilities** |  |  |
| **35** | **The solution should be able to log/search text commands for all sessions on RDP** |  |  |
| **36** | **All logs created by the solution should be tamper proof and should have legal hold** |  |  |
| **37** | **The solution logs 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 tool can generate — on-demand or according to an administrator-defined schedule — reports showing user activity filtered by an administrator, end user or user group.** |  |  |
| **38** | **The tool can restrict access to different reports by administrator, group or role.** |  |  |
| **39** | **The tool generates reports in at least the following formats: HTML, CSV and PDF** |  |  |
| **40** | **System should be able to define critical commands for alerting & monitoring purpose through SMS or Email alerts** |  |  |
| **41** | **The solution should provide separate logs for commands and session recordings. Session recordings should be available in image/ video based formats** |  |  |
| **42** | **The session recording should be SMART to help jump to the right session through the text logs** |  |  |
| **43** | **Secure and tamper-proof storage for audit records, policies, entitlements, privileged credentials, recordings etc.**  |  |  |
| **44** | **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.**  |  |  |
| **E** | **PIM Security** |  |  |
| **45** | **The solutions should use minimum FIPS 140-2 validated cryptography for all data encryption.** |  |  |
| **46** | **The Solution should be TLS 1.2 and SHA-2 compliant for PCI-DSS compliance** |  |  |
| **47** | **All communication between system components, including components residing on the same server should be encrypted.**  |  |  |
| **48** | **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)** |  |  |
| **49** | **The Administrator user cannot see the data (passwords) that are controlled by the solution.**  |  |  |
| **50** | **The solution should secure master data, records, entitlement, policy data and other credentials in tamper proof storage container.**  |  |  |
| **F** | **PIM Administration** |  |  |
| **51** | **The solution should have central administration web based console for unified administration.**  |  |  |
| **52** | **The tool uses Active Directory/LDAP as an identity store for administrators and end users.** |  |  |
| **53** | **Administrative configurations (e.g. configuration of user matrix) shall be accessible via a separate client where client access is controlled by IP address.**  |  |  |
| **54** | **Important configuration changes in the solutions (example changes to masters) should be based on at least 5 level workflow approval process and logged accordingly** |  |  |
| **55** | **Segregation of Duties - The Administrator user cannot view the data (passwords) that are controlled by other teams/working groups (UNIX, Oracle etc.).** |  |  |
| **56** | **The solution should provide for self-service portal for users and devices for ease of on boarding both users and devices.** |  |  |
| **57** | **All administrative task should be done LOB wise i.e. Line of Business Wise** |  |  |
| **G** | **System Architecture** |  |  |
| **58** | **The solution architecture should be highly scalable both vertically as well as horizontally.** |  |  |
| **59** | **The proposed solution shall provide multi-tier architecture where the database and application level is separated.**  |  |  |
| **60** | **The solution should work at the network layer instead through a jump server. This will have achieve large number of sessions.** |  |  |
| **61** | **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.**  |  |  |
| **62** | **The proposed solution shall have the ability to support multiple mirrored systems at offsite Disaster Recovery Facilities across different data center locations.**  |  |  |
| **63** | **The proposed solution shall have built-in options for backup or integration with existing backup solutions**  |  |  |
| **64** | **The proposed solution shall handle loss of connectivity to the centralized password management solution automatically.**  |  |  |
| **65** | **The proposed solution shall not require any network topology changes in order to ensure all privileged sessions are controlled by the solution.**  |  |  |
