Request for Proposal (RFP)

For

Selection of System Integrator for Implementation, Maintenance and Facility Management for System Security Tools for Cyber Security Operation Centre (C-SOC)

Head Office-2
Department of Information Technology
5th Floor, 3 & 4 DD Block, Sector -1
Salt Lake, Kolkata-700 064

RFP REF NO: DIT/BPR&BTD/OA/5033/2018-19 Date: 15/02/2019

The information provided by the bidders in response to this RFP Document will become the property of the Bank and will not be returned. The Bank reserves the right to amend, rescind or reissue this RFP Document and all amendments will be advised to the bidders and such amendments will be binding on them. The Bank also reserves its right to accept or reject any or all the responses to this RFP Document without assigning any reason whatsoever and without any cost or compensation therefor.

This document is prepared by UCO Bank for the Selection of System Integrator for Implementation, Maintenance and Facility *Management for System Security Tools for Cyber Security Operation Centre (C-SOC). It should not be reused or copied or used either partially or fully in any form.*

Disclaimer

While the document has been prepared in good faith, no representation or warranty , express or implied, is or will be made, and no responsibility or liability will be accepted by UCO BANK or any of its employees, in relation to the accuracy or completeness of this document and any liability thereof expressly disclaimed. The RFP is not an offer by UCO BANK, but an invitation for bidder's responses. No contractual obligation on behalf of UCO BANK, whatsoever, shall arise from the offer process unless and until a formal contract is signed and executed by duly authorized officials of UCO BANK and the selected Bidder.

TABLE OF CONTENTS

Bid Control Sheet

Tender Reference	**RFP Ref No: HO/DIT/BPR&BTD/OA/5033/2018-19 Date: 15/02/2019**
Cost of Tender documents	**Rs.10,000/- (Rupees Ten Thousand Only)**
Date of issue of RFP	**15/02/2019**
Earnest Money Deposit (EMD)	**Rs.25,00,000/- (Rupees Twenty Five Lacs only)**
Date of commencement of sale of tender document	**15/02/2019**
Last date for submitting queries for the Pre-bid Meeting	**27/02/2019 upto 4 PM.**
Pre-Bid meeting /Venue	**01/03/2019 at 4:00 PM at Head Office-2 Department of Information Technology 5th Floor, Conference Room, 3 & 4 DD Block, Sector -1, Salt Lake, Kolkata-700 064**
Last Date and Time for receipts of tender bids	**15/03/2019 at 04:00 PM**
Opening of technical bids	**15/03/2019 at 04:30 PM**
Opening of Price Bid	**Will be informed subsequently to technically qualified bidders.**
Address of Communication	**Head Office-2 Department of Information Technology 5th Floor,3 & 4 DD Block, Sector -1 Salt Lake, Kolkata-700 064**
Email address	**hodit.calcutta@ucobank.co.in**
Contact Telephone	**Tel : 033-44559770/9775**
Bids to be submitted	**Tender box placed at: UCO BANK, Head Office-2, Department of Information Technology, 5th Floor, 3 & 4, DD Block, Sector -1, Salt Lake, Kolkata-700 064.**

Note: **Bids will be opened in presence of the bidders' representatives (maximum two representatives per bidder) who choose to attend. In case the specified date of submission & opening of Bids is declared a holiday in West Bengal under the NI act, the bids will be received till the specified time on next working day and will be opened at 4:30 p.m. UCO Bank is not responsible for non-receipt of responses to RFP within the specified date and time due to any reason including postal holidays or delays. Any bid received after specified date and time of the receipt of bids prescribed as mentioned above, will not be accepted by the Bank. Bids once submitted will be treated as final and no further correspondence will be entertained on this. No bid will be modified after the specified date & time for submission of bids. No bidder shall be allowed to withdraw the bid.**

PART – I

1.1 Introduction

UCO Bank, a body corporate, established under the Banking Companies (Acquisition and Transfer of Undertakings) Act 1970, having its Head Office at 10, B.T.M. Sarani, Kolkata-700001, India, and its Department of Information Technology at 3 & 4, DD Block, Sector-1, Salt Lake, Kolkata - 700064, hereinafter called "the Bank", is one of the leading public sector Banks in India having more than 3000+ Domestic Branches, two Overseas Branches one each at Singapore & Hong Kong Centres and 2500+ ATMs (including Biometric enabled ATMs), spread all over the country. All the branches of the Bank are CBS enabled through Finacle (Ver. 7.0.25) as a Core Banking Solution. Bank is having tie up with Visa & NPCI and distributes VISA and RuPay enabled debit cards to the customers. Bank has also installed some machines for cash deposit, cheque deposit and passbook printing. The existing Cash Deposit kiosks, Cheque Deposit Machines and Self-Service Passbook Printing Kiosks are directly integrated with Bank's Core Banking System.

1.2 Objective

To monitor, assess and defend Bank's information systems and to be equipped with set of tools such as Network Access Control (NAC) & Patch Management , Data Loss/Leakage Prevention (DLP), Automated Vulnerability Assessment Scanners (VAS), IT-Governance, Risk & Compliance (IT-GRC), Anti-Advanced Persistent Threat (APT) for Security Intelligence services given in detail under this RFP for implementation , maintenance , monitoring and response capabilities.

Bank intends to implement for information assets at Primary, DR sites and Branches. Bank expect system integrator to provide design, supply, implementation, configuration, customization, integration, monitor, manage, backup, documentation, training, warranty support, post warranty maintenance support, back to back arrangement with OEM and any other activities related to or connected to the Information Technology / Cyber security solutions, devices & technologies. The bidder is expected to do following but not limited to:

- Procurement of the necessary solutions and the corresponding hardware, software, database etc. required for implementing these solutions.
- Implementation of the respective solutions including configuration, customization of the products as per the requirement.

- Integration of the solutions to provide a comprehensive single dashboard view of the security risks/ incidents.
- Work with the existing System Integrator(s) to integrate the C-SOC solutions with existing application platforms, server and storage environment, enterprise network, EMS/ NMS solutions, security solutions, ticketing tools etc.
- Providing adequate resources for on-going operations of the Cyber Security Operations Centre (C-SOC).
- Development of operating procedures in adherence banks' policies.
- Security Monitoring/scanning of cyber-attacks into/on/against Bank's IT assets
- Manage security, configuration, availability, performance and fault management, advisory for the security devices and its software stipulated in scope.
- Ensure Scanning / Protection/ Presentation /Reporting as required by the Bank.
- Vulnerability Assessment & Penetration Testing for critical devices/ servers /applications/solutions.
- Risk assessment and mitigation, protection, execution support for the Security solutions, devices, software and applications under the scope of C-SOC.
- Ensure adequacy, appropriateness and concurrency of various policies as per the requirement of regulatory authorities and Government of India Security authorities, IT Act 2000 and subsequent amendments and guidelines in place.
- Ensure adherences to Bank's Information Security Policy and Cyber Security Policy.
- Provide forensics support as per the requirement of Bank in case of any incident.
- Dashboard for reporting and SLA management.
- Adherence to agreed Service Level Agreements (SLA) and periodic monitoring and reporting of the same to banks.
- Continual improvement of the Security Operations as defined in the SLA.

1.3 Eligibility Criteria

Only those bidders, who satisfy all the eligibility criteria as mentioned herein below, may respond. Documents in support of all eligibility criteria are required to be submitted along with the Technical Bid. Offers received from the bidders who do not fulfil any of the following eligibility criteria are liable to be rejected.

Sl. No	Eligibility Criteria	Document to be submitted
1	The bidder should be a registered company in India and should be in existence for a minimum period of Three years as on RFP date. (Proof, such as Registration/ Incorporation Certificate is to be submitted).	Certificate of Incorporation or Certificate of Commencement of business (whichever is applicable), MSME Registration (if applicable).
2	The bidder may be either an OEM or an Authorized Partner of the OEM (Original Equipment Manufacturer) whose product they are proposing. In case the OEM does not deal directly, an OEM may bid through their Authorized Service Partners or System Integrator.	Undertaking from the OEM mentioning a clause that OEM will provide support services during warranty period if the bidder authorized by them fails to perform. In case of an authorized representative, a letter of authorization (MAF) from original manufacturer must be furnished in original duly signed & stamped **(As per Annexure – J).**
3	The Bidder should have a minimum annual turnover of at least **Rs.100 Crores** in each of the **last three financial years (i.e. 2015-16, 2016-17 & 2017-18).**	Audited Balance Sheets for last 3 years, i.e., 2015-16, 2016-17 & 2017-18 and Certificate from Chartered Accountant stating Net Worth, Turnover and Profit/Loss for last 3 financial years, i.e. 2015-16, 2016-17 & 2017-18 are to be submitted.
4	The Bidder should have posted net profit in each of the **last three financial years (i.e. 2015-16, 2016-17 & 2017-18).**	Audited Balance Sheets for last 3 years, i.e., 2015-16, 2016-17 & 2017-18 and Certificate from Chartered Accountant stating Net Worth, Turnover and Profit/Loss **for last 3 financial years i.e. 2015-16, 2016-17 & 2017-18** are to be submitted.

5	The bidder should be providing IT security services (i.e. in the area of implementation, monitoring and management of various types of security solutions, devices, Technologies and software DLP,VAS,NAC,IT-GRC,APT) for a minimum period of two years as on RFP date.	Proof of purchase order/work order/sign off documents with Installation Report showing implementation of various security solutions stated above to be submitted indicating the company is providing such service for the past 2 years. The Bank reserves the right to inspect the information provided by the bidder.
6	The bidder should be currently in the service of providing Security Operation Centre (SOC)/Managed services in proposed Security solutions including at least two Government/Public/Private organisations in India out of which one should be a BFSI/ RBI/NPCI (excluding RRBs and Co-operative Bank).	Proof of Client Certificate is to be submitted.
7	Bidder shall have their own Security Operation Center (SOC) in India.	An undertaking in this regard on company letter head to be submitted.
8	The bidder should have minimum 3 skilled staff on their payroll with certification with for the product proposed.	An undertaking in this regard on company letter head to be submitted. He should be minimum BE/ B. Tech with certification such as CCNA/CISA/ CCNP/CISM.
9	Whose hardware/ software, Bidder is proposed to be supplied to the Bank, must have presence in India.	An undertaking in this regard from the OEM with office address and contact person details to be submitted
10	The OEM products offered by the Bidder under this RFP should have been supplied & implemented in any BFSI/ RBI/NPCI/ Government Organisation (excluding RRBs and Co-operative Bank) in India.	Completion certificate from respective organisations where the OEM Products have been implemented to be submitted

11	The bidder should have not been black listed by any of Government Authority or Public Sector Undertaking (PSUs) or any Scheduled Commercial Banks or IBA and the bidder shall give an undertaking to this effect. In case, in the past, the name of their Company was black listed by any of the said authorities, the name of the company or organization must have been removed from the black list as on date of submission of the tender, otherwise the bid will not be considered.	An undertaking to this effect in the company's letterhead signed by authorized signatory to be submitted.
12	The Bidder should not be existing System Integrator for Network Equipment/ Data Centre Hardware for UCO Bank to avoid conflict of interest.	An undertaking to this effect in the company's letterhead signed by authorized signatory to be submitted

Note: -

All eligibility requirements mentioned above should be complied by the bidders as applicable and relevant support documents should be submitted for the fulfillment of eligibility criteria failing which the Bids may be summarily rejected. Non-compliance of any of the criteria will entail rejection of the offer summarily. Photocopies of relevant documents / certificates should be submitted as proof in support of the claims made for each of the above-mentioned criteria and as and when the Bank decides, originals / certified copies should be shown for verification purpose. The Bank reserves the right to verify / evaluate the claims made by the Bidder independently. Any deliberate misrepresentation will entail rejection of the offer ab-initio. Any decision of UCO BANK in this regard shall be final, conclusive and binding upon the bidder.

Please note that under this RFP either OEM or its authorised representative can bid but both cannot bid simultaneously.

PART – II

INVITATION FOR BIDS AND INSTRUCTIONS TO BIDDERS

2.1 Invitation for Bids

This Request for Proposal (RFP) is to invite proposals from eligible bidders desirous of taking up the project for Implementation, Maintenance and Facility Management for System Security Tools for Cyber Security Operation Centre (C-SOC) in Sealed offers/Bids (Bid) prepared in accordance with this RFP should be submitted as per details given in the Bid Details table and in the RFP clauses. The criteria and the actual process of evaluation of the responses to this RFP and subsequent selection of the successful bidder will be entirely at Bank's discretion.

2.2 Due Diligence

The Bidder is expected to examine all instructions, forms, terms and specifications in this RFP and study the RFP document carefully. Bid shall be deemed to have been submitted after careful study and examination of this RFP with full understanding of its implications. The Bid should be precise, complete and in the prescribed format as per the requirement of this RFP. Failure to furnish all information required by this RFP or submission of a Bid not responsive to this RFP in each and every respect will be at the Bidder's own risk and may result in rejection of the Bid and for which UCO Bank shall not be held responsible.

2.3 Tender Document & Fee

A complete set of tender document can be obtained from the following address during office hours on all working days on submission of a written application along with a non-refundable fee of **Rs.10,000/- (Rupees Ten thousand Only**) in the form of Demand Draft in favour of UCO BANK, payable at Kolkata.

The tender document may also be downloaded from the bank's official website www.ucobank.com . The bidder downloading the tender document from the website is required to submit a non-refundable fee of **Rs.10,000/- (Rupees Ten Thousand Only)** in the form of Demand Draft in favor of UCO BANK, payable at Kolkata, at the time of submission of the technical bid, failing which the bid of the concerned bidder will be rejected.

A copy of the RFP should be submitted along with the bid duly signed and stamp on each page by the bidder.

Note:

As per recommendations of GOI, Bank has decided to waive off Tender Cost & EMD for NSIC registered MSME entrepreneurs.

We clarify that:

Exemption from submission of EMD and Tender Cost shall be given to bidders who are Micro, Small & Medium Enterprises (MSME) and are registered with National Small Scale Industrial Corporation Ltd. (NSIC) under its "Single Point Registration Scheme". The bidder has to submit necessary document issued by NSIC to avail the exemption. To qualify for EMD exemption, firms should necessarily enclose a valid copy of registration certificate issued by NSIC which are valid on last date of submission of the tender documents. MSME firms who are in the process of obtaining NSIC registration will not be considered for EMD exemption.

Bids received without tender cost and EMD for bidders not having valid NSIC registered documents for exemption will not be considered.

UCO BANK reserves the right to accept or reject in part or full any or all offers without assigning any reason thereof and without any cost or compensation therefor. Any decision of UCO Bank in this regard shall be final, conclusive and binding upon the bidders. The Bank reserves the right to accept or reject any Bid in part or in full, and to cancel the Bidding process and reject all Bids at any time prior to contract award, without thereby incurring any liability to the affected Bidder or Bidders or any obligation to inform the affected Bidder or Bidders of the grounds for Bank's action. During the evaluation process at any stage, if it is found that the bidder does not meet the eligibility criteria or has submitted false / incorrect information the bid will be rejected summarily by The Bank.

This non-refundable tender fee of can also be submitted through the **electronic mode** to the below mention account. Proof of successful deposit of tender fee has to be submitted along with tender document.

The details of the account are as under:-

The Bank details are as below:

- **Account Number-18700210000755**
- **Account Name – M/s HO DIT**
- **Branch- DD Block, Salt Lake Branch**
- **IFSC- UCBA0001870**
- **MICR-700028138**

2.4 Earnest Money Deposit

The Bidder(s) must submit Earnest Money Deposit in the form of Bank Guarantee valid for a period of **180 days** with a further claim period of **30 days** in favor of UCO Bank payable at Kolkata for an amount mentioned hereunder:

Particulars of Job to be undertaken	EMD
Implementation, Maintenance and Facility Management for System Security Tools for Cyber Security Operation Centre (C-SOC)	**Rs. 25,00,000/-**

Non-submission of Earnest Money Deposit will lead to outright rejection of the Offer. The EMD of unsuccessful bidders will be returned to them on completion of the procurement process without any interest thereon. The EMD of successful bidder(s) will be returned to them on submission of Performance Bank Guarantee (s) either at the time of or before the execution of Service Level Agreement (SLA).

The Earnest Money Deposit may be forfeited under the following circumstances:

a. If the bidder withdraws its bid during the period of bid validity (180 days from the date of opening of bid).

b. If the bidder makes any statement or encloses any form which turns out to be false, incorrect and / or misleading at any time prior to signing of contract and/or conceals or suppresses material information; and / or

c. The selected bidder withdraws his tender before furnishing on unconditional and irrevocable Performance Bank Guarantee.

d. The bidder violates any of the provisions of the terms and conditions of this tender specification.

e. In case of the successful bidder, if the bidder fails:

   - To sign the contract in the form and manner to the satisfaction of UCO BANK
   - To furnish Performance Bank Guarantee in the form and manner to the satisfaction of UCO BANK either at the time of or before the execution of Service Level Agreement (SLA).

2.5 Rejection of the Bid

The Bid is liable to be rejected if:

a. The document doesn't bear signature of authorized person on each page signed and duly stamp.

b. It is received through Telegram/Fax/E-mail.

c. It is received after expiry of the due date and time stipulated for Bid submission.

d. Incomplete Bids, including non-submission or non-furnishing of requisite documents / Conditional Bids/ deviation of terms & conditions or scope of work/ incorrect information in bid / Bids not conforming to the terms and conditions stipulated in this Request for proposal (RFP) are liable for rejection by the Bank.

e. Bidder should comply with all the points mentioned in the RFP. Noncompliance of any point will lead to rejection of the bid.

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

2.6 Pre Bid Meeting

The queries for the Pre-bid Meeting should reach us in writing or by email on or before the date mentioned in the Bid Control Sheet by e-mail to **hodit.calcutta@ucobank.co.in.** It may be noted that no query from any bidder shall be entertained or received after the date mentioned in the bid control sheet. Queries raised by the prospective bidder and the Bank's response will be hosted at Bank's web site. No individual correspondence will be accepted in this regard. Only authorized representatives of bidder will be allowed to attend the Pre-bid meeting.

2.7 Modification and Withdrawal of Bids

No bid can be modified by the bidder subsequent to the closing date and time for submission of bids. In the event of withdrawal of the bid by successful bidders, the EMD will be forfeited by the Bank.

2.8 Information Provided

The RFP document contains statements derived from information that is believed to be 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 employees, agents, contractors, or advisers gives any representation or warranty, express or implied as to the accuracy or completeness of any information or statement given or made in this RFP document.

2.9 For Respondent Only

The RFP document is intended solely for the information to the party to whom it is issued ("the Recipient" or "the Respondent") and no other person or organization.

2.10 Confidentiality

The RFP document is confidential and is not to be reproduced, transmitted, or made available by the Recipient to any other party. 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 terms and conditions as this original and 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, suppliers, or agents without the prior written consent of Bank.

2.11 Disclaimer

Subject to any law to the contrary, and to the maximum extent permitted by law, Bank and its officers, employees, contractors, agents, and advisers disclaim all liability from any loss or damage (whether foreseeable or not) suffered by any person acting on or refraining from acting because of any information, including forecasts, statements, estimates, or projections contained in this RFP document or conduct ancillary to it whether or not the loss or damage arises in connection with any negligence, omission, default, lack of care or misrepresentation on the part of Bank or any of its officers, employees, contractors, agents, or advisers.

2.12 Costs Borne by Respondents

All costs and expenses incurred by Recipients / Respondents 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.

2.13 No Legal Relationship

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

2.14 Errors and Omissions

Each Recipient should notify Bank of any error, omission, or discrepancy found in this RFP document.

2.15 Acceptance of Terms

A Recipient will, by responding to Bank RFP, be deemed to have accepted the terms as stated in the RFP.

2.16 RFP Response

If the response to this RFP does not include the information required or is incomplete or submission is through Fax mode or through e-mail, the response to the RFP is liable to be rejected.

All submissions will become the property of Bank. Recipients shall be deemed to license, and grant all rights to, Bank to reproduce the whole or any portion of their submission for the purpose of evaluation, to disclose the contents of the submission to other Recipients who have registered a submission and to disclose and/or use the contents of the submission as the basis for any resulting RFP process, notwithstanding any copyright or other intellectual property right that may subsist in the submission or Banking documents.

2.17 RFP Response Validity Period

RFPs response will remain valid and open for evaluation according to their terms for a period of at least 6 months from the time the RFP response submission process closes.

2.18 Notification

Bank will notify the Respondents in writing as soon as possible 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.

2.19 Language of Bids

The bid, correspondence and supporting documents should be submitted in English.

2.20 OEM Authorization

In case the successful bidder is not ready to provide the support during the warranty period, support will be provided by OEM directly or their other authorized partners for the remaining period of warranty of the product without any additional cost to the Bank. An authorization letter from OEM regarding this must be attached with the technical bid.

2.21 Undertaking to use new components

Bidder should give an undertaking to the Bank that the equipment's (including all components) delivered to the Bank are brand new. The bidder should also give an undertaking in writing that all the software supplied by the bidder is licensed and legally obtained. The proposed equipment's are not declared end of support or end of life. This undertaking to the Bank is to be signed by a Director or Head of marketing of the Company.

2.22 Compliance To Labour Act

As per Government (Central / State) Minimum Wages Act in force, it is imperative that all the employees engaged by the bidder are being paid wages / salaries as stipulated by government in the Act and it should be complied.

2.23 Compliance

The products & services offered to the Bank must be in compliance with all Laws, Regulations & Government guidelines of India. It also should not violate any of the provisions of the IT Act 2000 and all its subsequent addendums in anyway or any other legal provisions relating to such products or services in India.

The bidder must ensure that application /solution is free from embedded Malicious/ fraudulent code being implemented by them in the Bank. The bank reserves the right for audit.

2.24 Authorized Signatory

The selected bidder shall indicate the authorized signatories who can discuss, sign negotiate, correspond and any other required formalities with the bank, with regard to the obligations. The selected bidder shall submit, a certified copy of the resolution of their Board, authenticated by Company Secretary, authorizing an official or officials of the company to discuss, sign with the Bank, raise invoice and accept payments and also to correspond. **The bidder shall furnish proof of signature identification for above purposes as required by the Bank.**

In this regard, a Power of Attorney on a Judicial Stamp Paper is to be submitted from the Bidder side indicating the authorized signatory.

A true copy of Board Resolution of the Company has to be submitted, indicating the name of the person on whose Power of Attorney has been provided to act as Authorized signatory.

2.25 Consortium and System Integrator

The bidder may form a consortium and bid for the RFP document , as it is the Bank's expectation to maintain and implement the most appropriate hardware and software products and maintain policies and procedures to serve the Bank. However, in this case the Bank will deal with only the successful bidder as a single point of contact who shall have the sole responsibility for the entire assignment irrespective of the fact that it is only the part of the consortium.

The successful bidder shall have the single point responsibility for the consortium in their bid responses. The bidder which shall have the single point responsibility of the bid will be deemed to be the system integrator and will be deemed to play the lead role in the bid and hall have single point responsibility of the bid.

2.26 Submission of offer – Bid System

Separate Eligibility, Technical and Commercial Bids along with the soft copies duly sealed and super-scribed as **Implementation, Maintenance and Facility Management for System Security Tools for Cyber Security Operation Centre (C-SOC) (Eligibility Bid), — Implementation, Maintenance and Facility Management for System Security Tools for Cyber Security Operation Centre (C-SOC) (Technical Bid)** and **— Implementation, Maintenance and Facility Management for System Security Tools for Cyber Security Operation Centre (C-SOC) (Indicative Commercial Bid)** respectively should be put in a single sealed outer cover duly sealed and super-scribed as — **Implementation, Maintenance and Facility Management for System Security Tools for Cyber Security Operation Centre (C-SOC)** as per the below mentioned diagram and as per bid details given in the RFP.

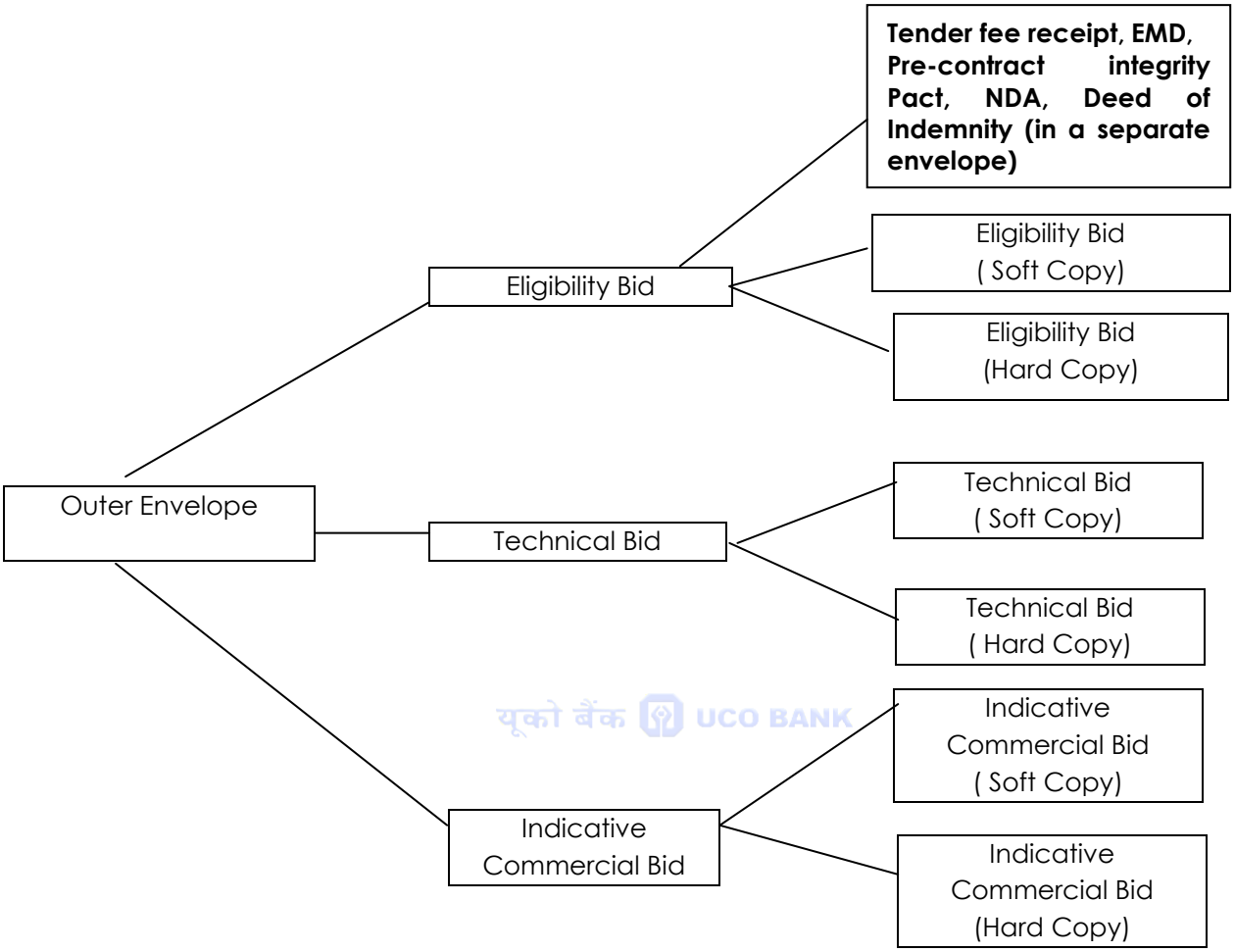
(Separate Envelopes for Eligibility Bid, Technical Bid & Commercial Bid. One Separate envelope containing Tender Fee Receipt, EMD, Non-Disclosure Agreement , Deed of Indemnity and Pre-Contract Integrity Pact should invariably be placed in Eligibility Bid envelope).

