Bank of Maharashtra

(One Family… One Bank… Mahabank)

REQUEST FOR PROPOSAL

FOR

IMPLEMENTATION AND MAINTENANCE OF CYBER SECURITY OPERATIONS CENTRE (C-SOC) ON CAPTIVE MODEL

TENDER REFERENCE # 052017

बैंक ऑफ महाराष्ट्र
Bank of Maharashtra
ONE FAMILY ONE BANK

Head Office, 'LOKMANGAL'
1501, Shivaji Nagar, Pune – 411 005

Cost of Tender Document: Rs.25,000/-

Important Clarifications:

Following terms are used in the document interchangeably to mean:

1. Bank means ' Bank of Maharashtra'
2. Bidder means the respondent to the RFP document.
3. RFP means the Request for Proposal document
4. DC means Data Center, DR / DRC/ DRS means Disaster Recovery Site
5. CSOC means Cyber Security Operations Center…
6. SIEM means Security Information and Event Management……
7. Collector means the device that collects the logs from the security devices in raw format, and forwards the same to the SIEM solution database by applying necessary filters, if configured to do so.
8. CBS means Core Banking Solution implemented in the Bank
9. Bidder and Bank shall be individually referred to as 'Party' and collectively as 'Parties'.
10. APT means Advanced Persistent Threat
11. PIM means Privilege Identity Management
12. FIM means File Integrity Monitoring
13. TTP means Tactics, Techniques and Procedures.
14. Bidder / Respondent – signifies those who purchase this tender document and submits response to it..
15. SMTP means Simple Mail Transfer Protocol
16. IDS/ IPS means Intrusion Detection System/ Intrusion Prevention System
17. OEM means Original Equipment Manufacturer.
18. SOCDesk means infrastructure to monitor CSOC operations through Dashboards on 24X7 basis.

Contents

1. Invitation to the Tender

Tender for the Implementation and Maintenance of Cyber Security Operation Centre (CSOC) on Captive Model

This is to inform that Bank of Maharashtra (BoM) intends to implement Cyber Security Operation Centre (CSOC) on Captive Model. This would cover the phases from supply, installation, commissioning, Integration, Implementation and maintenance of the proposed CSOC along with other services, training and documentation as specified by the Bank.

act

The bidders are expected to examine all instructions, forms, terms, BoM project requirements and other information in the RFP documents. Failure to furnish all information required as per the RFP document or submission of a proposal not substantially responsive to the RFP document in every respect will be at the Bidder's risk and may result in rejection of its Proposal and forfeiture of the Bid Earnest Money Deposit. .

A complete set of tender documents may be purchased by eligible bidder upon payment of a non-refundable fee, mentioned in the important information regarding bid submission, by demand draft / banker's cheque in favour of Bank of Maharashtra and payable at Pune.

Important information regarding Bid submission

Tender Reference	**052017**
Price of Tender copy	**Rs. 25,000 /- (Non Refundable)**
Date of commencement of issue of tender document	**02.08.2017**
Date of closure of tender document	**23.08.2017 up to 14:00 hours**
Bid Security Deposit (EMD) – See Section 7.3	**Rs. 25,00,000/- (Rupees Twenty Five Lacs Only)**
Queries to be mailed by	**09.08.2017**
Pre Bid Meeting	**11.08.2017 at 11:00 hours**
Last Date and Time for receipt of tender offers	**23.08.2017 up to 14:00 hours**
Date of opening of technical bids	**23.08.2017 at 16.00 hours**
Address of Communication	Deputy General Manager Information Technology Bank of Maharashtra,

	IT Department, Head Office, "Lokmangal" 1501, Shivajinagar PUNE – 411 005.
Contact Telephone Numbers	***(020) 25536051 / 25520708 / 25532731- 35***
Fax No.	***(020) 2552 1568***
E-mail Id	***agmitprocurement@mahabank.co.in*** ***sachin.shintre@mahabank.co.in***
Website	www.bankofmaharashtra.in

The copy of RFP document may be obtained during office hours on aforesaid working days in person by paying an amount of **Rs.25,000/- (Non Refundable)** by way of Demand Draft / Pay Order favoring "BANK OF MAHARASHTRA" payable at Pune.
The Bank reserves the right to reject any or all offers without assigning any reason.

Please note that the prospective bidder needs to purchase the tender document from the Bank and is invited to attend the pre bid meeting on above date and time at Bank of Maharashtra, Central Office, Pune. In case the prospective bidder downloads the document from website of the Bank, the cost of tender document should be paid along with the Bid response. However in order to participate in the pre-bid meeting, that tender document must be purchased by the prospective bidder.

Earnest Money Deposit must accompany all tender offers as specified in this tender document. EMD amount/Bank Guarantee in lieu of the same should not be mixed with Technical / Commercial bid. It should be in separate cover to be handed over to the department.

Tender offers will be opened in the presence of the bidder representatives who choose to attend the opening of tender on the above-specified date, time and place.

Technical Specifications, Terms and Conditions and various formats and pro forma for submitting the tender offer are described in the tender document.

General Manager
Information Technology

2.Introduction

Bank of Maharashtra is a public sector bank with a standing of more than 82 years. It has a three tier organizational set up consisting of branches, Zonal Offices, and Head Office. Bank of Maharashtra, a leading Public Sector Bank has 1981 fully computerized branches spread across the country. In the state of Maharashtra itself it has 1000 branches, the largest network of branches by any Public Sector Bank in the state. The Bank has set up specialized branch offices to cater to the needs of SMEs, Corporate, agriculturists and importers & exporters.

The bank has fine-tuned its services to cater to the needs of various sections of society and incorporated the latest technology in banking offering a variety of services. The products and services offered by the Bank include demand deposits, time deposits, working capital finance, term lending, trade finance, retail loans, government business, Bancassurance business, mutual funds and other services like demat, lockers and merchant banking etc.

The Bank has also implemented its CORE BANKING SOLUTION across all branches.

In order to streamline comprehensive information security monitoring and compliance, the Bank proposes to implement and maintain Cyber Security Operation Centre (CSOC) for its Information Technology setup comprising critical locations such as DC, DR, CBS Project Management Office, Head Office and other IT locations which may come up in future. The Bank intends to issue this bid document to the bidders to participate in the competitive bidding for implementation and maintenance of Security Operation Centre and other services on captive CSOC model.

The Period of Contract shall be for a period of five years. **The contract period will start from the date of acceptance of the project by the Bank.**

This request for proposal document ('RFP document' or RFP) has been prepared solely for the purpose of enabling Bank of Maharashtra ('Bank') to select a bidder for implementing and maintaining the Cyber Security Operations Center.

The RFP document is not 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 the bank and any successful bidder as identified by the bank, after completion of the selection process as detailed in this document.

2.1 Information Provided

The RFP document contains statements derived from information that is believed to be true and reliable at the date obtained 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 Bank in relation to the provision of services. Neither Bank nor any of its directors, officers, employees, agents, representative, contractors, or advisers gives any representation or warranty (whether

oral or written), express or implied as to the accuracy, updating or completeness of any writings, information or statement given or made in this RFP document. Neither Bank nor any of its directors, officers, employees, agents, representative, contractors, or advisers has carried out or will carry out an independent audit or verification or investigation or due diligence exercise in relation to the contents of any part of the RFP document.

2.2 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") i.e. Government Organization/PSU/ limited Company or a partnership firm and no other person or organization.

2.3 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 arises 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.

2.4 Costs Borne by Respondents

All costs and expenses (whether in terms of time or money) incurred by the Recipient / Respondent in any way associated with the development, preparation and submission of responses, including but not limited to attendance at meetings, discussions, demonstrations, etc. and providing any additional information required by Bank, will be borne entirely and exclusively by the Recipient / Respondent.

2.5 No legal relationship

No binding legal relationship will exist between any of the Recipients / Respondents and the Bank until execution of a contractual agreement to the full satisfaction of the Bank.

2.6 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.

2.7 Evaluation of offers

Each Recipient acknowledges and accepts that the Bank may, in its sole and absolute discretion, apply whatever criteria it deems appropriate in the selection of organizations, not limited to those selection criteria set out in this RFP document.

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. The Recipient unconditionally acknowledges by submitting its response to this RFP document that it has not relied on any idea, information, statement, representation, or warranty given in this RFP document.

2.8 Errors and Omissions

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

2.9 Acceptance of terms

By responding to the Bank's RFP document, the Recipient will be deemed to have accepted the terms as stated in this RFP document.

3.RFP Response terms

3.1 Lodgment of RFP Response

3.1.1 Tender Fee

The non-refundable tender fee as mentioned in section 1 above shall be paid by way of Bankers Cheque / Demand Draft / Pay Order favoring Bank of Maharashtra, Payable in Pune, which is non refundable, must be submitted separately along with RFP response

3.1.2 RFP Closing date

RFP Response should be received by the officials indicated not later than the date and time mentioned in Section 1 of this RFP.

3.2 Late RFP policy

RFP responses received after the deadline for lodgment of RFPs at the address mentioned will not be accepted by the Bank and hence bidders are advised to submit their responses within the time and no excuses / reasons for delay will be accepted by the Bank.

3.3 RFP Validity period

RFP responses will remain valid and open for evaluation according to their terms for a period of at least six (6) months from the RFP closing date. The Bank / its subsidiaries shall have the right at its sole and absolute discretion to continue the assignment / contract on the selected bidder for future requirement on the rates finalized in this processing for various items / activities as described in the Price Bid after expiry of current assignment period.

3.4 Requests for information

The bidders are required to direct all communications for any clarification related to this RFP, to the Bank officials as mentioned in Section 1 of this document and in writing. All queries relating to the RFP, technical or otherwise, must be in writing only. 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 initiated by respondents later than five business days prior to the due date for lodgment of RFP response. However, 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(es) as responses to queries will only be provided to the Respondent via email. If Bank in its sole and absolute discretion deems that the originator of the query will gain an advantage by a response to a question, then Bank reserves the right to communicate such response to all Respondents. Bank may in its sole and absolute discretion engage in discussion or negotiation with any Respondent (or simultaneously with more than one Respondent) after the RFP closes to improve or clarify any response.

3.5 Notification

Bank will notify the Respondents in writing as soon as practicable, but not later than 10 working days from the RFP Evaluation Complete date, about the outcome of the RFP evaluation process, including whether the Respondent's RFP response has been accepted or rejected. Bank is not obliged to provide any reasons for any such acceptance or rejection.

3.6 Disqualification

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

3.7 Timeframe

The timeframe for the overall selection process will be as mentioned in this RFP in section 1:"Invitation to the Tender"

The Bank reserves the right to vary this timeframe at its absolute and sole discretion and without providing any notice/intimation or reasons thereof. Changes to the timeframe will be relayed to the affected Respondents during the process.

The time schedule will be strictly followed. Interested parties should adhere to these timelines. However, the bank reserves the right to change the aforementioned timelines.

3.8 Adoption of Integrity Pact

1. 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.

2. Only those bidders, who commit themselves to the above pact with the Bank, shall be Considered eligible for participate in the bidding process.

3. The Bidders shall submit signed integrity pact as per **Annexure - 10** along with Conformity to Eligibility Criteria. Those Bids which are not containing the above are liable for rejection.

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. The name and contact details of the Independent External Monitors (IEM) nominated by the Bank are as under:

Shri. Nilmoni Bhakta Address - A-801, PBCL CHS Ltd. Plot No. 3, Sector 46 A Nerul, Navi Mumbai, 400706 Email - nilmoni.bhakta@gmail.com	**Shri. Madan Lal Sharma** Address - K-23, Jangpura Extention New Delhi Email - ml.sharma1965@yahoo.com

4.Project Details

4.1 Purpose

Bank of Maharashtra is a nationalized Bank serving the nation for over 82 years. It has a three tier organizational set up consisting of Branches, Zonal Offices and Head Office, The Head Office of the Banfk is at 1501, Shivajinagar, Pune – 411005. (hereinafter referred to as the "Bank" intends to issue this bid document, hereinafter called RFP, to eligible bidders, to participate in the competitive bidding for appointment of bidder for implementation and maintenance of CSOC using SIEM.

The Bank, for this purpose, invites proposal from bidders for primarily undertaking inter-alia the activities mentioned under the section 4.2 – Project Scope; for the Bank in respect of implementing and maintaining the CSOC using SIEM:-

The proposed solution should be scalable so as to support legacy applications used by bank or the Bank may go in for upgradation at a later date.

4.2 Project Scope

The broad project scope includes having **System Integrator (SI)** for design, setup, implement and maintenance of the proposed CSOC solution with SIEM. The Following are the broad activities bidder should perform:

1. Cyber Security Operations Centre should collect, correlate and monitor various logs / incidents in real time / near real time. The bidder shall appropriately manage and provide protection within and outside organization borders/ network, taking into consideration how the data/ information are stored, transmitted, processed, accessed and put to use within/ outside the bank's network, and level of risk they are exposed to depending on the sensitivity of the data/ information.

2. The CSOC shall consolidate functions of incident monitoring, detection, response, coordination, and computer network defense tool engineering, operation, and maintenance. These services are to be rendered 24X7X365 ensuring at least 99.95% uptime of CSOC setup.

3. The CSOC shall develop context to reliably distinguish an event from a non-event and prioritize protection based on business-critical rules.

4. CSOC shall provide adaptive incidence response through
 a. Continuous Threat analysis
 b. Network and host scanning for vulnerabilities in conjunction with network behavioral data, NAC, DLP, end-point malware protection, DAM etc.
 c. Co-ordinate in deployment of countermeasures for any real and probable cybersecurity incident.

5. CSOC Bidder shall conduct vulnerability assessment and penetration testing as per the frequency decided by the Bank. The bidder shall be able to use the vulnerability data effectively for mapping of security profile of IT enabled services.

6. The CSOC 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.

7. CSOC bidder shall provide Anti-phishing/ anti-rogue application service for identifying and taking down phishing websites/ rogue applications.

8. As a part of CSOC, the bidder shall also be supplying
 a. Solution for Advanced Persistent Threat.
 b. Solution for Privilege Identity Management
 c. Solution for File Integrity Monitoring.
 d. Solution for Network Behavioural Analysis including mapping

The bidder shall fully integrate all the existing security solutions of the Bank and the above-proposed solutions with the proposed SIEM.

9. Reporting and Escalation: Providing various levels of management reports to the Bank and implementing Escalation Matrix in order to handle Information Security Incidents efficiently.

Bidder will have to provide the services for a period of five years as per the detailed Requirement given under section 5. The tenure of the project will start from the date of acceptance of the project by the Bank. The Bank will be reviewing the performance of the bidder after 3 years from acceptance of project. After that, the Bank reserves the right to extend the contract by another 2 years

depending upon the performance of the bidder. All the hardware, software and licenses shall be covered under warranty for 3 years and under AMC for rest of the contract period.

Thus the bidder establishing CSOC will be responsible for the overall security of Bank's Enterprise-wide information systems, and collects, investigates and reports any suspected and confirmed security violations. The bidder shall suggest the tools required to achieve the resilient CSOC setup.

4.3 Project Schedule

#Stage	Activity	# Weeks	Project Duration (Weeks)	Time period for Completion
1.	Submission of Detailed Project Plan including integrating all the present security solutions	2	2	2 Weeks of issuing the Purchase order to SI
2	Deployment of CSOC Resources at Bank's premises	3	3	3 Weeks of issuing the Purchase order to SI
3	Training for the Bank Team	1	4	4 Weeks of issuing the Purchase Order to SI
4	Prepare CSOC Processes	2	5	5 Weeks of issuing the Purchase Order to SI
5.	Delivery of CSOC Hardware/ Software and licenses and resources	1	6	6 Weeks of issuing the Purchase Order to SI
6	Installation & Configuration of SIEM including HA and DR setup.	2	8	2 Weeks after the delivery of SIEM & VA Components
7	Integration of various devices (servers, Network devices and Databases of the Bank) and various current and proposed security solutions	6	12	14 weeks from issuing purchase order
8	UAT and making the CSOC operational	2	16	16 weeks from issuing purchase order

Pert Chart

Description	W1	W2	W3	W4	W5	W6	W7	W8	W9	W10	W11	W12	W13	W14	W15	W16
Project Plan																
Deployment of CSOC Resources																
Training for the Bank Team																
Prepare CSOC Processes																
Delivery of Hardware																
Installation & Configuration																
Integration of various devices & security solutions																
UAT																

5.Detailed Requirements

5.1 Cyber Security Operations center Requirements

The scope of the job is to implement, maintain and carry out various functions of the Cyber Security Operations Center for critical devices listed in the scope along with associated hardware & network infrastructure and equipment supporting them.

5.2 General

Bank has a list of identified Business Applications, which are dependent on IT. Bank expects the bidder to identify the data flow, the architecture, associated hardware/ software/ network devices, associated key persons (vendor and Bank), the dependent services etc. so as to correlate and report possible security loop-holes, suggest the remedial measures, ensure that the security loopholes are closed and compliance is reported to the management.

Bank has various security solutions in place as follows:

1. DLP
2. NAC
3. Patch Management Solution
4. Endpoint Encryption
5. Enterprise Antivirus
6. Web Filtering
7. Email Security
8. DDoS Mitigation Service
9. VPN
10. DAM
11. Server and Network Health Monitoring Tools
12. IDS, IPS, Firewalls etc.

The CSOC should take inputs from these various security measures, should normalize the logs, correlate events relevant to the service under scrutiny and should report any uncommon behavior as an incident for that service.

The CSOC shall check all the egress points (perimeter touch points) present in the network of the Bank, shall check for any unauthorized data flowing out of the network. The CSOC should also be able to collect information about the behavior of unauthorized software and report any unknown behavior.

CSOC shall conduct deep scan of packets including secure traffic passing through internet/ web gateway of the Bank and shall use the intelligence to correlate with other logs and generate meaningful reports / alert

Thus the CSOC shall develop rules based on the behavior analysis, should develop use cases for the service based on the data stored/ transmitted and report the latest security profile of the service as a dashboard to the Bank's Management.

The CSOC should be well prepared to face emerging cyber-threats such as 'zero-day' attacks, remote access threats, and targeted attacks.

CSOC should also take necessary preventive and corrective measures in addressing various types of cyber threats including, but not limited to, denial of service, distributed denial of services (DDoS), ransom-ware / crypto ware, destructive malware, business email frauds including spam, email phishing, spear phishing, whaling, vishing frauds, drive-by downloads, browser gateway fraud, ghost administrator exploits, identity frauds, memory update frauds, password related frauds, etc.