| **66** | **The proposed solution shall support distributed network architecture where different segments need to be supported from a central location.**  |  |  |
| **67** | **The proposed solution shall support both client based (in the case where browser is not available) as well as browser based administration** |  |  |
| **68** | **The proposed solution should be 100% agentless that includes password storage, password management and session recording features.**  |  |  |
| **69** | **The solution must support parallel execution of password resets for multiple concurrent requests.** |  |  |
| **70** | **The solution if required should be available to install on a virtual sever** |  |  |
| **71** | **The system should be highly available (24x7x365) and redundant from a hardware failure, application failure, data failure, and or catastrophic failure. Please elaborate** |  |  |
| **72** | **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** |  |  |
| **73** | **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.** |  |  |
| **74** | **Ability to integrate with Bio-Metric Solutions** |  |  |
| **K** | **Application Password Management (Hard-Coded Password Management)** |  |  |
| **75** | **The solution should have an ability to eliminate, manage and protect privileged credentials in applications, scripts, configuration files etc.** |  |  |
| **76** | **The solution should be able to authenticate and trust the application requesting the privileged password based on various authentication methods** |  |  |
| **77** | **Application Servers Support - The product should support removing static hard coded passwords from Data Sources in Application Servers. Please elaborate.**  |  |  |
| **L** | **Auto Discovery of Privileged Accounts** |  |  |
| **78** | **The solution should be able to perform auto discovery of privileged accounts on target systems and perform two way reconciliation.**  |  |  |
| **79** | **Ability to quickly identify all non-built-in local administrator accounts in your environment (flag possible 'backdoor' accounts)**  |  |  |
| **80** | **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** |  |  |
| **M** | **Notification Engine**  |  |  |
| **81** | **The solution should have capability to provide alerts and notification for critical PIM events over SMS & Email** |  |  |
| **82** | **The solution should have capability to provide alerts and notification for all administration/configuration activities over SMS & Email** |  |  |
| **83** | **Customizable notification for command executed on SSH and Telnet based devices** |  |  |
| **84** | **Customizable notification for command/Process executed on Windows** |  |  |
| **85** | **Notification on target being access on criteria like Line of Business or Groups** |  |  |
| **N** | **Solution Workflow** |  |  |
| **86** | **The solution should have inbuilt workflow to manage** |  |  |
| **87** | **Electronic Approval based Password Retrieval** |  |  |
| **88** | **Onetime access / Time Based / Permanent Access** |  |  |
| **89** | **5 level approval workflow with E-mail and SMS notification with delegation rules** |  |  |
| **90** | **Ability to provide for delegation at all levels in the workflow** |  |  |
| **91** | **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** |  |  |
| **92** | **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).**  |  |  |
| **93** | **Supports a workflow approval process that requires approvers to be in sequence before final approval is granted.**  |  |  |
| **94** | **Ability to log workflow processes and/or have the ability to be reported or audited.**  |  |  |
| **O** | **Dashboard & Reporting &Built-in Ticketing system** |  |  |
| **95** | **Dashboard Capabilities should include real-time view of activities performed by the administrators** |  |  |
| **96** | **The solution should have ability to report on all system administrative changes performed by PIM Administrators with relevant auditable records** |  |  |
| **97** | **Proposed solution should have its own built in ticketing systems** |  |  |
| **98** | **The vendor should have a local depot in India for support for faster replacements.** |  |  |
| **99** | **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.** |  |  |