If Tender fee receipt, EMD and Pre-contract integrity Pact is not present inside Eligibility Bid, the bid will be treated as incomplete and that bid will be liable for rejection.

The bids (along with soft copy) shall be dropped/submitted at UCO Bank's address given in Bid Control Sheet Table, on or before the date specified therein.

All envelopes must be super-scribed with the following information:

- Name of the Bidder
- Offer Reference
- Type of Offer (Eligibility or Technical or Indicative Commercial)



The Eligibility and Technical Offers should be complete in all respects and contain all information asked for, in the exact format of eligibility and technical specifications given in the RFP, except prices. The Eligibility and Technical offers must not contain any price information. UCO BANK, at its sole discretion, may not evaluate Eligibility or Technical Offer in case of non-submission or partial submission of eligibility or technical details. Any decision of UCO BANK in this regard shall be final, conclusive and binding upon the bidder.

The Technical bid should have mandatorily comprise of the followings:-

1) All the pages of the RFP duly signed and stamped by the bidder.
2) All pages and documents in individual bids should be numbered as page no. – (Current Page No.) of page no – (Total Page No.) and should contain tender reference no. and Bank's Name.

3) The entire clause mentioned in the RFP should be complied by the bidder. Conditional remarks will not be accepted by the Bank.

4) Documentary proof in support of Eligibility Criteria mentioned in the RFP.

5) All **Annexures- A,B,C,D,E,F,G,H,I,J,K,L,M,N,O,P,Q,R,S,T** of the this RFP should be duly signed and complied.

The Commercial Offer (Hard Copy) should contain all relevant price information as per **Annexure – G**.

Note:

i. If the outer cover / envelop are not sealed & super scribed as required, the Bank will assume no responsibility for bid documents misplacement or premature opening.

ii. If any inner cover / envelop of a bid is found to contain both Eligibility/ Technical & Indicative Commercial Bids together then that bid will be rejected summarily.

iii. If any outer envelope is found to contain only the eligibility bid or technical bid or indicative commercial bid, it will be treated as incomplete and that bid will be liable for rejection.

iv. If indicative commercial bid is not submitted in a separate sealed envelope duly marked as mentioned above, this will constitute grounds for declaring the bid non-responsive.

v. The Bank reserves the right to resort to re-tendering without providing any reason whatsoever. The Bank shall not incur any liability on account of such rejection.

vi. The Bank reserves the right to modify any terms, conditions or specifications for submission of bids and to obtain revised Bids from the bidders due to such changes, if any, at any time prior to completion of evaluation of technical / eligibility bids from the participating bidders.

vii. Canvassing of any kind will be a disqualification and the Bank may decide to cancel the bidder from its empanelment.

Part – III

BID OPENING AND EVALUATION CRITERIA

There would be a three (3) stage process.

The Stages are:

I) Eligibility Criteria Evaluation

II) Technical Evaluation

III) Commercial Bid(**E-Tendering**)

The Eligibility Criteria would be evaluated first for the participating bidders. The bidders, who qualify all Eligibility Criteria as mentioned in RFP, will be shortlisted for the Technical bid evaluation. A detailed technical evaluation would be undertaken for eligible bidders and only the technically qualified bidders would be shortlisted for commercial bid (E-Tendering).

The Bank will **adopt e-Tendering process for Reverse Auction of Commercial Bid.** Only those Bidders will be eligible for Reverse Auction who qualifies in Technical evaluation. Post Reverse Auction, Bidder shall submit the price breakup matching its final Reverse Auction price in the format of commercial bid (**Annexure- G**). The Commercial Bid should contain price information only and to be submitted strictly as per the format provided in **Annexure –G.**

3.1 Evaluation Methodology

The objective of evolving this evaluation methodology is to facilitate the selection of the most cost-effective solution (Total Cost of Ownership) **over a 5-year period** that appropriately meets the requirements of the Bank identified in this RFP.

3.2 Technical & Commercial evaluation process

- The proposals will be evaluated in three stages. In the first stage, i.e. Eligibility Evaluation, the bidders will be shortlisted, based on bidder's responses. In the second stage, the Technical Evaluation will be done and finally the Commercial Bids.
- During the period of evaluation, bidders may be asked to provide more details and explanations about information provided in the proposals. Bidders should respond to

such requests within the time frame indicated in the letter/e-mail seeking explanation.

- The resources offered should meet all the technical requirements mentioned in scope of work and technical requirement of bank. Non-compliance to any of the technical specification may attract rejection of the proposal without assigning any reason and without any cost or compensation thereof.
- The bidders should submit the Indicative commercial bill of materials covering cost for each solution (for each line item) and total cost for the Bank as per Annexure-G.
- Commercial Bids of bidders, who qualified in the technical evaluation stage, will be considered for participation in commercial evaluation.
- Commercial evaluation will be done through a Reverse Auction as per the guidelines given in Annexure-H.
- After the completion of reverse auction, the bidders are required to provide the final commercial bids (FCB) by 4:00 pm next day, matching the final reverse auction price. The FCB will comprise of the Total cost for Bank (TCB) with detailed breakup.
- L1 price will be determined after giving effect to arithmetical correction, if any.
- L1 bidder will be determined on the basis of the lowest price quoted in the final commercial bid (FCB).
- The Bank might recognize the L1 bidder for signing the contract for the scope of work defined within the RFP document.
- The indicative commercial bid shall be opened post the technical evaluation. The bids shall be opened only for the technically qualified bidders.
- The prices and other terms offered by the bidder must be firm for an acceptance period of 180 days from opening of the commercial bids.
- The Bank reserves the right to modify any terms, conditions and specifications of the RFP and Bank reserves right to obtain revised price bids from the bidders with regard to change in the RFP clauses. The bank reserves the right to accept any bid in whole or in part.

3.3 Short Listing

The bidder needs to qualify as per eligibility criteria. Only eligible bidders will be qualified for the Technical evaluation process and only technically qualified bidders are to be called for commercial bid (e-Tendering Process). Only those bidders who achieve technical requirements mentioned in scope of work would be short-listed for commercial bid process.

i) **Normalization of bids:** The Bank will go through a process of Eligibility evaluation followed by the technical evaluation and normalization of the bids to the extent possible and feasible to ensure that bidders are more or less on the same technical

ground. After the normalization process , if the Bank feels that any of the bids needs to be normalized and that such normalization has a bearing on the price bids; the Bank may at its discretion ask all the technically short-listed bidders to resubmit the technical and indicative commercial bids once again for scrutiny in part or full. The resubmissions can be requested by the Bank in the following two manners:

- Incremental bid submission in part of the requested clarification by the Bank.
- Revised submissions of the entire bid in the whole.

The Bank can repeat this normalization process at every stage of bid submission or till the Bank is satisfied. The bidder has to agree that they have no reservation or objection to the normalization process and all the technically short listed bidders will, by responding to this RFP, agree to participate in the normalization process and extend their co-operation to the Bank during this process. The bidder, by submitting the response to this RFP, agrees to the process and conditions of the normalization process.

ii) The bidder will be solely responsible for complying with any applicable Export / Import Regulations. The Bank will no way be responsible for any deemed Export benefit that may be available to the bidder.

iii) The bidder needs to provide Unit costs for components and services; unit rates would be considered for the TCO purposes.

iv) In the event the vendor has not quoted or mentioned the component or services required, for evaluation purposes the highest value of the submitted bids for that component or service would be used to calculate the TCO. For the purposes of payment and finalization of the contract, the value of the lowest bid would be used.

PART-IV

4.1 Order Details

The purchase order will be placed by Bank Head Office, Information Security Wing (CISO Office) in the name of selected bidder as per requirement. The payment will be made by Information Security Wing (CISO Office), Head Office – I and the Performance Bank Guarantee for order will be required to be submitted in the Information Security Wing (CISO Office), Head Office – I.

4.2 Performance Bank Guarantee

The successful bidder shall be required to provide a Bank Guarantee for 10% of the Total Order Value issued by any scheduled commercial bank (other than UCO Bank) valid for **63 months (60+3 months claim period),** from the issuance of Purchase Order (PO), indemnifying any loss to the Bank, as per the format of **Annexure – K.**

The bank guarantee shall be provided to the bank either before or at the time of execution of the Service Level Agreement (SLA). **Upon furnishing the Performance Bank Guarantee, the EMD of the selected bidder shall be returned.**

The Performance Bank Guarantee shall act as a security deposit and either in case the successful bidder is unable to start the project within the stipulated time or start of the project is delayed inordinately beyond the acceptable levels, the Bank reserves the right to forfeit the same.

Further, the Bank reserves the right to invoke the Performance Bank Guarantee in case the successful bidder is not able to fulfill any or all conditions specified in the document or is unable to complete the project within the stipulated time. This is independent of the LD on delivery and implementation.

4.3 Project Timeline

Bidders are requested to keep the following timelines in regard to the implementation of solutions/requirements.

T denotes the date of release of PO to the Bidder. For example: T+3 represents that the solution needs to be implemented within Three (3) months of the release of the Purchase Order (PO).

Solutions	Network Access Control (NAC) & Patch Management	Data Loss / Leakage Prevention (DLP)	Automated Vulnerability Assessment Scanners (VAS)	IT-Governance, Risk & Compliance (IT-GRC)	Anti-Advanced Persistent Threat (APT)
Timelines	**T+6**	**T+6**	**T+3**	**T+3**	**T+3**

Weekly meeting will be held on every Monday during implementation period and every 1st Day of the Month (tentatively) during the contract period.

4.4 Facility Management

Experienced Man power resource will be deployed at Bank's SOC location for facility management, implementation and monitoring. The resource should be available 24*7*365 days at Bank's SOC location. The bidder should provide Experienced Man power resource for required services and reports mentioned in the RFP. The resources should be Engineer (BE/ B. Tech or equivalent as per govt. guidelines and with CCNA/CSP/CCSP to provide for the scope of work mentioned in the RFP.

The no. of man power resources provided by the bidder for facility management 24*7*365 at Bank's SOC location should be mentioned in Technical Bid **Annexure-F** and accordingly it should be mentioned in commercial bid.

4.5 Delivery and Implementation

4.5.1 Deliveries of the software, implementation and operationalization of complete solution at all locations should be made within the project timeline mentioned in the RFP.

4.5.2 If however, the delay is caused by any action pending from the Bank end, the corresponding period will not be considered while calculation of delay period.

4.5.3 The process will be deemed complete when all the proposed solution have been implemented and made operationalized as per the scope, terms & conditions of the RFP and satisfactory acceptance given by the Bank. The selected bidder has to resolve any system software/hardware problems during successful implementation and operationalization. It will be the responsibility of the successful bidder to resolve the issues if it arises due to Bank's existing IT Infrastructure either by providing the solution or resolving with existing vendor/system integrator at no extra cost to the Bank.

4.5.4 All the equipment supplied by the Bidder shall be legal and Bidder shall give indemnity to that effect.

4.5.5 Any license, if required, need to be provided by the selected bidder. The selected bidder is solely responsible for any legal obligation related to licenses during contract period for solution proposed as implemented by the bidder.

4.5.6 The equipment's are considered accepted (Commissioned and Operationalized) after signing the Acceptance Test document jointly by the representative from the Bank and engineer from the successful bidder. The component level checking for individual item may be included during the acceptance test.

4.5.7 The selected bidder is required to transport the goods to a specified place of destination within India, defined as the Project Site, transport to such place of destination in India, shall be arranged by the bidder, and the related costs shall be included in the quoted price. Cost for obtaining necessary road permits and other related permits will be the responsibility of the selected bidder.

4.5.8 The licenses for all solutions should be perpetual in the name of UCO Bank. The OEMs should certify the same on their letterhead.

4.6 Deployment Locations

Primary Data Center (Bangalore), Disaster Data Center (Kolkata), Near Data Center (Bangalore), Zonal Offices, Branches, SOC (Kolkata).

4.7 Payment Terms

The term of the contract will be Five years. Hardware to be provided for execution of project should be sized for Five years by considering functional & technical requirements as per in-scope solutions.

However, if it is found that the hardware is not sized adequately or the hardware utilization goes beyond the threshold limit of 80%, the Bidder has to provide additional hardware at no additional cost to meet the performance parameters set by the Bank during the contract period.

The Bidder must accept the payment terms proposed by the Bank as proposed in this Section.

The scope of work is divided in different areas and the payment would be linked to delivery and acceptance. All/any payments will be made subject to LD/compliance of Service Levels defined in the RFP document. The Bank shall have the right to withhold any payment due to the Bidder, in case of delays or defaults on the part of the Bidder. Such withholding of payment shall not amount

to a default on the part of the Bank. If any of the items / activities as mentioned in the price bid is not taken up by the bank during the course of the assignment, the bank will not pay the fees quoted by the Bidder in the price bid against such activity / item.

Procedure for claiming payments

The Bidder's requests for payment shall be made to the Bank in writing accompanied by Original Invoice detailing the systems, software delivered, installed and accepted by the bank.

The payment after deducting applicable TDS will be released by the Bank. All payments will be made only by electronic transfer of funds either by NEFT or RTGS. The Bidder therefore has to furnish the bank account number to where the funds have to be transferred for effecting payments.

Payments as per the schedule given below will be released only on acceptance of the order and on signing of the agreement/contract by the selected bidder and also on submission of Performance Bank guarantee.

Deliverables	% OF PAYMENT	STAGES (On completion of the activities)
Hardware/Appliance/ Software/ License	10%	Successful delivery and acceptance of the Hardware with Environment Setup after post-delivery audit, on submission of invoice with Proof of Delivery and other documents
	80%	On individual Solution implementation Sign-off of individual solution.
	10%	On Completion of the Warranty Period or Submission of Bank guarantee for the Warranty period.
Payment for Managed services	--	Payment will be made quarterly in arrears post sign-off and acceptance of all the relevant requirements under the scope.
AMC/ATS	--	Actual amount as per the Bill of Material will be paid quarterly in arrears.

- There shall be no escalation in the prices.
- No advance payment will be made.
- All applicable taxes and duties will be deducted at source as per applicable laws.

- Any penalties / liquidated damages imposed on the bidder for non-performance will be deducted from the payment as deemed necessary
- The Selected Bidder shall be responsible for delivery; implementation and rollout of all the solutions required under this RFP and also must adhere to the timeline as specified in project timeline in the RFP.
- In the event of Bidder's failure to deliver and/or implement all required components of a fully functional system (pertaining to the scope of the project) within the stipulated time schedule or by the date extended by the Bank, unless such failure is due to reasons entirely attributable to the Bank, it will be a breach of contract. In such case, the Bank would be entitled to charge a penalty or will have the right to terminate the contract, as specified in this RFP.

4.8 Confidentiality

The bidder/selected bidder must undertake that they shall hold in trust any Information received by them under the Contract/Service Level Agreement, and the strictest of confidence shall be maintained in respect of such Information. The bidder has also to agree:

- To maintain and use the Information only for the purposes of the Contract/Agreement and only as permitted by BANK;
- To only make copies as specifically authorized by the prior written consent of the Bank and with the same confidential or proprietary notices as may be printed or displayed on the original;
- To restrict access and disclosure of Information to such of their employees, agents, strictly on a "need to know" basis, to maintain confidentiality of the Information disclosed to them in accordance with this Clause, and
- To treat all Information as Confidential Information.
- Conflict of interest: The Vendor shall disclose to BANK in writing, all actual and potential conflicts of interest that exist, arise or may arise (either for the Vendor or the Bidder's team) in the course of performing the Service(s) as soon as practical after it becomes aware of that conflict.

The selected Bidder is required to execute a SLA (Service Level Agreement), DOI (Deed of Indemnity) and NDA (Non-Disclosure Agreement) to the bank as per bank's format before or at the time of execution of the Master Contract.

4.9 Paying Authority

The payments which is/are inclusive of GST and other taxes, fees etc. as per the Payment Schedule covered herein above shall be paid by Information Security Wing (CISO Office), UCO Bank, Head Office – I, Kolkata. However, Payment of

the Bills would be released, on receipt of advice / confirmation for satisfactory delivery and commissioning, live running and service report etc. after deducting all penalties.

4.10 Service Level Agreement (SLA)

4.10.1 The bidder shall perform its obligations under the service level agreement entered into with the Bank.

4.10.2 If any act or failure by the bidder under the agreement results in failure or inoperability of systems and if the Bank has to take corrective actions to ensure functionality of its property, the Bank reserves the right to impose penalty, which may be equal to the cost it incurs or the loss it suffers for such failures.

4.10.3 If the bidder fails to complete the due performance of the contract in accordance with the specification and conditions of the offer document, the Bank reserves its right either to cancel the order or to recover a suitable amount as deemed reasonable as Penalty for non-performance.

4.10.4 SLA violation will attract penalties as mentioned in the penalty clause.

4.10.5 The selected bidder shall ensure uptime (to be calculated on monthly basis). The bank reserves the right to impose / waive any such penalty.

4.10.6 The purchaser may without prejudice to its right to effect recovery by any other method, deduct the amount of penalty from any money belonging to the bidder in its hands (which includes the purchaser's right to claim such amount against bidder's Bank Guarantee) or which may become due to the Bidder. Any such recovery of penalty shall not in any way relieve the Bidder from any of its obligations to complete the works/services or from any other obligations and liabilities under the Contract.

4.11 Penalty

If the Vendor fails to maintain guaranteed monthly uptime of 99.5 % of each individual solution, the Bank shall impose penalty as mentioned below on slab basis:

Monthly Uptime	Penalty as % of overall monthly uptime
Above 99.5%	**No Penalty**
98% to 99.5%	**2%**
96% to 97.99%	**4%**
94% to 95.99%	**6%**
92% to 93.99%	**8%**

90% to 91.99%	**10%**
Less than 90%	**Bank reserves the right to invoke the Performance Bank Guarantee (PBG) and the contract will be terminated.**

- Bidder will provide on-site support for addressing Hardware/ Software/application related issues.
- The new releases (minor / major), versions, bug fixes etc. for the system solution will be supplied to the Bank at no extra charge, with necessary documentation.
- The Bidders should submit a list of support centre addresses, contact person & the resolution/response matrix for the locations.

- **Availability and Uptime (Solution Uptime):**

  The vendor shall ensure that a **minimum 99.5% uptime** will be maintained for all the proposed solution calculated on a monthly basis.

  The percentage uptime is calculated on a monthly basis (24 hours a day):
  (Total contracted minutes in a month - Downtime minutes within contracted minutes in a month) x 100 / Total Contracted Minutes in a Month.

- Bank may recover such amount of penalties due to delay in service from any payment being released to the vendor, irrespective of the fact whether such payment is relating to this contract or otherwise. The same may be recovered from the payment due towards the vendor or from the retention money at the end of contract period.
- The sum total of penalties will not exceed 10% of the Total Cost of Ownership (TCO) within the contract period. Thereafter, the contract/purchase order may be cancelled and performance bank guarantee may be revoked.

4.12 Liquidated Damage

Notwithstanding the Bank's right to cancel the order, liquidated damages **at 1% (One percent**) of the Total Cost of Ownership (TCO) price per week will be charged for every week's delay in the specified implementation schedule from the date of issuance of Purchase Order (PO). The Liquidated Damages including Service Level Penalties would be subject **to a maximum of 10% of the total project cost**. Bank will have right to recover these amounts by any mode such as adjusting from any payments to be made to the selected bidder or from the performance Bank Guarantee. Liquidated damages will be calculated per week basis.

The Bidder shall perform its obligations under the agreement entered into with the Bank, in a professional manner. Bank may invoke the Bank Guarantee for further delay in start of the services.

4.13 Warranty

4.13.1 The Bidder further represents and warrants that all licenses delivered / rendered under and in accordance with contract shall have no defect, arising from design or from any act, error/defect or omission of the Bidder.

4.13.2 The warranty period will be **36 months** from date of successful deployment of proposed solution at the respective location/s for Support and warranty period.

4.13.3 Upon receipt of notice of such defect / error or deficiency, the Bid shall, with all reasonable speed, repair or replace the defective equipment/software or parts thereof, without cost to Purchaser.

4.13.4 If the Bidder having been notified fails to remedy the defect(s) within the period specified period by the Bank, Purchaser may proceed to take such remedial action as may be necessary, at the Bidder's risk and expense and without prejudice to any other rights, which Purchaser may have against the Bidder under and in accordance with the Contract.

4.13.5 All updates and upgrades during the contract have to be provided at no cost to the bank.

4.13.6 The bidder shall be fully responsible for the manufacturer's warranty in respect of proper design, quality and workmanship of all equipment, accessories etc. covered by the tender.

4.13.7 The vendor must warrant all equipment, accessories, spare parts etc. against any manufacturing defects during the warranty period.

4.13.8 During the contract period, the bidder shall maintain the systems and repair/replace at the installed site, at no charge to the bank, all defective components that are brought to the bidder's notice.

4.13.9 As far as possible, the equipment should be repaired at the site and where the equipment is taken for repairs outside the Bank, a substitute of the similar or higher configuration / capacity equipment should be provided and data should be transferred to the substitute machine besides creating back-up.

4.13.10 The bidder must provide for all services to be supplied under this period of contract covering all spare parts & service from the date of acceptance of the systems by UCO Bank at the respective locations.

4.13.11 During the contract period, the bidder will have to undertake comprehensive maintenance of the entire hardware, software, services and accessories supplied by the selected bidder. This service is to be provided on all days of the Bank notwithstanding the fact whether on such days the selected bidder's office remains closed or not. The request for support shall have to be attended by the vendor even if the request is made over telephone / SMS or by e-mail / fax by the respective sites, as per SLA. The entire equipment should be repaired within 24 hours (Resolution time). In case of vendor failing above standards, a standby arrangement should be provided till the machine is repaired.

4.13.12 The bidder shall be fully responsible for the manufacturer's warranty & services for all equipment, accessories, spare parts etc. against any defects arising from design, material, manufacturing, workmanship, or any act or omission of the manufacturer / Vendor or any defect that may develop under normal use of supplied equipment during the contract period. Warranty shall not become void even if UCO Bank buys any other supplemental software from a third party and implements it with / in these machines. However, the warranty will not apply to such software implemented. Besides the above, the selected bidder will have to enter into Service Level Agreement.

4.14 Annual Maintenance Charges (AMC) and Annual Technical Support (ATS)

4.14.1 The bidders shall quote AMC/ATS Charges for **Implementation, Maintenance and Facility Management for System Security Tools for Cyber Security Operation Centre (C-SOC)** for a period of two years after the initial comprehensive onsite warranty period of three years in commercial bid.

4.14.2 The Bank shall not pay any separate AMC/ATS charges on any software & Hardware supplied and installed to meet the requirements of this RFP.

4.14.3 Preventive maintenance activity should be carried out once in a quarter.

4.14.4 The AMC/ATS payment will be made by Head Office on quarterly basis in arrear subject to satisfactory services rendered by the bidder.

4.14.5 Bank reserves its right to decide whether or not to enter into AMC/ATS with the successful bidder, for the post warranty period.

4.14.6 In case Bank decides to enter into AMC, the successful bidder shall ensure that the type of support/maintenance services extended for proposed solution during the AMC period of 2 years after the initial comprehensive onsite warranty period of three year, is similar to the support/maintenance extended during warranty period.

4.14.7 The Bank shall have the option to terminate the service contract at any time during the contract period by giving a written notice of 30 days, without assigning any reason thereof. However, the selected bidder shall commit himself to service for a minimum period of 5 years, unless the service contract is terminated by the Bank and the selected bidder will have no right to terminate the contract within this period.

4.14.7 In case of any disputes in uptime, it should be resolved amicably/mutually agreed upon. However the successful bidder shall submit the necessary proof that the failures are not on account of hardware & software and its related equipments.

4.15 Force Majeure

Force Majeure is herein defined as any cause, which is beyond the control of the selected bidder or the Bank as the case may be which they could not foresee or with a reasonable amount of diligence could not have foreseen and which substantially affect the performance, such as:

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

Provided either party shall within ten (10) days from the occurrence of such a cause notify the other in writing of such causes. The Selected bidder or the Bank shall not be liable for delay in performing his / her obligations resulting from any Force Majeure cause as referred to and / or defined above.