The bidder shall develop specific observable patterns (Indicators) to understand modus operandi of adversaries. The indicators may consist of data such as time-related information, geo-locations, parties involved, assets affected, impact assessment, related Indicators, related Observables, leveraged TTP, attributed Threat Actors, intended effects, nature of compromise, response Course of Action requested, response Course of Action taken, confidence in characterization, handling guidance, source of the Incident information, log of actions taken, etc.

CSOC shall generate alert/ report of unusual behaviour/ cyber security incident as mandated by RBI, CERT-IN, IB-CART etc to enable bank to make such reporting within prescribed timelines.

CSOC shall also be responsible for categorization of incidents and shall perform root cause analysis and come out with solutions to contain further incident of similar types.

CSOC will be subjected to Bank's internal audit or third party audit. The bidder shall have to close all the observations reported by the auditor as per the policy of the Bank. Closure of audit observations is also subjected to SLA.

The bidder shall use only standard tools/ agents for sending logs to the SIEM, freeware tools are not allowed. Bidder will also supply all the necessary Network Switches / power cables / fiber optic cables/ connectors / hardware /software etc. for integration of the components supplied for CSOC. Bank will supply only office space and maintenance thereof, power and Network points, office furniture, equipment, filing supplies and telephone service, access to network connections, printer, and workstations necessary to fulfill the requirements of the task. But the bidder is responsible for maintaining all assigned space(s) in a clean, safe, and orderly fashion during the tenure of this contract.

The bidder/ OEM shall provide End of Sale, End of Support and End of Life date for each component provided in the solution in the format as mentioned in Annexure – 3 along with undertaking that these dates are beyond the extension period.

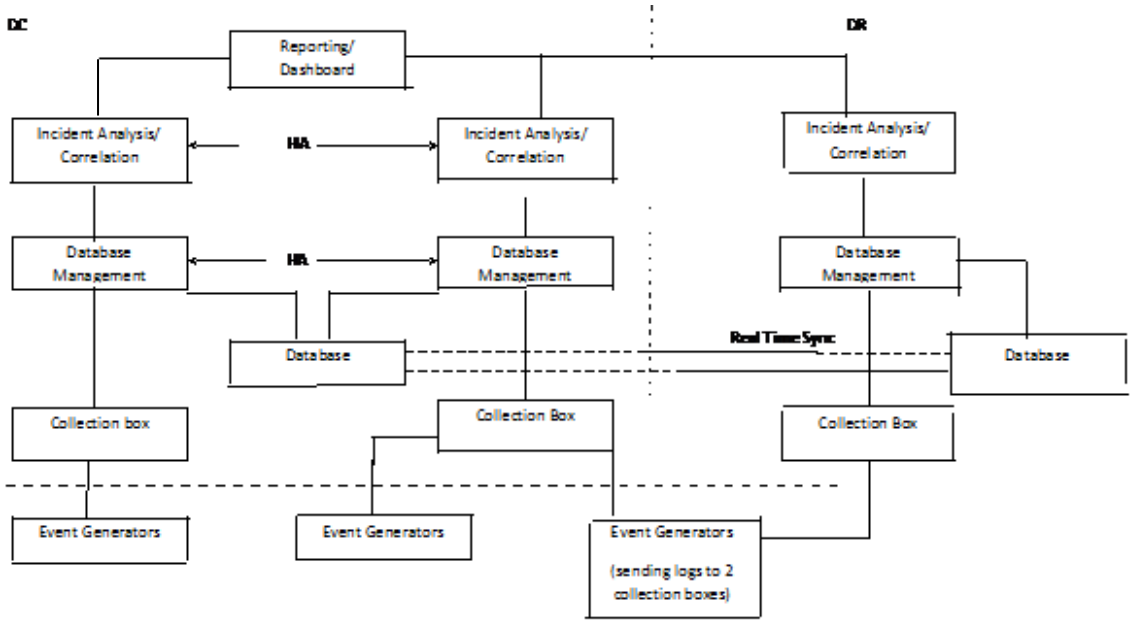
As a part of CSOC, the bidder shall provide Tools that cater to below needs at a minimum:

1. SIEM infrastructure
2. Anti-Phishing
3. Automated Network Discovery and Management – grouping of devices based on the business service they cater to (Network mapping)
4. File Integrity Monitoring
5. Privilege Identity Management
6. Behavior Learning
7. Appliance based Anti-APT solution.

5.2.1 Security Information and Event Management (SIEM):

1. The Bank intends to have various modules of SIEM placed in DC to be in HA (High Availability) mode, also the Bank intends to have SIEM modules in DR for redundancy.
2. The bidder may propose any architecture at the time of technical bid submission, which is cost effective, takes care of high availability and also redundancy, in case DC fails and during DR drill as well.

3. The sample architecture is as follows:



4. The bidder shall participate in the DR drill whenever conducted by Bank.

5. For DC-DR replication, the solution should also have the capabilities to replicate it during non-business hours. The storage should have the option to support backup on tape library.
6. The bidder shall provide complete list of supported devices in excel/ PDF file, which should contain at least those fields as mentioned in Annexure – 2. The list cannot be older than December 2016. As such the bidder shall provide latest list.
7. Bidder shall ensure that no component is declared either End of Support, End of Sale or End of Life during tenure of the contract. The bidder shall provide such data in the format as given in Annexure – 3. The data provided by the bidder shall be considered as final and no changes will be accepted after submission.
8. In case the bidder/ OEM fails to give the above data for any specific component, and later on, any specific component is found to have date of end of sale/ support/ life which falls before the end date of the contract the bidder will have to replace / upgrade the component free of cost with the latest workable component.
9. In case the OEM declares later on a date for End of Sale/ Support/ Life which falls before the end date of the contract, the bidder will have to replace/ upgrade the component free of cost with the latest workable component.
10. In case the bidder fails to replace/ upgrade the component within 3 months from the date of declaration by OEM (even when the Bank notices it later) then that will be considered as breach of contract and the bidder will be liable to legal prosecution including termination of the contract. Additionally, till the time the component is replaced, the bidder shall be liable for penalty as per SLA clause from the date of declaration by OEM.
11. Bidder shall quote SIEM solution, which can support at least 20,000 EPS with all components in HA (High Availability) mode at the DC. The solution shall be scalable to support additional 5000 EPS if required by the Bank.
12. Bidder should provide a storage solution such that the storage never crosses threshold of 80% of total capacity.
13. The bidder has to provide 24X7 monitoring & Security Analysis of the infrastructure through SIEM solution
14. Patch the SIEM systems as and when required in case new updates available as per SLA.
15. The SIEM tool should be capable of sending automated email and SMS as other modes of communication for alerts related to critical incidents.
16. Log has to be retained for a period of 6 months Online and additional 6 months offline. Offsite storage is also required for additional 7 years.
17. Solution should be consisting of hardware, software, operating system, database, online / offline storage, analytical applications and tools, etc. as per the technical and operational specifications of the Bank. Refer SIEM Technical Specification.
18. The bidder shall integrate all the existing/ new critical devices/ servers within specified period as per RFP. The resource engaged in this activity shall remain with CSOC for 6 months from completion of UAT at all the locations.
19. In case if SIEM device does not support application / DB / device out of the box, in that case Bidder should include cost of development of parser and ensure that application / Database / device are integrated with SIEM solution.

Further any new application / Database device should be able to integrate with SIEM.

20. The Bank would also like the bidders to demonstrate their solution capabilities, integration services and any other innovative and creative services, which the bidder can offer to supplement bank's requirements during the RFP technical evaluation & presentation process.
21. Bank reserves the right to bring about any changes in Requirement/Scope of this RFP and the same will be communicated to the bidder well in time so as to allow the bidder to prepare their proposal.
22. All incidents detected by the SIEM tool and manual incidents detected by analysts have to be submitted to the incident management module of the security management Dashboard. There should be a feature to drill down to actual event in detail if required.
23. In case the bank changes network architecture, SIEM should be able to integrate accordingly.
24. The solution shall support the various Use Cases in order to provide log collection, event correlation, Alert Generation and escalation. Following list of Use Cases is given for example and to be treated as indicative
    i. Use Cases for Internet Banking Transactions
    ii. Use Cases for ATM Transactions
    iii. Use Cases for CBS Transactions
    iv. Use Cases for VPN user sessions
    v. Use Cases for Intranet Applications
    vi. Use Cases for Email Applications
    vii. Use Cases for Mobile / Phone /SMS Banking
    viii. Use Cases for Financial Inclusion Transactions
    ix. Use Cases for RTGS / NEFT Transactions
    x. Use Cases for SWIFT transactions
    xi. Use Cases for UPI/ IMPS Transactions
    xii. Any other Use Cases

23. Incident Management Solution

Bank intends to have framework in place for adaptive incidence response, management and recovery. The bidder shall establish such a framework considering the network architecture, implement security solutions and shall be able to dynamically and proactively take actions to reduce operational overhead.

The incident management solution shall make use of active and passive traffic analysis to determine threat. Once a threat is determined, the SIEM and Incident Management solution shall be able to leverage tools like Nessus to scan and analyse, in conjunction with network behavioural data and IDS alerts, to provide a true real time snapshot of what attacks are happening or what probable attacks can be. **It shall be able to assess likely impact and shall provide possible solutions/ work around for the threat.**

The incident management solution should be able to register any security alert events automatically and manually (using a form as set by the Bank) and generate automated tickets for the alert events generated by the SIEM. The solution should provide complete life cycle management of tickets from incident generation till closure of the incident. The Incident Management solution shall further analyse various tickets and report the incident automatically.

Incident Management Solution shall support multiple tasks integrated within a Single Incident / Single ticket, this is to ensure that all the Dependent Services are displayed/ actioned within a Single Incident. The SLA monitoring for incident closure should be possible using Incident Management solution.

The solution should have capability to structure rule-based workflow and calendar/ event based alerting capability. The tool should facilitate time/ event based automated escalation of tickets as per the escalation matrix defined by the Bank.

The solution shall support long term trending and metrics. The solution should be able to send notifications and alerts in different formats, such as e-mail, SMS, etc.

In case the Bank proposes to use its own Incident Management System or ticketing tool, the bidder shall integrate it with the SIEM.

24. VA Management

The bidder is responsible to provide all hardware, software, tools and resources for doing the vulnerability scanning As a part of adaptive incident management, the bidder shall automate the VA scan so as to integrate the results of VA scan into the advanced correlation rules.

Commercial tools must be provided for entire solution and freeware tools /software should not be used.

Also, the VA Management Solution should periodically scan (monthly) all IT assets across the critical sites of bank for vulnerability scanner and report vulnerabilities as per SLA. These VA scans shall also be seamlessly integrated with Adaptive Incident Management solution so as arrive at the security posture of the service/ asset. For such scheduled VA scans, the bidder shall provide the remediation plan to patch those vulnerabilities. All the vulnerabilities reported shall have CVE numbering. The bidder shall further help the Bank for closure of the vulnerabilities.

After approval, remediation plan has to be completely documented and executed as per ITIL based best practices. The same should be updated in the incident management module of the Security Management Dashboard.

Security Management Dashboard

The bidder is required to provide a Security Management Dashboard for reporting all the above activities including incidents from Anti-Phishing services, incidents from SIEM, vulnerability scan reports, asset databases, remediation process progress etc. This will be accessible to bank's authorized employees and analysts.
The SIEM solution should provide integrated dashboard functionality for all the above requirements.

The bidder shall feed all the asset information of the IT assets of banks, processes, applications details etc in the asset management module of SIEM dashboard.

The dashboard solution should be on premise and not a hosted solution. There should be a feature to create any kind of report from any of the available data from the feeds like top incidents by application, by hosts, users etc.

25. Anti-Phishing, Anti-Trojans and Anti-Rogue Services

The scope is for following websites. However, Bank reserves the right to add any number of additional URLs registered in its name.

- https://www.mahaconnect.in
- http://bankofmaharashtra.in

Bidder should be able to proactively monitor, detect and handle the following incidents (for the websites mentioned above:

- Phishing attempts
- Trojans
- Brand abuse cases
- Spoofed email ids that may be used for sending mails to the customers of the Bank, illegitimate from inside the bank also.

Monitoring of compromised servers for forensic information related to Bank's customers till the primary incident is closed.

Bidder should be able to handle (monitor, detect and block) proactively all kinds of frauds and simultaneously update itself with new frauds that may keep on coming. Bidder will have to provide countermeasures/ solutions for all existing frauds as well as frauds that may come in the near future.

For Anti-Phishing /Anti-Trojan/ Anti-Rogue solution, details of compromised accounts should be shared with the Bank as per SLA.

Bidder should have the capability to ensure fast closure of the incident. The bidder should have contacts with Browser vendors, ISP (Internet Service Provider) and enforcement bodies across globe, third parties etc.

A dedicated dashboard should be available for getting details on the Anti-Phishing and Anti-Trojan services. It should include features like display of high and low end reports, help menu, downloading extracted data, availability of screen shots etc. This will be accessible to bank's employees as communicated by bank to bidder.

Bidder's Managed Service CSOC team should be able to provide advisory services to the Bank in the form of

- Advisories on online threats
- Whitepapers
- Information on critical vulnerabilities
- Review calls
- Intelligence alerts and presentations etc.

Bidder should ensure that the analysis conducted for any incident must support the following:

- Underground intelligence analysis
- Correlation of all attacks and underground intelligence
- Capability to share and disseminate information on fraud related activities with members (May be a part of information sharing network such as Internet Relay Chat, Anti Phishing Work Group etc)
- Intelligence gathered should be coordinated and collaborated with other intelligence gathering groups/ teams/ organizations
- The feeds from Anti-Phishing, Anti-Trojan and Anti-Rogue Services should be integrated with SIEM using automated tooling standards.

26. Resources

All the resources to be deployed by the bidder for monitoring of the product & administration of the solution should be OEM certified. Certificates have to be submitted at the time of bidding. The Resource requirement is as follows:

1. Minimum two L1 and one L2 resources during 7AM to 11PM.
2. Minimum One L1 resource during 11PM to 7AM.
3. One CSOC Manager during 9AM to 6PM

L1 resource shall be available 24X7X365. L2 resource and CSOC manager shall be available on all working days and also on need basis.

The attrition of resources shall be governed by the SLA mentioned in this RFP.

The Bank will perform the technical competency of the resources provided by the bidder either on its own or through third party resources. However background verification and police verification of the resources shall be the responsibility of the bidder.

The Bank will also monitor the performance of the resources deployed during the tenure of the contract. Following will be the criteria on which the performance of the resources and overall CSOC will be measured:

1 Number of on-time reports submitted as per SLA.

2. Number of use cases developed and the rules deployed

3. Number of IoC (Indicators of Compromise) detected.

3. Number of security training sessions (ad-hoc/ scheduled) conducted.

4. Number of real incidents detected against the total number of false positives.

5. Number of devices added/ total number of devices integrated and are being reported in the security management dashboard.

6. Resolution times (a measure of the length of time from when the incident/ticket was received, the length of time from when the incident/ ticket was dispatched, etc.).

At the same time, the bidder shall demonstrate their Quality Control Plan/ Road map that addresses continuous improvement in the quality of service, work products, and deliverables. (Link to SLA) The road map given by bidder shall be acceptable to the Bank. The bidder shall configure dashboard such that the parameters of quality control map are seen as easily measurable units. Bank will conduct review of the performance/ quality control every quarter based on quality control plan.

It is mandatory for the vendor to provide the dedicated onsite resources having the minimum detailed skill sets and experience as per ANNEXURE 4.

For Reporting and Timings the followings should be ensured.

i. The onsite team would report to Bank personnel / Bank authorized representative.

ii. The Team should operate from the Bank's premises in Pune during the hours assigned to engineers as per the shifts

iii. In case of exigencies even during off business hours / Bank holidays, the resources may be required to be present onsite

iv. A replacement shall be given in case the resource proceeds for leave.

The vendor personnel deployed in the Bank premises shall comply with the Bank's Information Security Requirements.

Bank proposes set of professionals for management of CSOC as per Resource Plan Matrix – Annexure - 4.

The below mentioned skill-sets will be given due preference:

- Analytical Thinking (Expected from L1, groupL2 and CSOC Manager)
- Presentation skills (Expected from CSOC Manager)
- Research Skills (Expected from L2 and CSOC Manager)

- Scripting Knowledge (Expected from L2 and CSOC Manager)
- Knowledge of tools (SIEM, DLP, NAC, DAM etc) (Expected from L1, L2 and CSOC Manager)
- Experience on Unix, Windows and mobile operating system Platforms such as Android, IOS etc.(Expected from L1, L2 and CSOC Manager)
- Network Packet Analysis (Expected from L1, L2 and CSOC Manager)
- Knowledge of Vulnerability Assessment (Expected from L2 and CSOC Manager)
- Knowledge of Information Security Framework such as ISO27001, Risk Management Framework such as ISO31000, IT Service Management (ITIL V3) (Expected from L2 and CSOC Manager)

In case Bank selects the proposed resource, Bank will decide the role of the resource in the CSOC. In case it is found either at the time of deployment or during the tenure of the project, that the appointed resource lacks the competency in particular aspect as mentioned above, the Bank may suggest the bidder for enhancement of skillset for that resource. The bidder will have to ensure that the resource obtain related certification/ knowledge within 3 months from being notified by the Bank. (Linked to SLA)

Tasks to be performed by the resources

Monitoring and Analysis

a. Continuous monitoring, analysis and reporting of security alerts and event information from all approved security feeds to include investigation of reported incidents using system logs, event correlation between Intrusion Detection/ Prevention Systems (IDS/ IPS), Data Loss Prevention (DLP), Network Access Control (NAC), Database Activity Monitoring (DAM), Privilege Identity Management (PIM), firewalls and other means of detection.
b. Investigate and positively identify anomalous events that are detected by security devices or reported to the CSOC from external entities, system administrators, and the user constituency.
c. Provide notification, escalation, and daily summary reports based on security event analysis, post-analysis categorization, prioritization, and recommendation of event disposition.
d. Manage the resolution of computer security events through the use of an established ticketing system.
e. Monitor and analyze the emails for threats including phishing and malware, and make recommendation for email rules to minimize malicious or undesirable emails.
f. Continuously tune the furnished Security Information and Event Management (SIEM) System, to reduce false positives and discover previously unknown threats.
g. Make recommendations against security infrastructure threats and tune all security monitoring tools in the Bank.
h. Documentation of incident investigation and case analysis.

i. Use the ticket systems and system security information manager console to take appropriate action towards problem status documentation, resolution and prevention measures. Provide summary of ticket system activities.
j. Provide information to impacted users and management promptly regarding the status of changes, enhancements, and problem resolution.
k. Complete resolution or referral of all security problems after receiving notification of an incident or problem in accordance with established timelines given below.

