2018-19

इंडियन बैंक
Indian Bank

Request for Proposal for Supply and Maintenance of Application Security Testing Solution

RFP No. CO:ITD:CDC:1049/R1:2018-19 dated 24/10/2018.

Information Technology Department
Corporate Office , 254-260, Avvai
Shanmugham Salai, Royapettah
Chennai -600014
10/24/2018

Abbreviations	
IT	Information Technology
AMC	Annual Maintenance Cost
ATS	Annual Technical Support
OEM	Original Equipment Manufacturer
OSD	Original Software Developer
API	Application Programming Interface
ATM	Automated Teller Machine
CSRF	Cross-Site Request Forgery
DOM	Document Object Model
IPS	Intrusion Prevention System
SIEM	Security Information And Event Management
SAST	Static Application Security Testing
DAST	Dynamic Application Security Testing
OWASP	Open Web Application Security Project
IST	Indian Standard Time
DD	Demand Draft
BG	Bank Guarantee
EMD	Earnest Money Deposit
IP	Intellectual Property
PSU	Public Sector Undertaking
RFP	Request For Proposal

1. Invitation for Bids

Indian Bank is a Premier Nationalised Bank with over 2800 Branches. The Bank had been a forerunner in absorption of technology and has many first to its credit in implementation of IT in Banking. The Bank has overseas presence through one Branch each in Singapore, Colombo & Jaffna and has reciprocal arrangements with various Foreign Banks across the globe. Core Banking Solution has been implemented in all the Branches. The Bank has introduced Debit Cards, Credit Cards and Exclusive Credit Card "Bharat Card" for common man – first of its kind in the Banking industry. Banking services are offered through Multiple Delivery Channels like ATM, Internet Banking, Telebanking, Mobile Banking etc. The Bank is also partnering various e-governance initiatives of Govt of India and State Governments.

The Bank invites sealed bids from eligible bidders for the Supply, Installation, Integration and Maintenance of Application Security Testing solution. Part-I of the Bid Document will consist of Technical and other details. Part II of the Bid Document will have commercials, which should include price breakup details and to be submitted after online reverse auction process. Both Part I and Part II should be submitted manually.

Interested eligible bidders if required may obtain further information from the Bank, at the address given below from 10:00 hours to 17.00 hours on all working days from Monday to Saturday (except 2nd and 4th Saturdays of the month).

The address for communication is:-

Assistant General Manager,
Information Technology Department,
Indian Bank Head Office,
2nd floor,
66, Rajaji Salai, Chennai, India – 600001.
Phone: 044 -25279830
E-Mail - krishna.cp@indianbank.co.in
jayasankar.clbk@indianbank.co.in
uthayakumar.p@indianbank.co.in

The Bidder has to submit bid fee in the form of DD for Rs.2,000/- (Rupees Two Thousand only) at the time of pre-bid meeting. If bidder is not attending the pre-bid meeting then the DD should be submitted along with bid.

Bids must be delivered on or before 15.00 Hours IST on 14/11/2018 and must be accompanied by a Bid Security of Rs.50,000/- (Rupees Fifty Thousand only).

Late Bids will be summarily rejected. Part I of the Bid (consisting of Bid Form, Bid Security Form, Manufacturer's Authorisation Form & Partnership certificate, Qualification Criteria, and Undertaking of Authenticity) will be opened by the Bank at 15.30 Hours IST on 14/11/2018 in the presence of Bidders' representatives at Indian Bank Corporate Office, Chennai.

Interested Bidders may send their representative to participate in the Bid Opening process. After technical evaluation, only the eligible bidders will be communicated of the date and time of reverse auction.

Benefits to Micro and Small Enterprises (MSEs) as per the guidelines of Public Procurement Policy issued by Government of India:

(i) As per the above policy, Bank reserves the rights to procure 20% of the total requirements, from Micro and Small Enterprises (MSEs) provided such MSEs are complying with the eligibility criteria and technical specifications of the RFP, quote their price within the price band of L1+15% and agree to bring down their price to L1 price.

(ii) If L1 bidder is an MSE, 100% procurement will be done from the L1 bidder subject to the other terms and conditions of the RFP.

(iii) In case of more than one such MSE, the supply shall be shared proportionately to tender quantity.

(iv) Special provision for Micro & Small Enterprises owned by Scheduled Castes or Scheduled Tribes. 4% out of the 20% shall be allotted to such MSEs, if participated in the tender.

(v) MSEs are also exempted from payment of cost of bid documents and submission of bid security.

(vi) To avail the above benefits, the bidder should have registered with District Industries Centres or Khadi and Village Industries Commission or Khadi and Village Industries Board or Coir Board or National Small Industries Corporation or Directorate of Handicrafts and Handloom or any other body specified by Ministry of Micro, Small and Medium Enterprises.

(vii) Bidders seeking the above benefits shall submit the documentary proof for having registered with the above agencies (such as Entrepreneur's Memorandum – EM II, NSIC certificate/ Udyog Aadhar Memorandum) at the time of pre-bid meeting or during submission of the technical bids (only if the bidder is not attending the pre-bid meeting).

2. Instructions to Bidders

2.1 Introduction

The Bidder is expected to read the instructions, forms, terms and specifications in the Bidding Documents. Failure to furnish all information required by the Bidding Documents may result in the rejection of its bid and will be at the Bidder's own risk.

2.2 Pre-bid meeting

2.2.1 A pre-bid meeting is scheduled to be held at the following address at 11.00 hours IST on 30/10/2018. Bidder's designated representatives (maximum two persons) may attend the pre-bid meeting.

Information Technology Department,
Indian Bank Head Office,
2nd floor,
66, Rajaji Salai, Chennai, India – 600001.