4.16 Contract Period

The tenure of the Contract will be for a period of **5 (Five) years** with warranty effective from the date of execution of the Service Level Agreement (SLA) unless terminated earlier by the Bank by serving 90 days prior notice in writing to the selected bidder at its own convenience without assigning any reason and without any cost or compensation therefor. However, after the completion of

initial period of 5 (Five) years, the contract may be extended/renewed for further period on such terms and conditions as would be decided by the Bank.

The performance of the selected bidder shall be reviewed every quarter and the Bank reserves the right to terminate the contract at its sole discretion by giving 90 days' notice without assigning any reasons and without any cost or compensation therefor. Any offer falling short of the contract validity period is liable for rejection.

The selected bidder is required to enter into a Service Level Agreement (SLA), the format whereof is to be supplied by the Bank.

4.17 Completeness of the Project

The project will be deemed as incomplete if the desired objectives of the project as mentioned in the RFP are not achieved.

4.18 Order Cancellation

The Bank reserves its right to cancel the order/contract 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 implementation / testing beyond the specified period.
- Serious discrepancy in the quality of service expected during the implementation and rollout process.

- In case of cancellation of order, any payment made by the Bank to the selected bidder would necessarily have to be returned to the Bank, further the selected bidder would also be required to compensate the Bank for any direct loss suffered by the Bank due to the cancellation of the contract/purchase order and any additional expenditure to be incurred by the Bank to appoint any other vendor. This is after repaying the original amount paid.

- The selected bidder should be liable under this section if the contract/ purchase order has been cancelled in case sum total of penalties and deliveries do not exceed 10% of the TCO.

4.19 Indemnity

The selected bidder agrees to indemnify and keep indemnified the Bank against all losses, damages, costs, charges and expenses incurred or suffered by the Bank due to or on account of any claim for infringement of intellectual property rights.

The selected Bidder agrees to indemnify and keep indemnified the Bank against all losses, damages, costs, charges and expenses incurred or suffered by the Bank due to or on account of any breach of the terms and conditions contained in this RFP or Service Level Agreement to be executed.

The selected Bidder agrees to indemnify and keep indemnified Bank at all times against all claims, demands, actions, costs, expenses (including legal expenses), loss of reputation and suits which may arise or be brought against the Bank, by third parties on account of negligence or failure to fulfil obligations by the selected bidder or its employees/personnel.

All indemnities shall survive notwithstanding expiry or termination of Service Level Agreement and the Vendor shall continue to be liable under the indemnities.

The selected Bidder is required to furnish a separate Letter of Indemnity (As per Annexure-T) in Bank's favour in this respect before or at the time of execution of the Service Level Agreement.

4.20 Publicity

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

4.21 Privacy & Security Safeguards

The selected bidder shall not publish or disclose in any manner, without the Bank's prior written consent, the details of any security safeguards designed, developed, or implemented by the selected bidder under this contract or existing at any Bank location. The Selected bidder shall develop procedures and implementation plans to ensure that IT resources leaving the control of the assigned user (such as being reassigned, removed for repair, replaced, or upgraded) are cleared of all Bank Data and sensitive application software. The Selected bidder shall also ensure that all subcontractors who are involved in providing such security safeguards or part of it shall not publish or disclose in any manner, without the Bank's prior written consent, the details of any security safeguards designed, developed, or implemented by the selected bidder under this contract or existing at any Bank location.

4.22 Technological Advancements

The selected bidder shall take reasonable and suitable action, taking into account economic circumstances, at mutually agreed increase / decrease in charges, and the Service Levels, to provide the Services to the Bank at a technological level that will enable the Bank to take advantage of technological advancement in the industry from time to time.

4.23 Guarantees

Selected bidder should guarantee that all the material as deemed suitable for the delivery and management of the Implementation of the Proposed Solution. All software must be supplied with their original and complete printed documentation.

4.24 Resolution of Disputes

The selected Bidder and the Bank shall endeavour their best to amicably settle all disputes arising out of or in connection with the Contract in the following manner:

a. The Party raising a dispute shall address to the other Party a notice requesting an amicable settlement of the dispute within seven (7) days of receipt of the notice.

b. The matter will be referred for negotiation between General Manager (IT Department) of UCO BANK and the Authorized Official of the selected Bidder. The matter shall then be resolved between them and the agreed course of action shall be documented within a further period of 15 days.

In case the dispute(s)/difference(s) between the Parties is/are not settled through negotiation in the manner as mentioned above, the same may be resolved by arbitration and such dispute/difference shall be submitted by either party for arbitration within 15 days of the failure of negotiations. Arbitration shall be held in Kolkata and conducted in accordance with the provisions of Arbitration and Conciliation Act, 1996 or any statutory modification or re-enactment thereof. Each Party to the dispute shall appoint one arbitrator each and the two arbitrators shall jointly appoint the third or the presiding arbitrator.

The "Arbitration Notice" should accurately set out the disputes between the parties, the intention of the aggrieved party to refer such disputes to arbitration as provided herein, the name of the person it seeks to appoint as an arbitrator with a request to the other party to appoint its arbitrator within 30 days from receipt of the notice. All notices by one party to the other in connection with the arbitration shall be in writing and be made as provided in this tender document.

The arbitrators shall hold their sittings at Kolkata. The arbitration proceedings shall be conducted in English language. Subject to the above, the courts of law at Kolkata alone shall have the jurisdiction in respect of all matters connected with or arising out of the Contract/Service Level Agreement even though other Courts in India may also have similar jurisdictions. The arbitration award shall be final, conclusive and binding upon the Parties and judgment may be entered

thereon, upon the application of either party to a court of competent jurisdiction. Each Party shall bear the cost of preparing and presenting its case, and the cost of arbitration, including fees and expenses of the arbitrators, shall be shared equally by the Parties unless the award otherwise provides.

The selected Bidder shall not be entitled to suspend the Service/s or the completion of the job, pending resolution of any dispute between the Parties, rather shall continue to render the Service/s in accordance with the provisions of the Contract/ Service Level Agreement.

4.25 Exit Option and Contract Re-Negotiation

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

- Failure of the selected bidder to accept the contract / purchase order and furnish the Performance Bank Guarantee within 30 days of receipt of purchase order;
- Delay in offering;
- Delay in commissioning project beyond the specified period;
- Delay in completing commissioning / implementation and acceptance tests / checks beyond the specified periods;
- Serious discrepancy in project noticed during the testing;
- Serious discrepancy in functionality to be provided or the performance levels agreed upon, which have an impact on the functioning of the Bank.
- Serious discrepancy in completion of project.
- Serious discrepancy in maintenance of project.

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 selected Bidder.

The Bank will reserve a right to re-negotiate the price and terms of the entire contract with the selected bidder at more favourable terms in case such terms are offered in the industry at that time for projects of similar and comparable size, scope and quality.

The Bank shall have the option of purchasing the software from third-party suppliers, in case such equipment is available at a lower price and the selected bidder's offer does not match such lower price. Notwithstanding the foregoing, the selected bidder shall continue to have the same obligations as contained in

this scope document in relation to such equipment procured from third-party suppliers.

As aforesaid the Bank would procure the software from the third party only in the event that the software was available at more favourable terms in the industry, and secondly, the software procured here from third parties is functionally similar, so that the selected bidder can maintain such equipment.

The modalities under this right to re-negotiate /re-procure shall be finalized at the time of contract finalization.

Notwithstanding the existence of a dispute, and/or the commencement of arbitration proceedings, the Selected Bidder will be expected to continue the services. The Bank shall have the sole and absolute discretion to decide whether proper reverse transition mechanism over a period of 6 to 12 months, has been complied with. In the event of the conflict not being resolved, the conflict will be resolved through Arbitration.

The Bank and the Selected Bidder shall together prepare the Reverse Transition Plan. However, the Bank shall have the sole decision to ascertain whether such Plan has been complied with.

Reverse Transition mechanism would typically include service and tasks that are required to be performed / rendered by the Selected Bidder to the Bank or its designee to ensure smooth handover and transitioning of Bank's deliverables, maintenance and facility management.

4.26 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 anything of values to influence the action of an official in the procurement process or in contract execution

AND

"Fraudulent Practice" means a misrepresentation of facts in order to influence a procurement process or the execution of contract to the detriment of the Bank and includes collusive practice among bidders (prior to or after 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.

4.27 Termination

UCO BANK reserves the right to cancel the work/purchase order/contract or terminate the SLA by giving 90 (Ninety) days' prior notice in writing and recover damages, costs and expenses etc., incurred by Bank under the following circumstances: -

a) The selected bidder commits a breach of any of the terms and conditions of this RFP or the SLA to be executed between the Bank and the selected Bidder.

b) The selected bidder goes into liquidation, voluntarily or otherwise.

c) The selected bidder violates the Laws, Rules, Regulations, Bye-Laws, Guidelines, and Notifications etc.

d) An attachment is levied or continues to be levied for a period of seven days upon effects of the bid.

e) The selected bidder fails to complete the assignment as per the time lines prescribed in the Work Order/SLA and the extension, if any allowed.

f) Deductions on account of liquidated damages exceed more than 10% of the total work order.

g) In case the selected bidder fails to deliver the resources as stipulated in the delivery schedule, UCO BANK reserves the right to procure the same or similar resources from alternate sources at the risk, cost and responsibility of the selected bidder.

h) After award of the contract, if the selected bidder does not perform satisfactorily or delays execution of the contract, UCO BANK reserves the right to get the balance contract executed by another party of its choice by giving one month's notice for the same. In this event, the selected bidder is bound to make good the additional expenditure, which UCO BANK may have to incur in executing the balance contract. This clause is applicable, if the contract is cancelled for any reason, whatsoever.

i) UCO BANK reserves the right to recover any dues payable by the selected Bidder from any amount outstanding to the credit of the selected bidder, including the adjustment of pending bills and/or invoking the Performance Bank Guarantee under this contract.

The rights of the Bank enumerated above are in addition to the rights/remedies available to the Bank under the Law(s) for the time being in force.

4.28 Termination for Insolvency

The Bank may at any time terminate the Contract by giving written notice to the Bidder, if the Bidder becomes bankrupt or otherwise insolvent. In this event, termination will be without compensation to the Bidder, provided that such termination will not prejudice or affect any right of action or remedy, which has accrued or will accrue thereafter to the Bank.

4.29 Effect of Termination

In the event of termination of the Contract due to any reason, whatsoever, [whether consequent to the expiry of stipulated term of the Contract or otherwise], UCO BANK shall be entitled to impose any such obligations and conditions and issue any clarifications as may be necessary to ensure an efficient transition and effective business continuity of the Service(s) which the Vendor shall be obliged to comply with and take all steps to minimize loss resulting from the termination/breach, and further allow the next successor Vendor to take over the obligations of the erstwhile Vendor in relation to the execution/continued execution of the scope of the Contract.

In the event that the termination of the Contract is due to the expiry of the term of the Contract and the Contract is not further extended by UCO BANK, the Vendor herein shall be obliged to provide all such assistance to the next successor Bidder or any other person as may be required and as UCO BANK may specify including training, where the successor(s) is a representative/personnel of UCO BANK to enable the successor to adequately provide the Service(s) hereunder, even where such assistance is required to be rendered for a reasonable period that may extend beyond the term/earlier termination hereof.

Nothing herein shall restrict the right of UCO BANK to invoke the Performance Bank Guarantee and other guarantees, securities furnished, enforce the Letter of Indemnity and pursue such other rights and/or remedies that may be available to UCO BANK under law or otherwise.

The termination hereof shall not affect any accrued right or liability of either Party nor affect the operation of the provisions of the Contract that are expressly or by

implication intended to come into or continue in force on or after such termination.

4.30 Arbitration

All dispute or differences whatsoever arising between the selected bidder and the Bank out of or in relation to the construction, meaning and operation, with the selected bidder, or breach thereof shall be settled amicably. If, however, the parties are not able to resolve any dispute or difference aforementioned amicably, the same shall be settled by arbitration in accordance with the Rules of Arbitration of the Indian Council of Arbitration and the award made in pursuance thereof shall be binding on the parties. The Arbitrator / Arbitrators shall give a reasoned award.

Work under the Contract shall be continued by the Selected bidder during the arbitration proceedings unless otherwise directed in writing by the Bank unless the matter is such that the work cannot possibly be continued until the decision of the arbitrator or of the umpire, as the case may be, is obtained and save as those which are otherwise explicitly provided in the Contract, no payment due to payable by the Bank, to the Selected bidder shall be withheld on account of the on-going arbitration proceedings, if any unless it is the subject matter or one of the subject matters thereof. The venue of the arbitration shall be at KOLKATA, INDIA.

4.31 Applicable law & Jurisdiction of court

The Contract with the Selected bidder shall be governed in accordance with the Laws of India for the time being enforced and will be subject to the exclusive jurisdiction of Courts at Kolkata (with the exclusion of all other Courts).

4.32 Limitation of Liability

Bidder's aggregate liability under the contract shall be limited to a maximum of the contract value. This limit shall not apply to third party claims for

a. IP Infringement indemnity.

b. Bodily injury (including Death) and damage to real property and tangible property caused by Bidder/s' gross negligence. For the purpose of this section, contract value at any given point of time, means the aggregate value of the purchase orders placed by Bank on the Bidder that gave rise to claim, under this RFP.

c. Bidder shall be liable for any indirect, consequential, incidental or special damages under the agreement/ purchase order.

4.33 Independent External Monitors

a. The BUYER has appointed Independent Monitors (hereinafter referred to as Monitors) for this Pact in consultation with the Central Vigilance Commission (Names and Addresses of the Monitors given in the Pre Contract Integrity Pact to be submitted by the service provider as per **Annexure - L**).

b. 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.

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

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

e. 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.

f. The service provider (s) accepts that the Monitor has the right to access without restriction to all Project documentation of the BUYER including that provided by the service provider. The SERVICE PROVIDER will also grant the Monitor, upon his request and demonstration of a valid interest, unrestricted and unconditional access to his project documentation. The same is applicable to subcontractors. The Monitor shall be under contractual obligation to treat the information and documents of the service provider (s) with confidentiality.

g. 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.

h. 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 / SERVICE PROVIDER and should the occasion arise, submit proposals for correcting problematic situations.

i. The Buyer has appointed independent External Monitors for this Integrity Pact in consultation with the Central Vigilance Commission (Names and Addresses of the Monitors are given in RFP).

j. As soon as the integrity Pact is signed, the Buyer shall provide a copy thereof, along with a brief background of the case to the independent External Monitors.

k. The Service provider(s) / Seller(s) if they deem it necessary, May furnish any information as relevant to their bid to the Independent External Monitors.

l. If any complaint with regard to violation of the IP is received by the buyer in a procurement case, the buyer shall refer the complaint to the Independent External Monitors for their comments / enquiry.

m. If the Independent External Monitors need to peruse the records of the buyer in connection with the complaint sent to them by the buyer, the buyer shall make arrangement for such perusal of records by the independent External Monitors.

n. The report of enquiry, if any, made by the Independent External Monitors shall be submitted to MD & CEO, UCO Bank, Head Office at 10, Biplabi Trailokya Maharaj Sarani , Kolkata-700001 within 2 weeks, for a final and appropriate decision in the matter keeping in view the provision of this Integrity Pact.

o. The word "*Monitor*" would include both singular and plural.

4.34 Adoption of Integrity Pact

UCO Bank has adopted practice of Integrity Pact (IP) as per CVC guidelines. The Integrity Pact essentially envisages an agreement between the prospective vendors / service providers / sellers, who commit themselves to Integrity Pact (IP) with the Bank, would be considered competent to participate in the bidding process. In other words, entering into this pact would be the preliminary qualification. In case of bids for the purchase of Goods, Services, and Consultancy etc. not accompanied with signed IP by the service providers along with the technical bid, the offers shall be summarily rejected. The essential ingredients of the Pact include:

a. Promise on the part of the principal not to seek or accept any benefit, which is not legally available.

b. Principal to treat all service providers with equity and reason

c. Promise on the part of service providers not to offer any benefit to the employees of the Principal not available legally

d. Service providers not to enter into nay undisclosed agreement or understanding with other service providers with respect to prices, specifications, certifications, subsidiary contract etc.

e. Service providers not to pass any information provided by the Principal as part of business relationship to others and not to commit any offence under PC/IPC Act.

f. Foreign Service Providers to disclose the name and address of agents and representatives in India and Indian Service Providers to disclose their foreign principals or associates.

f. Service providers to disclose any transgressions with any other company that may impinge on the anti-corruption principle.

Integrity Pact, in respect of a particular contract, shall be operative from the date IP is signed by both the parties till the final completion of the contract. Any violation of the same would entail disqualification of the service providers and exclusion from future business dealings. IP shall cover all phases of contract i.e. from the stage of Notice Inviting Tenders (NIT)/Request for Proposals (RFP) till the conclusion of the contract i.e. final payment or the duration of warrantee/guarantee. Format of IP is attached as **Annexure – L** for strict compliance.

The following Independent External Monitors (IEMs) have been appointed by UCO Bank, who will review independently and objectively, whether and to what extent parties have complied with their obligation under the pact.

i. Shri S. R. Raman
1A-121, Kalpataru Gardens
i Near East-West Flyover Kandivali
East, Mumbai - 400101 E-mail:-
raman1952@gmail.com

ii. Ms. Vijayalakshmi R. Iyer
Flat No. - 1402, Barberry Towers, Nahar
Amrit Shakti, Chandivali, Powai,
Mumbai - 400072 E-mail:-
vriyer1955@gmail.com

PART-V

THE SCOPE OF WORK

The Scope of work for Implementation, Maintenance and Facility Management for System Security Tools for Cyber Security Operation Centre(C-SOC) including but not limited to design, supply, configuration, implementation, customization, integrations, monitor, manage, backup, documentation, training, warranty support, post warranty maintenance support and any other activities if contracted related to or connected to the IT security, Security solutions, devices and technologies. The bidder is expected to do following but not limited to:

- Overall scope to ensure successful implementation and 24*7*365 monitoring & management aspects of security solutions, devices, software, Applications for **NAC & Patch Management/DLP/VAS/IT-GRC/APT** for the Networking devices and devices at the Data Center, DR Site, NDR, Branches and Service Outlets identified by Bank and for the hardware/software applications of the Bank.
- Identify information security threats/ vectors targeting Bank's environment and prevent impact or breach by implementing adequate security mechanisms.
- Ensure that all aspects of Installation, De-Installation, integration, Configuration, Re-configuration, relocation (within the identified locations by Bank), enhancements, updates, upgrades, bug fixes, problem analysis, performance analysis, backups, audits, on-site as well as off-site support for the proposed hardware/software required for delivering the proposed Security services.
- Conduct the Risk Assessment activity for the devices and applications under the scope of C-SOC as per the Cyber Risk Management process of the bank.
- Provide forensic Support in case on any incident
- The solution, service, racks, hardware, software, storage, services would be provided by the bidder. The Bank will provide facilities to host the devices and seating arrangement for the personnel, including LEDs/ Desktops.
- Bidder should supply Products as specified, and Services which includes development, integration, management, maintenance, audit compliance, training and knowledge transfer.
- Procurement of the necessary solutions and the corresponding hardware, software, database, licenses etc. required for implementing these solutions at the Bank.
- Implementation of the respective solutions at the Bank including configuration, customization of the products, as per the Bank's requirement.

- Integration of the solutions to provide a comprehensive single dashboard view of the security risks/ incidents for the bank.
- Work with the existing System Integrator(s) of the Bank to integrate the C-SOC solutions with existing application platforms, server and storage environment, enterprise network, EMS, NMS solutions, security solutions, ticketing tools etc.
- Providing adequate resources.
- Development of operating procedures(SOP) in adherence with the bank's policies.
- Adherence to agreed Service Level Agreements (SLA) and periodic monitoring and reporting of the same to the bank.
- Bidder has to develop the project plan, get it approved from the Bank and then implement the project based on timelines given in the RFP.
- Bidder will prepare all documents related to deployment architecture, operation, maintenance including the Standard Operating Procedures (SOP) for all the processes, roles and responsibilities of the personnel. Provide the complete set of Operation and System Manuals in 3 sets of Hardcopies as well as in Softcopies of all the systems/components provided as part of the project implementations.
- The bidder would be responsible for updates, patches, bug fixes, version upgrades for the entire infrastructure without any additional cost to the Bank during the contract period.

- The Bidder should provide the latest version of the Solution. The bidder would be responsible for replacing the out-of-support, out-of-service, end-of-life, undersized, infrastructure elements at no extra cost to the Bank during the entire contract period of 5 Years. Replacement to be done before due date of the product/service and the intimation to be given to Bank at least one month before in case of any of the above scenario.
- The Bidder, do a gap analysis and submit a detailed study of the Bank's infrastructure and requirements relating to the proposed solution, prepare a detailed plan document/ road map mentioning all the pre-requisites, time-frame of mile-stones/ achievements leading to the full operationalization of the solution vis-a-vis Bank's requirement. This exercise should not affect the normal day to day functionality of the Bank.
- The system should be in hot-standby/ high-availability mode at Log collection and Logger level and with BC (Business Continuity) set-up at Bank's DR (Disaster Recovery) site. The Bidder would be responsible for installation, testing, commissioning, configuring, patching, regular backup, warranty and maintenance of the system.
- Selected Bidder would be responsible for all technical support to maintain the required uptime. Initial installation, configuration and integration should be done by the Bidder. The Bidder would be the single point of contact. The Bidder should

have necessary agreement with the OEM for all the required onsite support for entire contract period of five years. Bidder should have back-to-back support with OEM during the total contract period for necessary support. Bidder would submit a letter by OEM issued to bidder in this regard.

- Solution being provided should be scalable and user configurable to cater to the future requirement of the Bank.
- Bidder will deploy on-site resources on 24*7*365 basis at Bank's premises to support proposed solution.
- Bank will have the right to use the tools for the functions provided by the tools in any manner and for any number of branches, offices, subsidiary units, joint ventures, RRBs, irrespective of the number of users, geographical location of the devices being monitored. Bank will also have a right to relocate any one or all the tools to different locations.
- Bidder shall provide list and details of licenses to be procured and also maintain the inventory database of all the licenses and the updates installed. All licenses should be in the name of the Bank.
- The period of support coverage would be for 5 years from the date of sign off of all security solutions and services covered under this RFP.
- It will be the Bidder's responsibility to liaison with the OEM to provide full technical support to the satisfaction of the Bank for the complete tenure of agreement i.e. project.
- The Bank has a complex infrastructure with multiple resources maintained and managed through multiple vendors. So for seamless implementation close coordination is required with other vendors and bank personnel. A robust documentation system needs to be in place for all to understand the process and their responsibilities. Therefore the bidder has to provide the documentation for the project including but not limited to references regarding scope, functional and operational requirements, resource requirements, project design/plan, product description, guidance for best practices, implementation guidelines, user acceptance test plan, operation manual, security implementation, training materials, evaluation scoreboards and matrices.
- The bidder is expected to size the Hardware/appliance/storage as per the requirements mentioned in this RFP. The bidder's response should include the calculations/ logic used to arrive at the sizing.
- Adherence to agreed Service Level Agreements (SLA) and periodic monitoring and reporting of the same to the bank through a portal, which should be accessible to the Bank officials over iPAD, Mobile, Desktop, Laptop, Tablet etc. irrespective of platforms used.
- In case a device goes down at DC, the function being performed by the device should be taken over by a corresponding device at DR site and vice versa.

- In case the systems are not able to send the logs to the collector device, system should be able to extract the logs stored in the temporary memory of the devices at that site.
- If connectivity between log collection agents and logger is down then the Log collector agents should store the logs of at least 4 days and send them once connectivity is established.
- Bidder will be responsible to store logs in industry standard solution and format.
- Bidder needs to ensure that proposed solution will integrate with the IT System using standard methods/ protocols/ message formats without affecting the existing functionality of Bank.
- The configured correlation alerts and dashboards should be displayed on LED display at the SOC and Desktops/Laptops used at the SOC.
- The proposed solution by bidder will be audit from Bank and/or third party and/or regulatory body. It shall be responsibility of the Bidder to co-operate and provide necessary information and support to the auditors. The Bidder must ensure that the audit observations are closed on top priority and to the satisfaction of the Bank, regulator and its appointed auditors. Extreme care should be taken by the Bidder to ensure that the observations do not get repeated in subsequent audits. Such non-compliance by Bidder shall attract penalty as per the contract.
- The bidder shall also provide support in technical / functional / operational training, documenting policies / SOPs for proposed security tools, monitoring of incidents and logs, raising alerts, design and customize reports and product support for Security Tools implemented on 24x7x365 basis.
- All Log (raw or normalized) data must remain within the Bank's premises. Under no circumstances these data travel outside Bank's premises without Bank's consent.
- Further the bidder must follow the best practices for all compliances related to data and its security.
- The proposed solution should be capable of retrieving the archived logs for analysis, correlation, reporting and forensic purposes.
- The proposed solution has the incident management / ticketing system workflow and solution shall support creating incident automatically based on the rules defined and tracking them.
- The bidder shall provide different dashboard and screens for different roles, provide online secured portal (web-based dashboard) for viewing real-time incidents / events, alerts, status of actions taken etc.
    - Top Management
    - Department Heads (View to the data associated with their function group / business line).
    - CISO (complete and detailed dashboard).

- System Administrator (for the systems associated with this administrator).
- Network / Security Administrator (for devices / equipment for which he/she is administrator).
- Application Administrator.
- Auditor (Internal Auditors, IT Auditor, or any other authorized official of the organization).