Project Management

a. Maintain system-engineering processes such as parts management, license continuity, quality assurance, system safety, reliability etc.
b. Provide input in creating and maintaining value for the Bank through better design, introduction and operations of cybersecurity services. Experience and knowledge of the latest security technology in all stages of the system life cycle.
c. Perform impact analysis to overall security and possess a high level of expertise in developing long-term strategies and understanding about various cyber threats and mitigation techniques.
d. Conduct Root Cause Analysis and report accordingly.
e. Ensure compliance to Bank's certification requirements and Bank's policies & procedures.
f. Ensure continuity of operations in CSOC in case of any emergencies

Vulnerability Management

a. Ensure complete and accurate scans for all BOM devices. Provide analysis of scan data to identify critical and high risk vulnerabilities for each BOM system
b. Use approved test procedures, information collect scripts, and VA tools that are industry standard, the latest versions of tools with up-to-date lists of vulnerability checks; appropriate to BOM's policies, needs and technologies.
c. Conduct specialized VA testing to include Database and Web application assessments, penetration testing, and all Wireless technology testing and analysis.

System Security Administration

The bidder personnel shall be responsible for advising and assisting with maintenance and update of the CSOC infrastructure to include hardware and software for managing the lifecycle of all CSOC changes with minimum disruption to CSOC services.

Provide continuous recommendations to improve cybersecurity capabilities and reduce security vulnerabilities; provide quality of service improvements for access control in order to meet the varied Quality of Service (QoS) requirements for BOM end-users based on site type, location, and processing needs.

Deliverables (link the reports to be delivered to SLA)

Technical monthly report which shall consist of a summary of all CSOC activities and reference analysis of CSOC performance metrics, track status of security

incidents by category, tickets, call logs, investigatory cases, security event notifications and actions accomplished for the month.

Program Management monthly status reports -- work completed during the current period, planned activities and problem/issues with recommended solutions, anticipated delays, and resources expended.

Daily status report

1. Intrusion Detection Reports
2. Computer Security Incident Reports
3. Security Event Notifications
4. Security Alerts, Advisories and Bulletins
5. Report on devices not sending the logs to collector
6. Any other ad-hoc report as per requirement of the Bank.

The bidder must keep a daily log. Each shift must enter in the daily log all incoming phone calls, e-mails, when an update is made to an Incident or a Security Event Notification (update, closure, or opening).

Vulnerability Assessment and Reporting

1. How many databases were assessed
2. How many web applications were assessed
3. How many vulnerabilities were identified per system
4. How many Information Security Vulnerability Management Reports/ Advisories were released, applicable to BOM.

Threat Intelligence Feed

The bidder CSOC team should regularly track and advise the Bank about new global security threats and vulnerabilities. The advisories should be customized to suit the Bank's security infrastructure. Bidder should advise the bank for upgrades /changes in the security infrastructure of the Bank against evolving threats and responsibilities.

The bidder shall integrate threat intelligence feeds directly with the SIEM using API or any other automated method. The bidder shall demonstrate the system alignment of threat intelligence available with the bidder with the Banking scenario. The number of threat intelligence feeds integrated with SIEM are linked with SLA.

27. Training

Selected bidder shall provide the training to the bank's personnel as described below:

i. The training should include the architecture, hardware, software, integration, and customization, policy installation, troubleshooting reporting and other aspects of the solution.

ii. SIEM Training- This faculty should be solution certified up to advance level and should provide courseware with adequate lab facility as well. The training should be provided by the OEM employee and should be of five days, 8 hours a day. Pre implementation training must be provided before project implementation and post implementation training must be provided after successful implementation. At the end of training participants shall be given certificate of successful completion by the OEM.

iii. Bidder should submit detailed course content and provisional agenda along with the Bid.

Refresher training- Post acceptance test, selected bidder shall conduct more refresher trainings for the Bank's team and for the bidder's CSOC team on quarterly basis. The participants of these programs shall be nominated by the Bank. The course duration will be of 1 day (link to SLA).

5.2.2 Anti-APT Solution

The Bank is looking for appliance based in-premise anti-apt solution. The bidder shall integrate the Anti-APT appliance with the SIEM so as have in-depth analysis of advanced targeted attacks.

It shall monitor all traffic across physical and virtual network segments, all network ports, and all network protocols to identify ransomware, targeted attacks, and advanced threats anywhere on Bank's network.

5.2.3 Network Behavior Analysis using automated network discovery and management

Bank wants to put in place network flow based behaviour analysis tool. The tool shall not introduce any latency in the network and it shall be able to collect and analyse Network Traffic irrespective of Network Speed/Bandwidth.

The bidder shall be able to seamlessly integrate the Network Behaviour analysis (NBA) tool with SIEM for further correlation of data collected by this tool

Regardless of obfuscation techniques, behaviour tool shall identify popular peer-to-peer file sharing applications that introduce new vulnerabilities, consume significant bandwidth and create substantial liabilities. The tool shall also be able to analyse the anomaly existing in encrypted traffic.

5.2.4 FIM (File integrity module)

The FIM solution shall

1. Track file, directory and registry access, movement and shares in real time by integrating it with SIEM. The bidder shall provide information such as the chain of events that caused the change, who did the change and when the change was done etc.

2. Identify unwarranted file changes

3. Meet regulatory compliance standards such as PCI-DSS.

The FIM solution shall be using wide variety of cryptographic generation algorithms so as to detect evasion through signature weaknesses.

The FIM shall be capable of identifying grouping of servers based on service and applying same policy. These servers may have different OS and different applications running on it.

5.2.5 Privilege Identity Management (PIM)

The PIM solution shall

1. Manage identities, roles, privileges across heterogeneous resources without any modifications to active directory or loading any agent on domain controller.
2. Manage session of each host

5.3 Service Levels

The service levels are defined for all the products of CSOC which are mentioned in this RFP; it constitutes SIEM, Anti-APT solution, Network Behavioural Tool, Privilege Identity Management and File Integrity Monitoring

Uptime (Solution Uptime)

The vendor shall ensure that the system gives minimum 99.95% uptime (Calculated on monthly basis, which includes servers, storage, switches, collectors, co-relation engine and solution as a whole). For every 0.10% or fraction thereof of additional downtime, Bank will impose a penalty of 1% of the monthly payment (subject to maximum of 10% of the contract value during warranty and AMC contract value during AMC period).

Service Level Agreement

The bidder and /or OEM will also have to enter into a Service level agreement for Service Support as per the terms and conditions of this RFP and covering the scope of work and technical requirements.

Broad SLA parameters for all components

	Component	**Parameter**	**SLA**
1	Closure of Audit Observations for CSOC	Compliance to be submitted within 7 working days for all High Risk Observations. For all other observations, compliance to be submitted within 1 month.	High Risk observations = Penalty of 1% of billing cycle payment after 7 days, per week thereafter, till the full compliance Other Observations = Penalty of 1% of billing cycle payment after 1 month, per week thereafter, till the full compliance.

2	End of sale/ end of support/ end of life of any component	The bidder will have to replace the component within 3 months from the date of declaration of End of Sale, End of Support/ End of Life of the contract.	Penalty of 1% of the cost of the component (as per bill of material submitted by the bidder) after 3 months from date of declaration, per week thereafter from billing cycle payment, till the replacement of the component.
3	Any component becoming faulty even though remaining solution is working	In case of faulty component, the bidder will have to replace the component within 7 days. Moreover it should be ensured by the Bidder that the Faulty/Out dated component should not hamper the working of the Solution	Penalty of 1% of the cost of the component (as per bill of material submitted by the bidder) after 7 days from date of device becoming faulty, per week thereafter from billing cycle payment, till the replacement of the component.
4	Patching/ loading latest versions of the software components in place	The latest software versions/ patches to be installed after testing within 1 month from release of the version/ patch.	Penalty of 1% of billing cycle payment after 1 month, per week thereafter, till the report of patching/ version upgrade is submitted to the Bank
4	Vulnerability Assessment	VA of critical devices to be conducted every month and report to be submitted before 10th of subsequent month VA of all other devices to be conducted quarterly and report to be submitted before 10th of subsequent month. Status report every week for closure.	Penalty of 1% of billing cycle payment after 10th of the subsequent month, per week thereafter, till submission of the VA report.
	Incident Management	SIEM shall be generating Alert within 15 minutes from occurrence of event. SIEM shall be logging ticket for each alert generated within 5 minutes from alert notification Low Risk Incidents to be notified within 3 days of occurrence of alert/s to Bank's SOC manager. Incident to be closed within 1 week from	1% of the monthly billing payment after discovery of the performance lacunae per week thereafter, till the problem is resolved.

		incident notification. Medium Risk Incidents to be notified within 1 day from occurrence of alert/s. Incident to be closed within 1 day from Incident Notification. High Risk Incidents to be reported within 4 hours from occurrence of alert/s Incident to be closed within 4 hours from Incident Notification	
		False Negative Incident – Any cyber security Incident not detected by CSOC, which resulted into monitory/ performance/ reputation loss to the Bank	1% of monthly billing payment in the affected quarter.
5	Anti Phishing and Anti-Trojan Services	Bidder should detect such sites within reasonable time and take it down within 24 hours from notification by the Bank	Rs.1000/= per day after 24 hours from notification by the Bank
6	Attrition of Resources	The bidder has to give 3 months advance notice in case any resource deployed by the bidder for this project is leaving this project. The bidder shall deploy another resource within 3 months from date of notification to the Bank. Any L1 resource going on leave (Absentee) shall be replaced by another L1 resource immediately.	Bank will not leave the resource till 3 months are completed from date of notification. In case the resource leaves before that, then that will be considered as "Absent" till the completion of 3 months period. For absentee penalty is as follows: 1. L1 Resource = Rs.500/= per day. 2. L2 Resource = Rs.1000/= per day 3. For CSOC Manager = Rs.3000/= per day. In case the replacement resource is not deployed

			within 3 months from notification, Bank will deduct penalty as follows: 1. L1 Resource = Rs.500/= per day. 2. L2 Resource = Rs.1000/= per day 3. For CSOC Manager = Rs.3000/= per day. Penalty will be applied in quarterly billing cycle. In case the bidder fails to meet the resource requirement for any quarter, Bank shall impose penalty as mentioned above and would also not make payment for the absent resource.
	Quality Control Plan	(Bidder to suggest additional parameters apart from specified below) Quality of service - Identifying and responding to risk (Response Time Rate), Responses time shall be less than 30 minutes from occurrence of the alert. Identifying of true positive shall be less than 2 hours from occurrence of an alert. Number of IoC (Indicators of Compromise) found in the IT service Integrating various other security projects of the Bank in fixed time. Educating the Bank staff about Information Security 2. Work Products Data Collection activities (log delivery methods,	The parameters are subjected to the values specified by the bidder in the Quality Control Map/ Quality Control Road Map subjected by the bidder. The deviation shall be subjected to penalty of 1% of quarterly billing cycle for every quarter, until the improvement is shown in quarterly review report. (The quarterly review meeting shall be attended by senior person above SOC Manager from bidder side)

		bandwidth usage etc) Status of security incidents by category, Number of advisories linked with CSOC 3. Deliverables On-time Reports and dashboard improvements Number of vulnerabilities detected for critical devices Setting up of new rules Percentage of real alerts against false positives 4. Resources – No resource shall be subjected to more than 9 hours of workload in 24 hours period. The bidder shall provide measurable units for performance improvement of the resources.	
	Reporting	Daily status report Monthly status report Dashboard Maintenance	Non-submission of daily and monthly reports will attract penalty of Rs.300 per report per day. Penalty will be calculated during quarterly payment cycle
	Threat Intelligence Feeds	Bidder shall integrate at least NCIIPC, IB-CART and CERT-In Feeds.	1% of quarterly billing payment for the quarter till the problem is resolved.
	Training	Pre-Implementation Post-Implementation Refresher Training	1% of quarterly billing payment for each training missed.
	Database maintenance	Availability of relevant logs online for last 6 months Making archived logs available for analysis. Ensuring there is no Log Loss	The deviation shall be subjected to penalty of 1% of quarterly billing cycle for every quarter, until the improvement is shown in quarterly review report.

		Data backup Archiving of logs older than 6 months	

Bank's Escalation Matrix: Following is the tentative Escalation Matrix for the Bank and subject to change.

SOC is responsible to recommend about the steps to be taken by the Bank officials having authorities to take a decision before making any change in the system. Although CSOC cannot enforce, the "say" of CSOC will be weighed against other stakeholders before taking any decision about a change. Accordingly, following escalation matrix is suggested for CSOC.

1. L1 resource shall respond to an alert within 30 minutes.
2. L1 resource shall decide if the alert is false positive within 2 hours from occurrence of alert. In case it is false positive, L1 resource will close the alert and report to the CSOC manager and Bank Staff at End of Day.
3. If alert is true positive, L1 will report to L2 resource for further analysis within 2 hours.
4. L2 responds within 30 minutes of receiving the alert. Checks if it is critical alert. (decision about criticality of alert)
5. If it is critical alert, L2 resource shall report to CSOC Manager and Bank Staff and CISO of the bank within 2.30hours from occurrence of the alert.
6. If it is not critical alert, L2 resource shall further analyze the incident and report the remediation plan to CSOC Manager within 3 hours from occurrence of the alert.
7. SOC manager shall report about all the alerts and incidents at the end of the day to Bank Staff and CISO of the bank.

6.Evaluation process

The competitive bids shall be submitted in three stages
Stage 1 – Eligibility criteria

Stage 2 – Technical Evaluation Criteria

Stage 3 – Commercial Bid evaluation through reverse auction

All bids shall be evaluated by Technical Evaluation Committee set up for this purpose by the Bank. The evaluation shall be on the basis of Eligibility criteria, Technical evaluation criteria and the commercial offer obtained through reverse auction.

The bidder will have to pass eligibility criteria to get considered for technical evaluation. The marks obtained in technical evaluation will get 70% weightage while comparing the commercial offer.

Resultant score will be calculated for all qualified bidders using following formula:

Score (S) = [(C1 / C) x 0.3] + [(T / TMax) x 0.7]

S: Resultant Score

C1: Lowest Commercial Bid

C: Commercial Bid of bidder

T: Technical score of bidder

TMax: Highest Technical score

Illustrative Example:

Sr. No.	Bidder	Technical Evaluation Marks (T)	Commercial Bid (C)	[(C1 / C) x 0.3]	[(T / TMax) x 0.7]	Score (S)
1	ABC	95	80	(60 / 80) x 0.3 = 0.225	(95 / 95) x 0.7 = 0.7	0.925
2	PQR	80	70	(60 / 70) x 0.3 = 0.257	(80 / 95) x 0.7 = 0.589	0.846
3	XYZ	75	60	(60 / 60) x 0.3 = 0.3	(75 / 95) x 0.7 = 0.553	0.853

In this above example bidder ABC, with highest score becomes the successful bidder.

The eligibility criteria, technical evaluation criteria and commercial bid formats are provided in annexures. The bidder will have to provide the information in the prescribed formats only. Any deviation from these formats may lead to disqualification of bidder.

6.1 Eligibility Criteria

Eligibility criterion for the bidder to qualify this stage is clearly mentioned in Annexure 6. Bidder meeting the eligibility criteria would only qualify for the second stage of evaluation. Bidder would also need to provide supporting documents for eligibility proof. All the credentials of the bidder necessarily need to be relevant to the Indian market.

The decision of the bank shall be final and binding on all the bidders to this document. The bank may accept or reject an offer without assigning any reason whatsoever.

6.2 Technical Evaluation Criteria

Technical evaluation criterion for the bidder is clearly mentioned in Annexure 1. The technical evaluation would be carried out under 3 heads – Organization's credentials, Capability of the solution and Approach & Methodology and Site visit. The marks will be allocated based on the information provided in the proposal, client feedback and the outcome of presentation.

The technical team of the bidder shall demonstrate the usage of the solution and generating sample alerts. At a minimum, the bidder shall demonstrate

1. The use of the SIEM solution to demonstrate the ease with which L1 resource can operate the solution.
2. Demonstrate steps for writing a rule for generated events.
3. Demonstrate the alert generation for the generated events.
4. Demonstrate the alert classification and assignment.
5. Demonstrate the escalation flow of the incident.
6. Steps for integration of Anti-APT solution.
7. Demonstrate adaptive incident mechanism.
8. Demonstrate identification of IoC for generated alerts/ incidents.
9. Demonstrate the network mapping of any banking application using bandwidth monitoring and network traffic analysis
10. Demonstrate PCI-DSS compliance using FIM.
11. Demonstrate the data format of data provided by PIM solution.

The evaluation will be done on a total score of 500. The bidder needs to achieve a cut – off score of 400 marks in the technical bid evaluation to be qualified for commercial bid opening. Only those bidders who achieve the specified cut – off scores would be short-listed for Phase 3 - commercial bid evaluation. In case none of the bidders score a minimum of 400 marks then the bidders who have achieved the top 4 scores will qualify for the commercial evaluation stage. In case only one bidder scores 400 points or above, the Bank reserves the right to select the lone successful bidder. The break-up of the scoring is mentioned in the bidder scoring chart; Annexure 7.

Bank reserves the right not to declare the technical evaluation score to the bidders before commercial evaluation (through reverse auction) takes place. But Bank will inform the bidders about their eligibility for reverse auction. The technical evaluation score may be declared only after receiving commercial offers through reverse auction.

6.3 Commercial Bid Evaluation

The commercial bid format is provided in Appendix 1 Form 02. The fees should be quoted strictly in the format provided. The commercial bid offers are to be submitted by all the bidders participating in the reverse auction in the format provided.

Only those bidders who have qualified in eligibility Criteria and scored more than 300 marks in technical evaluation would be eligible further participation in e-procurement process. The details of e-Procurement process are given in Annexure – 9. The bidder has to quote the total cost of items mentioned in Appendix 1 Form 02 of RFP (Total cost of the project for 5 Years). Bank will arrive at TCO as per the format mentioned in the Appendix 1 Form 02 after closure of bidding.

The amounts in commercial bid should be written in figures as well as in numbers. If there is any discrepancy between words and figures, the amount in words will prevail. If the successful Bidder does not accept the correction of the errors, it’s Bid will be rejected, and it’s Bid Security may be forfeited.

The bidder shall not add any conditions / deviations in the commercial bid. Any such conditions / deviations may make the bid liable for disqualification.