**Annexure D.3: Anti APT (Advanced Persistent Threat)**

**Name of the Security tool / solution proposed:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**OEM details:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Whether MAF is submitted (Y/N):\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

| **Sr. No.** | **Anti APT :- Functional Description** | **Compliance (Y/N)** | **Vendor comments if any** |
| --- | --- | --- | --- |
|  | **General Specs** |  |  |
| **1** | **Proposed solution should have breach detection rate of more than 99.5% as per NSS lab Breach Detection Systems test report & the test report should be submitted** |  |  |
| **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.** |  |  |
| **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.** |  |  |
| **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**  |  |  |
| **5** | **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. Bank reserves the option of using deployment as Inline or out-of-band.** |  |  |
| **6** | **Proposed Anti-APT solution should perform advanced network detection and analysis of the enterprise's internal network. Upon detection of the threat, the proposed solution should be able to perform behaviour analysis for advance threats.** |  |  |
| **7** | **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.** |  |  |
| **8** | **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.** |  |  |
| **9** | **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.** |  |  |
| **10** | **The proposed solution should be able to store packet captures (PCAP) of all Malicious communications detected by sandbox.** |  |  |
| **11** | **The proposed solution should be able to support XFF (X-Forwarded-For) to identify the IP Address of a host in a proxy environment.** |  |  |
| **12** | **Solution should be able to integrate with its own threat intelligence portal for further investigation, understanding and remediation of an attack.** |  |  |
| **13** | **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.**  |  |  |
| **14** | **The Proposed solution should be able to detect and block communications to known command and control servers, detect reputation of URL being accessed.** |  |  |
| **15** | **The proposed solution should be able to identify and help understand the severity and stage of each attack.** |  |  |
| **16** | **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.** |  |  |
| **17** | **The Proposed solution must provide a web service interface/API for customer to customize integration.** |  |  |
| **18** | **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.** |  |  |
| **19** | **The solution should support SIEM integration using varied methods like open standards/API/Syslog/CEF/LEEF etc.** |  |  |
|  | **Detection and Analysis** |  |  |
| **20**  | **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 behaviour** |  | **.** |
| **21** | **Solution must have the capability to analyse large files, Must be able to support minimum 100MB file size.** |  |  |
| **22** | **The proposed solution should have grayware detection capabilities and should detect network Attacks and Exploits.** |  |  |
| **23** | **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** |  |  |
| **24** | **The proposed solution must provide the capability to export network packet files and encrypted suspicious files for further investigation.** |  |  |
| **25** | **The proposed solution have the capability to performs tracking and analysis of virus downloads and suspicious files.** |  |  |
| **26** | **The proposed solution should support exporting of analysis results such as C&C server IP and malicious domain listing.** |  |  |
| **27** | **The proposed solution should have capabilities to scan inside archives.** |  |  |
| **28** | **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.** |  |  |
| **29** | **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.** |  |  |
| **30** | **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.** |  |  |
| **31** | **The proposed solution should be able to correlate local APT attacks with Global historical APT attacks.** |  |  |
| **32** | **The proposed solution should have usable storage of 2 TB and support at least 6 Ethernet Interfaces** |  |  |
| **33** | **The proposed solution should have capability to detect attacker behaviour using the full-featured Network Behaviour Analysis (NBA) capability of the solution with the same appliance to detect threats emerging from inside the network. This includes the capability to establish “normal” traffic baselines through flow analysis techniques and the ability to detect and alert Bank's administrators on any deviations from normal baselines.** |  |  |
| **34** | **The Proposed solution for Email Anti-APT should be deployable in inline mode as MTA.** |  |  |
| **35** | **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.** |  |  |
| **36** | **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** |  |  |
| **37** | **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,** |  |  |
| **38** | **The Proposed solution should be able to Identify suspicious embedded object in document file like OLE, Macro extraction, Shell code & exploit matching.** |  |  |
| **39** | **The Proposed solution should be able to detect malicious zero day attacks by leveraging behaviour analysis and built in NBA capabilities onto the system.** |  |  |
| **40** | **The proposed solution should be able to detect and take action if file has suspicious attributes like True-file type & Naming trick.** |  |  |
| **41** | **The proposed Anti-APT solution should have the capability to get integrated with NAC solution and upon seeing a specific bad file like (.exe .pdf) trigger an action to contain the host and put it onto a remediation workflow.** |  |  |
|  | **Reporting** |  |  |
| **42** | **The proposed solution should have an intuitive Dashboard that offers real time threat visibility and attack characteristics.** |  |  |
| **43** | **The proposed solution should provide reports with (but not limited to) HTML/CSV/PDF formats.** |  |  |
| **44** | **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).** |  |  |
| **45** | **The proposed solution should support logging of important parameters like Source IP, Destination IP, ports, protocol, Domain, time stamp etc. of the attacks sessions.** |  |  |
| **46** | **The proposed solution should have the flexibility to provide customizable dashboard.** |  |  |
| **47** | **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.**  |  |  |
| **48** | **The proposed solution should be able to provide in-depth reporting including the level of risk, sandbox assessment, and network activity analysis.** |  |  |
| **49** | **The proposed solution must be able to provide intelligence portal for malware information, threat profile, source, destination, &user where applicable.** |  |  |
| **50** | **The Proposed solution should be able to generate out of box reports to highlight Infections, C&C behaviour, Lateral Movement, Asset and data discovery.** |  |  |
| **51** | **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.** |  |  |
| **52** | **The proposed solution shall support Local Password & Radius for authentication schemes** |  |  |
| **53** | **The proposed solution shall support Remote administration using SSH/HTTPS.** |  |  |
| **54** | **The proposed solution shall support CLI, GUI/Web based Administration Console.** |  |  |
| **55** | **Server security solution should support virtual patching for both known and unknown vulnerabilities until the next scheduled maintenance window.** |  | **.** |
| **56** | **The proposed Sandbox shall also be capable of analysing URLs.** |  |  |
| **57** | **The vendor should have a local depot in India for support for faster replacements.** |  |  |
| **58** | **Solution should address known/unknown malwares using multi layered security methodology and should not be only dependent on Sandboxing.** |  |  |
| **59** | **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.This ensures not every file is sandboxed before user delivery. AS per RBI Cyber Security Guideline suggestion on Controlling use of Macros.** |  |  |
| **60** | **In case of non-availability of proposed APT solution at DC, production should not be impacted.**  |  |  |