- The bidder must ensure that once the logs are written to the disk/ database no one including database / system administrator should be able to modify or delete the stored raw logs.
- The bidder must ensure that for each security incidents, solution should provide online and real time remediation guidance.
- Proactively inform about potential security threats/vulnerabilities, new global security threats/ zero day attacks in circulation and suggest and implement suitable countermeasures to safeguard Bank's IT assets and customer data against such evolving threats / attacks along with the analysis.
- The bidder should develop custom plug-ins / connectors / agents for business application monitoring.
- 24x7x365 onsite service availability for monitoring of the devices / servers / applications under scope and support for troubleshooting.
- Service availability monitoring of devices / servers configured and submit a report in case of service non-availability of the devices along with the status.
- Provide assistance during cyber security drills / audits as and when conducted.
- Alerting events / incidents and recommending remedial actions.
- Daily report of events / incidents, correlation, analysis, recommendations and protection.
- Monthly report summarizing the list of events / incidents reported correlation analysis, recommendations, status of actions and other security advisories.
- It should include the trend analysis comparing the present reporting cycle data with the previous reporting cycle data (Weekly, Monthly, Quarterly and annual.
- The bidder should develop a Standard Operating Procedure (SOP) for alert management, incident management, forensics, report management, log storage and archiving, Business Continuity. SOP should also cover log monitoring tool management including configuration, agent deployments, backup and recovery.
- The bidder should provide knowledge transfer and training on the technology, functionality and operations.
- The bidder has to maintain all the listed devices in the optimal configuration as required by Bank's security architecture.

- The bidder has to provide an incident management and integrate with ticketing tool to generate automated tickets for the alert events generated by proposed tool.
- The bidder will also provide a detailed process for managing incidents - describing each phases of the process - prepare, identify, contain, eradicate, recover and learn from the incidents responded to.
- Develop response plan/ strategy which will describe the prioritization of incidents based on the organizational impact
- Bidder should also develop/document Crisis Management Plan based upon various threat scenarios. Crisis management Plan should be quarterly tested along with various stakeholders in Bank/Other relevant service providers. Crisis management plan should also be reviewed periodically or as and when required.
- The solution should have capability to structure rule based work flow 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.
- Establishing process for identifying, preventing, detecting, analyzing & reporting Information Security incidents as per the internal policies of the bank, this may revise time to time.
- Investigating Information Security (IS) incidents through various modes like forensic evidence collection & preservation, log analysis etc.
- Incident and problem Management, resolution, root cause analysis, and reporting within time limit as per the requirement of Bank.
- Troubleshooting the problem/issue reported in the context of security solutions & devices and coordinate with the respective vendor/supplier till the closure of the call. Trouble shooting should be performed within accepted time limit.
- Virus alerts through SMS/e-Mail for the viruses, worm's activity observed at the security solutions and devices under the bidder scope. Subsequent activities of remediation & closure are the responsibility of Antivirus service provider. Bidder will track the status of the Trouble Ticket opened in this context.
- Overall management of security solutions and devices in compliance with regulatory and legal requirement (Information Technology Act 2000 & related amendments).
- The bidder must provide the activities such as Rule-base user management, Security configuration management, Fault management, Performance and availability monitoring , Security posture assessment , Patch Management & upgradation ,Continuous tracking of global threats and vulnerabilities to tackle evolving threats and vulnerabilities , Advisories to bank on relevant threats and vulnerabilities supported with mitigation against identified risk exposure.

- The solution shall be easy to install, manage, configure and upgrade.
- Solution should provide a highly powerful and flexible attribute-based access control solution that combines authentication, authorization and accounting (AAA), Network Admission Control (NAC), profiling, guest management services.
- The proposed solution should allow authenticating and authorizing users and endpoints via wired, wireless and VPN with consistent policy throughout the enterprise and should support variety of authentication methods.
- The proposed solution should have self-service registration for authorised user, guest, and IT device on boarding automates user identification, device profiling so it's easy for employees to get their devices on-net and comply with security policy.
- Access/Admission Control Policy – Device must Offers rules-based, attribute-driven policy model for creating flexible and business-relevant access control policies. Provides the ability to create fine-grained policies by pulling attributes from predefined dictionaries that include information about user and endpoint identity, posture validation, authentication protocols and profiling identity.
- The solution should have an automated discovery function to identify network devices and capture information such as IP address, OS, services provided, other connected hosts.
- The solution should capture signature / heuristics based alerts and block the same.
- The solution should identify the source of an attack and should not block legitimate users.
- The solution should identify worms through techniques such as identifying the use of identification of network scanning activities.
- The solution should be capable of conducting protocol analysis to detect tunnelled protocols, backdoors, the use of forbidden application protocols etc.
- The solution should utilize Anomaly detection methods to identify attacks such as zero-day exploits.
- The solution should provide user Identity information in addition to IP address information throughout the system & allow groups based on Identity or Active Directory workgroup & Provides full historical mapping of User Name to IP address logins in a searchable format.
- The solution for Patch, Software and Hardware asset inventory management broadly covers Windows, Unix, Linux Solution for Patch, Software and Hardware asset inventory management broadly covers Windows, Unix, Linux, Ubuntu.
- The Solution should be compatible with different Hardware provider OEM (HP, IBM, Dell, Wipro, Cisco, SIS, Netpower, SUN etc.)

- The Solution should have web or GUI based dashboard console to monitored, maintain and apply patches to the registered assets.
- The Solution should be able to do assessment for currently deployed patches, software and hardware status for all the infra servers and scope to deploy latest patches on all the assets of the Bank during contract period
- The Solution should cover 3 requirement (Patch and software & hardware asset inventory management).
- The Solution should provide following hardware detail for the registered assets (Physical or Virtual) – Manufacture, CPU, family, no. of socket, no. of Cores, Install memory details and system type, Computer name, Domain, Activation etc.
- The proposed DLP solution should consist of following functionalities:
    - Discover Sensitive data
    - Monitor user actions to understand the risk involved
    - Educate the users and the management so as to reduce the risk.
    - Enforce security controls
    - Identify data leakage across all vectors, irrespective of policy being in place or not
    - Protect data
    - Have flexible control over Remediation of Data Leakage
    - Ease of Use and Quick to Deploy
- Proposed Data Loss Prevention Solution should able to have controls that encompass the entire Corporate Network of Bank. It shall encompass Network, storages and endpoints as well. The solution shall be able to start at the very basic level and progress to subsequent advanced levels of usage. The solution shall be device agnostic.
- Data protection Solution should also involve being able to identify known and unknown plug and play devices being connected to critical data resources. Also, the solution shall seamlessly integrate with Encryption which shall be intelligent enough to enforce Encryption of sensitive data
- The DLP solution should be able to go beyond known policies and provide Forensic capability on all historic data. Thus, the DLP shall safeguard sensitive data and ensure compliance by protecting sensitive data wherever it lives—on the network or in storage systems.
- Quick Deployment capability and Management Console for configuring Policies across Network.
- Integrate Vulnerability Management Tool with Bank's Existing SIEM solution to provide a correlated view of threats and vulnerabilities associated with them along with remediation mechanism and Configure Vulnerability policies to

Improve the policies configured on an on-going basis to reduce the occurrence of false positives and include new vulnerabilities.

- As and when required Vulnerability Assessment of the Security & Network Devices, servers, Security solutions, Applications, Databases etc.
- Bidder is responsible for sizing the infrastructure required for the in-scope activities under this RFP and shall ensure that the hardware proposed does not reach end of life during the contract period.
- The bidder shall ensure that any additional hardware/software/network equipment including racks required to operationalize the respective solutions/devices must be detailed in the technical and commercial bill of material. If the same is not ensured, the bidder shall be responsible to provide such hardware/software/networking equipment free of cost to the Bank at the time of implementation. In case additional storage is required then the bidder is liable to procure the additional storage at no additional cost to the Bank.
- The bidder shall provide training to the identified Bank team at least for 5 days on the product architecture, functionality and the design for each solution under the scope of this RFP before implementation.
- The bidder is required to provide all trainees with detailed training material and 3 additional copies to the Bank for each solution. This training material should cover installation, operation, integration, maintenance, troubleshooting and other necessary areas for each solution.
- Bidder shall be responsible for timely compliance of all Device level audit (DLA) and Vulnerability Assessment (VA) audit observations as and when shared by the bank.
- Support central management (CLI & GUI) if multiple appliances/servers are involved.
- Daily Reports: Critical reports should be submitted twice a day.

  (First report at 10 am and second report at 5pm every day).

  Weekly Reports: By 10:00 AM, Monday

  Monthly Reports: 5th of each calendar month
- **Vulnerability Assessment** to be conducted for identified devices once every month based on a calendar documented in coordination with the Bank to ensure that business operations are not impacted. Ad-hoc scan to be conducted as and when required by the bank.
- Bidder/ proposed solution have to comply with all the given requirements in **Annexure - A**. Bidder has to mark "Y" as compliance to particular requirement. Non-Compliance to any solution/requirement is not accepted to the Bank

Bidder/ proposed solution have to comply with all the given requirements. Bidder has to mark "Y" as compliance to particular requirement. Non-Compliance to any solution/requirement is not accepted to the Bank.

A) Network Access Control (NAC) & Patch Management

Sl. No.	Solution / Requirement Description	Compliance (Y)
A.1	The solution should support continuous detection of devices attempting to connect to the network	
A.2	The solution should gather the following data before an endpoint has access to network: ➢ Device type ➢ Operating system ➢ User identity ➢ Operating system ➢ Patch status ➢ Anti-virus status ➢ Host firewall status ➢ Known/Unknown device status ➢ Past policy compliance and threat history	
A.3	The solution should have a registration process for the external devices to access internal network and maintain guest access.	
A.4	The solution should not allow infection of already quarantined elements by other quarantined elements	
A.5	The solution should support quarantine mechanism performed both at Layer 2 and Layer 3	
A.6	The solution should detect handheld devices with platforms such as iPhone/iPad, Android and Windows etc.	
A.7	The solution should detect devices without IP addresses, such as stealthy packet capture devices designed to steal sensitive data.	
A.8	The solution should be able to integrate with existing directory services/ identity and access management system for Role-based access facility.	
A.9	The solution should be able to report violations based on bank's defined device baseline to the SIEM. For example all endpoints should be in compliance with Bank's antivirus policy, should be properly patched and free of unauthorized software etc.	
A.10	The solution should support existing standard-based authentication and directories such as 802.1x, Directory	

Sl. No.	Solution / Requirement Description	Compliance (Y)
	services, AAA mechanisms etc.	
A.11	The solution should be able to link to existing databases for developing policies. For example, retrieve a list of MAC addresses of the Bank's assets that are owned by the Bank, and then a policy can be created to block other laptop/iPads etc.	
A.12	The solution should support existing third party hardware/software such as Network switches, Wireless Access Points, VPN, Antivirus, Patch Management, Ticketing, SIEM, Vulnerability assessment scanners and MDM.	
A.13	The solution should support the following mechanisms for access control and policy validation: VLAN Steering, DHCP, Anti ARP spoofing, Agent based enforcement, Policy based routing, Mac Authentication etc.	
A.14	The solution should capture audit logs that contain the following user name , IP, roles , groups, resources accessed, compliance status of endpoint etc.	
A.15	The Solution should provide remote management/ wiping/ locking devices including mobile, laptops, etc.	
A.16	The Solution should provide remote wipe facility on the containerized app, rendering the data unreadable.	
A.17	The solution should be able to detect through periodic monitoring if endpoint security configurations are modified after obtaining access to the network and identify users who have violated in the past.	
A.18	The solution should support alerting mechanism such as e-mail, SMS etc.	
A.19	The solution should be able to control access to network as per time, location of user, mode of access, type of system used to access etc.	
A.20	The solution should be able to detect endpoint Mac address, IP addresses, network resources devices, resources such as printers and scanners, network zones etc. through auto discovery.	
A.21	The solution should be able to identify and authenticate VPN users	
A.22	The solution should be able to support virtualized environments.	
A.23	The solution should integrate with existing service desk tools to support automated workflow for providing access , change management and exception control	
A.24	The solution should permit admin to define thresholds for threat levels received from the NAC	

Sl. No.	Solution / Requirement Description	Compliance (Y)
A.25	The solution should be able detect and manage hand held devices used for financial inclusion process	
A.26	The solution should support In-line deployment modes.	
A.27	The Solution should be easily scalable to large number of users.	
A.28	The Solution should be able to integrate with the existing SIEM solution.	
A.29	The proposed solution must have the ability to 'push' user-specific device configuration.	
A.30	The proposed solution must support mainstream versions of Android, iOS, Windows desktop and Linux Operating Systems.	
A.31	The proposed solution should be integrated seamlessly into the existing infrastructure of the Bank.	
A.32	The proposed solution must have the ability to deploy an enterprise and bank-specific app catalogues so users can view, install, and update approved apps.	
A.33	The proposed solution must have the ability to restrict mobile OS versions.	
A.34	The proposed solution must have the ability to remotely lock and wipe a device.	
A.35	The proposed solution must have the ability to provide and enforce data encryption.	
A.36	The proposed solution must have a jailbreak/root detection mechanism.	
A.37	The proposed solution must have the ability to view location information/GPS tracking on lost or stolen devices.	
A.38	The proposed solution must have the ability to allow the Bank to create and manage specified policies, such as enforcing password policies (password length, unique password, change frequency), as well as manage groups of devices by individual agency.	
A.39	The proposed solution must have the ability to restrict users from installing Bank-restricted apps.	
A.40	The proposed solution must have the ability to maintain inventory database of devices by ID, hardware model, and firmware version	
A.41	The proposed solution should be able to automatically decommission devices that are lost or based on user status.	
A.42	The proposed solution must have the ability to view application and network performance.	
A.43	The proposed solutions must have the ability to block connections to the untrusted networks	
A.44	The proposed solution should deliver real-time monitoring of enrolled devices and their activities in a configurable dash-	

Sl. No.	Solution / Requirement Description	Compliance (Y)
	boards	
A.45	The Proposed solution should provide a detailed historical report on the device user activities, interactions with business servers and networks.	
A.46	The proposed solutions should have log events, provide timely alert notifications	
A.47	The proposed solution should be able to separate personal and private user data from business data.	
A.48	The proposed solution should have the capability to containerize the business data.	
A.49	The proposed solution should have the ability to restrict deployment of corporate applications on rooted or jail broken devices.	
A.50	The proposed solution has geo-fencing capabilities.	
A.51	The patch management solution should have regular patch update facility for all terminal devices (desktops & severs) including Software and Hardware asset inventory management broadly covers Number of OS instances, Types of Server - Physical and Virtual Environment, various Server Operating system, Various types of Operating system - Windows, Unix and Linux with CPU/cores counts running in Desktops & Servers.	
A.52	The patch management solution should be compatible with different Hardware provider OEM (HP, IBM, Dell, Wipro, Cisco, etc.)	
A.53	Onsite Installation and implementation of the solution.	
A.54	Solution should have web or GUI based dashboard console to monitored, maintain and apply patches to the registered servers.	
A.55	Solution should be able to do assessment for currently deployed patches, software and hardware status for all the assets.	
A.56	Vendor should provide interface to integrate to multiple monitoring and reporting tools (SIEM).	
A.57	Licenses should consider based on concurrent asset reported to console at any given point of time.	
A.58	Able to identify and report the machines that have installed the patch that is to be rolled back.	
A.59	Able to determine if the patches on a machine are correctly installed.	
A.60	The solution must detect if a patch that has been applied becomes corrupt.	
A.61	Allow console user to deploy patches to all agents via a	

Sl. No.	Solution / Requirement Description	Compliance (Y)
	central console.	
A.62	Allow console user to set start and end date/time for each action deployed.	
A.63	Allow console user to define different patch deployment policies.	
A.64	The system must be intelligent to check the relevance of the computer before deploying a patch after download on the endpoint.	
A.65	Solution should allow to add manual entry of all licenses software's procured for the assets of the Bank.	
A.66	Solution should provide comparison/ consumption of the license software's installed with manually fed data to the above system/ solution for industry standard products like WebSphere, MS SQL, Oracle, JBOSS, MS-Office etc. License comparison should be user based, server based or CPU based for product like WebSphere, MS SQL, Oracle, MS Office, JBOSS etc. in line with licenses methodology of the product and report should generate.	
A.67	The product shall use the methods to determine if a patch has been installed on a machine by Inspecting the registry, Examining if the required files exist , Inspecting the version number of existing files on the machine	
A.68	The proposed solution must consist of Anti-Malware, Anti-Spyware, anti-virus with Host Intrusion Protection, Port and Device Control, Full Disk and File Encryption, Endpoint Data Loss Prevention, Application Vulnerability Management and Application Control.	
A.69	The proposed solution should have the option to have integrated URL filtering capability to block known malicious websites, as well as productivity filtering to block categorized websites.	
A.70	The proposed solution should scan files and identifies infections based on behavioural characteristic of viruses.	
A.71	The proposed solution should scan files as they are opened, executed, or closed allowing immediate detection and treatment of viruses.	
A.72	The proposed solution should provide basic application control capabilities that enable administrators to block installations of unwanted applications or application classes.	
A.73	The proposed solution should be platform agnostic and able to run on all devices such as Windows, MAC and Linux Operating System based computers, Cell phones running on IOS & Android and Servers.	

Sl. No.	Solution / Requirement Description	Compliance (Y)
A.74	The proposed solution should support optimized scanning processes by examining unknown, suspicious, or modified files, and can adapt to each computer within networks throughout the process	
A.75	The proposed solution should be able to record critical endpoint data- even while devices are offline or outside the Bank's network to quickly detect infected systems.	
A.76	The proposed solution should be able to eliminate zero-day attacks with continuous and real-time monitoring.	
A.77	The proposed solution should check most common areas of file system and registry for traces of spyware.	
A.78	The proposed solution should allow configurable scanning and controlling of amount of CPU resources dedicated to a scan process.	
A.79	The proposed solution should be able to lock down all anti-virus configurations on the system.	
A.80	The proposed solution should be able to totally protect endpoint from spyware, adware, trojans, key loggers, P2P threats, Hacker Tools, DDoS attack agents in real-time.	
A.81	The proposed solution should provide real time active protection.	
A.82	The proposed solution should auto-quarantine spyware or adware without end- user interaction.	
A.83	The proposed solution should provide mechanisms to update definitions and scan on the fly without need for reboot or stopping of service on the Bank's Assets.	
A.84	The Proposed solution should be able to control through policies at Endpoint such that it can block specific process, file, or network activity when not connected to Enterprise.	
A.85	The proposed solution should be able to discover bad connections to malicious IP domains and block network access of such connections.	
A.86	The proposed solution should have ability to quarantine undetonated malicious executables within the environment with the ability to hunt for such malicious executables.	
A.87	The proposed endpoint solution should be able to automatically prevent the execution of even unknown executable files even if the endpoint does not have the latest signatures and without heuristics or behavioural patterns.	
A.88	The proposed solution should be able to block on certificate basis such that only trusted certificates are allowed to execute.	
A.89	The solution should have the ability to log and be capable of	

Sl. No.	Solution / Requirement Description	Compliance (Y)
	audit-trails.	
A.90	The proposed solution should support report customization and allow viewing directly using a dashboard.	
A.91	The proposed solution should support granular role based access control.	
A.92	The proposed solution should prevent tampering of applications which are white listed either on disk or on memory when running.	
A.93	The solution should provide the capabilities to log administrative activities such as changes to policies, agent override activities, agent termination and agent uninstall key generation in the management console.	
A.94	The proposed solution should support downloadable product upgrades from OEM official websites.	
A.95	The proposed solution should be able to retain history of attacker's actions.	
A.96	The proposed solution should be able to collect data from the sources including: User, endpoint and network events.	
A.97	The proposed solution should be able to continuously monitor analyse and record attacker activity.	
A.98	The proposed solution should provide visibility to conduct analyses of the threat to inspect and analyse present and past network alerts at the Endpoint.	
A.99	The proposed solution should be able to detect advanced Malware attacks using dynamic real-time monitoring and analyses of application and process behaviour based on OS activities, including memory, disk, registry, network and more.	
A.100	The proposed solution should be able to provide the automated response feature: - Isolating an endpoint from the network.	
A.101	The proposed solution should monitor all essential endpoint activities - Binaries, processes, file activity, configuration changes, network connections - Continuous always-on monitoring - Kernel-Mode monitoring - Cross platform support	
A.102	The proposed solution's management console should be customizable with user-specific policy views across multiple devices for each administrator.	
A.103	The proposed solution should provide range of malware protection options including and not limited to : - Critical resource and process protection	

Sl. No.	Solution / Requirement Description	Compliance (Y)
	- exploit protection - Vulnerability detection and shielding - Behavioural monitoring.	
A.104	The solution must be able to generate report on different parameters. i.e Compliance , Non-Compliance , corporate , Guest , Bring Your Own Device (BYOD), Mobile Devices , IOT's etc.	
A.105	The solution Should have ability to generate reports in different formats, such as Html, Excel, CSV and PDF. Reports should be available in real time on demand and should automatically be generated on a scheduled basis.	
A.106	The solution should be capable of being bypassed in the event of any failure of the solution. This should be applicable in both managed and unmanaged switch environment.	
A.107	The solution should operate within a heterogeneous network with switches from multiple vendors (e.g. - Cisco, D-Link, Juniper, 3com, Nortel, Linksys, Extreme Networks, etc and legacy switches). NAC appliance should support vendor agnostic switch infrastructure. It must support the same with & Without 802.1x mechanism	
A.108	The solution should have a provision to support non- NAC capable hosts (i.e., printers, IP phones, IOT's etc.) based on Mac address or other parameter and it should support exception lists for non-NAC capable hosts.	
A.109	The solution should provide granular compliance checks for Windows, MAC and Linux in terms of: a. Ability to run custom scripts and policies b. Hardware/Asset Management information c. Event driven properties for compliance checks	
A.110	Advanced Guest Networking Capabilities 1. Solution should include a guest networking application 2. Solution should provide mechanism for notification of user credentials to Guest Users	
A.111	The proposed NAC solution should support, verify authentication and integrate with Active Directory server.	
A.112	The proposed solution must able to integrate with Antivirus solution for Auto- Remediation.	
A.113	The proposed solution should have the capability of traffic log retention for a period of 3 months.	
A.114	A. The following is a list of functions that should encompass a NAC solution: B. Element Detection - detecting new elements as they are introduced to the network. C. Authentication – authenticating each user accessing the network no matter where they are authenticating from	

Sl. No.	Solution / Requirement Description	Compliance (Y)
	and/or which device they are using. D. Endpoint Security Assessment – assessing whether a newly introduced network element complies with the security policy of the organization. These checks may include the ability to gather knowledge regarding an element's operating system, the list of installed patches, the presence of anti-virus software and its virus signature date, etc. E. Remediation– quarantining an element that does not comply with the defined security policy until the issues causing it to be non-compliant are fixed. When quarantined, the element may be able to access a defined set of remediation servers allowing the user fixing the non-compliant issues and to be reintroduced, now successfully, to the network. F. Enforcement – restricting the access of an element to the network if the element does not comply with the defined security policy. G. Authorization – verifying access by user to network resources according to an authorization scheme defined in an existing authorization system, such as Active Directory, allowing the enforcement of identity-based policies after an element is allowed on the network. H. Post-Admission Protection – continuously monitoring users, elements and their sessions for suspicious activity (i.e. worms, viruses, malware, etc.). If detected, the action taken by a NAC solution may vary from isolating the offending system to dropping the session.	
A.115	The Network Access Control (NAC) solution should be an automated security control platform that can monitor and control everything on the network—all devices, all operating systems, all users. The solution shall let employees and guests remain productive on the network while critical network resources and sensitive data remain protected.	
A.116	Solution should Maintain an up-to-date/centralized inventory of authorized devices connected to bank's network (within/outside bank's premises).	