7. Bid Submission

7.1 Bid Submission Details

1. **Eligibility and Technical Bids shall be submitted in separate sealed sub-envelopes super scribing**

a) "ELIGIBILITY BID FOR BANK OF MAHARASHTRA IMPLEMENTATION AND MAINTENANCE OF CYBER SECURITY OPERATIONS CENTER ON CAPTIVE MODEL BY M/S…….. ON …….…. AT PUNE, DUE DATE _____" on top of the sub-envelope containing the Eligibility bid

b) "TECHNICAL BID FOR BANK OF MAHARASHTRA IMPLEMENTATION AND MAINTENANCE OF CYBER SECURITY OPERATIONS CENTER ON CAPTIVE MODEL SUBMITTED BY M/s….. ON…..AT PUNE, DUE DATE _____ " on top of the sub-envelope containing the technical bid.

These two separate sealed sub-envelopes should be put together in another sealed master envelope super scribing

BID for BANK OF MAHARASHTRA - IMPLEMENTATION AND MAINTENANCE OF CYBER SECURITY OPERATIONS CENTER ON CAPTIVE MODEL REFERENCE NO 042011 SUBMITTED BY …….. ON ……. AT PUNE, DUE DATE _____"

The response should be organized and submitted in the following manner:

i. Eligibility Bid

- Covering letter certifying Eligibility criteria compliance (as given in Appendix 1 Form 01)
- Duly filled up Annexure 6 – Eligibility criteria compliance
- Integrity Pact (Annexure 10) duly signed on stamp paper of Rs.500/=
- Supporting credential letters or copies of documentation from clients or bidders certifying compliance

ii. Technical Bid

- Table of Contents (list of documents given in technical proposal format)
- One copy of the technical proposal with pages properly numbered. The technical proposal should be bound in such a way that the sections of the proposal could be removed and separated easily;
- One copy of the masked price bid (masked price bid is a copy of the price bid **without any prices.** Please note that the masked price bid should be an **exact reflection of the commercial bid** submitted by the vendor as part of the commercial offer except that the masked price bid **should not contain any financial information.)**

- One compact disk (CD) containing the soft copy of technical proposal should be provided.

  The BIDDERshould certify that the contents of the CDs are the same as that provided by way of hard copy. In the event of a discrepancy, details provided in the hard copy will be true.

Copy of the tender document duly putting the seal and signature on all the pages of the document for having noted the contents and testifying conformance to the terms and conditions set out therein should also be enclosed in the Master Envelope.

The proposal should be prepared in English in MS Word / Excel / Power point format. The email address and phone / fax numbers of the bidder shall also be indicated on sealed envelopes.

Bidder should submit two separate demand drafts/banker's cheques / pay orders drawn in favor of Bank of Maharashtra payable at PUNE towards Application Money and Bid security as stated in section 1 of this document.

Paper copies of RFP response should be submitted along with Demand draft / Banker's cheque / Pay order for application money (which shall be non-refundable) and bid security deposit and electronic copy (Microsoft word and Excel on CD ROM) of technical bid submissions must be submitted to the bank at the following address:

Deputy General Manager
Information Technology
Bank of Maharashtra
Head Office,
Lokmangal, Shivaji Nagar,
Pune - 411005

The sealed bid envelopes as mentioned above should be dropped in the Tender Box kept in the IT Department. Following officials shall be available for any assistance.

i) Shri Sachin Shintre	Senior Manager-IT
ii) Shri Vijayakumar C.	Senior Manager-IT

Submission will be valid only if:

- Copies of the RFP response documents are submitted as per defined clauses in this section and before the mentioned RFP closing date and time
- Submission is not by Fax transmission

Only one Submission of response to RFP by each bidder will be permitted. In case of partnerships / consortium, only one submission is permitted through the lead bidder.

Last date for submission of the response to the tender document is mentioned in Section 1 of this document.

All responses would be deemed to be irrevocable offers / proposals from the bidder's and may if accepted by the Bank form part of the final contract between the Bank and the selected bidder. Bidder is requested to attach a letter from an authorized signatory attesting the veracity of information provided in the responses (Appendix 1 Form 01 – COVER TO). Unsigned responses would be treated as incomplete and are liable to be rejected.

7.2 Technical Proposal Format

The bidder's proposal must effectively communicate their solution and be formatted in the specified formats in order for the Bank to evaluate the proposal. Therefore, proposals must be submitted with the following sections in proper order and bound.

The technical bid should be structured in the following sequence

1. Covering letter as per Appendix 2 Form 01.
2. Executive Summary: The Executive Summary should be limited to a maximum of five pages and should summarize the content of the response. The Executive Summary should initially provide an overview of bidder's organization and position with regards to CSOC services for Banking Sector. A summary of the bidder's facilities and services that will be provided as a part of this procurement should follow. A brief description of the unique qualifications of the bidder should then be provided followed by a summary on capabilities such as resources and past experience of providing such services. Information provided in the Executive Summary is to be presented in a clear and concise manner.
3. Technical Requirements compliance: The CSOC Solution Features Section of the bidder's proposal must consist of a response to the technical requirements in Annexure 1. The bidder's response must explain the technical specifications wherever required.
4. Copy of Price Bid without commercials as per Appendix 1 Form 02 – Commercial Bid Details;
5. Queries in the format as given in Appendix 2 Form 02;
6. Conformity with Hardcopy Letter in Annexure 5.
7. OEM Authorization form as given in Appendix 2 Form 02.
8. Information about Expiry of the components as given in Annexure - 3
9. List of supported devices as given in Annexure - 2
10. Bid Security Deposit as given in Annexure – 8

7.3 Bid Security Deposit

The bidder shall furnish, as part of its bid, bid security of an amount mentioned in section 1 of this document. The bid security is required to protect the Bank against the risk of bidder's conduct.

The bid security shall be denominated in the INDIAN RUPEES only and shall be in the form of a Demand Draft favoring "Bank of Maharashtra" by a Scheduled Commercial Bank or a foreign bank located in India in the form provided in the RFP (Annexure - 8 - Bid Security Form). Any bid not secured in accordance with the above will be rejected by Bank of Maharashtra as non-responsive.

Unsuccessful bidder's bid security will be returned by the Bank.

The successful bidder's bid security will be discharged upon the bidder signing the Contract and furnishing the performance security.

The bid security may be forfeited:

a. If a bidder withdraws its bid during the period of bid validity specified by the bidder on the Bid Form; or

b. In case of the successful SI, if the BIDDERfails to:

   i. Sign the Contract within 1 month of issue of purchase order / letter of intent.

   ii. Furnish performance bank guarantee within 10 days of signing the contract.

8. Terms and conditions

8.1 General

The bidders should adhere to the terms of this tender document and the Bank would not accept any deviations to 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 in Appendix 2 Form 02 - Query Format. The Bank reserves its right to not accept such deviations to the tender terms.

The bidder appointed under the tender document shall have the single point responsibility for fulfilling all obligations and providing all deliverables and services required for project of “Implementation and Maintenance of Cyber Security Operations Center on Captive Model”.

Unless agreed to specifically by the Bank in writing for any changes to the tender document issued, the bidder responses would not be incorporated automatically in the tender document. Unless expressly overridden by the specific agreement to be entered into between the Bank and the SI, the tender document shall be the governing document for arrangement between the Bank and the SI.

8.2 Rules for responding to the tender document

Response document

All responses should be in English language. All responses by the bidder to this tender document shall be binding on such bidder for a period of 180 days after opening of the commercial bids

The technical bid, submitted cannot be withdrawn / modified after the last date for submission of the bids unless specifically permitted by the Bank. In case, due to unavoidable circumstances, the Bank does not award the contract within six months from the last date of the submission of the bids, and there is a possibility to award the same within a short duration, the bidder would have the choice to maintain the bid security with the Bank or to withdraw the bid and obtain the security provided.

The bidder may modify or withdraw its offer after submission, provided that, the Bank, prior to the closing date and time, and receives a written notice of the modification or withdrawal prescribed for submission of offers. No offer can be modified or withdrawn by the bidder subsequent to the closing date and time for submission of the offers.

The bidder is required to quote for all the components/services mentioned in the Section 4.2 “Project scope” and Section 5 “Detailed Requirements” and all other requirements of this RFP. In case the bidder does not quote for any of the components/services, the response would be deemed to include the quote for such unquoted components/service. It is mandatory to submit the details in the formats provided along with this document duly filled in, along with the offer. The Bank reserves the right not to allow / permit changes in the technical

specifications and not to evaluate the offer in case of non-submission of the technical details in the required format or partial submission of technical details.

The offer should specify only a single product for the CSOC solution and for each of the components required as a part of solution implementation, which is cost-effective and meeting the tender document specifications. It is the responsibility of the bidder to provide the best suitable solution. However, bidder should not offer more than one product for the entire solution or any component of the solution.

For example, Product A & Product B both offer SIEM solution; a bidder should offer either Product A or Product B. And if the solution requires an Anti-Phishing component provided by Product X & Product Y, the bidder may choose to offer only Product X or only Product Y for Anti Phishing. This means a bidder's offer may cover Product A or Product B (not both) for SIEM solution and Product X or Product Y (not both) for Anti-Phishing.

In the event the bidder has not quoted for any mandatory or optional items as required by the Bank and forming a part of the tender document circulated to the bidder's and responded to by the SI, the same will be deemed to be provided by the bidder at no extra cost to the Bank.

In the event optional prices (if requested in RFP) are not quoted by the vendor, for items where such prices are a must and required to be quoted for, the highest price quoted by any of the participating vendor will be taken as the costs, for such alternatives and also for arriving at the Total Cost of Ownership for the purpose of evaluation of the vendor. The same item has to be supplied by the vendor free of cost.

The Bank is not responsible for any assumptions or judgments made by the bidder for proposing and implementing solution. The Bank's interpretation will be final.

The Bank ascertains and concludes that everything as mentioned in the tender documents circulated to the bidder and responded by the bidder have been quoted for by the SI, and there will be no extra cost associated with the same in case the bidder has not quoted for the same.

In the event the Bank has not asked for any quotes for alternative prices, and the bidder furnishes the alternative price in the bidder's financial bid, the higher of the prices will be taken for calculating and arriving at the Total Cost of Ownership. However payment by the Bank will be made at the lower price. The Bank in this case may also reject the offer outright.

In the event optional prices (if requested in RFP) are not quoted by the bidder, for items where such prices are must and required to be quoted for, the highest price quoted by any of the participating bidder will be taken as the costs, for such alternatives and also for arriving at the Total Cost of Ownership for the purpose of evaluation. The same item has to be supplied by the bidder free of cost.

The bidder at no point in time can excuse themselves from any claims by the Bank whatsoever for their deviations in confirming to the terms and conditions, payments schedules, time frame for site readiness and availability etc. as mentioned in the tender document circulated by the Bank. bidder shall be fully

responsible for deviations to the terms & conditions, site readiness etc. as proposed in the tender document

8.2.1 Price Bids (through e-procurement process)

The bidder is requested to quote in Indian Rupees ('INR'). Bids in currencies other than INR would not be considered. The date for e-procurement would be communicated separately to the successful bidder post the completion of the eligibility and technical evaluation.

The prices and other terms offered by the bidders must be firm for an acceptance period of 180 days from the date of e-procurement process.

The prices quoted by the bidder shall include all costs such as, taxes, levies, cess, excise and custom duties wherever applicable that need to be incurred except Service Tax and VAT.

If the bidder makes any conditional or vague offers, without conforming to these guidelines, the Bank will treat the prices quoted as in conformity with these guidelines and proceed accordingly.

Terms of payment as indicated in the Purchase Contract that will be issued by the Bank on the selected bidder will be final and binding on the bidder and no interest will be payable by the Bank on outstanding amounts under any circumstances. If there are any clauses in the Invoice contrary to the terms of the Purchase Contract, the bidder should give a declaration on the face of the Invoice or by a separate letter explicitly stating as follows "Clauses, if any contained in the Invoice which are contrary to the terms contained in the Purchase Contract will not hold good against the Bank and that the Invoice would be governed by the terms contained in the Contract concluded between the Bank and the bidder". Bidder should ensure that the project should not suffer for any reason.

8.2.2 Price Comparisons

The Bank will consider the Total Cost of Ownership (TCO) over a five-year period starting from date of acceptance of the Solution. The optional (if requested in RFP) items would also be considered in the TCO.

Comprehensive charges must be quoted, on yearly basis, after taking due consideration for the requirements and support period and providing the adequate benefit to the Bank.

The Bank, may decide to choose to avail the optional items at any point during the contract on the same cost.

For comparison purposes the Bank will consider the Optional (if requested in RFP) Items as well.

The Price offer shall be on a fixed price basis and should include: All taxes, duties and levies, Service Tax of whatsoever nature if any; and Services which are required to be extended by the bidder in accordance with the terms and conditions of the contract. The bidder must provide and quote for all the services as desired by the Bank as mentioned in this tender document.

8.2.3 Performance Guarantee

If the contract is awarded, the bidder should furnish a Performance Bank Guarantee in the format as required by the Bank to the extent of 10% of the value of the contract within 10 days of the date of receipt of the purchase contract. The performance guarantee would be for the entire period of the Contract. If the Performance guarantee is not submitted, the Bank reserves the right to cancel the contract. The Performance Guarantee would be returned to the bidder after the expiry or termination of the contract.

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.

Responses to this tender document should not be construed as an obligation on the part of the Bank to award a purchase contract for any services or combination of services. Failure of the Bank to select a bidder shall not result in any claim whatsoever against the bank. The Bank reserves the right to reject any or all bids in part or in full, without assigning any reason whatsoever.

By submitting a proposal, the bidder agrees to promptly contract with the Bank for any work awarded to the bidder. Failure on the part of the awarded bidder to execute a valid contract with the Bank will relieve the Bank of any obligation to the bidder, and a different bidder may be selected.

Any additional or different terms and conditions proposed by the bidder would be rejected unless expressly assented to in writing by the Bank and accepted by the Bank in writing.

The bidder must strictly adhere to the delivery dates or lead times identified in their proposal. Failure to meet these delivery dates, unless it is due to reasons entirely attributable to the Bank, may constitute a material breach of the bidder's performance. In the event that the Bank is forced to cancel an awarded contract (relative to this tender document) due to the bidder's inability to meet the established delivery dates, that bidder will be responsible for any re-procurement costs suffered by the Bank. The liability in such an event could be limited to the amount actually spent by the Bank for procuring similar deliverables and services or is limited to 10% on the total cost whichever is higher.

The bidder represents and acknowledges to the Bank that it possesses necessary experience, expertise and ability to undertake and fulfill its obligations, of providing services for effective Cyber Security Operations Center. 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 tender document, the bidder should fulfill all the terms and conditions of this tender document.

The bidder represents that the proposed Solution and its documentation and/or use of the same by the Bank shall not violate or infringe the rights of any third

party or the laws or regulations under any governmental or judicial authority. The bidder further represents that the documentation to be provided to the Bank shall contain a complete and accurate description of the proposed solution. The bidder represents and undertakes to obtain and maintain validity throughout the contract, of all appropriate registrations permissions and approvals, which are statutorily required to be obtained by the bidder for performance of the obligations of the bidder. The bidder further undertakes to inform and assist the Bank for procuring any registrations, permissions or approvals, which may at any time during the Contract Period be statutorily required to be obtained by the Bank for availing services from the bidder.

All terms and conditions, payments schedules, time frame for expected service levels as per this tender will remain unchanged unless explicitly communicated by the Bank in writing to the bidder. The Bank shall not be responsible for any judgments made by the bidder with respect to any aspect of the Service. The bidder shall at no point be entitled to excuse themselves from any claims by the Bank whatsoever for their deviations in confirming to the terms and conditions, payments schedules, expected service levels, time frame for site availability etc. as mentioned in this tender document.

The Bank and the bidder covenants and represents to the other Party the following:

It is duly incorporated, validly existing and in good standing under as per the laws of the state in which such Party is incorporated.

It has the corporate power and authority to enter into Agreements and perform its obligations there under. The execution, delivery and performance of terms and conditions under Agreements by such Party and the performance of its obligations there under are duly authorized and approved by all necessary action and no other action on the part of such Party is necessary to authorize the execution, delivery and performance under an Agreement.

The execution, delivery and performance under an Agreement by such Party:

- Will not violate or contravene any provision of its documents of incorporation;
- Will not violate or contravene any law, statute, rule, regulation, licensing requirement, order, writ, injunction or decree of any court, governmental instrumentality or other regulatory, governmental or public body, agency or authority by which it is bound or by which any of its properties or assets are bound;
- Except to the extent that the same have been duly and properly completed or obtained, will not require any filing with, or permit, consent or approval of or license from, or the giving of any notice to, any court, governmental instrumentality or other regulatory,

governmental or public body, agency or authority, joint venture party, or any other entity or person whatsoever;

- To the best of its knowledge, after reasonable investigation, no representation or warranty by such Party in this Agreement, and no document furnished or to be furnished to the other Party to this Agreement, or in connection herewith or with the transactions contemplated hereby, contains or will contain any untrue or misleading statement or omits or will omit any fact necessary to make the statements contained herein or therein, in light of the circumstances under which made, not misleading. There have been no events or transactions, or facts or information which has come to, or upon reasonable diligence, should have come to the attention of such Party and which have not been disclosed herein or in a schedule hereto, having a direct impact on the transactions contemplated hereunder.

- *The* bidder *undertakes to provide appropriate human as well as other resources required, to provide the requirement for Bank's Cyber Security Operations Center as part of the contract, from time to time.*

The Bank would not return the bid documents to the bidders. The Bank shall not be held liable for costs incurred during any negotiations on proposals or proposed contracts or for any work performed in connection therewith.

8.2.4 Changes to the tender document

This tender document may undergo change by either additions or deletions or modifications before the actual award of the contract by the Bank. The Bank also reserves the right to change any terms and conditions of the tender document and its subsequent addendums as it deems necessary at its sole discretion. The bank will inform all bidders about changes, if any.

The Bank may revise any part of the tender document, by providing a written addendum to all short-listed bidders at stage till the award of the contract. The Bank reserves the right to issue revisions to this tender document at any time before the award date.

The Bank reserves the right to extend the dates for submission of responses to this document.

Bidders shall have the opportunity to clarify doubts pertaining to the tender document in order to clarify any issues they may have, prior to finalizing their responses. All questions are to be submitted to the General Manager, IT at the address mentioned in earlier, and should be received by the point of contact no later than the time specified in Section 1 of this document. Responses to inquiries and any other corrections and amendments will be distributed to all the bidders in the form of electronic mail or hardcopy or updated on the Bank's website or newspaper journals; the preference for distribution would be with the Bank. The SI, who posed the question, will remain anonymous.