**Annexure D.4: Firewall Analyzer**

**Name of the Security tool / solution proposed:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**OEM details:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Whether MAF is submitted (Y/N):\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

| **Sr. No** | **Firewall Analyzer:- Features and Must to have Requirements** | **Status (Yes/No)** |
| --- | --- | --- |
|  | **OEM's to provide the relevant documentation supporting below requirements** |  |
| **1** | **Product should support all the major Firewall and devices such as Juniper, Cisco, PaloAlto, Checkpoint, Forcepoint, and Fortinet.** |  |
| **2** | **Product OEM should have its fully owned regional support center in India. OEM to confirm the same in writing with complete address for verification.** |  |
| **3** | **OEM to submit minimum 2 references from public sector Banks/Financial institution where the proposed product have been Implemented successfully. End user Email ID and contact details to be shared.** |  |
| **4** | **Proposed solution should conduct risk analysis by analyzing all possible traffic passing through the Firewalls** |  |
| **5** | **It should have risk identification capability for the traffic passing from non-secured to secured Zones enforcing strong network segmentation** |  |
| **6** | **Solution should support application based Risk analysis for Next Generation Firewalls** |  |
| **7** | **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** |
| **8** | **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** |
| **9** | **Solution should provide information on Rule Reordering - with Actionable reordering recommendation and also the expected improvements after reordering the rules** |  |
| **10** | **Solution should provide information on both un-attached and unused objects** |  |
| **11** | **Solution should specifically suggest consolidation of Firewall rule sets for optimizing the rules for better manageability, audit and performance** |  |
| **12** | **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.** |  |
| **13** | **Solution should generate enterprise-wide interactive network map based on the routing information and topology of the added devices** |  |
| **14** | **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** |  |
| **15** | **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** |  |
| **16** | **From a scalability and best practices perspective below requirements are to be met and mandatory in the proposed solution -** |  |
| **17** | **Solution should have a change management capability and should support Bulk change request submission through Excel file** |  |
| **18** | **Solution should Auto-detect, and respond to FW Change Requests where the traffic is already allowed based on source, destination and service details** |  |
| **19** | **Solution should Allow change planning through a simulation of traffic path and find all the rules in all the firewalls that block requested traffic** |  |
| **20** | **Automatically compute and push policies on Cisco IOS Routers** |  |
| **21** | **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** |  |
| **22** | **The proposed solution should automatically detect violations of regulatory requirements introduced by Change Request before implementing on the Firewalls.** |  |
| **23** | **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** |  |
| **24** | **The proposed change management 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.** |  |
| **25** | **The change management 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.** |  |
| **26** | **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** |  |
| **27** | **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** |  |
| **28** | **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** |  |
| **29** | **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.** |  |
| **30** | **Solution should identify Blocked and allowed flows from an application perspective to enable application team to collaborate with the operations team.** |  |
| **31** | **Solution should present Firewalls/Routers that intercepts the application flow** |  |
| **32** | **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.** |  |
| **33** | **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.** |  |
| **34** | **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.** |  |
| **35** | **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.** |  |
| **36** | **The vendor should have a local depot in India for support for faster replacements.** |  |

**Annexure D.5: Network Access Control (NAC)**

**Name of the Security tool / solution proposed:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**OEM details:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Whether MAF is submitted (Y/N):\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

| **Sr No** | **Network Access Control** | **High Priority (H)****Low Priority (L)** | **Compliance****Yes /****No** | **Remarks. Please provide adequate reference to product manuals/ documentation to substantiate how the product confirms to each requirement.** |
| --- | --- | --- | --- | --- |
| **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: Device type,** | **H** |  |  |
| **a)       Operating system,** |
| **b)       User identity,** |
| **c)       Operating system,** |
| **d)       Patch status,** |
| **e)       Anti-virus status,** |
| **f)        Host firewall status,** |
| **g)       Known/Unknown device status,** |
| **h)       Past policy compliance and threat history,** |
| **i)         Wired/Wireless connection,** |
| **j)         Windows registry settings** |
| **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 identify iPads that are owned by the Bank, and block other iPads** | **H** |  |  |
| **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:** | **H** |  |  |
|  **VLAN Steering, DHCP, Anti ARP spoofing, Agent based enforcement, Mac Authentication etc.** |
| **15** | **The solution should capture audit logs that contain the following 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 solution should be able detect and manage hand held devices used for financial inclusion process** | **L** |  |  |
| **25** | **From time to time Bank gets indicators of compromise (IOC's) from the external sources. Therefore the solution should provide IOC scanning to discover and mitigate threats from infected endpoints.** | **L** |  |  |
| **26** | **The solution should support non-disruptive, out-of-band deployment with built-in configuration wizards and customizable policy templates for rapid time-to-value.** | **L** |  |  |
| **27** | **In case of non-availability of proposed NAC solution at DC,end users across all locations should be able to login to the network without any issues.** | **H** |  |  |