B) Data Loss Protection (DLP)

Sl. No.	Solution / Requirement Description	Compliance (Y)
B.1	The proposed solution should be deployable in inline as well as in listening mode.	
B.2	The proposed solution should be able to block/alert pdf content access /Cut/Copy by image writer ,or by application like screen capturing /session recording tools etc.	
B.3	The proposed solution should have wide range of out of the box rule sets.	
B.4	The proposed solution should support the following for rules creation and updation:- a. centralized console for rule creation and updation b. Ability to whitelist legitimate data format c. Ability to create custom rule set and apply it on select IP addresses/email IDs / directory groups etc.	
B.5	The proposed solution should also capture violations made by users to defined policies when they are out of the Bank's network.	
B.6	The proposed Solution should make sure that the agent deployed should not be removed via unauthorized methods or from unauthorized service stoppage.	
B.7	The proposed solution should provide SSL decryption and destination awareness capability on the gateway to identify any sensitive content uploading to online web properties, even when it is tunnel over SSL.	
B.8	The solution should have pre-defined applications and applications groups and allow each application/application group to monitor operations like Cut/Copy, Paste, File Access and Screen Capture and also can add the custom applications.	
B.9	The proposed solution must have the mechanism to index and retain all documents by monitoring all traffic policy rules.	
B.10	The proposed solution should be able to perform following searches: a. e-mail sent from or to any email address b. traffic sent across protocols or ports c. Documents leaving the network based on document type	
B.11	The proposed solution should support : a. Scanning file formats such as (Word, excel, ppt, xls) b. Non textual pds, xps c. data in archival tools (.zip/rar/.7z/.tar). Alert presence of encrypted archived files	

Sl. No.	Solution / Requirement Description	Compliance (Y)
	d. analyse encrypted data over web proxies e. analyse data sent over email (Organizational/non-organizational such as Gmail etc), mobile Devices.	
B.12	The proposed solution should be able to monitor IM Traffic even if it is tunnelled over HTTP protocol, and FTP traffic including fully correlating transferred file data with control information.	
B.13	The proposed solution should be able to prevent content getting posted or uploaded to specific geo-location.	
B.14	The provided solution should monitor and control sensitive emails downloaded to mobile devices.	
B.15	The proposed solution should be able to monitor data copied to network file shares and should enforce structured and unstructured fingerprint policies even when disconnected from corporate network.	
B.16	The proposed solution should create an incident in the central management server or ticketing tool for all critical or high level impacts.	
B.17	The proposed solution should be able to discover and identify sensitive information stored on endpoints, databases, file shares, SharePoint, SAN, NAS etc.	
B.18	The proposed solution should have a mechanism to highlight any deviation from bank policies for storage of sensitive information.	
B.19	The proposed solution should be able to deploy both pattern matching and document tagging with 3rd party and fingerprinting.	
B.20	The proposed solution should be able to schedule periodically recurring scans to identify sensitive data at rest.	
B.21	The proposed solution should have the capability to encrypt the sensitive content when copied.	
B.22	The proposed solution should Encrypt data transferred to portable media with encryption of 256 bit and above.	
B.23	The proposed solution should be able to monitor movement of sensitive data at endpoint through various channels such as bus, Bluetooth, LPT etc.	
B.24	The proposed solution should be able to inspect documents embedded in other documents.	
B.25	The proposed solution should be able to track the copying of data into USB drives, media cards and mobile phones if they considered as removable media.	
B.26	The proposed Solution should notify the end user of a policy violation using a customizable pop-up message and should	

Sl. No.	Solution / Requirement Description	Compliance (Y)
	capture content that violates a policy and store it in an evidence repository.	
B.27	The proposed solution should control access to USB based on various parameters such as designation of individuals.	
B.28	The proposed solution should restrict access to sensitive data based on user roles.	
B.29	The proposed solution should restrict sensitive information from being printed.	
B.30	The proposed Solution should be able to enforce policies for virtual desktops or thin clients.	
B.31	The proposed solution should allow encryption of complete hard drive sector by sector.	
B.32	The proposed solution should be able to configure policies to detect on fingerprints and files from share/repository/date created etc.	
B.33	The proposed solution should enforce policies to detect low and slow data leaks.	
B.34	The proposed solution should have a comprehensive list of pre-defined policies and templates to identify and classify information pertaining to Banking industry and preferably India IT Act.	
B.35	The proposed solution should be able to enforce policies to detect data leaks even on image files.	
B.36	The proposed solution should have a dashboard view.	
B.37	The proposed solution should support reports in different formats such as PDF, Excel or CSV format.	
B.38	The proposed solution should allow the Bank to develop reports built around stakeholder requirements such as top policy violations, senders, content type, protocol and historical reports etc.	
B.39	The proposed solution should support the following type of Analysis: - • Regular expression/pattern matching/indexing/tag • Based on file names • Full text/ URL requested • Should have the capability to check with full/partial Documents • Should be able to provide information on how many times a user has violate DLP policies	
B.40	The proposed solution should support the following for analysis • Capture the metadata for further inspection • Capture SMTP headers, from and destination IP addresses, date/time	

Sl. No.	Solution / Requirement Description	Compliance (Y)
B.41	The proposed solution should provide an ability to perform full scans and incremental scans.	
B.42	The endpoint agent should be compatible with : • Windows OS (32/64 bit) • MAC OS • Linux	
B.43	The proposed solution should have options to see summary reports, trend reports.	
B.44	The proposed solution should have options to see summary reports and high-level metrics etc.	
B.45	The proposed solution should have a mechanism for incidents to be sorted by severity level, sender, recipient, source, destination, protocol and content type.	
B.46	The proposed solution should be able to alert and notify sender, sender's manager and the policy owner whenever there is a policy violation, different notification templates for different audience should be provided.	
B.47	The proposed solution should support quarantine as an action for email policy violations and should allow the sender's manager to review.	
B.48	The incident should include a clear indication of how the transmission or file violated policy (not just which policy was violated), including clear identification of which content triggered the match and should allow opening of original attachment directly from the UI.	
B.49	The proposed solution should trigger only one incident per event, even if the event violates multiple policies.	
B.50	The proposed solution should have a mechanism to support easily downloadable upgrades from OEM official website	
B.51	The proposed solution should be able to integrate with the existing SIEM solution in the Bank.	

C) <u>Vulnerability Assessment Solution (VAS)</u>

Sl. No.	Solution / Requirement Description	Compliance (Y)
C.1	The proposed solution should have minimal impact on traffic, server performance, networks etc. during deployment and operation.	
C.2	The system should work in any network topology	
C.3	The proposed solution should maintain an updated database for latest vulnerabilities	

Sl. No.	Solution / Requirement Description	Compliance (Y)
C.4	The proposed solution should perform a targeted scan (i.e. check for a specific set of vulnerabilities or IP Addresses).	
C.5	The proposed solution should support centralized management of scan operations, reporting and administration.	
C.6	The proposed solution should be able to identify applications running on non-standard ports.	
C.7	The proposed solution should track hosts over time in a dynamic IP environment (DHCP).	
C.8	The vulnerability signature database should include breakdown of types of signatures (i.e. CGI, RPC, etc.) and number of signatures that map directly to CVE IDs.	
C.9	The proposed solution should be able to conduct vulnerability assessment for all operating systems and their versions including but not limited to: Windows, Unix, Linux, etc.	
C.10	The proposed solution should provide mechanism to upload IP lists of devices through XLS format	
C.11	The proposed solution should provide configurable Vulnerability assessment policy and individual test configuration.	
C.12	The proposed solution should be able to scan workstation, servers, network and security equipment and other devices such as printers, mobiles, webcams, tablets etc.	
C.13	The proposed solution should be able to run scans on network segments as well as entire network.	
C.14	The proposed solution should be able to perform authenticated and unauthenticated scans and manage credentials centrally for authenticated scans.	
C.15	The proposed solution should be able to scan application databases for vulnerabilities.	
C.16	The proposed solution should be able to detect weak password for databases and point out accounts with simple, weak and shared passwords.	
C.17	The proposed solution should be able to identify out-of-date software versions, applicable patches and system upgrades.	
C.18	The proposed solution should provide remediation information in the reports including links to patches etc.	
C.19	The proposed solution should produce a report listing all applications on a host or network, regardless of whether the application is vulnerable	
C.20	The proposed solution should be able to support "scan windows",scan scheduling, and automatic/manual pausing/stopping/restarting of scans.	

Sl. No.	Solution / Requirement Description	Compliance (Y)
C.21	The proposed solution should support users to modify existing rules or create their own rules	
C.22	The proposed solution should include a library of potential vulnerabilities and rules. This library should be customizable by the administrator and changes to the same should be traceable.	
C.23	The proposed solution should produce reports in the following formats: XLS, PDF, CSV, XML etc.	
C.24	The proposed solution vendor should assist the bank in reducing the number of false positives identified by the solution.	
C.25	The proposed solution should be able to track the closure of all vulnerabilities identified and should include parameters such as responsible person, date of closure, action taken etc.	
C.26	The proposed solution should generate reports on trends in vulnerabilities on a particular asset.	
C.27	The proposed solution should be able to integrate with other security solutions (i.e. Security Information/Event Management, Patch Management, IDS, IPS, etc.)	
C.28	The proposed Solution should have an Application Programming Interface (API) to integrate with other systems	
C.29	The proposed solution should support integration with threat feeds, allowing vulnerabilities to be correlated against real-time threat information.	
C.30	The proposed solution should be able to detect both wireless and rogue devices	
C.31	The proposed solution should support all kind of standard platforms like UNIX, Linux, MAC OS and Windows Etc.	
C.32	The proposed solution should provide both pre-configured and fully customizable report templates for various stakeholders across organization.	
C.33	The proposed solution should provide Built-in reports that include but not limited to audit, baseline comparison, executive summary, PCI, policy compliance, remediation planning, top remediation, vulnerability verification report etc.	
C.34	The proposed solution should support automatic, manual and offline application updates	
C.35	Provide trusted detailed reports on newly discovered malicious threats and malware in the wild	
C.36	Detail the threat with the information appropriate to the Bank such as: • The threat type	

Sl. No.	Solution / Requirement Description	Compliance (Y)
	• Risk involved • Systems affected	
C.37	Technical description of the threat and exploit parameters	
C.38	Mitigation strategies and the recommendations for the Bank to prevent the threat from causing harm to the environment	
C.39	Infiltration of malicious hackers and other communities	
C.40	Monitoring of network activities and discern risks to the Bank environment	
C.41	Customized Advisories as per requirements of the IT assets/Application in the Bank on relevant threats and vulnerabilities.	
C.42	Benchmark Bank's environment against evolving threats and vulnerabilities.	
C.43	The intelligence content should be able to look at the goals of the threat actor, variants of the threat, current activities implicating the threat, the outcomes for Bank if the threat is successful as well as provide defense against the threat.	
C.44	Track mitigation against identified risk exposure.	
C.45	Assists the Bank to ensure such threats and vulnerabilities are mitigated in the Bank's systems and Provide from the short term plans to the very long term strategies.	
C.46	Assist the Bank in taking relevant decisions Assessment of inherent and residual risk, preferably expressed as impact on business processes, rather than the underlying technology	
C.47	The intelligence content should focus more on technical attacks against infrastructure	
C.48	Solution should deliver a comprehensive range of timely adversary and technical cyber threat intelligence through a customizable portal as well as data feeds for automated consumption by the security infrastructure.	
C.49	The solution should provide Cyber Threat Intelligence both adversary and technical intelligence that is: --Relevant: enables intelligence to become a strategic advantage by knowing who, how, and why you are being targeted --Context-rich: enables informed countermeasures for current and future threats to be put in place --Timely: helps prioritize resources by providing insight into current and emerging threats and vulnerabilities	

Sl. No.	Solution / Requirement Description	Compliance (Y)
	--Accurate: drives efficient operations and reduces the time and effort for SOC and response teams to investigate incidents	
C.50	The solution should provide Intelligence portal as threat intelligence service to allow the Bank to view security information such as vulnerability data, malcode, cyber threats and adversary information.	
C.51	The Intelligence Datafeeds shall provide Bank access to one or more datafeeds containing various security data.	
C.52	The solution portal should provide the Global Cyber Threat Intelligence for a complete range of adversary and technical intelligence. It incorporates supporting research tools, vulnerabilities, malware, security risks, indications of compromise, tactics, techniques, and procedures, and adversary profiles to provide a complete view of relevant threats and exposures.	
C.53	The solution portal should provide the Global Cyber Threat Intelligence with following:- • Complete threat picture: End-to-end picture of threats from attack surface vulnerabilities to malware and actors behind the attacks. • Adversary intelligence: Intelligence on adversaries targeting banking industry, along with their tactics, techniques and procedures, so one can proactively plan counter-measures to reduce risk to your business while educating each level of organization on the risk posed by these adversaries. • Risk mitigation: Provides the broadest range of information to prioritize remediation of vulnerability and security risk exposures across various technologies – various vendor products and applications.	
C.54	The solution portal should provide the Global Cyber Threat Intelligence portal and should have the following capabilities: • Managed Service Portal: Access should be limited to authorized personnel. • Administrators: - authorized personnel. • Alert creation: - Portal should be able to configure alerts to the authorized personnel on new / updated vulnerabilities, malcode and security risks.	

Sl. No.	Solution / Requirement Description	Compliance (Y)
	• Email delivery: - Portal should be able to configure email notifications to the authorized personnel.	
C.55	The solution should provide global Cyber Threat Datafeeds include the following: • Security Risk datafeed to provide visibility into malicious code, adware/spyware, and other security risks. Combining prevalence, risk, and urgency ratings with disinfection techniques and mitigation strategies ensures that you can protect against both known and emerging threats in an accurate and timely manner. • Vulnerability datafeed to provide you with up-todate information necessary to analyze vulnerabilities in IT infrastructure, while enabling to track and remediate them. Comprehensive tracking of vulnerabilities enables the accurate assessment of the current state of IT infrastructure for risk management and compliance purposes. • Reputation datafeeds to provide actionable intelligence on IP addresses and Domains/URLs exhibiting malicious activity such as malware distribution and botnet command and control server communication. The reputation datafeeds should be derived from observed activity on the Internet and a reputation score along with additional contextual attributes should be provided for each of the IP address and Domains/URLs.	
C.56	The solution should provide the Global Cyber Threat Reputation datafeeds and it should be available in multiple formats (CSV, XML, CEF).	
C.57	The solution should have the capability and to provide firewall rules incorporated in Bank's Network.	

D) <u>IT Governance, Risk & Compliance Solution (IT-GRC)</u>

Sl. No.	Solution / Requirement Description	Compliance (Y)
D.1	Proposed IT Governance, Risk and Compliance (GRC) solution/service should provide a single, federated framework to integrate various IT processes and security solutions and	

Sl. No.	Solution / Requirement Description	Compliance (Y)
	support those processes for the purpose of defining, maintaining and monitoring GRC.	
D.2	Proposed solution should include the following attributes: -Information Security Risk Management -Business Continuity -Audit Management -Third Party Risk Management -Regulatory and Compliance Management	
D.3	All sub-modules must be relatable; i.e. centrally stored regulations should be accessible from each module; audit findings should be accessible in compliance/ERM modules, etc.	
D.4	Leverage Microsoft Office Products (particularly Word, Excel, and PowerPoint) to allow data and chart exports for external reporting needs and to allow current data to be migrated into GRC product to create baseline policy and procedures library as well as programmatic templates, etc.	
D.5	Scalable (capable of implementing one module/service at a time and adding users as needed)	
D.6	The solution must be configurable to allow access to screens and data based on user roles and organisation level.	
D.7	The proposed solution should be a web-based system which can be centrally accessible without any installation to be done on client systems.	
D.8	The solution should have inbuilt user management system which can be integrated with active directory.	
D.9	The solution should have the capability for bulk creation of users from an external data sources	
D.10	The solution should have ability to define organization hierarchy	
D.11	Tight and finite user access control through roles, job-title department, office, location.	
D.12	Automated email notification for actions items or important tasks	
D.13	The product principle should have direct presence in ME, Office address and primary contact person details should be provided.	
D.14	Ability to establish business context and policies for IT and security and manage IT risks, vulnerabilities, and security incidents	
D.15	Ability to bring risk information together from siloes risk	

Sl. No.	Solution / Requirement Description	Compliance (Y)
	repositories to identify, assess, evaluate, treat, and monitor risks in one central solution	
D.16	Ensure controls are defined, implemented and measured to meet constantly changing compliance obligations	
D.17	Automate risk and compliance processes to meet the challenge of regulatory change	
D.18	Provide a consistent, risk-based approach to drive greater efficiency in the execution of audit program	
D.19	Provide an integrated approach to business resiliency to lessen the impact of disruptions and crisis events on your organization	
D.20	Manage third party relationships and engagements	
D.21	Ability to leverage people, process, and technology to build an integrated approach to Assessment & Authorization, Continuous Monitoring and overall risk management	
D.22	Provide common taxonomies, processes, and data stores to streamline risk and compliance functions in the organization, ensuring risk is managed effectively and efficiently	
D.23	Does not require any custom coding	
D.24	Provide scalable and interactive reporting and trending tools to empower decision makers	
D.25	Ability to integrate with vulnerability management tool, application security tool (SAST and DAST) and other security solutions. The bidder should develop custom integration APIs according to Bank's needs, which will be communicated from time to time	
D.26	Ability to provide customizable dashboards and reports	
D.27	Should provide a search capability	
D.28	Should have the ability to suppress / disable functionality that is not required on the go	
D.29	Should be able to display drop down boxes, free text fields and minimum acceptable responses	
D.30	Should have the ability to create online surveys / questionnaires for documenting sign-offs, controls self-assessment and attestations	
D.31	Ability to control access across modules and within a module	
D.32	Ability to track changes to controls in order to have an audit trail.	
D.33	Contain formatting/editing tools such as spell check and ability to underline, italicize, change font, etc.	
D.34	Allow Bank to define and configure business unit hierarchy	

Sl. No.	Solution / Requirement Description	Compliance (Y)
	and associate users with a business unit or units with the hierarchy.	
D.35	Support auto log out after a period of time has expired, as determined by Bank. |	
D.36	Support advanced approval workflow with visual drag and drop of nodes to configure flexible workflow within applications.	
D.37	Integrate with existing SIEM solutions with no customization or code changes involved in integration of such platforms	
D.38	The system provides the ability to define and report the full scope of the information security management system (ISMS).	
D.39	The system provides the ability to report on ISO 27001 conformance in conjunction with a certification effort.	
D.40	Ability to capture the relevant data for each business process as well as underlying assets, application, information assets, products and services, business unit, devices, etc.	
D.41	Ability to document and maintain external benchmarks, frameworks, laws and regulations identified for meeting the corporate objectives.	
D.42	Ability to document unique and comprehensive control standards identified and documented from the internal policies for meeting the corporate objectives.	
D.43	Ability to import data related to employees from an export from systems such as an HRMS system Or an Excel sheet.	
D.44	Capability to identify, document, track and monitor corporate objectives against policies, risks and metrics such as Key Performance indicators (KPIs).	
D.45	The platform should support the identification and criticality definition of business processes and assets.	
D.46	The system allows users to filter and view policies by statically or dynamically defined criteria such as business unit, geography, impact area, role, etc.	
D.47	The system supports easy addition of new regulations and requirements and has interfaces to feeds that provide for and update regulations, legislation and self-regulating bodies.	
D.48	The system supports IT policy, IS Policy and controls versioning.	
D.49	The system provides advanced technical baselines written against control standards and mapped to regulatory requirements, best practices, and international standards.	
D.50	Ability to document control activities and capture details like control owners, testing requirements, mapping with	

Sl. No.	Solution / Requirement Description	Compliance (Y)
	compliance, risk, business unit etc.	
D.51	Ability to integrate automated test results from technical controls.	
D.52	Ability to provide built-in assessments and questionnaires as well as manually create assessments and questionnaires per defined guidelines for conducting compliance testing.	
D.53	Content (policies, controls, report templates, reference documentation) is available as part of the standard solution.	
D.54	Should have pre-mapped controls (such as ISO, COBIS, PCI) that are maintained and updated by OEM on a periodic basis.	
D.55	Provide a mechanism to track and remediate control deficiencies identified during testing.	
D.56	The system automatically generates findings for incorrect answers and allows the management of findings through remediation tasks or exception requests.	
D.57	The system calculates compliance scores for each regulation.	
D.58	The system can be used to perform a gap analysis.	
D.59	Ability to link and map identified risk to Authoritative Sources, departments, asset, divisons as well as other elements via cross reference and mapping capabilities without coding etc.	
D.60	Mapping against industry-standard frameworks is supported such as COBIT, ISO27001, ITIL/ITSM, CMM, BASEL, or Solvency II, etc.	
D.61	Provide an out of the box risk register in order to capture currently maintained and tracked risks as well as ability to configure the application via no coding to accommodate our requirements.	
D.62	Risk assessments support both qualitative and quantitative approaches and both approaches can be applied consistently and harmonized in one risk assessment view	
D.63	Core functions of the solution should include a catalog of IT assets, central repository and taxonomy for security alerts, integration to SIEM, log and packets, full lifecycle support for incident management, incident investigation, incident response and issues management	
D.64	Solution can align and help customers deploy incident response best practices aligned with industry standards	
D.65	Solution can map incidents to security controls and provide a view of how effective security controls are in capturing security incidents	

Sl. No.	Solution / Requirement Description	Compliance (Y)
D.66	Solution centralizes security incident management with integrated business context	
D.67	Solution helps customers establish effective breach response capabilities aligned with industry standards and best practices	
D.68	Solution integrates with ticket management systems to forward findings at the end of security investigation additionally, IT operations can get access to the findings	
D.69	Solution is focused on the SOC personas and processes - reports, dashboards and workflow is specific to security analysts, security incident coordinators, SOC Managers, CISO, and IT Operations	
D.70	Solution measures and reports on the SOC program with KPIs, dashboards and reports	
D.71	The solution provides a centralized system to catalog IT assets for incident prioritization and provide business context for prioritization of events	
D.72	Obtain a clear view of the organization's state of compliance.	
D.73	Prioritize activities that address the regulatory requirements having the greatest impact on the business.	
D.74	Limiting overcompensating responses and ability to direct more resources back to strategic areas of the business.	
D.75	Policy Program Management	
D.76	Provide the framework to establish a scalable and flexible environment to manage corporate and regulatory policies and ensure alignment with compliance obligations.	
D.77	This shall include documentation of policies and standards, assigning ownership, and mapping policies to key business areas and objectives.	
D.78	Provide the necessary tools and capabilities to document external regulatory obligations. Establish a systematic review and approval process for tracking changes to those obligations, understanding the business impact, and prioritizing a response.	
D.79	Improve the linkage between organizational compliance requirements and internal controls, thereby reducing the compliance gaps and give senior management better insight into issues impacting the business	
D.80	Provide an agile policy framework to keep pace with changing business and IT compliance risk.	
D.81	Enable the support of compliance mapping mandatorily to	

Sl. No.	Solution / Requirement Description	Compliance (Y)
	ISO 27001 and ISO 22301 upfront including other international standards and policies.	
D.82	Offer a framework and taxonomy to systematically document the control universe, and assess and report on the performance of controls at the business hierarchy and business process level.	
D.83	Consolidate the organizational compliance projects into a single platform.	
D.84	Give business owners visibility into critical risk and compliance data, thereby enabling them to make fully informed risk based business decisions in support of organizational priorities	
D.85	Control the complete audit lifecycle, enabling improved governance of audit-related activities, while also providing integration with risk and control functions.	
D.86	The solution should enable Internal Audit to use a consistent, risk-based audit approach to drive greater efficiency in the execution of the audit plan.	
D.87	Include risk-based prioritization of the audit universe, resource scheduling and staffing, management of audit engagements, creation of audit reports, and tracking of findings and remediation plans.	
D.88	Adjust audit plans and projects based on a dynamic view of risk.	
D.89	Allow audit teams to share operational risk and control data that enables them to align audit plans and prioritize their efforts based on the organization's business priorities and latest assessment of operational risk.	
D.90	Recognize interdependences and analyze metrics	
D.91	Provides fluid risk identification, giving Internal Audit the ability to compare their view of risk to management by using comparative risk metrics at a macro (audit plan) or micro (audit engagement) level.	
D.92	Easily integrate with third-party systems to enable analysis of critical data and metrics.	
D.93	Facilitate interactions across the business	
D.94	Catalogue within one central system to provide a holistic view of all functions and organizations' significance and remediation status.	
D.95	Tailor internal audit, risk, and compliance processes to their unique requirements without custom code or development resources.	

Sl. No.	Solution / Requirement Description	Compliance (Y)
D.96	Audit programs can be directly linked to key strategic objectives such as compliance, risk management, and other regulatory obligations (SEBI).	
D.97	All issues, whether they are raised by Internal Audit, other risk and compliance teams, or management, should be housed and catalogued within one central system and provide business workflow and a holistic view of their significance and remediation status	
D.98	Identify the universe of all auditable entities, perform Audit Universe Risk Assessments, and compare to management's assessments of risk	
D.99	Create and approve the Audit Plan, scope the entities that will be audited, schedule the audits, manage resources, report to the Audit Committee, communicate with management, and monitor the overall status of the audit plan on an on-going basis.	
D.100	Perform audit testing, document findings, draft the audit report, create and manage work papers, and document and manage the lifecycle of work paper review notes all in an online or offline mode from the intended solution	
D.101	Provide a centralized, consistent and automated approach to business continuity and disaster recovery planning, allowing to respond swiftly in crisis situations to protect the ongoing operations.	
D.102	Ability to offer a three-in-one approach to business continuity, disaster recovery and crisis management in a single management system	
D.103	Should allow organizations to respond swiftly in crisis situations to protect ongoing operations	
D.104	Capability to assess the criticality of their business processes and supporting technologies	
D.105	Capability to develop detailed business continuity and disaster recovery plans, utilizing automated workflow for plan testing and approval	
D.106	Ability to align continuity planning with the organization's priorities and business objectives, and recovery strategies	
D.107	Enable automated, up-to-date BC/DR plans for the organization's latest environments and business processes to be easily accessed during a disruption of service.	
D.108	Provide visibility into the current state of the organization's plan statuses, review dates, test results, test remediation statuses	

Sl. No.	Solution / Requirement Description	Compliance (Y)
	and crisis tasks	
D.109	Ability to apply a consistent approach to the evaluation of third party risk and controls	
D.110	Ability to capture and store supplemental documents such as SSAE-16s, financial statements, and PCI assessments, and monitor when refreshed documents are due.	
D.111	Ability to customize risk and control assessment questions	
D.112	Ability to manage third party control exceptions.	
D.113	Ability to route new relationships and engagements for approval of various stakeholders prior to contract finalization.	
D.114	Efficient program management and understanding of program status.	
D.115	Ability to capture declared critical fourth party relationships and understand the quality of governance your third party applies to their own third party relationships.	
D.116	Visibility into known risks and efforts to close/address risks.	
D.117	The solution should be able to generate report of statement of applicability on the basis of controls already existing or controls which are planned to be implemented.	
D.118	The solution should be able to generate report on Risk levels on risk assessment and risk treatment to showcase mitigation status.	
D.119	The solution should be able to generate report on control effectiveness metrics for continual improvement of ISMS	
D.120	The solution should be able to generate risk treatment plan implementation progress report.	
D.121	The solution should be able to generate consolidated asset inventory reports and custom reports on the basis of user selected fields.	
D.122	The solution should be able to demonstrate open risk status with implementation progress, control gaps and assets affected.	
D.123	The solution should be able to demonstrate control effectiveness metrics measurements in a comparable way against thresholds decided for metrics.	
D.124	The solution should show audit activity status from dashboard including current audit status, findings and risk levels associated with findings.	
D.125	The solution should be able to demonstrate audit findings remediation status from dashboard and also generate	

Sl. No.	Solution / Requirement Description	Compliance (Y)
	remediation reports on the same.	
D.126	The solution should be able to generate reports on audit findings, remediation, responsibility and status.	
D.127	The solution should be able to generate reports on scores of users in various training sessions.	
D.128	The tool should have in built management dashboard with options to drill down	
D.129	The tool should have options to display all the asset, risk, audit, action items and training related metrics in one single dashboard	
D.130	The tool should be able to display the risk information from the all the organization levels including universe, location, department, business process and assets.	