Preliminary Scrutiny – The Bank will scrutinize the offers to determine whether they are complete, whether any errors have been made in the offer, whether required technical documentation has been furnished, whether the documents have been properly signed, and whether items are quoted as per the schedule. The Bank may, at its discretion, waive any minor non-conformity or any minor deficiency in an offer. This shall be binding on all bidders and the Bank reserves the right for such waivers and the Banks decision in the matter will be final.

Clarification of Offers – To assist in the scrutiny, evaluation and comparison of offers, the Bank may, at its discretion, ask some or all bidders for clarification of their offer. The Bank has the right to disqualify the bidder whose clarification is found not suitable to the proposed project.

The Bank reserves the right to make any changes in the terms and conditions of purchase. The Bank will not be obliged to meet and have discussions with any bidder, and / or to listen to any representations.

Erasures or Alterations – 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 of the product being offered must be filled in. Filling up of the information using terms such as "OK", "accepted", "noted", "as given in brochure /

manual" is not acceptable. The Bank may treat the offers not adhering to these guidelines as unacceptable.

Bidder presentation – Bidders are requested to be prepared to make presentations and arrange for reference site visits, as part of the final evaluation in accordance with the responses given for the identified requirements, any time after the last date for submissions of bids. The Bank will communicate a date and time to the bidder any time after the last date for submission of bids.

Details of Sub-contracts, as applicable – If required by the Bank, bidders should provide complete details of any subcontractor/s used for the purpose of this engagement. It is clarified that notwithstanding the use of sub contractors by the bidder, the bidder shall be solely responsible for performance of all obligations under the tender document irrespective of the failure or inability of the subcontractor chosen by the bidder to perform its obligations. The bidder shall also have the responsibility for payment of all dues and contributions, as applicable, towards statutory benefits for its employees and sub-contractors.

If the Bank is not satisfied with the technical specifications as specified in the tender document and observes major deviations, the bidder will have to submit the clarification within 3 days from the day it was conveyed to the bidder regarding the same.

The solution will not be accepted as complete if any facility /service as required is not available or not up to the standards projected by bidder in their response and the requirement of this tender.

There will be an acceptance inspection by the Bank or its nominated consultants for the Solution. In case of discrepancy in facilities /services provided, the Bank reserves the right to cancel the entire purchase contract. The inspection will be arranged by the bidder at the sites in the presence of the officials of the Bank and / or its consultants. The contract tenure for the Solution will commence after acceptance of the Solution by the Bank. The Bank will accept the solution on satisfactory completion of the above inspection. The Installation cum Acceptance Test & Check certificates jointly signed by bidder's representative and Bank's official or any consultant / auditor appointed by the Bank should be received at IT Department, Pune along with invoice etc. for scrutiny before taking up the request for consideration of payment.

The bidder is responsible for managing the activities of its personnel or the personnel of its subcontractors/franchisees and will be accountable for both. The bidder shall be vicariously liable for any acts, deeds or things done by their employees, agents, contractors, subcontractors etc. which is outside the scope of power vested or instructions issued by the Bank. Bidder shall be the principal employer of the employees, agents, contractors, subcontractors etc. engaged by bidder and shall be vicariously liable for all the acts, deeds or things, whether the same is within the scope of power or outside the scope of power, vested under the purchase contract to be issued for this tender. No right of any employment shall accrue or arise, by virtue of engagement of employees, agents, contractors, subcontractors etc. by the bidder, for any assignment under the purchase contract to be issued for this tender. All remuneration, claims, wages, dues etc. of

such employees, agents, contractors, subcontractors etc. of bidder shall be paid by bidder alone and the Bank shall not have any direct or indirect liability or obligation, to pay any charges, claims or wages of any of bidder's employee, agents, contractors, and subcontractors. The bidder shall hold the Bank, its successors, Assignees and Administrators fully indemnified and harmless against loss or liability, claims actions or proceedings, if any, that may arise from whatsoever nature caused to the Bank through the action of its employees, agents, contractors, subcontractors etc. However, the bidder would be given an opportunity to be heard by the Bank prior to making of a decision in respect of such loss or damage.

The Bank shall inform the bidder all breaches and claims of indemnification and shall grant the bidder sole authority to defend, manage, negotiate or settle such claims; and make available all reasonable assistance in defending the claims (at the expense of the bidder). The written demand by the Bank as to the loss / damages mentioned above shall be final, conclusive and binding on the bidder and bidder shall be liable to pay on demand the actual amount of such loss / damages caused to the Bank.

In respect of demands levied by the Bank on the bidder towards breaches, claims, etc. the Bank shall provide the bidder with details of such demand levied by the Bank.

For the purposes of this Clause, the indemnity may be restricted to the areas mentioned, i.e., "claims arising out of employment, non-payment of remuneration and non-provision of statutory benefits by the bidder to its employees, its agents, contractors and sub contractors."

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

The Bank will scrutinize the technical bill of material and conformity to the requirements as specified in the RFP. As part of this process the Bank will try and normalize to the extent possible technical requirements and comparisons to the extent possible between vendors. In the event of major deviations in the technical bids submitted by the bidder, the Bank may choose to provide for a re-pricing option to all the technically short-listed bidder's. The bidder agrees that it has no reservations with this process.

9. Terms of Reference

9.1 Contract Commitment

The Bank intends that the contract, which is contemplated herein with the SI, shall be for a period of FIVE years. The Bank at its sole discretion may enter into the 5 year contract for “Implementation and Maintenance of Cyber Security Operations Center on Captive Model”. The contract period will start from the date of acceptance of the project.

9.2 Payment terms

The bidder must accept the payment terms proposed by the Bank. The financial bid submitted by the bidder during the e-procurement process 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.

Hardware Payment – 75% of hardware payment will be done after delivery of hardware. For payment of delivery, complete set of hardware will be considered, partial delivery will not be considered for payment. Remaining 25% of hardware payment will be done after successful acceptance of the project by the Bank.

Cost of Licenses – 100% payment on delivery of evidence for License. All the licenses must be in the name of the Bank.

One Time Charges – One time charges for installation and configuration for all CSOC components will be paid on successful acceptance by the Bank.

SOC Operation - The payment for CSOC Operations will be divided into 4 equal installments for the year and paid quarterly in arrears post the successful commissioning of the project and acceptance of all the relevant requirements under this tender.

Annual Maintenance Charges - The payment for Annual Maintenance of hardware and software will be divided into 4 equal installments for the year and paid quarterly in arrears post the successful commissioning of the project and acceptance of all the relevant requirements under this tender.

Training Charges – On successful completion of training.

9.3 Acceptance of the Project

The Bank will carry out the inspection of the Project Implementation prior to the Project Acceptance. The bidder shall ensure that all the deliverables are in place and will submit to the Bank all the required evidences and records for the Bank to carry out Project Acceptance

9.4 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/staff/ 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.

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/ staff/ 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 there from and the Bank will give notice of any such claim or demand of liability within reasonable time to the bidder.

This indemnification is only a remedy for the Bank. The bidder is not absolved from its responsibility of complying with the statutory obligations as specified above. Indemnity would be limited to court awarded damages and shall exclude indirect, consequential and incidental damages. However indemnity would cover damages, loss or liabilities suffered by the bank arising out of claims made by its customers and/or regulatory authorities.

9.5 Order cancellation

The Bank reserves its right to cancel the order in the event of one or more of the following situations, that are not occasioned due to reasons solely and directly attributable to the Bank alone:

- Delay in site readiness and handing over the site to the Bank.
- Serious discrepancy in the quality of service / facility / security.
- In case of order cancellation, any payments made by the Bank to the bidder would necessarily have to be returned to the Bank with interest @ 15% per annum, further the bidder would also be required to compensate the Bank for

any direct loss incurred by the Bank due to the cancellation of the contract and any additional expenditure to be incurred by the Bank to appoint any other bidder. This is after repaying the original amount paid.

9.6 Indemnity

Bidder shall indemnify, protect and save the Bank and hold the Bank harmless from and against all claims, losses, costs, damages, expenses, action suits and other proceedings, (including reasonable attorney fees), relating to or resulting directly or indirectly from (i) an act or omission of the bidder, its employees, its agents, or employees of the consortium in the performance of the services provided by this contract, (ii) breach of any of the terms of this tender document or breach of any representation or warranty by the bidder, (iii) use of the allocated site and or facility provided by the bidder, (iv) infringement of any patent, trademarks, copyrights etc. or such other statutory infringements in respect of all components used to facilitate and to fulfill the scope of the site requirement. The bidder shall further indemnify the Bank against any loss or damage arising out of loss of data, claims of infringement of third-party copyright, patents, or other intellectual property, and third-party claims on the Bank for malfunctioning of the equipment/s providing facility to Bank's equipments at all points of time, provided however, (i) the Bank notifies the bidder in writing immediately on aware of such claim, (ii) the bidder has sole control of defense and all related settlement negotiations, (iii) the Bank provides the bidder with the assistance, information and authority reasonably necessary to perform the above, and (iv) the Bank does not make any statement or comments or representations about the claim without prior written consent of the SI, except under due process of law or order of the court. It is clarified that the bider shall in no event enter into a settlement, compromise or make any statement (including failure to take appropriate steps) that may be detrimental to the Bank's (and/or its customers, users and bidders) rights, interest and reputation.

The bidder's should indemnify the Bank (including its employees, directors or representatives) from and against claims, losses, and liabilities arising from:

- Non-compliance of the bidder with Laws / Governmental Requirements
- IP infringement
- Negligence and misconduct of the SI, its employees, and agents
- Breach of any terms of tender document or Representation made by the bidder.
- Act or omission in performance of service.
- Loss of data due to bidder provided facility.

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

The bidder shall not indemnify the Bank for

(i) Any loss of profits, revenue, contracts, or anticipated savings or

(ii) Any consequential or indirect loss or damage however caused, provided that the claims against customers, users and bidders of the Bank would be considered as a “direct” claim.

9.7 Inspection of records

All records captured – video, security register, access control of Bank’s, hardware movement, helpdesk tickets, escalations etc for the allocated server room, NOC room and any other area provided to the Bank shall be made available to the Bank or its designees at any time during normal business hours, as often as the Bank deems necessary, to audit, examine, and make excerpts or transcripts of all relevant data. Said records are subject to examination. Bank’s auditors would execute confidentiality agreement with the bidder, provided that the auditors would be permitted to submit their findings to the Bank, which would be used by the Bank. The cost of the audit will be borne by the Bank. The scope of such audit would be limited to Service Levels being covered under the contract, and financial information would be excluded from such inspection, which will be subject to the requirements of statutory and regulatory authorities.

9.8 Publicity

Any publicity by the bidder in which the name of the Bank is to be used should be done only with the explicit written permission of the Bank.

9.9 Solicitation of Employees

Both the parties agree not to hire, solicit, or accept solicitation (either directly, indirectly, or through a third party) for their employees directly involved in this contract during the period of the contract and one year thereafter, except as the parties may agree on a case-by-case basis. The parties agree that for the period of the contract and one year thereafter, neither party will cause or permit any of its directors or employees who have knowledge of the agreement to directly or indirectly solicit for employment the key personnel working on the project contemplated in this proposal except with the written consent of the other party. The above restriction would not apply to either party for hiring such key personnel who (i) initiate discussions regarding such employment without any direct or indirect solicitation by the other party (ii) respond to any public advertisement placed by either party or its affiliates in a publication of general circulation or (iii) has been terminated by a party prior to the commencement of employment discussions with the other party.

9.10 Penalties and delays in bidder’s performance

The bidder should provide uninterrupted services for ensuring implementation and maintenance of the Cyber Security Operations Center as per the requirements of this tender. Inability of the bidder to either ensure deliverables as per specifications within defined timelines or to meet the service levels as specified in this RFP shall be treated as breach of contract and would invoke the penalty clause.

The proposed rate of penalty with respect to non-adherence to service levels is mentioned in Service level in this RFP. Overall cap for penalties will be 10% of

the contract value. Thereafter, the contract may be cancelled. The bank also has the right to invoke the performance guarantee. Penalties on delay will be applicable when the delay is not attributable to the bank.

Notwithstanding anything contained above, no such penalty will be chargeable on the bidder for the inability occasioned, if such inability is due to reasons entirely attributable to the Bank.

Delivery of the Goods and performance of the Services shall be made by the bidder in accordance with the time schedule specified by the Bank.

If at any time during performance of the Contract, the bidder should encounter conditions impeding timely delivery of the Goods and performance of the Services, the bidder shall promptly notify the Bank in writing of the fact of the delay, its likely duration and its cause(s). As soon as practicable after receipt of the bidder's notice, the Bank shall evaluate the situation and may at its discretion extend the bidder's time for performance, with or without liquidated damages, in which case the extension shall be ratified by the parties by amendment of the Contract.

Any delay by the bidder in the performance of its delivery obligations shall render the bidder liable to the imposition of liquidated damages, unless extension of time is agreed upon without the application of liquidated damages

LIQUIDATED DAMAGES

The Bank will consider the inability of the bidder to deliver or install the equipment within the specified time limit, as a breach of contract and would entail the payment of Liquidation Damages on the part of the bidder. The liquidation damages represent an estimate of the loss or damage that the Bank may have suffered due to delay in performance of the obligations (relating to delivery, installation, Operationalization, implementation, training, acceptance, warranty, maintenance etc. of the Cyber Security Operations Center) by the bidder.

Installation will be treated as incomplete in one/all of the following situations:

- Non-delivery of any component or other services mentioned in the order
- Non-delivery of supporting documentation
- Delivery/Availability, but no installation of the components and/or software
- No Integration
- System operational, but unsatisfactory to the Bank

If the bidder fails to deliver any or all of the Goods or perform the Services within the time period(s) specified in the Contract, the Bank shall, without prejudice to its other remedies under the Contract, deduct from the Contract Price, as liquidated damages, a sum equivalent to 0.50% of the complete contract amount until actual delivery or performance, per week or part thereof (3 days will be treated as a week); and the maximum deduction is 10% of the contract price. Once the maximum is reached, the Bank may consider termination of the contract.

9.11 Confidentiality

The RFP document is confidential and is not to be disclosed, reproduced, transmitted, or made available by the Recipient to any other person. The RFP document is provided to the Recipient on the basis of the undertaking of confidentiality given by the Recipient to Bank. 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.

Responses received become the property of the Bank and cannot 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.

“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:

(a) Relates to the Disclosing Party; and

(b) 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

(c) Is prepared or performed by or on behalf of the Disclosing Party by its employees, officers, directors, agents, representatives or consultants.

(d) Without limiting the generality of the foregoing, Confidential Information shall mean and include any information, data, analysis, compilations, notes, extracts, materials, reports, drawings, designs, specifications, graphs, layouts, plans, charts, studies, memoranda or other documents, or materials that may be shared by the Bank with the bidder to host Banks equipments at the site.

(e) “Confidential Materials” shall mean all tangible materials containing Confidential Information, including, without limitation, written or printed documents and computer disks or tapes, whether machine or user readable.

(f) Information disclosed pursuant to this clause will be subject to confidentiality for the term of contract plus two years.

1. 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:

2. 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.

3. In maintaining confidentiality hereunder the Receiving Party on receiving the confidential information and materials agrees and warrants that it shall:

   - 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;
   - 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;
   - Limit access to such Confidential Information and materials to those of its directors, partners, advisers, agents or employees, sub contractors and contractors who are directly involved in the consideration/evaluation of the Confidential Information and bind each of its directors, partners, advisers, agents or employees, sub contractors and contractors 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.

4. The Receiving Party who receives the confidential information and materials agrees that on receipt of a written demand from the Disclosing Party:

   a. 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;

   b. 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;

   c. So far as it is practicable to do so immediately expunge any Confidential Information relating to the Disclosing Party or its projects from any computer, word processor or other device in its possession or under its custody and control; and

   d. 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.

5. The restrictions in the preceding clause shall not apply to:
    a. 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.
    b. 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.
    c. 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.
    d. The confidentiality obligations shall survive the expiry or termination of the agreement between the bidder and the Bank.

9.12 Force Majeure

1. The bidder shall not be liable for forfeiture of its performance security, liquidated damages or termination for default, if any to the extent that its delay in performance or other failure to perform its obligations under the contract is the result of an event of Force Majeure.
2. For purposes of this Clause, "Force Majeure" means an event explicitly beyond the reasonable control of the bidder and not involving the bidder's fault or negligence and not foreseeable. Such events may include, Acts of God or of public enemy, acts of Government of India in their sovereign capacity and acts of war.
3. If a Force Majeure situation arises, the bidder shall promptly notify the Bank in writing of such conditions and the cause thereof within fifteen calendar days. Unless otherwise directed by the Bank in writing, the bidder shall continue to perform bidder’s 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.
4. In such a case the time for performance shall be extended by a period (s) not less than duration of such delay. If the duration of delay continues beyond a

period of three months, the Bank and the bidder shall hold consultations in an endeavor to find a solution to the problem.

9.13 Resolution of disputes

1. The Bank and the supplier bidder shall make every effort to resolve amicably, by direct informal negotiation between the respective project directors of the Bank and the bidder, any disagreement or dispute arising between them under or in connection with the contract.
2. If the Bank project director and bidder project director are unable to resolve the dispute after thirty days from the commencement of such informal negotiations, they shall immediately escalate the dispute to the senior authorized personnel designated by the bidder and Bank respectively.
3. If after thirty days from the commencement of such negotiations between the senior authorized personnel designated by the bidder and Bank, the Bank and the bidder have been unable to resolve contractual dispute amicably, either party may require that the dispute be referred for resolution through formal arbitration.
4. All questions, disputes or differences arising under and out of, or in connection with the contract or carrying out of the work whether during the progress of the work or after the completion and whether before or after the determination, abandonment or breach of the contract shall be referred to arbitration by a sole Arbitrator: acceptable to both parties OR the number of arbitrators shall be three, with each side to the dispute being entitled to appoint one arbitrator. The two arbitrators appointed by the parties shall appoint a third arbitrator shall act as the chairman of the proceedings. The award of the Arbitrator shall be final and binding on the parties. The Arbitration and Reconciliation Act 1996 or any statutory modification thereof shall apply to the arbitration proceedings and the venue of the arbitration shall be Mumbai.
5. If a notice has to be sent to either of the parties following the signing of the contract, it has to be in writing and shall be first transmitted by facsimile transmission by postage prepaid registered post with acknowledgement due or by a reputed courier service, in the manner as elected by the Party giving such notice. All notices shall be deemed to have been validly given on (i) the business date immediately after the date of transmission with confirmed answer back, if transmitted by facsimile transmission, or (ii) the expiry of five days after posting if sent by registered post with A.D., or (iii) the business date of receipt, if sent by courier.
6. This tender document shall be governed and construed in accordance with the laws of India. The courts of Mumbai alone and no other courts shall be entitled to entertain and try any dispute or matter relating to or arising out of this tender document. Notwithstanding the above, the Bank shall have the right to initiate appropriate proceedings before any court of appropriate jurisdiction, should it find it expedient to do so.