**Annexure D.6: VAPT Advisory & Remediation Services**

|  |  |  |  |
| --- | --- | --- | --- |
| **Sr No** | **VAS** | **Compliance (Yes/No)** | **Remarks****(Please provide adequate reference to product manuals / documentation to substantiate how the product conforms to each requirement)** |
|  |  **VAPT service**  |  |  |
| **1** | **Should perform a targeted scan (i.e. check for a specific set of vulnerabilities or IP Addresses).** |  |  |
| **2** | **Should provide info on applications running on non-standard ports.** |  |  |
| **3** | **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.** |  |  |
| **4** | **Should scan workstation, servers, network and security equipment and other devices such as printers, mobiles, webcams, tablets etc.** |  |  |
| **5** | **Should authenticated and unauthenticated scans** |  |  |
| **6** | **Should scan application databases for vulnerabilities** |  |  |
| **7** | **Should detect weak password for databases and point out accounts with simple, weak and shared passwords.** |  |  |
| **8** | **Should identify out-of-date software versions, applicable patches and system upgrades.** |  |  |
| **9** | **Should provide remediation information in the reports including links to patches etc.** |  |  |
| **10** | **Should produce a report listing all applications on a host or network, regardless of whether the application is vulnerable**  |  |  |
| **11** | **Should generate report in line with RBI, PCI DSS and ISO 27001 Guidelines** |  |  |
| **12** | **Should produce reports in the following formats: XLS, PDF, CSV, XML etc.** |  |  |

**Annexure D.7: Indicative List of hardware / network / security devices**

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

| **Sr No** | **List of network and security devices** | **Make** | **Quantity** |
| --- | --- | --- | --- |
| **A.** | **Data Center** |
| **1** | **Network Switch (L2/L3)** | **Cisco / HP** | **19** |
| **2** | **Firewall**  | **Checkpoint / Fortigate** | **6** |
| **3** | **Checkpoint Firewall Management Server** | **Dell** | **1** |
| **4** | **Fortigate Log Collector** | **Fortigate** | **1** |
| **5** | **Network Intrusion Prevention System** | **Cisco** | **2** |
| **6** | **IPS Management Server** | **Virtual Machine** | **1** |
| **7** | **Web Gateway Security** | **Bluecoat** | **2** |
| **8** | **BlueCoat Management and Reporting Server** | **Dell** | **1** |
| **9** | **Link Load Balancer** | **Radware** | **2** |
| **10** | **Router (WAN)** | **Cisco / Juniper** | **13** |
| **B.** | **DR Site** |
| **1** | **Network Switch (L2/L3)** | **HP / Cisco** | **11** |
| **2** | **Firewall- Perimeter** | **Checkpoint / Fortigate** | **4** |
| **3** | **Fortigate Log Collector** | **Fortigate** | **1** |
| **4** | **Web Gateway Security** | **Bluecoat** | **2** |
| **5** | **Router (WAN)** | **Cisco / Juniper** | **6** |

| **Sr** **No** | **No of Windows and Linux servers** | **Quantity** |
| --- | --- | --- |
| **A.** | **Data Center** |  |
| **1** | **Windows Servers (all versions)** | **46** |
| **2** | **Linux Servers (all flavours)** | **27** |
| **B.** | **DR Site** |  |
| **1** | **Windows Servers (all versions)** | **5** |
| **2** | **Linux Servers (all flavours)** | **8** |

**The asset list given above in this section  is an indicative list and the vendor 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 D.8: Non-disclosure Agreement**

 **(Sample Format - TO BE EXECUTED ON A NON-JUDICIAL STAMPED PAPER of Rs100/-)**

**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 400/2018/1279/BYO/RiMV dated November 06, 2017 for Small Industries Development Bank of India, having its registered office ………………………………………., 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.**

**Authorised Signatory**

**Name:**

**Designation:**

**Office Seal:**

**Annexure D.9: Performance Bank Guarantee**

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

**BANK GUARANTEE**

**Small Industries Development Bank of India**

**SIDBI Tower**

**15, Ashok Marg**

**Lucknow - 226001**

**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 authorising 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, which ever 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 .........................2017 .**

**SIGNED, SEALED AND DELIVERED.**

**BY**

**AT**

**IN THE PRESENCE OF WITNESS :**

**1. Name ..........................**

**Signature.....................**

**Designation..................**

**2. Name .............................**

**Signature.........................**

**Designation.....................**

**End of Document**