E) Anti-Advanced Persistent Threat (APT)

Sl. No.	Solution / Requirement Description	Compliance (Y)
E.1	The solution should be able to inspect and block all network sessions regardless of protocols for suspicious activities or files at various entry/exit sources to the Bank's network.	
E.2	The solution should be able to protect against Advanced Malware, zero-day web exploits and targeted threats without relying on signature database.	
E.3	The solution should be able to identify malware present in file types and web objects such as (JPEG, doc, docx, exe, gif, hip, htm, , pdf, png, ppsx, ppt, pptx, qt, rm, rtf, swf, tiff, url, vbs, vcf, xls, xlsx. etc.) and be able to quarantine them.	
E.4	The solution should be able to block malware downloads over different protocols.	
E.5	The solution should be able to identify spear phishing email containing malicious URLs and attachments that bypass the anti spam technologies.	
E.6	The solution should support Sandbox test environment which can analyze threats to various operating systems, browsers, desktop applications and plug-ins etc.	
E.7	The solution should support both inline and out of the band mode.	
E.8	The solution should be able to detect and prevent bot outbreaks (via multiple channels like SMTP, HTTP, HTTPS etc.) including identification of infected machines.	

Sl. No.	Solution / Requirement Description	Compliance (Y)
E.9	The solution should be appliance based with hardened OS. No information should be sent to third party system for analysis of malware automatically.	
E.10	The solution should be able to block the call back tunnel including fast flux connections.	
E.11	The solution should be able to conduct forensic analysis on historical data.	
E.12	Dashboard should have the feature to report Malware type, file type, CVE ID, Severity level, time of attack, source and target IPs, IP protocol, Attacked ports, Source hosts etc.	
E.13	The solution should generate periodic reports on attacked ports, malware types, types of vulnerabilities exploited etc.	
E.14	The solution should integrate with Bank's existing SIEM solution.	
E.15	Solution should be able to monitor encrypted traffic	
E.16	The management console should be able to provide information about the health of the appliance such as CPU usage, traffic flow etc.	
E.17	Sandboxing capabilities of following Operating Systems (32 and 64 bit) : Win7, Win8.x, Win10.x, Server 2008 R2, 2012 R2 and static analysis for Linux platform by the solution is preferable.	
E.18	The solution should display the geo-location of the remote command and control server.	
E.19	Detection of Command and Control and Botnet that are carried by Any protocol	
E.20	The solution should be able to capture packets for deep dive analysis.	
E.21	Inspect SMTP, POP3, IMAP traffic	
E.22	Product should be able to detect threat based on customized inputs(signatures/hashes/IOCs).	
E.23	The proposed solution should maintain an update database for latest vulnerability.	
E.24	Solution shall use agentless approach for detection of infections via network activities analysis from the endpoints.	
E.25	Solution should have usable storage of 1TB.	
E.26	Solution should provide reports with (but not limited to) HTML/CSV/PDF/.xls/.xlsx formats.	
E.27	The proposed solution should support to monitor traffic from multiple segments like WAN, DMZ, Server Farm and MPLS links etc. simultaneously on a single appliance	
E.28	A solution must support minimum 10 data port (including 5 in	

Sl. No.	Solution / Requirement Description	Compliance (Y)
	and 5 out) for one appliance and for another appliance 6 data port (including 3 in and 3 out).	
E.29	The solution must support minimum throughput 4(Four)Gbps for the Appliance which is having **10 Data port** (including 5 in and 5 out) and **for the other appliance** must support minimum throughput 2 (Two)Gbps for the Appliance which is having **6 Data port** (including 3 in and 3 out).	
E.30	A solution must support minimum1Gbps for an individual port with Copper Gigabit Ethernet (GBE). (1Gigabit Fiber (LC) interfaces optional).	

ANNEXURE –B -Tender offer forwarding letter

(Tender offer forwarding letter)

Date: ___/____/2019

To

The Deputy General Manager
DIT, BPR & BTD
UCO Bank, Head Office
5th Floor, 3&4, DD Block, Sector-I
Salt Lake, Kolkata -700064

Dear Sir,

Sub: RFP for the Implementation, Maintenance and Facility Management for System Security Tools for Cyber Security Operation Centre (C-SOC) vide RFP Ref No.: DIT/BPR&BTD/OA/5033/2018-19 Date: 15/02/2019

With reference to the above RFP, having examined and understood the instructions including all annexure, terms and conditions forming part of the Bid, we hereby enclose our offer for **the RFP for the Implementation, Maintenance and Facility Management for System Security Tools for Cyber Security Operation Centre (C-SOC)** and will be Providing Services mentioned in the RFP document forming Technical as well as Commercial Bids being parts of the above referred Bid.

In the event of acceptance of our Technical as well as Commercial Bids by The Bank we undertake for **the RFP for the Implementation, Maintenance and Facility Management for System Security Tools for Cyber Security Operation Centre(C-SOC)** and Provide Services as per your purchase orders.

In the event of our selection by the Bank for **RFP for the Implementation, Maintenance and Facility Management for System Security Tools for Cyber Security Operation Centre (C-SOC)** , we will submit a Performance Guarantee for a sum equivalent to 10% of the order value to be valid for a period of 60 months + 3 month i.e. 63 months in favour of **UCO BANK** effective from the month of execution of Service Level Agreement or successful go live whichever is earlier.

We agree to abide by the terms and conditions of this tender and our offer shall remain valid 180 days from the date of commercial bid opening and our offer shall remain binding upon us which may be accepted by the Bank any time before expiry of 180 days.

Until a formal contract is executed, this tender offer, together with the Bank's written acceptance thereof and Bank's notification of award, shall constitute a binding contract between us.

We understand that The Bank is not bound to accept the lowest or any offer the Bank may receive. We also certify that we have not been blacklisted by any PSU Bank/IBA/RBI and also at the time of bid submission.

We enclose the following Demand Drafts/Pay Orders:

1. DD No. _____dated_____ for **Rs 10,000/- (Rupees Ten Thousand Only)** as Cost of RFP Document &

2. BG No. _____dated_____ for **Rs 25,00,000/- (Rupees Twenty Five Lacs only)** as EMD.

BG and DDs are issued in favour of **UCO BANK** by.....Bank ,..... Branch payable at Kolkata.

Dated this __day of _____2019

Signature: _____

(In the Capacity of) _____

Duly authorized to sign the tender offer for and on behalf of

Eligibility Criteria Compliance

Sl. No	Eligibility Criteria	Document to be submitted
1	The bidder should be a registered company in India and should be in existence for a minimum period of Three years as on RFP date. (Proof, such as Registration/ Incorporation Certificate is to be submitted).	Certificate of Incorporation or Certificate of Commencement of business (whichever is applicable), MSME Registration (if applicable).
2	The bidder may be either an OEM or an Authorized Partner of the OEM (Original Equipment Manufacturer) whose product they are proposing. In case the OEM does not deal directly, an OEM may bid through their Authorized Service Partners or System Integrator.	Undertaking from the OEM mentioning a clause that OEM will provide support services during warranty period if the bidder authorized by them fails to perform. In case of an authorized representative, a letter of authorization (MAF) from original manufacturer must be furnished in original duly signed & stamped **(As per Annexure – J).**
3	The Bidder should have a minimum annual turnover of at **least Rs.100 Crores** in each of the **last three financial years** **(i.e. 2015-16, 2016-17 & 2017-18).**	Audited Balance Sheets for last 3 years, i.e., 2015-16, 2016-17 & 2017-18 and Certificate from Chartered Accountant stating Net Worth, Turnover and Profit/Loss for last 3 financial years, i.e. 2015-16, 2016-17 & 2017-18 are to be submitted.
4	The Bidder should have posted net profit in each of the last **three financial years** **(i.e. 2015-16, 2016-17 & 2017-18).**	Audited Balance Sheets for last 3 years, i.e., 2015-16, 2016-17 & 2017-18 and Certificate from Chartered Accountant stating Net Worth, Turnover and Profit/Loss for last 3 financial years, i.e., 2015-16, 2016-17 & 2017-18 are to be submitted.

Sl. No	Eligibility Criteria	Document to be submitted
5	The bidder should be providing IT security services (i.e. in the area of implementation, monitoring and management of various types of security solutions, devices, Technologies and software DLP,VAS,NAC,IT-GRC,APT) for a minimum period of two years as on RFP date.	Proof of purchase order/work order/sign off documents with Installation Report showing implementation of various security solutions stated above to be submitted indicating the company is providing such service for the past 2 years. The Bank reserves the right to inspect the information provided by the bidder.
6	The bidder should be currently in the service of providing Security Operation Centre (SOC)/Managed services in proposed Security solutions including at least two Government/Public/Private organisations in India out of which one should be a BFSI/ RBI/NPCI (excluding RRBs and Co-operative Bank).	Proof of Client Certificate is to be submitted.
7	Bidder shall have their own Security Operation Center (SOC) in India.	An undertaking in this regard on company letter head to be submitted.
8	The bidder should have minimum 3 skilled staff on their payroll with certification with for the product proposed.	An undertaking in this regard on company letter head to be submitted. He should be minimum BE/ B. Tech with certification such as CCNA/CISA/ CCNP/CISM.
9	Whose hardware/ software, Bidder is proposed to be supplied to the Bank must have presence in India.	An undertaking in this regard from the OEM with office address and contact person details to be submitted

Sl. No	Eligibility Criteria	Document to be submitted
10	The OEM products offered by the Bidder under this RFP should have been supplied & implemented in any BFSI/ RBI/NPCI/ Government Organisation (excluding RRBs and Co-operative Bank) in India.	Completion certificate from respective organisations where the OEM Products have been implemented to be submitted
11	The bidder should have not been black listed by any of Government Authority or Public Sector Undertaking (PSUs) or any Scheduled Commercial Banks or IBA and the bidder shall give an undertaking to this effect. In case, in the past, the name of their Company was black listed by any of the said authorities, the name of the company or organization must have been removed from the black list as on date of submission of the tender, otherwise the bid will not be considered.	An undertaking to this effect in the company's letterhead signed by authorized signatory to be submitted.
12	The Bidder should not be existing System Integrator for Network Equipment/ Data Centre Hardware for UCO Bank to avoid conflict of interest.	An undertaking to this effect in the company's letterhead signed by authorized signatory to be submitted

Annexure – D- General Details of the Bidder

General Details of the Bidder

1. Profile of Bidder
2. Name of bidder:
3. Location
   Regd. Office:
   Controlling Office:
4. Constitution
5. Date of incorporation & Date of Commencement of business:
6. Major change in Management in last three years
7. Names of Banker /s

B. Financial Position of Bidder for the last three financial years

	2015-16	2016-17	2017-18
Net Worth			
Turnover			
Profit after Tax			

N.B. Enclose copies of Audited Balance Sheets along with enclosures

C. Proposed Service details in brief

- **Description of service :**
- **Details of similar service provided to PSU organization/BFSI in India specifying the number of Banks and branches**

Details of Experience in RFP for the Implementation, Maintenance and Facility Management for System Security Tools for Cyber Security Operation Centre(C-SOC) :

PSU Organization / BFSI		
Name of Organization	**Period**	
	From	**To**

N.B. Enclose copies of Purchase Orders as references

Signature of Bidder: _____

Place: **Name:** _____

Date: **Business Address:** _____

Format of Bank Guarantee (EMD)

To,

The Deputy General Manager
DIT, BPR & BTD
UCO Bank, Head Office
5th Floor, 3&4, DD Block, Sector-I
Salt Lake, Kolkata – 700064.

Dear Sir,

Sub: RFP for the Implementation, Maintenance and Facility Management for System Security Tools for Cyber Security Operation Centre(C-SOC) vide RFP Ref No.: DIT/BPR&BTD/OA/5033/2018-19 Date: 15/02/2019

In response to your invitation to respond to your RFP for **Implementation, Maintenance and Facility Management for System Security Tools for Cyber Security Operation Centre(C-SOC)** M/s _____having their registered office at _____hereinafter called the 'Bidder') wish to respond to the said Request for Proposal (RFP) and submit the proposal for **Implementation, Maintenance and Facility Management for System Security Tools for Cyber Security Operation Centre(C-SOC)** as listed in the RFP document.

Whereas the 'Bidder' has submitted the proposal in response to RFP, we, the _____Bank having our Head Office _____ hereby irrevocably guarantee an amount of **Rs. 25,00,000/-** (**Rupees Twenty Five Lacs Only)** as bid security as required to be submitted by the 'Bidder' as a condition for participation in the said process of RFP.

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

1. If the Bidder withdraws his proposal during the period of the proposal validity; or
2. If the Bidder, having been notified of the acceptance of its proposal by the Bank during the period of the validity of the proposal fails or refuses to enter into the contract in accordance with the Terms and Conditions of the RFP or the terms and conditions mutually agreed subsequently.

We undertake to pay immediately on demand to UCO BANK the said amount of **Rupees 25,00,000/-** (**Rupees Twenty Five Lacs Only)** without any reservation, protest, demur, or recourse. The said guarantee is liable to be invoked/ enforced on the happening of the contingencies as mentioned above and also in the RFP document and we shall pay the amount on any Demand made by UCO BANK which shall be conclusive and binding on us irrespective of any dispute or difference raised by the

Bidder.

Notwithstanding anything contained herein:

1. Our liability under this Bank guarantee shall not exceed **Rs. 25,00,000/- only (Rupees Twenty Five Lacs Only).**
2. This Bank guarantee will be valid up to_____; and
3. We are liable to pay the guarantee amount or any part thereof under this Bank guarantee only upon service of a written claim or demand by you on or before_____.

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

Yours faithfully,

For and on behalf of
_____ Bank

Authorised Official

Note: This guarantee will require stamp duty as applicable and shall be signed by the official whose signature and authority shall be verified. The signatory shall affix his signature, name and designation.

RFP for the Implementation, Maintenance and Facility Management for System Security Tools for Cyber Security Operation Centre(C-SOC) vide RFP Ref No.: DIT/BPR&BTD/OA/5033/2018-19 Date: 15/02/2019

Technical Bill of Material

Solution	For Devices	Number of Devices at DC	Number of Devices at DR	Appliance Make/ Model	Version	CPU	Memory	Hard Disk	Licensing Details	Warranty	AMC Details
Network Access Control (NAC) & Patch Management	2800 Managed Switches, 24 Firewall, 25000 Endpoints devices										
Data Loss/Leakage Prevention (DLP)	20000 end points										
Automated Vulnerability Assessment Scanners (VAS)	500 devices										

Solution	For Devices	Number of Devices at DC	Number of Devices at DR	Appliance Make/ Model	Version	CPU	Memory	Hard Disk	Licensing Details	Warranty	AMC Details
IT-Governance, Risk & Compliance (IT-GRC)	10 concurrent users										
Anti-Advanced Persistent Threat (APT)		———	2								

Any other tools/ solution required (Use as many lines as required)													
Module	Product Details	No of Devices at DC	No of Devices at DR	Hardware			Software						
				CPU	Memory	Hard Disk Size	Purpose	Version Detail	Licensing Details	Database	OS	Warranty	AMC Details

Facility Management Services On Site resource 24*7*365	
No. of Resource	

RFP for the Implementation, Maintenance and Facility Management for System Security Tools for Cyber Security Operation Centre (C-SOC) vide RFP Ref No.: DIT/BPR&BTD/OA/5033/2018-19 Date: 15/02/2019

Indicative Commercial Format - Bill of Materials in Indian Rupees(INR)

Cost for Application, Software & Hardware based on the scope of work & solutions/requirements mentioned in the RFP

Table A		Hardware Cost with 3 years warranty				
Sl. No	Solution	Devices/Hardware with make and model	Qty	Unit Price	%Taxes	Total Price including Taxes
1	Network Access Control (NAC) & Patch Management	A.				
		B.				
		. .				
2	Data Loss/Leakage Prevention (DLP)	A.				
		B.				
		. .				
3	Automated Vulnerability Assessment Scanners (VAS)	A.				
		B.				
		. .				
4	IT-Governance, Risk & Compliance (IT-GRC)	A.				
		B.				
		. .				
5	Anti-Advanced Persistent Threat (APT)	A				
		B				
Sub Total (A)						

Table B		4th & 5th Years AMC Cost for Hardware								
Sl. No.	Solution	Devices/Hardware with make and model	Qty.	4th Year AMC			5th Year AMC			Total 4th &5th Year AMC Cost with tax
				Unit Price	%Taxes	Total price with tax	Unit Price	%Taxes	Total price with tax	
1	Network Access Control (NAC) & Patch Management	A.								
		B.								
		. .								
2	Data Loss/Leakage Prevention (DLP)	A.								
		B.								
		. .								
3	Automated Vulnerability Assessment Scanners (VAS)	A.								
		B.								
		. .								
4	IT-Governance, Risk & Compliance (IT-GRC)	A.								
		B.								
		. .								
5	Anti-Advanced Persistent Threat(APT)	A.								
		B.								
Sub Total (B)										

Table C	Software/License Cost with 1st Year Support					
Sl. No	Solution	Software/ License	Qty.	Unit Price	%Taxes	Total Price including Taxes
1	Network Access Control (NAC) & Patch Management	A.				
		B.				
		. .				
2	Data Loss/Leakage Prevention (DLP)	A.				
		B.				
		. .				
3	Automated Vulnerability Assessment Scanners (VAS)	A.				
		B.				
		. .				
4	IT-Governance, Risk & Compliance (IT-GRC)	A.				
		B.				
		. .				
5	Anti-Advanced Persistent Threat (APT)	A				
		B				
Sub Total (C)						

Table D		2nd , 3rd , 4th & 5th Years Software/ License ATS Cost														
Sl No	Solution	Software / License	Qty.	2nd Year ATS			3rd Year ATS			4th Year ATS			5th Year ATS			Total with tax
				Unit Price	% Tax	Total price with tax	Unit Price	%Tax	Total price with tax	Unit Price	%Tax	Total price with tax	Unit Price	%Tax	Total price with tax	
1	Network Access Control (NAC) & Patch Management	A.														
		B.														
		•														
2	Data Loss/Leakage Prevention (DLP)	A.														
		B.														
		• . • .														
3	Automated Vulnerability Assessment Scanners (VAS)	A.														
		B.														
		• •														
4	IT-Governance, Risk & Compliance (IT-GRC)	A.														
		B.														
		• •														
5	Anti-Advanced Persistent Threat (APT)	A.														
		B.														
Sub Total (D)																

Table E	Implementation Cost			
Sl No	Solution	Implementation cost	%Taxes	Total implementation cost with Taxes
1	Network Access Control (NAC) & Patch Management			
2	Data Loss/Leakage Prevention (DLP)			
3	Automated Vulnerability Assessment Scanners (VAS)			
4	IT-Governance, Risk & Compliance (IT-GRC)			
5	Anti-Advanced Persistent Threat (APT)			
Subtotal (E)				

Table F	Facility Management (24 x7)				
Sl. No.	Solution	No. of Resources	Cost for each Resource	% Taxes	Total FM Cost with Tax
1	Facility Management 1st Year				
2	Facility Management 2nd Year				
3	Facility Management 3rd Year				
4	Facility Management 4th Year				
5	Facility Management 5th Year				
Sub Total (F)					

Table G	Total Cost Ownership (TCO)	
Sl. No.	Description	Sum Total Cost
1	Hardware Cost with 3 years warranty (A)	
2	4th & 5th Years AMC Cost for Hardware (B)	
3	Software/License Cost with 1st Year Support (C)	
4	2nd , 3rd , 4th & 5th Years Software/ License ATS Cost (D)	
5	Implementation Cost (E)	
6	Facility Management (24 x7) (F)	
Total Cost Ownership G= A+B+C+D+E+F		

Total Cost Ownership (Word)……

Note:

In case of discrepancy between figures and words, the amount in words shall prevail.

- Bidders should strictly quote in the format and for periods as mentioned above. No counter condition / assumption in response to commercial bid will be accepted. Bank has a right to reject such bid.
- Present Rate of tax, if applicable, should be quoted in respective columns. The Bank will pay the applicable taxes for the above mentioned tax type ruling at the time of actual delivery of service/implementation and resultant billing. However, no other tax type will be paid. The Octroi / Entry Tax will be paid extra, wherever applicable on submission of actual tax receipt.
- Commercial Bid will be opened for the technically qualified vendors.
- The bidders with lowest **Total Cost of ownership (TCO)** will be selected as L1 bidder.
- The calculation for arriving at TCO is properly mentioned in the appropriate columns and we confirm that the above mentioned rates are accurate. In case of any anomalies in the calculation for arriving at TCO, the Bank will have the right to rectify the same and it will be binding upon our company.
- If the cost for any line item is indicated as zero or blank then Bank may assume that the said item is provided to the Bank without any cost.
- Bank has discretion to keep any of the line item mentioned above as optional as per Bank's requirement.
- We have ensured that the price information is filled in the Commercial Offer at appropriate column without any typographical or arithmetic errors. All fields have been filled in correctly.
- We have not added or modified any clauses / statements / recordings / declarations in the commercial offer, which is conditional and / or qualified or subjected to suggestions, which contain any deviation in terms & conditions or any specification.
- We have understood that in case of non-adherence to any of the above, our offer will be summarily rejected.
- Please note that any commercial offer which is conditional and / or qualified or subjected to suggestions will also be summarily rejected. This offer shall not contain any deviation in terms & condition or any specifications, if so such offer will be summarily rejected.
- All prices should be quoted in **Indian Rupees (INR)** only.
- The TCO (Total Cost of Ownership) will be inclusive of GST and other applicable taxes. However the GST and other applicable taxes will be paid as per actuals.

Place
Date

Authorised Signatory
Name
Designation

General guidelines

The detailed procedure and Business rules for the Reverse auction are as follows:

- Only the technically qualified/shortlisted bidders will be invited to participate in the Reverse auction process that will be conducted by an Auction company authorized by the Bank. Specific rules for this particular event viz., date and time, start price, bid decrement value, duration of event etc. shall be informed by the Bank, before the event to the participating shortlisted bidders.
- The bidders should furnish indicative prices for the project in their Indicative Commercial Bid (ICB) for finalizing the start bid amount for "Reverse auction".
- The lowest Indicative commercial offer (total cost) or any price decided by the Bank will be taken as the starting bid of the Reverse Auction and NOT for deciding the L-1 status. Bidders should note that the indicative commercial bid is considered for the purpose of conducting Reverse Auction process only.
- All participating bidders at the end of the Reverse Auction process shall be required to submit the break-up of their Final price(last bid price)again as detailed on the next day before 4 PM at UCO Bank, HO, Department of Information Technology, 5th Floor, Salt Lake , Sector -1 , Kolkata -700 064 . Please note that, failure or refusal to offer the services/goods at the price committed through Reverse Auction shall result in forfeiture of the Bid Security Deposit to Bank. This is not withstanding UCO Bank right to take any other action deemed fit, including claiming damages & "Black Listing" the bidder from participating in future Tenders that would be floated by the UCO Bank for a period found fit by the UCO Bank.
- The Bank reserve the right to reject any or all proposals. Similarly, they reserve the right NOT to include any bidder in the final short-list, if found or otherwise proved to have furnished wrong details/documents, at any point of time.
- The Final Commercial Bid should give all relevant price information and should not contradict the Technical Bid and masked commercial bid in any manner.
- The bidder shall indicate on the appropriate Price Schedule, specifying the unit price of the proposed service to be delivered.
- The bidders are advised in their own interest, to quote the best possible offer for each of the item offered at the time of preparing Indicative Commercial Bid itself. The Indicative Commercial Bid and the final Commercial Bid shall be as per the Commercial Bill of Material form as mentioned in RFP.

Reverse Auction Business Rules

The UCO BANK, DIT, HEAD OFFICE, Kolkata, proposes to conduct procurement through Online E-Auction subject to terms and conditions & schedule mentioned below:

SCOPE OF AUCTION: OFFER FOR APPOINTMENT of System Integrator for Implementation, Maintenance and Facility Management for System Security Tools for Cyber Security Operation Centre(C-SOC) for UCO Bank.

Schedule of Program: On-Line Auction Date & Time	Date, Time of Auction Starting & Ending time inclusive of extension time to be informed to the shortlisted vendors by email/ on their given contact nos.
Decrement Value	To be informed well before the Reverse Auction.
Prior extension time (minutes)	To be informed well before the Reverse Auction.
No. of Extensions & Extension time (minutes)	To be informed well before the Reverse Auction.

The Reverse Auction will be conducted through a service provider empanelled by the Bank. Usage of Digital signature is mandatory for participating through Reverse Auction Portal.

Terms & Conditions of the Online Reverse Auction Definitions

- Buyer:- Buyer referred herein, is the UCO Bank as defined in the Section1.1 of the main RFP document.
- SERVICE PROVIDER is an e-auction service provider appointed by the Bank to facilitate virtual auction. E-Auction Service Provider will only facilitate online auction solution to process UCO bank's procurement needs and are considered as third party not particularly interested in the item/s being purchased/sold on behalf of UCO bank.
- Bidder - means the party or his authorized representative who has participated in the RFP /Tender Process/Reverse Auction, Technically qualified, having valid Digital Certificate, and willing to complying with all the instructions, terms and conditions of RFP. All notices to the bidders shall be sent by E-mail, during the process of this auction by the Bank and/or by the e-Auction service provider.
- All such notices sent by email by the Bank as well as by e-Auction services provider shall, therefore, be deemed as valid notices. Hence bidders are required to indicate their own corporate e-mail id.
- The bidders who are qualified for bidding prices of offered products(on the basis of evaluation of their technical offer) shall be required to participate in an electronic reverse auction process to submit their price quotations against the items covered by this tender within a limited time period on the date as announced by the Bank. Such bidders shall be allowed to participate in the

reverse auction using their secured user id & password along with their digital signature to place their best bids during the auction period. The date & time for conducting the reverse auction will be duly communicated to qualified bidders in advance.