9.14 Exit option and contract re-negotiation

1. The Bank reserves the right to cancel the contract in the event of happening one or more of the following Conditions:
    a. Failure of the successful bidder to accept the contract and furnish the Performance Guarantee within 10 days of receipt of purchase contract;
    b. Delay in providing the site with complete readiness;
    c. Serious discrepancy in functionality of any service, which has an impact on the Bank's equipments in production environment;
2. In addition to the cancellation of purchase contract, Bank reserves the right to appropriate the damages through encashment of Bid Security / Performance Guarantee given by the bidder.
3. The Bank will reserve a right to re-negotiate the price and terms of the entire contract with the bidder at more favorable terms in case such terms are offered in the industry at that time.
4. Notwithstanding the existence of a dispute, and/or the commencement of arbitration proceedings, the bidder should continue to provide the facilities to the Bank at the site.
5. Reverse transition mechanism would be activated in the event of cancellation of the contract or exit by the parties or 6 months prior to expiry of the contract. The bidder should perform a reverse transition mechanism to the Bank or its selected vendor. The reverse transition mechanism would be over a period of 6 months post the completion of the 90 day notice period to facilitate an orderly transfer of services to the Bank or to an alternative 3rd party / vendor nominated by the Bank. Where the Bank elects to transfer the responsibility for service delivery to a number of vendors Bank will nominate a bidder who will be responsible for all dealings with the bidder regarding the delivery of the reverse transition services.
6. The reverse transition services to be provided by the vendor shall include the following:
    a. The vendor shall suitably and adequately train the Bank's or its designated team for fully and effectively manning, operating and maintaining the data center.
    b. Vendor shall provide adequate documentation thereof.
    c. The vendor shall jointly manage the data center with the bank or designated team for a reasonable period of time
    d. The vendor shall assist the bank in relocation of disaster recovery site facility, if desired by the bank.
7. Knowledge transfer: The Vendor shall provide such necessary information, documentation to the Bank or its designee, for the effective management and maintenance of the Deliverables under this Agreement. Vendor shall provide documentation (in English) in electronic form where available or otherwise a

single hardcopy of all existing procedures, policies and programs required to support the Services. Such documentation will be subject to the limitations imposed by Vendor's Intellectual Property Rights of this Agreement.

8. Warranties:
    a. All the warranties held by or in the name of the vendor shall be assigned or transferred as-is, in the name of the bank. The vendor shall execute any and all such documents as may be necessary in this regard.
    b. The parties shall return confidential information and will sign off anc acknowledge the return of such confidential information.
    c. The vendor shall provide all other services as may be agreed by the parties in connection with the reverse transition services. However, in case any other services, in addition to the above are needed, the same shall be scoped and priced.
    d. The vendor recognizes that considering the enormity of the assignment, the transition services listed herein are only indicative in nature and the vendor agrees to provide all assistance and services required for fully and effectively transitioning the services provided by the vendor under the scope, upon termination or expiration thereof, for any reason whatsoever.

9. The cost for reverse transition if any should be part of the commercial offer.
10. During which the existing SI would transfer all knowledge, know how and other things necessary for the Bank or new vendor to take over and continue to manage the services. The bidder agrees that the reverse transition mechanism and support during reverse transition will not be compromised or affected for reasons whatsoever be for cancellation or exist of the parties.
11. The Bank shall have the sole and absolute discretion to decide whether proper reverse transition mechanism over a period of 6 months, has been complied with. In the event of the conflict not being resolved, the conflict will be resolved through Arbitration.
12. The Bank and the bidder shall together prepare the Reverse Transition Plan. However, the Bank shall have the sole decision to ascertain whether such Plan has been complied with.
13. The bidder agrees that in the event of cancellation or exit or expiry of the contract it would extend all necessary support to the Bank or its selected vendors as would be required in the event of the shifting of the site

9.15 Corrupt and fraudulent practices

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

"Corrupt Practice" means the offering, giving, receiving or soliciting of any thing of values to influence the action of an official in the procurement process or in contract execution AND

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

The Bank reserves the right to reject a proposal for award if it determines that the bidder recommended for award has engaged in corrupt or fraudulent practices in competing for the contract in question.

The Bank reserves the right to declare a firm ineligible, either indefinitely or for a stated period of time, to be awarded a contract if at any time it determines that the firm has engaged in corrupt or fraudulent practices in competing for or in executing the contract.

9.16 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 tender document 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 plarty 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 tender document 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.

9.17 Violation of terms

The Bank clarifies that the Bank shall be entitled to an injunction, restraining order, right for recovery, suit for specific performance or such other equitable relief as a court of competent jurisdiction may deem necessary or appropriate to restrain the bidder from committing any violation or enforce the performance of the covenants, obligations and representations contained in this tender document. 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.

9.18 Termination

1. The Bank shall be entitled to terminate the agreement with the bidder at any time by giving ninety (90) days prior written notice to the bidder.
2. The Bank shall be entitled to terminate the agreement at any time by giving notice if:
    a. The bidder breaches its obligations under the tender document or the subsequent agreement and if the breach is not cured within 15 days from the date of notice.

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

3. The bidder shall have right to terminate only in the event of winding up of the Bank.

9.19 Effect of termination

1. The bidder agrees that it shall not be relieved of its obligations under the reverse transition mechanism notwithstanding the termination of the assignment.
2. Same terms (including payment terms) which were applicable during the term of the contract should be applicable for reverse transition services
3. The bidder agrees that after completion of the Term or upon earlier termination of the assignment the bidder shall, if required by the Bank, continue to provide facility to the Bank at no less favorable terms than those contained in this tender document. In case the bank wants to continue with the bidder's facility after the completion of this contract then the bidder shall offer the same or better terms to the bank. Unless mutually agreed, the rates shall remain firm.
4. The Bank shall make such prorated payment for services rendered by the bidder and accepted by the Bank at the sole discretion of the Bank in the event of termination, provided that the bidder is in compliance with its obligations till such date. However, no payment for “costs incurred, or irrevocably committed to, up to the effective date of such termination” will be admissible. There shall be no termination compensation payable to the bidder.
5. Termination shall not absolve the liability of the Bank to make payments of undisputed amounts to the bidder for services rendered till the effective date of termination. Termination shall be without prejudice to any other rights or remedies a party may be entitled to hereunder or at law and shall not affect any accrued rights or liabilities or either party nor the coming into force or continuation in force of any provision hereof which is expressly intended to come into force or continue in force on or after such termination.

10. Disclaimer

The scope of work document is not an offer made by Bank of Maharashtra but an invitation for response based on which the Bank may further evaluate the response or call for alternate or more responses from other bidders. The Bank has the right to ask for other competitive quotations and can award any part or complete work to another bidders whom so ever they feel eligible for the same taking into consideration the price and quality.

Annexure -1: Bidder's Compliance to Technical requirement for Cyber Security Operations Center

Product	Sr No	Specifications	OEM/ Bidder Compliance	Marks Obtained	Maximum Marks allotted
SOC	1	Log Management shall support at least 20000 EPS			3
		Log collector at DC - 20000 EPS			3
		Log Collecor at DR - 10000 EPS			3
		Log Collector at HO - 5000 EPS			3
		Log Collector at PMO - 5000 EPS			3
	2	Collector shall be able to support store and forward method in case connectivity with log management system is not available			3
	3	Log Collector shall receive logs in its original form.			3
	4	Specify maximum number of log sources that can be connected to the collector in			12
		DC			
		DR			
		HO			
		PMO			
	5	The vendor solution shall handle surges in data events lasting up to 12 hours without interfering with its ability to operate. Any gaps in data events shall be noted along with the reason (for example, "data events are missing from 10:23:47 to 10:25:23 due to packet buffer overflow").			3
	6	Support for proposed heterogeneous devices and applications			45
		DLP			
		NAC			
		Patch Management Solution			
		Endpoint Encryption			
		Enterprise Antivirus			
		Web Filtering			
		Email Security			
		DDOS Mitigation Service			

		VPN			
		DAM			
		Server and Network Health Monitoring Tools			
		Privilege Identity Management Solution			
		File Integrity Management			
		Anti-APT solution			
		IDS, IPS Firewalls, Routers, Switches, Virtual Manager, etc.			
	7	Log Collector shall support Bandwidth Managament i.e rate limiting at the collector level			3
	8	The system shall provide filters options including the following that can be applied to all fields in the captured events.			15
		=			
		!=			
		>			
		AND			
		OR			
		NOT			
		begins with			
		ends with			
		Contains			
		starts with specified substring			
		ends with specified substring			
	9	The log management shall be able to evaluate 2 different rows in a single relationship (e.g. queries like JOIN, INNER JOIN, OUTER JOIN			3
	10	The CSOC bidder shall configure log collection is such a way, that if one log collector fails, the other log collector shall be able to collect logs from the sources and forward it to log management			3
	11	All the log collectors shall be configured under health monitoring of Bank's Health monitoring tool.			3
	12	The vendor solution shall include the ability to add a time stamp to each collected event. The vendor solution shall include the ability to automatically synchronize its timestamp clock to external servers			3

		using NTP.			
	13	The system shall be capable of supporting common log delivery methods. These shall include			24
		Syslog			
		OPSEC			
		SDEE			
		SNMP			
		raw text file			
		ODBC/ JDBC			
		JSON			
		XML			
	14	Bidder should provide list of tools used for log collection and VA scan			8
		a. Log collection tools for syslog			
		b. Log collection tools for OPSEC			
		c. Log collection tools for SDEE			
		d. Log collection tools for SNMP			
		e. Log collection tools for raw text file			
		f. Log collection tools for ODBC/ JDBC			
		g. Log collection tools for JSON			
		H. Log collection tools for XML			
	15	The logs should be stored in a format to ensure security of the logs from any unauthorized modification			3
	16	The bidder solution shall ensure the integrity of the data events against inadvertent changes. At a minimum, the bidder solution shall be able to identify that stored data events have been altered, removed, or had events inserted.			3
	17	SIEM shall be able to leverage vulnerability data to integrate it with SIEM using API or without API			3
	18	The log management shall detect and provide alarm/ ticket in case any source stops sending logs			3
	19	Dashboard shall support			12
		security profile of each IT enabled service			

		customizable at-a-glance security view			
		drill down to packet level event details			
		Real time monitoring of storage in each collector			
	20	SOC shall support Real Time Monitoring and Notification - Notify analysts by their preferred method, including e-mail, SMSs etc.			3
	21	The proposed solution shall have the ability to accept vulnerability scan and integrate it fully for rule correlation			3
	22	Customization of dashboard as per requirement of individual viewer shall be possible			3
	23	The vendor solution shall have the ability to report on the data events, including trending. The vendor response shall contain list of all included reports and a representative sample of those reports. (provide separate attachment)			3
	24	Bidder should provide a storage solution of at least 20 TB at the DC and DR separately.			3
	25	In case the bank changes network architecture, SIEM should be able to integrate accordingly.			3
	26	The SIEM solution shall have integrated Incident Management Module			3
	27	The SIEM solution shall be able to use Bank's Incident Management module for adaptive incident management, if required by the Bank			3
	28	The SLA monitoring for incident closure should be possible using Incident Management solution.			3
	29	Incident Management tool should support generation of single incident for multiple tickets generated due to various alerts such that a Parent - child relationship can be established between incidents and tickets/ tasks assigned.			3

	30	The incident management solution should have capability to structure rule-based workflow and calendar/ event based alerting capability.			3
	31	SOC should have read only access to all the integrated hosts and network devices through direct console access, database extracts, regular reporting, or a combination of all three.			3
	32	Ability to offer a bundle of various predefined reports in multiple formats, such as HTML, text, CSV, web and graphs that are customizable to the needs			3
	33	The proposed solution shall have the ability to produce, out of box, standard range of compliance reports, including HIPAA, ISO, SOX, PCI, and others. The solution shall also be able to generate customized compliance reports as per the extant RBI & GOI guidelines.			3
	34	The system shall be able to capture and store 100% of the information in the original event data, logs and alert messages and normalize them into a common standard event schema for further analysis, troubleshooting and other data processing needs. Also there should be a feasibility to send the raw logs.			3
	35	The system shall capture and fully integrate feeds from CERT-IN, IB-CART and NCIIPC			3
Anti-APT	36	The Anti-APT solution should be appliance based and should offer a minimum throughput of 10Gbps			45
	37	Appliance should support 1G, 10G and 40GigE ports and shall have provision to add a maximum of 24 ports			
	38	Appliance should support both Copper and Fibre Interfaces			
	39	Appliance shall provide a separate management port			
	40	Appliance should provide at least 500,000 new connections per			

		second and 30 Million concurrent sessions			
	41	Appliance should be capable of working in Inline Blocking mode			
	42	Appliance shall offer both fail-open and HA options to choose from			
	43	Appliance should have dual hot-swappable power supplies			
	44	The proposed solution must come with built-in performance profiling feature that tracks statistics on rule utilization that could be of benefit when it comes to tuning and determining how well the customized rules are performing.			
	45	The detection engine must be capable of detecting and preventing a wide variety of threats (e.g., malware, network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, zero-day threats, etc.).			
	46	The detection engine must be capable of inspecting traffic associated with different network segments differently (as opposed to having only one policy per interface).			
	47	The proposed solution should also support both Layer 2 and Layer 3 deployment. In Layer 2 deployment, it should support virtual switch configuration where it provides packet switching and inspection between two or more network segments. In Layer 3 deployment, it should support virtual router configuration where it can route and inspect traffic between two or more layer 3 interfaces.			

	48	The Solution include an on-premise sandbox and no file shall be sent outside of customer premises			
	49	Solution should be capable of blocking callbacks to CnC Servers and not just detect them			
	50	Solution should be capable of blocking threats based on both signatures and behavior			
	51	The Sandbox should be a propreitary custom built malware analysis solution and not open source or generic sandbox			
	52	The anti-APT Solution should be capable of employing an extensive set of contextual information (e.g., pertaining to the composition, configuration, and behavior of the network and its hosts) to improve the efficiency and accuracy of both manual and automatic analysis of detected events.			
	53	The proposed solution should be able to support continuous and root cause analysis to help in triaging of security incidents.			
	54	Detection rules should be based on an extensible, open language that enables users to create their own rules, as well as to customize any vendor-provided rules.			
	55	The proposed solution shall be capable of protecting different types of gateways including but not limited to web and email gateways.			
	56	The solution should be capable of inspecting MS Office Documents, Portable Documents, Archive Files, Multimedia Files and executable binaries			

	57	The proposed solution should be able to provide the impact analysis of the malware threat with capability to escalate the incident severity due to multiple related security incidents. Use of industry's definition on indicator of compromise as criteria for incident severity should be supported.			
	58	A hash of the malware should be created for tracking purposes and should support MD5, SHA1 and SHA256 lookups.			
	59	'Visual representation of the malware movement within network and host system is preferred to reduce investigation and aid forensic.			
	60	The solution should be capable of protecting against spear phishing attacks			
	61	The solution should have blocked at least 95% of threats in the NSS Labs Breach Detection test			
	62	The solution should be capable of exempting specific hosts from specific compliance rules and suppressing corresponding compliance events and alerts.			

	63	The solution should be capable of gathering Active Directory user identity information, mapping IP addresses to username and passively gathering information about network devices including but not limited to: ● Operating system vendor ● Operating system version ● Network protocols used, e.g. IPv6, IPv4 ● Network services provided, e.g. HTTPS, SSH ● Open ports, e.g. TCP:80 ● Client applications installed and type, e.g. Chrome - web browser ● Web applications access, e.g. Facebook, Gmail ● Risk and relevance ratings should be available for all applications ● Potential vulnerabilities ● Current User ● Device type, e.g. Bridge, Mobile device ● Files transferred by this device / user			
	64	The solution should be capable of gathering Active Directory user identity information, mapping IP addresses to username, and making this information available for event management purposes as well as access control policy decisions.			
	65	The solution should detect and classify mobile devices as mobile devices. For example: iPad, iPhone and Blackberry devices. These devices should be discovered and related back to the user, applications, and possible services they offer			
	66	The solution should be capable of whitelisting trusted applications from being inspected to avoid			

		business applications from being affected & in turn productivity			
	67	The solution should be capable of blocking traffic based on geo locations to reduce the attack landscape and to protect communication to unwanted destinations based on geography			
	68	The Solution should provide visibility into how network bandwidth is consumed to aid in troubleshooting network outages and detecting Advanced Malware related DoS & DDoS activity from within the network			
	69	The proposed solution should integrate seamlessly into the network and shall not warrant any replacement of existing devices or re-architecture of network			
	70	All the devices shall be managed centrally and should be capable of • Centralized, life cycle management for all sensors • Aggregating all events and centralized, real-time monitoring and forensic analysis of detected events • Must provide a highly customizable dashboard			
	71	The solution shall be able to graphically represent the path of a file from the time it enters the network and shall also point out the first point of compromise/ target for the event			
	72	The solution shall be able to point out the top applications introducing malware into the network along with top file types that are associated with malware in the network			

	73	Solution should be capable of blocking callbacks to CnC Servers actively without depending on other network components			
	74	Anti-APT appliance shall block new threats and new variants of a known malware at near real-time without any dependency on other network devices			
	75	The maximum file size for inspection shall be 100MB			
	76	The proposed sandbox shall act as a Malware Analysis Solution and the adminstrator shall be able to manually submit samples to the system for analysis			
	77	The proposed Sandbox shall also be capable of analysing URLs			
	78	The sandbox shall have the VM environment pre-installed without the need for manual effort in populating the environment			
	79	The proposed sandbox shall be fully tamper proof, not based on commercial VM version and shall not allow any changes to be made to the VM environment			
Network Behaviour Analysis	80	Behaviour analysis tool shall provide real time visibility into top applications using bandwidth monitoring and traffic analysis.			3
	81	The tool shall also be able to make use of information from IDS/ IPS of the Bank.			3
	82	NBA tool shall provide analysis based on			12
	83	1. Automated network flow mapping for critical applications of the Bank			
	84	2. Transaction Types			
	85	3. Resources used			
	86	4. Duration of sessions			
	87	It shall be able to detect (regardless of obfuscation technique)			24
	88	1. Protocol anomalies			
	89	2. DDOS,			

	90	3. Worms			
	91	4. malware			
	92	5. botnets			
	93	6. p2p apps			
	94	7. policy violations			
	95	8. internal misuse			
	96	Changes in information classification and operational changes shall be incorporated automatically.			3
FIM	97	The solution shall provide chain of events such as			6
	98	1 What caused the change			
	99	2. Who did the change			
	100	3. When the change was done			
	101	It shall detect unwanted file change			3
	102	Meet regulatory compliance standards such as PCI-DSS.			3
	103	List cryptographic generation algorithms being used by the solution			8
	104	SHA-256			
	105	SHA-384			
	106	SHA-3			
	107	Other (please list)			
	108	It shall identify grouping of servers based on service (irrespective of OS)and applying same policy.			3
PIM	109	The solution should not require to load any agent on the domain controller			3
	110	It shall manage session of each host			3
	111	The PIM solution shall be able to provide below data for analysis:			22
	112	a) Host name			
	113	b) Media access control (MAC) address			
	114	c) IP address			
	115	d) OS and version			
	116	e) Service pack and patch level			
	117	f) Installed and running software			
	118	g) Hardware details and configuration			
	119	h) System settings			
	120	i) Purchase date			
	121	j) Personal owner, if applicable			

	122	k) Organizational or project association, in some cases.			
Resources	123	Bidder shall provide optimum number of resources so as to take care of SIEM and proposed security solutions			
	124	Total L1 resources to be deployed by bidder (less than 5 =1 mark, 5 L1 = 2 marks, more than 5 = 3 marks			3
	125	Total L2 resources to be deployed by bidder (One L2 = 1 mark, 2 L2 = 2 marks, more than 2 L2 = 3 marks			3
	126	Total L3 resources to be deployed by bidder (One L3 resource = 2 marks. More than one L3 resource = 3 marks)			3
Quality Control Plan	127	Bidder should submit Quality Control Plan with adequate parameters (Less than 15 parameters = 5 Mark, between 15 to 20 = 7 marks, more than 20 = 10 marks)			10

Annexure – 2 – List of supported devices by OEM

Sr No	vendor	Name of the device	Device type	Versions of devices supported	Protocol (parser) used for log reading	Method of log collection	Supporting Version of SIEM	Knowledge base reference	remarks

Annexure 3 – End of Sale/ End of Support/ End of Life Information

Sr no	Solution	Component Type	End of Sale	End of Support	End of Life
	SIEM Solution	Hardware (add rows if required)			
		Software (add rows if required)			
		License			
		Supporting hardware if any (such as NAS, Hardware agent etc)			
		Supporting software if any (such as OS, parser etc)			
		Database			

***** Similar information is to be provided for all other proposed solutions.**

Annexure 4: Resource Plan Matrix

		Experience					Complied (Y/N)
Role	**Type**	**Total Years**	**in IT Security Years**	**Qualifications**			
SOC Monitoring, Alert Tracking, Regular SIEM Administration	L1 Operator	2	1	B.E. / B.Tech in Computer/ Electronics/ IT or any graduate degree in computer security	CCNA/ CCDA/ CCSP/ CCSA / MCSE and Trained on CSOC Solution		
SOC Administration, Rule base Management, SOC Fine tuning	L2 CSOC Administrator	6	4 (out of this, minimum 1 years' experience on proposed CSOC solution)	B.E./ B.Tech. in Computer/ Electronics/ IT	CISA/ CISSP/ CEH/ SSCP		
SOC Manager (L3)	Sr. CSOC Administrator	7	6 (out of this, minimum 2 years' experience on proposed CSOC solution)	B.E./ B.Tech./ in Computer/ Electronics/ IT	CISA/ CISSP/ CEH/ SSCP		

Annexure-5: Proforma of letter to be given by all the Vendors participating in the Cyber Security Operations Center Project on their official letterheads.

To

General Manager - IT

Bank of Maharashtra

Head Office,

Lokmangal, Shivaji Nagar,

Pune - 411005

Sir,

Sub: RFP for Implementation and Maintenance of Cyber Security Operations Center

Further to our proposal dated XXXXXXX, in response to the tender Document issued by Bank of Maharashtra (**"Bank"**) we hereby covenant, warrant and confirm as follows:

The soft-copies of the proposal submitted by us in response to the TENDER DOCUMENT and the related addendums and other documents including the changes made to the original tender documents issued by the Bank, conform to and are identical with the hard-copies of aforesaid proposal required to be submitted by us, in all respects.

Yours faithfully,

Authorised Signatory

Designation

Bidder's corporate name

Appendix 1 Form 01: Proforma of letter to be given by all the vendors participating in the Cyber Security Operations Center Project on their official letter-head.

To

General Manager –IT

Bank of Maharashtra

Head Office,

Lokmangal, Shivaji Nagar,

Pune - 411005

Sir,

Sub: RFP for Implementation and Maintenance of Cyber Security Operations Center

Further to our proposal dated XXXXXXX, in response to the tender Document (hereinafter referred to as **"TENDER DOCUMENT"**) issued by Bank of Maharashtra (**"Bank"**) we hereby covenant, warrant and confirm as follows:

We hereby agree to comply with all the terms and conditions / stipulations as contained in the TENDER DOCUMENT 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 Appendix 2 Form 02 of the main TENDER DOCUMENT which are expressly accepted by the Bank and communicated to us in writing, shall form a valid and binding part of the aforesaid TENDER 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.

Yours faithfully,

Authorised Signatory

Designation

Bidder's corporate name

Annexure 6: Eligibility criteria compliance for RFP for Cyber Security Operations Center

The bidder should not be a consultant / System Integrator/ Information Security Auditor in Bank of Maharashtra for Network Infrastructure/ CBS to avoid any conflict of interest

S.No.	Eligibility Criteria	Documents required	Complied Y/N
A) General Criteria			
1	Bidder agrees to all the clauses as mentioned in the integrity Pact (Annexure 8 of RFP)	Signed Integrity Pact on a stamp paper of. Rs.500/=	
2	Shall be a PSU/PSE/partnership firm or a limited company having existence in India. The necessary certificates viz., Certificate of Incorporation in case of Limited company, Registration Certificate along with the latest partnership deed in case of partnership firm shall be submitted with the offer.	Partnership firm-Certified copy of Partnership Deed. Limited Company-Certified copy of Certificate of Incorporation and Certificate of Commencement of Business. Reference of Act/ Notification For other eligible entities-Applicable documents	
3	Shall have been in existence in India for three years as on 31-03-2016.	Partnership firm-Certified copy of Partnership Deed. Limited Company-Certified copy of Certificate of Incorporation and Certificate of Commencement of Business. For other eligible entities-Applicable documents	
4	The firm shall not be blacklisted / barred by Government of India or any regulatory body in India.	Self Declaration	

B) Financial Criteria			
5	Shall have a minimum average annual Net Sales Turnover of Rs.100.00 crores (Rupees One Hundred Crores) during last three financial years viz. 2013-14, 2014-15 and 2015-16.	Copy of audited Balance Sheet and P&L statement for the financial years 2013-14, 2014-15 and 2015-16	
6	Shall have made net profits for the last 3 financial years viz. 2013-14, 2014-15 and 2015-16	Copy of audited Balance Sheet and P&L statement for the financial years 2013-14, 2014-15 and 2015-16	
C) Technical Criteria (Experience and other Technical Requirements)			
7	Bidder shall have their own Security Operation Center situated in India with ISO 27001 certification compliance	ISO 27001 Certificate	
8	Bidder should have implemented captive SOC in at least 2 BFSI organizations/ Government Organizations in India in last 3 years OR Bidder should be providing Managed Security Services and VA services in at least 2 BFSI organizations/ Government Organizations in India in last 3 years.	Copy of the Purchase Order & Signoff Document from the Customer	
9	The team members proposed for deployment by the bidders should have at least 2 years experience of working in SOC in financial institution in India	Customer reference letter on customer's letter head along with contact details for verification.	
10	SIEM solution provided by bidder shall be in Gartners Leaders Quadrant since last three years viz. 2014, 2015 & 2016	Gartner’s Report on SIEM Technology for the years 2014, 2015 & 2016	

Annexure 7: Bidder scoring chart - Technical evaluation

Sr. No.	Description	Maximum Score	Scoring Mechanism	Credentials
1	Compliance to Technical requirement	375	Maximum marks is 3 to each technical specification.	Compliance to Annexure 1
2	Reference Sites visit	50		Site visit
3	Presentation on Project Implementation Methodology	75		Documents submitted in Technical Bid and live demonstration of solution
	Total	**500**		

Note

1. The cutoff criteria of the above evaluation parameters is minimum 400 marks across all three above sections

2. In Section 1 - The bidder must score a minimum of 90% compliance, even if the bidder meets the 400 mark cut-off and does not meet the criteria of 90% compliance to section 1, the bidder would have deemed not to be meeting the RFP Technical requirements and would be dis-qualified.
3. This annexure is for bidders' reference and need not be submitted with Bid.
4. Bidders need to provide relevant credentials for all of the above points for scoring.

5. The overall proposal, description of the facilities provided at proposed site,etc. in Technical bid will be evaluated.

Annexure - 8: BID SECURITY FORM

(FORMAT OF BANK GUARANTEE (BG) FOR BID SECURITY.)

(ON A NON-JUDICIAL STAMP PAPER OF RS.100.00)

TO:

General Manager (IT),

Bank of Maharashtra

Information Technology,

Head Office,

Lokmangal, Shivaji Nagar,

Pune - 411005

WHEREAS _____ (hereinafter called "the Bidder") has submitted its bid dated_____ (*date of submission of bid*) for Implementation and Maintenance of Security Operations Centre in response to Bank of Maharashtra's Request for Proposal (RFP) No. _____ (hereinafter called "the Bid").

KNOW ALL PEOPLE by these presents that WE_____(*name of bank*) of _____ (*name of country*) having our registered office at_____ (address of bank) (hereinafter called "the Bank") are bound unto Bank of Maharashtra (hereinafter called "the Purchaser") in the sum of_____ for which payment will and truly to be made to the said Purchaser, the Bank binds itself, its successors and assigns by these presents. Sealed with the common seal of the said Bank this _____ day of_____ , 20___.

THE CONDITIONS of this obligation are:

1. If the Bidder withdraws its Bid during the period of bid validity specified by the Bidder on the Bid Form; or
2. If the Bidder, having been notified of the acceptance of its bid by the Purchaser during the period of bid validity :
   (a) fails or refuses to execute the mutually agreed Contract Form if required; or
   (b) fails or refuses to furnish the Performance Bank Guarantee, in accordance with the Terms and Conditions of the Contract;

We undertake to pay the Purchaser up to the above amount upon receipt of its first written demand, without the Purchaser having to substantiate its demand, provided that in its demand the purchaser will note that the amount claimed by it is due it owing to the occurrence of one or both of the two conditions, specifying the occurred condition or conditions.

This guarantee will remain in force up to and including 45 days after the period of the bid validity, and any demand in respect thereof shall reach the Bank not later than the above date.

Notwithstanding any other term contained herein

a) this guarantee shall be valid only up to _____ (Insert Guarantee End Date) whereupon it shall automatically expire irrespective of whether the original guarantee is returned to the Bank or not; and

b) the total liability of Bank under this guarantee shall be limited to Rs. 25,00,000/-(Rupees Twenty Five Lakhs only) only.

Place :

SEAL Code No.

SIGNATURE.

NOTE:

1. BIDDER SHALL ENSURE THAT THE SEAL & CODE NO. OF THE SIGNATORY IS PUT BY THE BANKERS, BEFORE SUBMISSION OF BG

2. STAMP PAPER IS REQUIRED FOR THE BG ISSUED BY THE BANKS LOCATED IN INDIA.

Annexure 10 - **PRE CONTRACT INTEGRITY PACT**

General:

This pre-bid pre-contract Agreement (hereinafter called the Integrity Pact) is made on _____ day of month of _____ 2016, between on one hand, Bank of Maharashtra through authorized official Shri. _____, General Manager, Information Technology Department, Bank of Maharashtra (hereinafter called the "BUYER", which expression shall mean and include unless the context otherwise required, his successors in office and assigns) of the First Part and M/s_____ represented by Shri. _____ Chief Executive Officer (herein 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 procure Services for Information Security Audit of various IT services and branches in the Bank and the BIDDER/Seller is willing to offer/has offered the services for Information Security Audit of various IT services and branches in the Bank.

and

WHEREAS the BIDDER is a private company/public company/Government undertaking/partnership/registered export agency/LLP, constituted in accordance with the relevant law in the matter and the BUYER is an Information Technology Department of Bank of Maharashtra

NOW, THEREFORE,

To avoid all forms of corruption by following a system that is fair transparent and free from any influence/ prejudiced dealings 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 Equipment/product/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 herby agree to enter into this Integrity Pact and agree as follows:

Commitments of the BUYER:

1.1. The BUYER undertakes that no officials of the BUYER, connected directly or indirectly with contract will demand, take a promise for or accept directly or through intermediaries any bribe, consideration gift reward favor or any material or immaterial benefit or any other advantage from the Bidders 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.

1.2. 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 that particular BIDDER in comparison to other BIDDERs.

1.3. 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.

2. 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 facie 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 such a person 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.

COMMITMENTS of BIDDERs

3. 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 contract stage in order to secure the contract or in furtherance to secure it and in particular commit itself to the following:-

3.1. The BIDDER will not offer, directly or through intermediaries, any bribe gift consideration reward favor, any material or immaterial benefit or other advantage, commission fees, brokerage or inducement to any official 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 advantages in the bidding, evaluation contracting and implementation of the contract.

3.2. The BIDDER further undertakes that it has not given, offered or promised to give, directly or indirectly any bribe, gift, consideration, reward, favor, any material benefit or other advantage commission fees brokerage or inducement to any officials 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 favor or disfavor to any person in relation to the contract or any other contract with Government.

3.3. BIDDERs shall disclose the name and address of agents and representatives and Indian BIDDERs shall disclose their foreign principals or associates.

3.4. BIDDERs shall disclose the payments to be made by them to agents/brokers or any other intermediary, In connection with bid/contract.

3.5. The BIDDER further confirms and declares to the BUYER that the BIDDER is the original manufacturer/integrator and not engaged any individual or firm or company whether Indian or foreign to intercede, facilitate or in 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, nor 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.

3.6. 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 the contract and the details of services agreed upon for such payments.

3.7. The BIDDER will not collude with other parties interested in the contract impair the transparency fairness and progress of the bidding process, bid evaluation contracting and implementation of the contract.

3.8. The BIDDER will not accept any advantage in exchange for any corrupt practice unfair means and illegal activities.

3.9. The BIDDER shall not use improperly, for purposes of competition or personal gain, or pass on to others any information provided by the BUYER as part of 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.

3.10. The BIDDER commits to refrain from giving any complaint directly or through any other manner without supporting it with full and verifiable facts.

3.11. The BIDDER shall not instigate or cause to instigate any third person to commit any of the actions mentioned above.

3.12. 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 of any of the officers of the BUYER, or alternatively, if any relative of an 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 filing of tender.

The term 'relative; for this purpose would be as defined in Section 6 of the Companies Act 1956

3.13. The BIDDER shall not lend to or borrow any money from or enter into any monetary dealings or transactions, directly or indirectly, with any employee of the BUYER.

4. Previous Transgression

4.1. 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.

4.2. The BIDDER agrees that if it makes incorrect statement on this subject, BIDDER can be disqualified from the tender process or the contract, if already awarded, can be terminated for such reason.

5. Earnest Money (Security Deposit)

5.1. While submitting commercial bid, the BIDDER shall deposit an amount _____ (*to be specified in RFP) as* Earnest Money Deposit/ Security Deposit, with the BUYER through any of the following instruments:

5.1.1. Bank Draft or Pay Order in Favor of **Bank of Maharashtra IT Department**

5.1.2. A Confirmed guarantee by an Indian Nationalized Bank, promising payment of the guaranteed sum to the BUYER on demand within three working days without any demure whatsoever and without seeking any reason whatsoever. The demand for payment by the BUYER shall be treated as conclusive proof of payment.

5.1.3. Any other mode or through any other instrument (to be specified in the RFP)

5.2. The Earnest Money/Security Deposit shall be valid up to a period of five years or the complete conclusion of the contractual obligations to the complete satisfaction of both the BIDDER and the BUYER, including warranty period, whichever is later.

5.3. 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 provisions of Sanctions for Violation shall be applicable for 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.

5.4. No interest shall be payable by the BUYER to the BIDDER in Earnest Money/Security Deposit for the period of its currency.

6. Sanctions for Violations:

6.1. Any breach of the aforesaid provisions by the BIDDER or any one employed by its or action on its behalf (Whether with or without the knowledge of the BIDDER) shall entitled the BUYER to take all or any one of the following actions, wherever required :-

6.1.1. To immediately call of the pre contract negotiations without assigning any reason or giving any compensation to the BIDDER. However, the proceedings with the other BIDDER(s) would continue.

6.1.2. The Earnest Money Deposit (in pre-contract stage) and /or Security Deposit / Performance Bond (after the contract is signed) shall stand

forfeited either fully or partially, as decided by the BUYER and the BUYER shall not be required to assigning any reason therefore.

6.1.3. To immediately cancel the contract, if already signed, without giving any compensation to the BIDDER.

6.1.4. To recover all sums already paid by the BUYER, and in case of an Indian BIDDER with interest thereon at 2% higher than the prevailing Prime Lending Rate of State Bank of India, while in case of a BIDDER from country other than India with interest thereon at 2% higher than the LIBOR. If any outstanding payment is due to the BIDDER from the Buyer in connection with any other contract for any other project such outstanding payment could also be utilized to recover the aforesaid sum and interest.

6.1.5. To encash the advance bank guarantee and performance bond/warranty bond, if furnished by the BIDDER, in order to recover the payments, already made by the BUYER, along with interest.

6.1.6. To cancel all or any other Contracts with the Bidder. The Bidder shall be liable to pay compensation for any loss or damage to the BUYER resulting from such cancellation/rescission and the BUYER shall be entitled to deduct the amount so payable from the money(s) due to the Bidder.

6.1.7. To debar the BIDDER from participating in future bidding processes of the Bank for a minimum period of five years, which may be further extended at the discretion of the BUYER.

6.1.8. To recover all sums paid in violation of this Pact by Bidder(s) to any middleman or agent or broker with a view to securing the contract.

6.1.9. In cases where irrevocable letter of credit have been received in respect of any contract signed by the BUYER with the BIDDER, the same shall not be opened

6.1.10. Forfeiture of Performance Bond in case of a decision by the BUYER to forfeit the same without assigning any reason for imposing sanctions for violation of this Pact.