- Reverse auction is the simulation of the manual tendering process on the Internet. i.e., the eligible bidders/contractors can log on to the internet site specified by the Bank, using unique user Id & Password, which will be provided to them by the e-Reverse auction service provider appointed by the Bank and place their price bids on-line. The eligible bidders will be provided training by e-Reverse auction service provider on the methodology of submitting the bids online. Instead of a one-time best price bid, the bidders shall now be able to interact and react on the spot to the changing competitive bids, taking advantage of the intrinsic transparency in the whole process.
- During e-Reverse auction process the bidders can respond on the spot to the price trends and can offer their competitive bids. The logged in bidders will know the prevailing lowest bid at any given point of time but not the identity of the other bidders.
- The bidders can place their bids from any place for which they need is a desktop computer with a browser interface and good internet connectivity.
- Suggested system configuration for computers to be used for online bidding.
- It is suggested that hardware and software of the following specification be used by the bidders for bidding so as to enable them to have better connectivity.
    - Processor Pentium IV and above PC/Laptop with USB Ports
    - Memory minimum512 MB
    - Operating system
    - Windows 2000 Professional
    - Windows7 Professional
    - Browser: Internet explorer IE 6, 7& 8
    - UPS: Suitable UPS for uninterrupted power supply.
- The Bank reserve their right not undertake any responsibility to procure any Permission/license etc. in respect of the auction item, if it so desires.

Eligibility of Bidders to participate in Reverse Auction:

- Bidders who are technically qualified in terms of the relative Terms & Conditions of the RFP and accept the Business Rules, Terms& conditions of Reversion Auction and submit the undertaking as per the prescribed in Annexure -S can only participate in Reverse Auction related to the procurement for which RFP is floated.

- Bidders not submitting the above undertaking or submitting with deviations/ amendments there to will be disqualified from further evaluation/participation in the process of relevant procurement.
- Bidders should ensure that they have valid digital certificate class III (Mandatory for login and submit) well in advance to participate in the Reverse Auction. Bank and/or Service Provider will not be responsible in case Bidder could not participate in Reverse Auction due to non-availability of valid digital certificate.
- The bidders participating in Reverse Auction shall submit the following duly signed by the same Competent Authority who signs the offer documents in response to the RFP floated by Bank.
  - Undertaking letter for acceptance of Business Rules for Online Reverse Auction and Letter of Authority authorizing the name/s of official/s to take part in Reverse Auction as per the Annexure – R (Compliance Statement)
  - Agreement between Service Provider and Bidder. This format will be given by the service provider prior to announcement of Reverse Auction.

Training:

- Bank will facilitate necessary training to representatives of all eligible Bidders for participation in Reverse Auction either on its own or through the Service Provider for the Reverse Auction.
- All rules & procedure related to Reverse Auction will be explained during the training.
- The Bank/Service Provider may also conduct a 'Mock Reverse Auction' to familiarize the vendor/s with Reverse Auction process.
- Date, Time, Venue etc. of training will be advised at appropriate time.
- Eligible Bidder/his authorized nominee have to attend the training as per the schedule and at the specified venue at his/Bidders own cost.
- No request from the Bidders for change in training schedule and/or venue will be entertained.
- However, Bank reserves the right to postpone/ change/ cancel the training schedule for whatsoever reasons without assigning any reasons therefore, even after its communication to eligible Bidders.
- Any Bidder not participating in the training process will do so at his own risk and it shall not be open for him to make any complaint/grievance later.

Reverse Auction Schedule:

- The date & time of commencement of Reverse Auction and its duration of time shall be communicated to the eligible Bidders at least a week prior to the Reverse Auction date.

- Bank reserves the right to postpone/change/ cancel the Reverse Auction event even after its communication to Bidders without assigning any reasons therefore.
- Reverse Auction will normally be for a period of one hour. If a Bidder places a bid price in last 10 minutes of closing of the Reverse auction, the auction period shall get extended automatically for another 10 minutes. Maximum 3 extensions each of 10 minutes will be allowed after auction period of 1hour i.e. entire process can last maximum for one and half hour only. In case there is no bid price in the last10 minutes of closing of Reverse Auction, the auction shall get closed automatically without any extension.
- The time period of Reverse Auction & Maximum number of its extensions &time are subject to change and will be advised to eligible Bidders before the start of the Reverse Auction event.
- During English Reverse (no ties) Auction, if no bid is received within the specified time, the Bank, at its discretion, may decide to revise Start price/scrap the reverse auction process/proceed with conventional mode of tendering.

Bidding Currency:

- Bidding will be conducted in Indian Rupees (INR) for the TCO.

Total Cost of Ownership

- TCO refers to aggregate amounts payable by the Bank for transfer of ownership.
- The TCO shall encompass but not limited to following:
  a) Cost of the equipment/products or services etc.
  b) Annual Maintenance Charges/ SLA Cost/ATS/SA etc.
- The TCO for the project will be defined by the concerned department in the RFP/Bid Document.
- The L1 bidder is arrived at based on the lowest TCO in reverse auction.
- Bank will pay the TCO price to the bidder as per the payment terms defined in RFP/Bid Document.

Start Price

- Bidder needs to give their indicative sealed commercial Bid to the Bank.
- Bank shall determine the Start Price for Reverse Auction-
- On its own and/ or Based on the indicative price information of Total Cost of Ownership(TCO) called for separately from each Bidder during conclusion of Technical Evaluation or at appropriate time before commencement of Reverse Auction.
- The start price of an item in online reverse auction is open to all the participating bidders. Bidders are required to start bidding after announcement of Start Price and decrement amount. Any bidder can start bidding, in the

online reverse auction, from the decrement price. Please note that the first online bid that comes in the system during the online reverse auction cannot be equal to the auction's start price, and lesser than the auction's start price by one decrement, or lesser than the auction's start price by multiples of decrement. The subsequent bid that comes into outbid the L1 rate will have to be lesser than the L1 rate by one decrement value or in multiples of the decrement value.

Decremented Bid Value

- The bid decrement value will be specified by Bank before the start of Reverse Auction event. It can be a fixed amount.
- Bidder is required to quote his bid price only at a specified decremented value. Bidder need not quote bid price at immediate next available lower level, but it can be even at 2 /3/4…… level of next available lower level.

Web Portal and Access

- Reverse Auction will be conducted on a specific web portal meant for this purpose with the help of the Service Provider identified by the Bank.
- Service Provider will make all necessary arrangement for fair and transparent conduct of Reverse Auction like hosting the web portal, imparting training to eligible Bidders etc., and finally conduct of Reverse Auction.
- Bidders will be participating in Reverse Auction event from their own office/place of their choice. Internet connectivity and other paraphernalia requirements shall have to be ensured by Bidder themselves.
- In the event of failure of their internet connectivity (due to any reason what so ever it may be) the service provider or Bank is not responsible.
- In order toward-off such contingent situation,
  - Bidders are advised to make all the necessary arrangements/ alternatives such as backup power supply, whatever required so that they are able to circumvent such situation and still be able to participate in the reverse auction successfully.
  - However, the vendors are requested to not to wait till the last moment to quote their bids to avoid any such complex situations.
  - Failure of power at the premises of vendors during the Reverse auction cannot be the cause for not participating in the reverse auction.
  - On account of this the time for the auction cannot be extended and BANK is not responsible for such eventualities.

- Bank and/or Service Provider will not have any liability to Bidders for any interruption or delay in access to site of Reverse Auction irrespective of the cause.
- For making the process of Reverse Auction and its result legally binding on the participating Bidders, Service Provider will enter into an agreement with each Bidder, before the start of Reverse Auction event. Without this Bidder will not be eligible to participate in the event.

- Bank nor service provider/auctioneer is not responsible for consequential damages such as no power supply, no internet connectivity, system problem, inability to use the system, loss of electronic information, power interruptions, UPS failure, or any force majeure etc.

TRANSPARENCY IN BIDS

- 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.

MASKING OF NAMES

- Bidder will be able to view the following on their screen along with the necessary fields in Reverse Auction:
    - Opening/Starting Price for the auction
    - Leading/Lowest Bid Price in Auction(only total price)
    - Last Bid Price placed by the respective Bidder.
    - Item Description
    - Time left for the auction
- Names of bidders/vendors shall be anonymously masked in the Reverse Auction process.
- After completion of Reverse Auction, the service provider/auctioneer shall submit a report to the Bank with all details of bid and the original names of the bidders as also the L1 bidder with his/their original names.

Finalization of the Successful Bidder

- At the end of Reverse Auction event Service Provider will provide the Bank all necessary details of the bid prices and reports of Reverse Auction.
- Upon receipt of above information from Service Provider, Bank will evaluate the same and will decide upon the winner i.e. Successful Bidder. Bank's decision on award of Contract shall be final and binding on all the Bidders.

- After the completion of the Auction event, all the Bidders have to submit the Price Breakup as per the RFP immediately to the Bank and to the Service provider for further proceedings.
- Any variation between the on-line Reverse Auction bid price and signed

  Document will be considered as sabotaging the tender process and will invite disqualification of Bidder/vendor to conduct business with Bank as per prevailing procedure.
- Successful Bidder has to give break-up of his last/lowest bid price as per Bill of Material at the end of Reverse auction event within 4 PM of next working day without fail.
- Successful Bidder is bound to supply at their final bid price of Reverse Auction. In case of back out or not supply as per the rates quoted, Bank will take appropriate action against such Bidder and/or forfeit the Bid Security amount, debar him from participating in future Tenders/Auctions
- In case Bank decides not to go for Reverse Auction related to the procurement for which RFP is floated and price bids if any already submitted and available with Bank shall be opened as per Banks standard practice.

Bidder's Obligation

- Bidder shall not involve himself or any of his representatives in Price manipulation of any kind directly or indirectly with other suppliers/Bidders at any point of time. If any such practice comes to the notice, Bank shall disqualify the vendor/bidders concerned from the reverse auction process.
- Bidder shall not divulge either his Bid details or any other details of Bank to any other party without written permission from the Bank.

Change in Business Rules, Terms & Conditions of Reverse Auction

- Any change in the Business Rules as may become emergent and based on the experience gained shall be made only by a Committee consisting of Senior Executives of Bank.
- Bank reserves the right to modify/withdraw any of the Business rules, Terms &conditions of Reverse Auction at any point of time.
- Modifications of Business rules, Terms &conditions of Reverse Auction will be made available on website immediately.
- Modifications made during the running of Reverse Auction event will be informed to participating Bidders immediately.

GRIEVANCES REDRESSAL

- Any aggrieved vendor/bidder through Reverse Auction process can make complaint in writing within 48 hours of the Reverse Auction to the Bank.
-

Errors and Omissions

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

Annexure – I- DECLARATION-CUM-UNDERTAKING

DECLARATION-CUM-UNDERTAKING

(TO BE EXECUTED ON NON-JUDICIAL STAMP PAPER OF REQUISITE VALUE)

To

The Deputy General Manager
DIT, BPR & BTD
UCO Bank, Head Office
5th Floor, 3&4, DD Block, Sector-I
Salt Lake, Kolkata -700064

Sub: Declaration-Cum-Undertaking regarding compliance with all statutory requirements

In consideration of UCO Bank, a body corporate, constituted under Banking Companies (Acquisition & Transfer of Undertakings) Act, 1970 as amended from time to time having its Head Office at 10, Biplabi Trailokya Maharaj Sarani, Kolkata-700001 (hereinafter referred to as "Bank" which expression shall include its successors and assigns), we, M/s……., having its Registered Office at……., do hereby, having examined the RFP including all Annexure, confirm and agree to comply with all Laws, Rules, Regulations, Bye-Laws, Guidelines, Notifications etc.

We do also hereby irrevocably and unconditionally agree and undertake to save and keep the Bank, including its respective directors, officers, and employees and keep them harmless from and against any claim, demand, losses, liabilities or expenses of any nature and kind whatsoever and any damage caused from and against all suits and other actions that may be instituted taken or preferred against the Bank by whomsoever and all losses, damages, costs, charges and expenses arising out of non-compliance with or non-adherence to any statutory/regulatory requirements and/or any other law for the time being in force.

Dated this _____ day of _____, 20 _____.

Place:

For M/s. …….

…….

[Seal and Signature(s) of the Authorised Signatory (s)]

Annexure – J - MANUFACTURERS' AUTHORIZATION FORM (MAF)

(Letter to be submitted by the Manufacturer on firm's letter head)

MANUFACTURERS' AUTHORIZATION FORM (MAF)

To

The Deputy General Manager
DIT, BPR & BTD
UCO Bank, Head Office
5th Floor, 3&4, DD Block, Sector-I
Salt Lake, Kolkata -700064

Dear Sir

Ref: RFP for the Implementation, Maintenance and Facility Management for System Security Tools for Cyber Security Operation Centre (C-SOC) vide RFP Ref No.: DIT/BPR&BTD/OA/5033/2018-19 Date: 15/02/2019

We _____who are established and reputable manufactures of _____ having factories at_____ and _____ do hereby authorize M/s _____ (Name and address of Bidder) to offer their quotation, negotiate and conclude the contract with you against the above invitation for Bid offer.

We hereby extend our full guarantee and warranty as per terms and conditions of the Bid and the contract for the equipment and services offered against this invitation for Bid offer by the above firm. We undertake to provide back-to-back support for spare and skill to the bidder for subsequent transmission of the same to the Bank. We also undertake to provide support services during warranty period if the above bidder authorized by us fails to perform in terms of the RFP.

Yours faithfully

(Name of manufacturers)

PROFORMA FOR PERFORMANCE GUARANTEE
(To be stamped in accordance with the stamp act)

In consideration of UCO BANK, a body corporate constituted under the Banking Companies (Acquisition & Transfer of Undertaking) Act, 1970, having its head office at 10 BIPLABI TRILOKYA MAHARAJ SARANI (BRABOURNE ROAD), Kolkata-700001 (hereinafter called "Purchaser") having agreed to exempt M/s **(Name of the Selected bidder Company)** a Company incorporated under the Companies Act, 1956 having its registered office at **(Address of the Selected bidder company)** (hereinafter called " SELECTED BIDDER") from the demand, under the terms and conditions of Purchaser's Letter of Intent bearing no. ….dated ……. issued to the Vendor (hereinafter called "Purchase Order") in pursuance of Request For Proposal no. ----------as modified, of security deposit for the due fulfillment by the VENDOR of the Terms and conditions contained in the Purchase Order, on production of a Bank Guarantee for Rs.…(Rupees…. Only).

We,…… [indicate the name of the bank ISSUING THE BANK GUARANTEE] (hereinafter referred to as "Bank") at the request of …….. [VENDOR] do hereby undertake to pay to Purchaser an amount not exceeding Rs……...against any loss or damage caused to or suffered or would be caused to or suffered by Purchaser by reason of any breach by the said VENDOR of any of the terms or conditions contained in the said Agreement.

We ……[indicate the name of the bank ISSUING THE BANK GUARANTEE] do hereby undertake to pay the amounts due and payable under this guarantee without any demur, merely on a demand from Purchaser stating that the amount claimed is due by way of loss or damage caused to or breach by the said VENDOR of any of the terms or conditions contained in the said Agreement or by reason of the VENDOR'S failure to perform the said Agreement. Any such demand made on the Bank shall be conclusive as regards the amount due and payable by the Bank under this guarantee. However, our liability under this guarantee shall be restricted to an amount not exceeding Rs. ……..

We undertake to pay to Purchaser any money so demanded notwithstanding any dispute or disputes raised by the VENDOR in any suit or proceeding pending before any court or Tribunal relating thereto our liability under this present being absolute and unequivocal. The payment as made by us under this bond shall be a valid discharge of our liability for payment there under and the VENDOR for payment there under and the VENDOR shall have no claim against us for making such payment.

We … [indicate the name of the bank ISSUING THE GUARANTEE] further agree that the guarantee herein contained shall remain in full force and effect during the period that would be taken for the performance of the said Agreement and that it

shall continue to be enforceable till all the dues of BANK under or by virtue of the said have been fully paid and its claims satisfied or discharged or till Purchaser certifies that the terms and conditions of the said Agreement have been fully and properly carried out by the said VENDOR and accordingly discharged this guarantee. Unless a demand or claim under this guarantee is made on us in writing on or before ……(Expiry of claim period), we shall be discharged from all liabilities under this guarantee thereafter.

We …… [Indicate the name of bank ISSUING THE GUARANTEE] further agree with Purchaser that Purchaser shall have the fullest liberty without our consent and without affecting in any manner our obligations hereunder to vary any of the terms and conditions of the said Agreement or to extend time of performance by the said VENDOR from time or to postpone for any time, or from time to time any of the powers exercisable by UCO BANK against the said VENDOR and to forebear or enforce any of the terms and conditions relating to the said agreement and we shall not be relieved from our liability by reason of any variation, or extension being granted to the said VENDOR or for any forbearance, act or omission on the part of UCO BANK of any indulgence by UCO BANK to the said VENDOR or by any such matter or thing whatsoever which under the law relating to sureties would, but for this provision, have effect of so relieving us.

This guarantee will not be discharged due to the change in the constitution of the Bank or the VENDOR.

We, …… [Indicate the name of Bank ISSUING THE GUARANTEE] lastly undertake not to revoke this guarantee during its currency except with the previous consent of Purchaser in writing. Notwithstanding anything contained herein:

i) Our liability under this Bank Guarantee shall not exceed Rs.…(Rupees……) only.

ii) This Bank Guarantee shall be valid upto …… and

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

Dated the …… day of …… for ..... [Indicate the name of Bank]

NOTE:

1. Selected vendor should ensure that the seal and CODE No. of the signatory is put by the bankers, before submission of the bank guarantee.
2. Bank guarantee issued by banks located in India shall be on a Non-Judicial Stamp Paper of requisite value as applicable to the place of execution.

PRE-CONTRACT INTEGRITY PACT

(To be stamped as per the Stamp Law of the Respective State)

1. Whereas UCO Bank having its registered office at UCO BANK, a body corporate constituted under The Banking companies (Acquisition & Transfer Act of 1970), as amended by The Banking Laws (Amendment) Act, 1985, having its Head Office at 10, Biplabi Trailokya Maharaj Sarani , Kolkata-700001 acting through its Department of IT, represented by Authorised Signatory hereinafter referred to as the Buyer and the first party, proposes to procure (Selection of System Integrator for Implementation, Maintenance and Facility Management for System Security Tools for Cyber Security Operation Centre (C-SOC)) hereinafter referred to as Stores and / or Services.

And

M/s_____ represented by_____ Authorised signatory, (which term, unless expressly indicated by the contract, shall be deemed to include its successors and its assignee), hereinafter referred to as the bidder/seller and the second party, is willing to offer/has offered the Stores and / or Services.

2. Whereas the Bidder/Seller is a private company/public company/ /partnership/registered export agency, constituted in accordance with the relevant law in the matter and the BUYER is a Public Sector Undertaking and registered under Companies Act 1956. Buyer and Bidder/Seller shall hereinafter be individually referred to as ―Party or collectively as the ―parties, as the context may require.

3. Preamble

Buyer has called for tenders under laid down organizational procedures intending to enter into contract /s for supply / purchase / etc. of Selection of System Integrator for Implementation, Maintenance and Facility Management for System Security Tools for Cyber Security Operation Centre (C-SOC) and the Bidder /Seller is one amongst several bidders /Proprietary Vendor /Customer Nominated Source/Licensor who has indicated a desire to bid/supply in such tendering process. The Buyer values and takes primary responsibility for values full compliance with all relevant laws of the land, rules, regulations, economic use of resources and of fairness / transparency in its relations with its Bidder (s) and / or Seller(s).

In order to achieve these goals, the Buyer will appoint Independent External Monitor(s) (IEM) in consultation with Central Vigilance Commission, who will monitor the tender process and the execution of the contract for compliance with the principles mentioned above.

4. Commitments of the Buyer

4.1 The Buyer commits itself to take all measures necessary to prevent corruption and fraudulent practices and to observe the following principles:-

(i) No employee of the Buyer, personally or through family members, will in connection with the tender, or the execution of a contract demand, take a promise for or accept, for self or third person, any material or immaterial benefit which the person is not legally entitled to.

(ii) The Buyer will during the tender process treat all Bidder(s) /Seller(s) with equity and reason. The Buyer will in particular, before and during the tender process, provide to all Bidder (s) /Seller(s) the same information and will not provide to any Bidders(s) /Seller(s) confidential /additional information through which the Bidder(s) / Seller(s) could obtain an advantage in relation to the process or the contract execution.

(iii) The Buyer will exclude from the process all known prejudiced persons.

4.2 If the Buyer obtains information on the conduct of any of its employees which is a criminal offence under the Indian Legislation Prevention of Corruption Act 1988 as amended from time to time or if there be a substantive suspicion in this regard, the Buyer will inform to its Chief Vigilance Officer and in addition can initiate disciplinary action.

***5* Commitments of the Bidder(s) /Seller(s):**

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

(i) The Bidder(s) /Seller(s) will not directly or through any other persons or firm, offer promise or give to any of the Buyer's employees involved in the tender process or the execution of the contract or to any third person any material or other benefit which he / she is not legally entitled to, in order to obtain in exchange any advantage during the tendering or qualification process or during the execution of the contract.

(ii) The Bidder(s) /Seller(s) will not enter with other Bidders / Sellers into any undisclosed agreement or understanding, whether formal or informal. This applies in particular to prices, specifications, certifications, subsidiary contracts, submission or non-submission of bids or any other actions to restrict competitiveness or to introduce cartelization in the bidding process.

(iii) The bidder(s) /Seller(s) will not commit any offence under the Indian legislation, Prevention of Corruption Act, 1988 as amended from time to time. Further, the Bidder(s) /Seller(s) will not use improperly, for purposes of competition or personal

gain, or pass on to others, any information or document provided by the Buyer as part of the business relationship, regarding plans, technical proposals and business details, including information constrained or transmitted electronically.

(iv) The Bidder(s) /Seller(s) shall ensure compliance of the provisions of this Integrity Pact by its sub-supplier(s) / sub-contractor(s), if any, Further, the Bidder /Seller shall be held responsible for any violation/breach of the provisions by its sub-supplier(s) /Sub-contractor(s).

5.2 The Bidder(s) /Seller(s) shall ensure compliance of the provisions of this Integrity Pact by its sub-supplier(s) / sub-contractor(s), if any, Further, the Bidder /Seller shall be held responsible for any violation /breach of the provisions by its sub-supplier(s) /sub-contractor(s).

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

5.4 Agents / Agency Commission

The Bidder /Seller confirms and declares to the Buyer that the bidder/Seller is the original manufacturer/authorized distributor / stockiest of original manufacturer or Govt. Sponsored /Designated Export Agencies (applicable in case of countries where domestic laws do not permit direct export by OEMS of the stores and /or Services referred to in this tender / Offer / contract / Purchase Order and has not engaged any individual or firm, whether Indian or Foreign whatsoever, to intercede, facilitate or in any way to recommend to Buyer or any of its functionaries, whether officially or unofficially, to the award of the tender / contract / Purchase order to the Seller/Bidder; nor has any amount been paid, promised or intended to be paid to any such individual or firm in respect of any such intercession, facilitation or recommendation. The Seller / Bidder agrees that if it is established at any time to the satisfaction of the Buyer that the present declaration is in anyway incorrect or if at a later stage it is discovered by the Buyer that the Seller incorrect or if at a later stage it is discovered by the Buyer that the Seller/Bidder has engaged any such individual /firm, and paid or intended to pay any amount, gift, reward, fees, commission or consideration to such person, party, firm or institution, whether before or after the signing of this contract /Purchase order, the Seller /Bidder will be liable to refund that amount to the Buyer. The Seller will also be debarred from participating in any RFP / Tender for new projects / program with Buyer for a minimum period of five years. The Buyer will also have a right to consider cancellation of the Contract / Purchase order either wholly or in part, without any entitlement of compensation to the Seller /Bidder who shall in such event be liable to refund agents / agency commission payments to the buyer made by the Seller /Bidder along with interest at the rate of 2% per annum above LIBOR (London Inter Bank Offer Rate) (for foreign vendors) and Base Rate of SBI (State Bank of India) plus 2% (for Indian vendors). The Buyer will also have the right to recover any such amount from any contracts / Purchase order concluded earlier or later with Buyer.

6. Previous Transgression

6.1 The Bidder /Seller declares that no previous transgressions have occurred in the last three years from the date of signing of this Integrity Pact with any other company in any country conforming to the anti-corruption approach or with any other Public Sector Enterprise in India that could justify Bidder's /Seller's exclusion from the tender process.

6.2 If the Bidder /Seller makes incorrect statement on this subject, Bidder /Seller can be disqualified from the tender process or the contract, if already awarded, can be terminated for such reason without any liability whatsoever on the Buyer.

7. Company Code of Conduct

Bidders /Sellers are also advised to have a company code of conduct (clearly rejecting the use of bribes and other unethical behavior) and a compliance program for the implementation of the code of conduct throughout the company.

8. Sanctions for Violation

8.1 If the Bidder(s) /Seller(s), before award or during execution has committed a transgression through a violation of Clause 5, above or in any other form such as to put his reliability or credibility in question, the Buyer is entitled to disqualify the Bidder(s) /Seller (s) from the tender process or take action as per the procedure mentioned herein below:

(i) To disqualify the Bidder /Seller with the tender process and exclusion from future contracts.

(ii) To debar the Bidder /Seller from entering into any bid from Buyer for a period of two years.

(iii) To immediately cancel the contract, if already signed /awarded without any liability on the Buyer to compensate the Bidder /Seller for damages, if any. Subject to Clause 5, any lawful payment due to the Bidder/Seller for supplies effected till date of termination would be made in normal course.

(iv) To encash EMD /Advance Bank Guarantees / Performance Bonds / Warranty Bonds, etc. which may have been furnished by the Bidder /Seller to the extent of the undelivered Stores and / or Services.

8.2 If the Buyer obtains Knowledge of conduct of Bidder /Seller or of an employee or representative or an associate of Bidder /Seller which constitutes corruption, or if the Buyer has substantive suspicion in this regard, the Buyer will inform to its Chief Vigilance Officer.

9. Compensation for Damages

9.1 If the Buyer has disqualified the Bidder(s) /Seller(s) from the tender process prior to the award according to Clause 8, the Buyer is entitled to demand and recover the damages equivalent to Earnest Money Deposit in case of open tendering.

9.2 If the Buyer has terminated the contract according to Clause 8, or if the Buyer is entitled to terminate the contract according to Clause 8, the Buyer shall be entitled to encash the advance bank guarantee and performance bond / warranty bond, if furnished by the Bidder / Seller, in order to recover the payments, already made by the Buyer for undelivered Stores and / or Services.

10. Price Fall Clause

The Bidder undertakes that it has not supplied /is not supplying same or similar product/systems or subsystems at a price lower than that offered in the present Bid in respect of any other Ministry /Department of the Government of India or PSU/PSBs during the currency of the contract and if it is found at any stage that same or similar product /Systems or Subsystems was supplied by the Bidder to any other Ministry /Department of the Government of India or a PSU or any Public Sector Bank at a lower price during the currency of the contract, then that very price 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.

11. Independent External Monitor(s)

11.1 The Buyer has appointed independent External Monitors for this Integrity Pact in consultation with the Central Vigilance Commission (Names and Addresses of the Monitors are given in RFP).

11.2 As soon as the integrity Pact is signed, the Buyer shall provide a copy thereof, along with a brief background of the case to the independent External Monitors.

11.3 The Bidder(s) / Seller(s) if they deem it necessary, May furnish any information as relevant to their bid to the Independent External Monitors.

11.4 If any complaint with regard to violation of the IP is received by the buyer in a procurement case, the buyer shall refer the complaint to the Independent External Monitors for their comments / enquiry.

11.5 If the Independent External Monitors need to peruse the records of the buyer in connection with the complaint sent to them by the buyer, the buyer shall make arrangement for such perusal of records by the independent External Monitors.

11.6 The report of enquiry, if any, made by the Independent External Monitors shall be submitted to MD & CEO, UCO Bank, Head Office at 10, Biplabi Trailokya

Maharaj Sarani , Kolkata-700001 within 2 weeks, for a final and appropriate decision in the matter keeping in view the provision of this Integrity Pact.

11.7 The word "Monitor" would include both singular and plural.

12. Law and Place of Jurisdiction

This Integrity Pact is subject to Indian Laws, and exclusive Jurisdiction of Courts at Kolkata, India.

13. 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 provision of the extant law in force relating to any civil or criminal proceedings.

14. Integrity Pact Duration.

14.1 This Integrity Pact begins when both parties have legally signed it. It expires of order / finalization of contract.

14.2 If any claim is made/ lodged during this time, the same shall be binding and continue to be valid despite the lapse of this Integrity Pact as specified above, unless it is discharged / determined by MD & CEO, UCO Bank .

14.3 Should one or several provisions of this Integrity Pact turn out to be invalid, the reminder of this Integrity Pact remains valid. In this case, the parties will strive to come to an agreement to their original intentions.

15 Other Provisions

15.1 Changes and supplements need to be made in writing. Side agreements have not been made.

15.2 The Bidders (s)/ Sellers (s) signing this IP shall not initiate any Legal action or approach any court of law during the examination of any allegations/complaint by IEM and until the IEM delivers its report.

15.3 In view of nature of this Integrity Pact, this Integrity Pact shall not be terminated by any party and will subsist throughout its stated period.

15.4 Nothing contained in this Integrity Pact shall be deemed to assure the bidder / Seller of any success or otherwise in the tendering process.

16. This Integrity Pact is signed with UCO Bank exclusively and hence shall not be treated as precedence for signing of IP with MoD or any other Organization.

17. In the event of any contradiction between the Integrity Pact and its Annexure L, the Clause in the Integrity Pact will prevail.

18. The Parties here by sign this Integrity Pact at_____on _____ (Seller/Bidder) and _____on _____ (Buyer)

BUYER	**BIDDER * /SELLER***
Signature:	**Signature:**
Authorized Signatory	**Authorized Signatory (*)**
Department of IT	
Place:	**Place:**
Date:	**Date:**
Witness :	**Witness :**
(Name & Address)	**(Name & Address)**

Undertaking Letter to the Bank on the vendor's letterhead

To

The Deputy General Manager
DIT, BPR & BTD
UCO Bank, Head Office
5th Floor, 3&4, DD Block, Sector-I
Salt Lake, Kolkata -700064

Sir,

Sub: RFP for the Implementation, Maintenance and Facility Management for System Security Tools for Cyber Security Operation Centre (C-SOC) vide RFP Ref No.: DIT/BPR&BTD/OA/5033/2018-19 Date: 15/02/2019

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

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

For……..

Designation:

(Signature and seal of authorized person)

Bidder's corporate name:
Place:
Date:

Annexure –N-Undertaking for Non-Blacklisting / Non-Debarment of the bidder

Undertaking for Non-Blacklisting / Non-Debarment of the bidder

To

The Deputy General Manager
DIT, BPR & BTD
UCO Bank, Head Office
5th Floor, 3&4, DD Block, Sector-I
Salt Lake, Kolkata -700064

Dear Sir(s),

Sub: RFP for the Implementation, Maintenance and Facility Management for System Security Tools for Cyber Security Operation Centre (C-SOC) vide RFP Ref No.: DIT/BPR&BTD/OA/5033/2018-19 Date: 15/02/2019.

We, M/s _____, the undersigned, hereby confirm that we have read and understood the eligibility criteria and fulfill the same.

a) We further confirm that all the information as per requirement of the Bank have been included in our bid.

b) Further, we hereby undertake and agree to abide by all terms and conditions and guidelines stipulated by the Bank. We understand that any deviation may result in disqualification of our bid.

c) We have not been blacklisted by any Nationalized Bank/RBI/IBA or any other Government agency/ICAI. No legal action is pending against us for any cause in any legal jurisdiction.

d) We undertake that adequate number of resources, if required by the Bank, will be deployed for the project to complete the assignment within stipulated time.

We, M/s _____, the undersigned, hereby confirm that we will provide service as mentioned in the RFP.

Bank reserves the sole right to decide by itself for discontinuation of contract if the quality of paper is maintained as mentioned in the RFP.

(Deviation to the above if any, the Bidder must provide details of such action(s))

(1)
(2)

(Signature and the capacity of the person duly authorized to sign the bid for and on behalf of)

Annexure – O - Format of Pre-Bid Queries to be submitted by the Bidder(s)

Format of Pre-Bid Queries to be submitted by the Bidder(s)

Name of the Bidder:

Name of the Contact Person of the Bidder:

Contact Number of the Contact Person:

Email id of the Contact Person:

Sl. No.	RFP Page No.	RFP Clause No.	Original RFP Clause	Subject/Description	Query sought/Suggestions of the Bidder

Undertaking Letter on the vendor's letterhead for GST Law

To
The Deputy General Manager
DIT, BPR & BTD
Bank, Head Office
5th Floor, 3&4, DD Block, Sector-I
Salt Lake, Kolkata -700064

Dear Sir,

Sub RFP for the Implementation, Maintenance and Facility Management for System Security Tools for Cyber Security Operation Centre (C-SOC) vide RFP Ref No.: DIT/BPR&BTD/OA/5033/2018-19 Date: 15/02/2019

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

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

Yours faithfully,

For……..

Designation:

(Signature and seal of authorized person)

Bidder's corporate name:

Place:

Date:

NON-DISCLOSURE AGREEMENT

This Non-Disclosure Agreement is entered into on this ….day of ……., 2019

BETWEEN

UCO Bank, a body corporate, constituted under the Banking Companies (Acquisition & Transfer of Undertakings) Act, 1970 as amended from time to time having its Head Office at No.10, BTM Sarani, Kolkata-700001 hereinafter referred to as "**the Bank**" (which expression shall unless excluded by or repugnant to the subject or context be deemed to mean and include its assigns, administrators and successors) **of the FIRST PART/ DISCLOSING PARTY**

AND

……
…… (which expression shall unless excluded by or repugnant to the subject or context be deemed to mean and include its assigns, administrator and successors) of the **SECOND PART/ RECEIVING PARTY**

(Each of Bank and the vendor is sometimes referred to herein as a "***Party***" and together as the "***Parties***").

WHEREAS the Vendor/Receiving Party is inter alia engaged for the **RFP for the Implementation, Maintenance and Facility Management for System Security Tools for Cyber Security Operation Centre (C-SOC) vide RFP Ref No.: DIT/BPR&BTD/OA/5033/ 2018-19 Date: 15/02/2019.**

The Vendor/Receiving Party would be the single point of contact for this project.

WHEREAS Bank/Disclosing Party is inter alia engaged in the business of Banking; and

WHEREAS the Parties presently desire to discuss and/or consult with each other's business for the purposes of entering into Agreements for the **RFP for the Implementation, Maintenance and Facility Management for System Security Tools for Cyber Security Operation Centre (C-SOC) vide RFP Ref No.: DIT/BPR&BTD/OA/5033/ 2018-19 Date: 15/02/2019.**

WHEREAS the Parties recognize that each other's business involves specialized and proprietary knowledge, information, methods, processes, techniques and skills peculiar to their security and growth and that any disclosure of such methods, processes, skills, financial data, or other confidential and proprietary information

would substantially injure a Party's business, impair a Party's investments and goodwill, and jeopardize a Party's relationship with a Party's clients and customers; and

WHEREAS in the course of consultation with respect to the potential business venture, the Parties anticipate disclosing to each other certain information of a novel, proprietary, or confidential nature, and desire that such information be subject to all of the terms and conditions set forth herein below;

NOW THEREFORE the Parties hereto, in consideration of the promises and other good and valuable consideration, agree such information shall be treated as follows:

1. ***Confidential Information: "Confidential Information"*** shall mean and include any information which relates to the financial and/or business operations of each Party, including but not limited to, specifications, drawings, sketches, models, samples, reports, forecasts, current or historical data, computer programs or documentation and all other technical, financial or business data, information related to each Party's customers, products, processes, financial condition, employees, intellectual property, manufacturing techniques, experimental work, trade secrets.

2. **Use of Confidential Information:** The Vendor/Receiving Party agrees not to use the Bank/Disclosing Party's confidential Information for any purpose other than for the specific consultation regarding the potential business venture. Any other use of such Confidential Information by the Receiving Party shall be made only upon the prior written consent from an authorized representative of the Disclosing Party which wishes to disclose such information or pursuant to subsequent agreement between the Parties hereto.

3. **Restrictions:** Subject to the provisions of paragraph 4 below, the Party receiving Confidential Information (the "Receiving Party") shall, for contract period of Five(5) years from the date of the last disclosure of Confidential Information made under this Agreement (except for personal customer data which shall remain confidential forever), use the same care and discretion to limit disclosure of such Confidential Information as it uses with similar confidential information of its own and shall not disclose, lecture upon, publish, copy, modify, divulge either directly or indirectly, use(except as permitted above under clause (2) or otherwise transfer the Confidential Information to any other person or entity, including taking reasonable degree of care and steps to:

a) Restrict disclosure of Confidential Information solely to its concerned employees, agents, advisors, consultants, contractors and /or subcontractors with a need to know and not disclose such proprietary information to any other parties; and

b) Advise all receiving Party's employees with access to the Confidential Information of the obligation to protect Confidential Information provided hereunder and

obtain from agents, advisors, contractors and/or consultants an agreement to be so bound.

c) Use the Confidential Information provided hereunder only for purposes directly related to the potential business venture.

4. Exclusions: The obligations imposed upon Receiving Party herein shall not apply to information, technical data or know how, whether or not designated as confidential, that:

a) Is already known to the Receiving Party at the time of the disclosure without an obligation of confidentiality;

b) Is or becomes publicly known through no unauthorized act of the Receiving Party;

c) Is rightfully received from a third Party without restriction and without breach of this Agreement;

d) Is independently developed by the Receiving Party without use of the other Party's Confidential Information and is so documented;

e) Is disclosed without similar restrictions to a third party by the Party owning the Confidential Information;

f) Is approved for release by written authorization of the Disclosing Party; or

g) Is required to be disclosed pursuant to any applicable laws or regulations or any order of a court or a governmental body; provided, however, that the Receiving Party shall first have given notice to the Disclosing Party and made a reasonable effort to obtain a protective order requiring that the Confidential Information and/or documents so disclosed be used only for the purposes for which the order was issued.

5. Return of Confidential Information: All Confidential Information and copies and extracts of it shall be promptly returned by the Receiving Party to the Disclosing Party at any time within thirty (30) days of receipt of a written request by the Disclosing Party for the return of such Confidential Information.

6. Ownership of Information: The Receiving Party agrees that all Confidential Information shall remain the exclusive property of the Disclosing Party and its affiliates, successors and assigns.

7. No License Granted: Nothing contained in this Agreement shall be construed as granting or conferring any rights by license or otherwise in any Confidential Information disclosed to the Receiving Party or to any information, discovery or improvement made, conceived, or acquired before or after the date of this Agreement. No disclosure of any Confidential Information hereunder shall be construed by the Receiving Party to be a public disclosure of such Confidential Information for any purpose whatsoever.

8. **Breach:** In the event the Receiving Party discloses, disseminates or releases any Confidential Information received from the Disclosing Party, except as provided above, such disclosure, dissemination or release will be deemed a material breach of this Agreement and the Disclosing Party shall have the right to demand prompt return of all Confidential Information previously provided to the Receiving Party and in such case, the Receiving party shall be bound to return all information within 30 days from the date of such demand. The provisions of this paragraph are in addition to any other legal right or remedies, the Disclosing Party may have under the Law for the time being in force.

9. Arbitration and Equitable Relief

(a) Arbitration: The Parties shall endeavor to settle any dispute/difference arising out of or relating to this Agreement through consultation and negotiation. In the event no settlement can be reached through such negotiation and consultation, the Parties agree that such disputes shall be referred to and finally resolved by arbitration under the provisions of the Arbitration and Conciliation Act, 1996 and the rules made thereunder from time to time. The arbitration shall be held in Kolkata. The language used in the arbitral proceedings shall be English. The arbitration proceeding shall be conducted by a panel of three arbitrators, each party shall appoint his own arbitrator and the two appointed arbitrators shall appoint the third arbitrator who shall act as presiding Arbitrator.

(b) Equitable Remedies: The Parties agree that in event of breach of any of the covenants contained in this Agreement due to negligence/fault/laches of the Receiving Party, the Disclosing party shall have, in addition to any other remedy, the right:

i) To obtain an injunction from a court of competent jurisdiction restraining such breach or threatened breach; and

ii) To specific performance of any such provisions of this Agreement. The Parties further agree that no bond or other shall be required in obtaining such equitable relief and the Parties hereby consent to the issuance of such injunction and to the ordering of specific performance.

(c) Legal Expenses: If any action and proceeding is brought for the enforcement of this Agreement, or because of an alleged or actual dispute, breach, default, or misrepresentation in connection with any of the provisions of this Agreement, each Party will bear its own expenses, including the attorney's fees and other costs incurred in such action.

(d) Indemnification: The Receiving Party shall indemnify the Bank and hold the Bank harmless against any loss caused to it as a result of the non-performance or improper performance of this Agreement by the Receiving Party, or its servants

or agents to perform any aspect of its obligations forming part of the subject matter of this Agreement.

10. **Term:** This Agreement may be terminated by either Party giving ninety (90) days' prior written notice to the other Party; provided, however, the obligations to protect the Confidential Information in accordance with this Agreement shall survive for a period of five (5) years from the date of the last disclosure of Confidential Information made under this Agreement (except for personal customer data which shall remain confidential forever).

11. **No Formal Business Obligations:** This Agreement shall not constitute create, give effect to or otherwise imply a joint venture, pooling arrangement, partnership, or formal business organization of any kind, nor shall it constitute, create, give effect to, or otherwise imply an obligation or commitment on the part of either Party to submit a proposal or to perform a contract with the other Party or to refrain from entering into an agreement or negotiation with any other Party. Nothing herein shall be construed as providing for the sharing of profits or loss arising out of the efforts of either or both Parties. Neither Party will be liable for any of the costs associated with the other's efforts in connection with this Agreement. If the Parties hereto decide to enter into any licensing arrangement regarding any Confidential Information or present or future patent claims disclosed hereunder, it shall only be done on the basis of a separate written agreement between them.

12. General Provisions

(a) **Governing Law:** This Agreement shall be governed by and construed in accordance with the laws of India.

(b) **Severability:** If one or more of the provisions in this Agreement is deemed void by law, then the remaining provisions shall remain valid and continue in full force and effect.

(c) Successors and Assign: This Agreement will be binding upon the successors and/or assigns of the Parties, provided however that neither Party shall assign its rights or duties under this Agreement without the prior written consent of the other Party.

(d) Headings: All headings used herein are intended for reference purposes only and shall not affect the interpretation or validity of this Agreement.

(e) Entire Agreement: This Agreement constitutes the entire agreement and understanding of the Parties with respect to the subject matter of this Agreement. Any amendments or modifications of this Agreement shall be in writing and executed by a duly authorized representative of the Parties.

(f) Jurisdiction of Court: All disputes under this Non-Disclosure Agreement are subject to the jurisdiction of Courts of Kolkata only.

***(g)* Two original sets of Non-Disclosure Agreement are executed and retained by either parties, Bank and _____ (the Bidder).**

The Parties, by the signature of their authorized representatives appearing below, acknowledge that they have read and understood each and every term of this Agreement and agree to be bound by its terms and conditions.

For and on behalf of
……

Signature: _____
Name: _____
Designation: _____
Date: _____

For and on behalf of
……
(The* Bidder*)

Signature: _____
Name: _____
Designation: _____
Date: _____

Annexure – R - Compliance Statement participating in Reverse Auction

Compliance Statement

(To be submitted by all the bidders participating in Reverse Auction)

The Deputy General Manager
DIT, BPR & BTD
UCO Bank, Head Office
5th Floor, 3&4, DD Block, Sector-I
Salt Lake, Kolkata -700064

DECLARATION

1. We_____ (Name of the company)here by confirm having Submitted our bid for participating in Bank's **RFP Ref No.: DIT/BPR&BTD/OA/ 5033/2018-19 Date: 15/02/2019** for UCO Bank.
2. We confirm having read and understood the terms and conditions of the RFP as well as the Procedures relating to the process.
3. We here by undertake and agree to abide by all the terms and conditions stipulated by the Bank in the RFP document including all annexures and the Procedure for Reverse Auction.
4. We shall participate in the on-line auction conducted by M/s. _____ System Ltd(auction service provider retained by the Bank)and submit our commercial bid. In doing so, we shall abide by the procedures prescribed for online auction by the auction company.
5. We, here by confirm that we will honor the Bids placed by us during the auction process, failing which we shall forfeit the EMD and shall be liable for any other consequential action that may be taken by the Bank including any debarment from participation in future procurement by the Bank.
6. We confirm having nominated our representative (Shri/Smt/Ms_____ designated_____ as of our company to participate in the Reverse auction on behalf of the company. We undertake that the company shall be bound by the actions made by him during the Reverse Auction process and thereafter.
7. We undertake to submit the confirmation of last bid price by us to the Bank within next day before 4 PM hours of the completion of event and any other specific requirement indicated in the RFP.

Signature with company seal Name-

Company /Organization - Designation within Company / Organization - Address of Company' Organization-

Date:

Name of Authorized Representative: -
Designation of Authorized Representative:
Signature of Authorized Representative

Letter of Authority for Participation in Reverse Auction

The Deputy General Manager
DIT, BPR & BTD
UCO Bank, Head Office
5th Floor, 3&4, DD Block, Sector-I
Salt Lake, Kolkata -700064

1. We_____ (Name of the company)have submitted our bid for participating in Bank's RFP_____ Dated_____for UCO Bank.
2. We confirm having read and understood the terms of RFP as well as the Procedure relating to the Reverse Auction for this RFP process.
3. As per the terms of RFP and Business rules, we nominate (Shri/Smt./Ms_____), designated as_____of our company to participate in the Reverse auction, who shall be the sole and single point of contact for any all matters relating to the Reverse Auction.
4. We accordingly authorize Bank and/or the Auction Company to issue user ID and password to the above named official of the company.

Signature with company seal Name-
Company/ Organization-Designation within Company/Organization-
Address of Company' Organization-
Date:

Name of Authorized Representative: -
Designation of Authorized Representative:
Signature of Authorized Representative:

PROFORMA FOR DEED OF INDEMNITY
(To be stamped as per the Stamp Law of the Respective State)

This Deed of Indemnity executed at …….. On the _____ day of _____ by M/s _____(hereinafter referred to as "the Obligor" which expression shall unless it be repugnant to the context, subject or meaning thereof, shall be deemed to mean and include successors and permitted assigns);

IN FAVOUR OF

UCO Bank a body corporate constituted under the Banking Companies (Acquisition and transfer of undertakings) Act, 1970, having its Head Office at No. 10, BTM Sarani, Kolkata-700001(hereinafter referred to as "UCO Bank", which expression unless expressly excluded or repugnant to the context shall also include its successor, assigns, attorneys, agents, representatives, authorized officer and all and any such officer having the power and authority to represent the Bank).

WHEREAS

1. The Obligor has

   A. offered to provide solution for the Implementation, Maintenance and Facility Management for System Security Tools for Cyber Security Operation Centre (C-SOC) with the specifications as prescribed in the Agreement / Contract dated _____ during the period of **five years** from the date of acceptance of the purchase orders issued by the Bank from time to time. The Supply of solution by the obligor is herein after referred to as "**Supply**".

   B. Agreed to install and provide comprehensive maintenance for the Equipments, material used and workmanship by them in terms of the Agreement / Contract dated _____ and respective Purchase Orders issued from time to time during the warranty period of **36 months** and also during the post warranty period if required at the discretion of UCO BANK. (The installation and maintenance are herein after collectively referred to as "**Service/s**").

   C. Represented and warranted that they have all permissions, consents, approvals from all authorities, both regulatory and non-regulatory, for providing solution for the Implementation, Maintenance and Facility Management for System Security Tools for Cyber Security Operation Centre (C-SOC).

   D. Represented and warranted that the aforesaid supply/services offered to UCO BANK do not violate any provisions of the applicable laws, regulations or guidelines including legal and environmental. In case there is any violation of any law, rules or regulation, which is capable of being remedied, the same will be got remedied immediately during the installation, maintenance and contract period

to the satisfaction of UCO BANK.

E. Represented and warranted that they are authorized and legally eligible and otherwise entitled and competent to enter into such Contract/ Agreement with UCO BANK.

2. One of the conditions of the aforesaid Agreement is that the Obligor is required to furnish an indemnity in favor of UCO BANK indemnifying the latter against any claims, losses, costs, actions, suits, damages and / or otherwise arising due to or on account of Obligor's violations of any trademarks, patents, copyrights and licenses, the applicable laws, regulations, guidelines during the Supply / Services to UCO BANK as also for breach committed by the Obligor on account of misconduct, omission and negligence by the Obligor.

3. In pursuance thereof, the Obligor has agreed to furnish an indemnity in the form and manner and to the satisfaction of UCO BANK as hereinafter appearing;

NOW THIS DEED WITNESSETH AS UNDER:-

In consideration of UCO BANK having agreed to award the aforesaid contract to the Obligor, more particularly described and stated in the aforesaid Agreement/Contract, the Obligor do hereby agree and undertake that:-

(1) the Obligor shall, at all times hereinafter, save and keep harmless and indemnified UCO BANK, including its respective directors, officers, and employees and keep them indemnified from and against any claim, demand, losses, liabilities or expenses of any nature and kind whatsoever and by whomsoever made in respect of the said contract and any damage caused from and against all suits and other actions that may be instituted taken or preferred against UCO BANK by whomsoever and all losses, damages, costs, charges and expenses that UCO BANK may incur by reason of any claim made by any claimant for any reason whatsoever or by anybody claiming under them or otherwise for any losses, damages or claims arising out of all kinds of accidents, destruction, deliberate or otherwise, direct or indirect, from those arising out of violation of applicable laws, regulations, guidelines and also from the environmental damages, if any, which may occur during the contract period.

(2) The Obligor further agrees and undertakes that the Obligor shall, during the contract period, ensure that all the permissions, authorizations, consents are obtained from the local and/or municipal and/or governmental authorities, as may be required under the applicable laws, regulations, guidelines, orders framed or issued by any appropriate authorities.

(3) The Obligor further agrees to provide complete documentation of all Equipments/accessories/and other software, they are having. The Obligor shall also indemnify and keep indemnified UCO BANK against any levies/penalties/claims/demands, litigations, suits, actions, judgments, in this regard.

(4) If any additional approval, consent or permission is required by the Obligor to execute and perform the contract during the currency of the contract, they shall procure the same and/or comply with the conditions stipulated by the concerned authorities without any delay.

(5)The obligations of the Obligor herein are irrevocable, absolute and unconditional, in each case irrespective of the value, genuineness, validity, regularity or enforceability of the aforesaid Agreement/Contract or the insolvency, bankruptcy, reorganization, dissolution, liquidation or change in ownership of UCO BANK or Obligor or any other circumstance whatsoever which might otherwise constitute a discharge or defence of an indemnifier.

(6) The obligations of the Obligor under this deed shall not be affected by any act, omission, matter or thing which, would reduce, release or prejudice the Obligor from any of the indemnified obligations under this indemnity or prejudice or diminish the indemnified obligations in whole or in part, including in law, equity or contract (whether or not known to it, or to UCO BANK).

(7) This indemnity shall survive the aforesaid Agreement.

(8) Any notice, request or other communication to be given or made under this indemnity shall be in writing addressed to either party at the address stated in the aforesaid Agreement and or as stated above.

(9) This indemnity shall be governed by, and construed in accordance with, the laws of India. The Obligor irrevocably agrees that any legal action, suit or proceedings arising out of or relating to this indemnity may be brought in the Courts/Tribunals at Kolkata. Final judgment against the Obligor in any such action, suit or proceeding shall be conclusive and may be enforced in any other jurisdiction, by suit on the judgment, a certified copy of which shall be conclusive evidence of the judgment, or in any other manner provided by law. By the execution of this indemnity, the Obligor irrevocably submits to the exclusive jurisdiction of such Court/Tribunal in any such action, suit or proceeding.

(10) UCO BANK may assign or transfer all or any part of its interest herein to any other person. Obligor shall not assign or transfer any of its rights or obligations under this indemnity, except with the prior written consent of UCO BANK

IN WITNESS WHEREOF the Obligor has signed these presents on the day, month and year first above written.

Signed and Delivered on behalf of (_____**)**

By the hand of (_____) the authorized official of the Obligor)