7. Fail Clause:

7.1. The Bidder undertakes that it has not supplied / is not supplying similar products/systems or subsystems/ services 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 products/systems or sub systems was supplied by the Bidder to any other Ministry/Department of Government of India or a PSU at a lower price, then that very price, with due allowance for elapsed time, will be applicable to the present case and the difference in the cost would be refunded by the BIDDER to the BUYER, if the contract has already been concluded.

8. Independent Monitors:

8.1. The BUYER has appointed Independent Monitors (hereinafter referred to as Monitors) for this Pact in consultation with the Central Vigilance Commission (Names and Address of the Monitors to be given).

8.2. 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.

8.3. The Monitors shall not be subject to instructions by the representatives of the parties and performs their functions neutrally and independently.

8.4. Both the parties accept that the Monitors have the right to access all the documents relating to the project/procurement, including minutes of meetings.

8.5. As soon as the Monitor notices, or has reason to believe, a violation of this Pact, he will so inform the Authority designated by the BUYER.

8.6. The BIDDER(s) accepts that the Monitors 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 pocket documentation. The same is applicable to subcontractors. The Monitor shall be under contractual obligation to treat the information and documents of the BIDDER/subcontract(s) with confidentiality.

8.7. The BUYER will provide to the Monitor sufficient information about all meetings among the parties related to the Project provided such meetings could have an impact on the contractual relations between the parties. The parties will offer to the Monitor the option to participate in such meetings.

8.8. The Monitor will submit a written report to the designated Authority of BUYER/Secretary in the Department/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 correction problematic situations.

9. Facilitation of Investigation

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

10. Law and Place of Jurisdiction

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

11. Other Legal Actions:

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

12. Validity:

12.1. The validity of this Integrity Pact shall be from date of its signing and extend up to 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.

12.2. Should one or several provisions of this 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.

13. The parties herby sign this Integrity Pact at _____ on _____

BUYER	BIDDER
Name of the Officer:	CHIEF EXECUTIVE OFFICER
Designation:	(Office Seal)
IT Department	
Bank of Maharashtra	

(Office Seal)

Place _____

Date _____

Witness:	Witness:
1 _____	1 _____
(Name & Address) : _____	(Name & Address) : _____
2 _____	2 _____
(Name & Address) : _____	(Name & Address) : _____

Appendix1 Form 02: Commercial Bid Format (To be submitted as "Masked Commercial Bid" with "Technical Bid" submission and also as "Commercial Bid Offer" after Reverse Auction)

Part 1: Commercial Proposal Format: Summary Sheet

Segment	Total Cost
A) SIEM Solution Charges Including Licensing Cost	
B) Anti-APT Solution Charges	
C) Charges for Network based Behaviour Analysis Tool	
D) File Integrity Solution	
E) Privilege Identity Management Solution	
C) CSOC Operations Charges	
D) One Time Charges (Including Installation, Configuration etc)	
E) Annual Maintenance Charges	
F) Training Charges including Refresher Training	
Grand Total	

Part 2: Segment wise Detailed Commercial Proposal Format: Summary Sheet

SrNo2	Item Description	Item Specification (Make/ Model/ Capacity)	HA Mode	License Cost (a)	Hardware Cost (b)	Software Cost (C)	Rate (a+b+c)	Quantity	Total (INR) (Rate * Qty)
A	**SIEM Solution including Licensing cost**								
A.1	**Data Center**								
1	Collector with minimum 20000 EPS		HA					1	
2	SIEM Database Management		HA					1	
3	SIEM Correlation/ Incident Analysis		HA					1	
4	SIEM Reporting/ Dashbaord		HA					1	
5	Storage for SIEM							1	
6	VA Scanner		No					1	
A.2	**DR Site**								
7	Collector with minimum 10000 EPS		No					1	
8	SIEM Database Management		No					1	
9	SIEM Correlation/ Incident Analysis		No					1	
10	SIEM Reporting/ Dashbaord		No					1	
11	Storage for SIEM		No					1	
A.3	**Head Office**								
12	Collector with minimum5000 EPS		No					1	
	Project Management Office								
13	Collector with minimum5000 EPS		No					1	
	Other Item in SIEM								

14	Collector for 1000 EPS (Optional)		No					1	
15	Any other Hardware, Software and License (please sepcify)		No					1	
A.4	**Other Security Solutions**								
16	Anti- APT Appliance		No					2	
17	Network Behaviour Analysis		No					1	
18	File Integrity Monitoring		No					1	
19	Privilege Identitiy Management		No					1	
Sub Total (A)							**(I)**		
B	**Other Services**								
20	Anti Phishing Services		X	X	X	X		100	
21	Anti Trojan Services		X	X	X	X		10	
22	VA Scanning (scheduled)		X	X	X	X		20	
Sub Total (B) for 1 Year									
Sub Total (B) for 5 Years (Sub Total B * 5)							**(II)**		
C	**SOC Operations**								
23	L1 Operator		X	X	X	X			
24	L2 Engineer		X	X	X	X			
25	SOC Manager		X	X	X	X			
Sub Total (C) for 1 Year									
Sub Total (C) for 5 Years (Subtotal C * 5)							**(III)**		
D	**One Time Charges (Including Installation, Configuration etc)**								
26	One Time Charges (Including Installation, Configuration etc)		X	X	X	X		1	
27	Any other Charges (Please specify)		X	X	X	X		1	
Sub Total (D) (One time only)							**(IV)**		

E	**Annual Maintenance Charges**								
28	Collector with minimum 20000 EPS		X	X	X	X		1	
29	Collector with minimum 10000 EPS		X	X	X	X		1	
30	Collector with minimum 5000 EPS		X	X	X	X		1	
31	Collector with minimum 1000 EPS (optional)		X	X	X	X		1	
32	SIEM Database Management		X	X	X	X		1	
33	SIEM Correlation/ Incident Analysis		X	X	X	X		1	
34	SIEM Reporting/ Dashbaord		X	X	X	X		1	
35	Storage for SIEM		X	X	X	X		1	
36	VA Scanner		X	X	X	X		1	
37	Anti- APT Appliance		X	X	X	X		2	
38	Network Behaviour Analysis		X	X	X	X		1	
39	File Integrity Monitoring		X	X	X	X		1	
40	Privilege Identitiy Management		X	X	X	X		1	
Sub Total (E) (for 1 year)									
Sub Total (E) for 2 Years (4th and 5th Years) (Sub Total E * 2) (V)									
F	**Training Charges**								
41	Pre Implementation Training		X	X	X	X		1	
42	Post Implementation Training		X	X	X	X		1	
43	Quarterly Refresher Training		X	X	X	X		20	
Sub Total (F) (VI)									
Total Cost of Ownership (I + II + III + IV + V + VI) for 5 Years									

Appendix 2 Form 01: Cover Letter (Technical Offer)

Date

To,
Deputy General Manager (IT)

Bank of Maharashtra

Information Technology,

Head Office,

Lokmangal, Shivaji Nagar,

Pune - 411005

Dear Sir,

1. Having examined the Tender Documents including all Annexures, the receipt of which is hereby duly acknowledged, we, the undersigned offer to supply, deliver, implement and commission ALL the items mentioned in the 'Request for Proposal' and the other schedules of requirements and services for your bank in conformity with the said Tender Documents in accordance with the schedule of Prices indicated in the Price Bid and made part of this Tender.
2. If our Bid is accepted, we undertake to abide by all terms and conditions of this tender and also to comply with the delivery schedule as mentioned in the Tender Document.
3. We agree to abide by this Tender Offer for 180 days from date of Tender (Commercial Bid) opening and our Offer shall remain binding on us and may be accepted by the Bank any time before expiry of the offer.
4. This Bid, together with your written acceptance thereof and your notification of award, shall constitute a binding Contract between us.
5. We undertake that in competing for and if the award is made to us, in executing the subject Contract, we will strictly observe the laws against fraud and corruption in force in India namely "Prevention of Corruption Act 1988".
6. We certify that we have provided all the information requested by the bank in the format requested for. We also understand that the bank has the exclusive right to reject this offer in case the bank is of the opinion that the required information is not provided or is provided in a different format.

Dated this……..by …….20

Authorised Signatory

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

(This letter shall be on the letterhead of the Vendor duly signed by an authorized signatory)

Appendix 2 Form 02: Queries on the Terms & Conditions, Services and Facilities provided:

[Please provide your comments on the Terms & conditions in this section. You are requested to categorize your comments under appropriate headings such as those pertaining to the Scope of work, Approach, Work plan, Personnel schedule, Terms & Conditions etc. You are also requested to provide a reference of the page number, state the clarification point and the comment/ suggestion/ deviation that you propose as shown below.]

Sr. No.	Page #	Point / Section #	Clarification point as stated in the tender document	Comment/ Suggestion/ Deviation
1				
2				
3				
4				
5				
6				
7				
8				
9				

Dated:

Authorized Signatory

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

Appendix 2 Form 03: Technical Bid/Commercial Bid - Table of Contents

Section #	Section Heading	Proforma Given for Technical bid submission	
1	Technical compliance	Annexure - 1	
2	List of supported devices	Annexure - 2	
3	End of Sale/ End of Support/ End of Life Information	Annexure - 3	
4	Resource Plan Matrix	Annexure - 4	
5	Cover Letter of Hardcopy	Annexure - 5	
6	Eligibility Criteria	Annexure - 6	
7	Bidder Scoring Chart	Annexure - 7	
8	Bid Security Form	Annexure - 8	
9	Guidelines, Terms & Conditions and Process Flow for e-Procurement Auction	Annexure - 9	
10	Pre-Contract Integrity Pact		Annexure - 10
11	Conformity Letter		Appendix 1 Form 01
12.	Commercial Bid Format	Appendix 1 Form 02	
4.	Cover Letter – Technical Offer	Appendix 2 Form 01	
13.	Query format / Comments on Terms and conditions and Terms of reference	Appendix 2 Form 02	

Dated:

Authorised Signatory

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

Annexure - 9 : GUIDELINES, TERMS & CONDITIONS AND PROCESS FLOW FOR E-PROCUREMENT AUCTION

Introduction:

Bank of Maharashtra intends to use E procurement Auction (Reverse Auction) process in place of submission of commercial bids of RFP.

This annexure consists of rules for E Procurement Auction, Terms and conditions and Formats for submission of acceptance by the bidders.

1. **Rules for E Procurement Auction (Reverse Auction)**:

a. APPLICABILITY:

i. Reverse Auctions are carried out under the framework of rules that are called Rules for Reverse Auction.

ii. All bidders participating in Reverse Auction shall understand/ accept and give an undertaking for compliance with the same to the Bank in the prescribed format as specified in Format-A.

iii. Any bidder not willing to submit such an undertaking shall be disqualified for further participation respecting the procurement in question.

b. ELIGIBILITY:

Only bidders who are technically qualified and who submit the prescribed undertaking to the Bank alone can participate in Reverse Auction relevant to the procurement for which RFP is floated.

c. COMPLIANCE/ CONFIRMATION FROM BIDDERS:

i. The bidders participating in Reverse Auction shall submit the following duly signed by the Competent Authority who signs the offer documents in response to the RFP:

1. Acceptance of Rules for Reverse Auction and undertaking The format will be shared to participants of reverse auction.
2. Agreement between System Integrator and bidder. (This format will be given by the System Integrator prior to announcement of Reverse Auction.)
3. Letter of authority authorizing the name/s of official/s to take part in Reverse Auction as per format in Format-B.

d. TRAINING:

i. The Bank will facilitate training for participation in Reverse Auction through the System Integrator for the Reverse Auction. During the training the Bidders shall be explained the rules related to the Reverse Auction to be adopted. Bidders are required to give compliance on it before the start of bid process.

ii. Where ever necessary, the Bank / System Integrator may also conduct a 'mock reverse auction' to familiarize the bidders with Reverse Auction process.

iii. Any bidder/ bidders not participating in training and/or 'mock reverse auction' shall do so at his own risk and it shall not be open for him to make any complaint/grievance later.

iv. Each bidder / bidder shall participate in the training at his / their own cost.

e. **DATE/ TIME FOR TRAINING:**

i. The Venue, Date, Time etc. for training in Reverse Auction shall be informed later.

ii. No request for postponement / fixing of Training Date / Time shall be entertained which in the sole view and discretion of the Bank might result in any avoidable delay to either the Reverse Auction or the whole process of selection of bidder.

f. **DATE/ TIME OF REVERSE AUCTION:**

i. The Date and Time of commencement of Reverse Auction as also Duration of 'Reverse Auction Time' shall be communicated at least 3 working Days prior to such auction Date.

ii. Any force Majeure or other condition leading to postponement of auction shall entitle the Bank to postponement of auction even after communication, but, the Bank shall be obliged to communicate to all participating bidders the 'postponement' prior to commencement of such 'Reverse Auction'.

g. **CONDUCT OF REVERSE AUCTION:**

i. The Reverse Auction shall be conducted on a specific web portal meant for this purpose.

ii. The Reverse Auction may be conducted by the Bank itself or through a System Integrator specifically identified/ appointed/ empanelled by the Bank.

h. **TRANSPARENCY IN BIDS:**

i. All bidders will be able to view during the auction time the current lowest price in portal. Bidder shall be able to view not only the lowest bid but also the last bid made by him at any point of time during the auction time.

i. **MASKING OF NAMES:**

i. Names of bidders shall be masked in the Reverse Auction process and bidders will be given dummy names.

j. **DECREMENTAL BID VALUE**

i. The bidders shall be able to bid only at a specified decrement value and not at any other fractions. The Bid decrement value shall be Rs.5,00,000/-.

ii. The bid decrement value shall be in multiples of Rs. 5,00,000/-.

iii. The web portal shall display the next possible decremental value of bid. It is not, however, obligatory on the part of bidders to bid at the next immediate lower level only. (That is, bids can be even at 2 or 3 lower levels than the immediate lower level).

k. **REVERSE AUCTION PROCESS:**

i. The procurement process shall be completed through a single Reverse Auction.

ii. The Bank shall however, be entitled to cancel the procurement of Reverse Auction process, if in its view procurement or reverse auction process cannot be conducted in a fair manner and / or in the interest of the Bank.

iii. All the ~~successful~~ bidders shall submit a confirmation of acceptance of the last bid price of auction within 30 minutes of closing of the auction to Bank either through Fax or E-Mail. The ~~successful~~ bidders have to submit the final bill of material as per Appendix 1 Form 02 of RFP duly signed by the authorized official to Bank within 2 hours of close of auction by mail / fax.

iv. In the event of circumstances like no power supply, system problem, loss of internet connectivity, inability to use the system, loss of electronic information, power interruptions, UPS failure, etc., the bidder has to ensure that they are able to convey their bidding price to the System Integrator by way of FAX, who will upload the Faxed price online on behalf of the bidder and confirm the receipt of FAX to the System Integrator. This shall be done before the closure of bid time. The bidder has to ensure that the sufficient time is given to the System Integrator to upload the faxed prices online. In case the required time is not available with the System Integrator at the time of receipt of fax message, the System Integrator will not be uploading the prices. It is thus requested from the bidders not to wait till the last moment to quote their bids so as to avoid any such complex situation.

l. **EXPENDITURE ON REVERSE AUCTION:**

i. All eligible bidders are requested to ensure that they have a valid digital certificate well in advance to participate in the Reverse auction process. The cost of digital certificate has to be borne by the bidder only.

ii. Bidders shall participate in the training or mock auction at their own cost.

m. **CHANGES IN BUSINESS RULES:**

i. Any changes made in Rules for Reverse Auction will be informed to the eligible bidders before commencement of Reverse Auction.

n. **OTHER INSTRUCTIONS:**

i. No bidder shall involve himself / itself or any of his / its representatives in any price manipulation directly or indirectly with other bidders. If any such practice comes to the notice, Bank shall disqualify the bidder / bidders concerned from the reverse auction process.

ii. Bidder shall not disclose details of his bids or any other details concerning Reverse Auction process of the Bank to any other third party without specific permission in writing from the Bank.

iii. Neither Bank nor System Integrator can be held responsible for

consequential damages such as no power supply, system problem, inability to use the system, loss of electronic information, power interruptions, UPS failure, etc.

o. **ERRORS AND OMISSIONS:**

i. On any issue or area of material concern respecting Reverse Auction not specifically dealt with in these Business Rules, the decision of the Bank shall be final and binding on all concerned.

2. Terms and conditions of Reverse Auction:

a. Each bidder will get a unique User Id and Password and bidders are requested to change the Password after the receipt of initial Password from the System Integrator. All bids made from the User ID given to the bidder will be deemed to have been made by the bidder.

b. The auction type is English Reverse No Ties.

c. The duration of Auction will be of 30 minutes. If some bidder is bidding during the last 5 minutes of Auction closing, the Auction time will get extended for another 5 minutes from the time of the last accepted bid. Such extension will be allowed to continue till no bid is placed within 5 minutes of the last quote of such extended time. Total number of the extensions is restricted to maximum 10.

d. Bank of Maharashtra reserves the right to reject any or all the bids without assigning any reason whatsoever.

e. There shall be no variation between the on-line bid value and signed document to be submitted by the bidders.

f. Bidding will be conducted in Indian Rupees (INR).

g. The bidders has to quote the total cost of items mentioned in Appendix 1 Form 02 of RFP. Bank will arrive at TCO as per the format mentioned in the Appendix 1 Form 02 after closure of bidding.

h. The TCO arrived by the Bank after closure of reverse auction is final and shall be accepted by all the bidders.

i. The bids (Commercials) shall be firm for a period as specified in RFP and shall not be subjected to any change whatsoever.

j. Bidder has to submit acceptance to the terms and conditions of Reverse Auction and required compliance and other formats as mentioned in this document along with technical bids.

k. Only those bidders who are technically qualified and competent to provide the required solution as per RFP 052017 are only eligible to participate in Reverse Auction Process.

l. All eligible bidders are requested to ensure that they have a valid digital certificate well in advance to participate in the Reverse auction process.

m. All other terms and conditions of the RFP no. 02017 remain unchanged.

Appendix 2 Form 01: Manufacturer's Authorization Form (MAF)

No. _____ dated_____

TO

_____

_____

_____

Dear Sir,

Tender Reference No._____

We _____who are established and reputable manufactures of _____ having factories at_____ and _____ do hereby authorize M/s _____ (Name and address of Agent/Dealer) 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 equipment and services offered against this invitation for tender offer by the above firm. In case the above firm is not able to perform the obligations as per contract during the period of contract, as Original Equipment Manufacturer, we are liable to provide the services as per the terms of contract.

Yours faithfully,

(Name)

for and on behalf of

M/s_____

(Name of manufactures)

Note: This letter of authority should be on the letterhead of the manufacturing concern and should be signed by a competent person of the manufacturer.