2.2.2 The purpose of the meeting will be to clarify the doubts raised by the probable bidders.

2.2.3 The bidder is requested to submit any queries/clarifications to the Bank at least two (2) days before the date of meeting.

2.2.4 The Bidder has to submit bid fee in the form of DD for Rs.2,000/- (Rupees Two Thousand only) at the time of pre-bid meeting. If bidder is not attending the pre-bid meeting then the DD should be submitted along with bid.

2.2.5 The text of the queries (without identifying the source of enquiry) and the responses given, together with amendment to the bid document, if any, will be ported in the Bank's website.

2.3 Amendment of bidding documents

2.3.1 At any time prior to the deadline for submission of bids, the Bank, for any reason, whether at its own initiative or in response to a clarification requested by prospective Bidder(s), may modify the Bidding Document by Amendment(s).

2.3.2 All prospective Bidders may check the Bank's website for amendment(s) and it will be binding on them.

2.4 Documents constituting the bid

2.4.1 The Part-I of the Bid prepared by the Bidder shall comprise the following components:

a) Technical Bid

The Bidder shall furnish as part of their bid, documents establishing the Bidder's eligibility to bid and their qualifications to perform the Contract, if their bid is accepted. As part of their bid, the bidder should submit documents agreeing to the bid's terms and conditions. The documentary evidence of the Bidder's qualifications to perform the Contract if their bid is accepted shall be established to the Bank's satisfaction:

i) that, the Bidder has the financial and technical capability necessary to perform the Contract;
ii) that, the Bidder meets the Qualification requirements.

b) A Bid Form of the Bid Document as per format in section 6.
c) Bid security (Earnest Money Deposit) for Rs.50,000/- (Rupees Fifty Thousand only).
d) DD for Rs.2,000/- (Rupees Two Thousand only), towards cost of the bid if the bidder has not attended the pre-bid meeting
e) An undertaking from the bidder that the bidder will extend support for a period of three (3) years from the date of delivery.
f) Other documents as mentioned in Checklist in section 19.

2.4.2 The Part-II of the Bid prepared by the Bidder shall comprise the commercial bid as per the format provided in section 17.

The Bank may, at its discretion, reject any bid document not accompanied by the above.

2.5 Documents establishing goods' conformity to Bidding Documents

2.5.1 The Bidder shall furnish, as part I of their bid, documents establishing conformity to the Bidding Documents of all goods and services, which the Bidder proposes to supply under the Contract.

2.5.2 The documentary evidence of conformity of the goods and services to the Bidding Documents may be in the form of literature, drawings and data, and shall consist of:

a) a detailed description of essential technical and performance characteristics of the goods;
b) an item-by-item commentary of the Purchaser's Technical Specifications demonstrating responsiveness of the goods and services to those specifications (compliance matrix as per format specified in section 20), or a statement of deviations and exceptions to the provisions of the Technical Specifications.

2.6 Bid Security (Earnest Money Deposit)

The Bidder shall furnish, as part of their bid, a Bid Security in the form of a Bank Guarantee issued by a Scheduled Commercial Bank located in India, as per the format provided in section 8 for a sum of Rs.50,000/- (Rupees Fifty Thousand only) and valid for One Hundred and Thirty Five (135) days from the last date for submission of Bid. The Bank may seek extension of Bank Guarantee, if required.

2.6.1 Unsuccessful Bidders' Bid Security will be discharged or returned after the issue of purchase order to the L1 bidder.

2.6.2 The successful Bidder's Bid Security will be discharged upon the Bidders signing the Contract and furnishing the Performance Security.

2.6.3 The bidder will forfeit the Bid Security

a) If the bidder withdraws its bid during the period of bid validity.
(or)
b) in the case of a Successful Bidder, if the Bidder fails to sign the Contract or to furnish Performance Security.

2.7 Period of validity of bids

Bids shall remain valid for the period of Ninety (90) days after the last date for submission of bid prescribed. A bid valid for a shorter period shall be rejected by the Bank as non-responsive. The Bank may seek extension of bid validity, if required.

2.8 Format and signing of Bid

2.8.1 The person or persons signing the bid shall sign all pages of the bid document, except for un-amended printed literature.

2.8.2 Any interlineations, erasure or overwriting shall be valid only if they are signed by the person or persons signing the Bid.

2.8.3 The Bidder should use the Bank's format downloaded from website for giving their compliance. Use of any other format shall make their bid liable for rejection.

2.9 Sealing and marking of Bids

2.9.1 The Bidder shall seal the Part I of the bid in separate envelope, duly marking the envelope as "Supply, Installation, Integration and Maintenance of Application Security Testing solution" – PART I – Technical". This envelope should be kept in a bigger sealed envelope duly marked as Bid for "Supply, Installation, Integration and Maintenance of Application Security Testing solution".

2.9.2 The envelope shall:

2.9.2.1 be addressed to the Bank at the address given below;

Assistant General Manager,
Expenditure Department,
Indian Bank Corporate Office,
254-260, Avvai Shanmugam Salai,
Royapettah, Chennai, India - 600014.

2.9.2.2 bear the Project name and a statement: "DO NOT OPEN BEFORE 15.30 Hours IST on 14/11/2018", to be completed with the time and the date specified below.

2.10 Deadline for submission of Bids

2.10.1 Deadline for bid submission is 14/11/2018, 15.00 hours IST. The Bid Document along with required enclosures should be submitted at the place mentioned in clause 2.9.2.1 either in person or by post, but it should reach the concerned officer on or before 15.00 hours IST on 14/11/2018.

2.10.2 In the event of the specified date for the submission of bids, being declared a Holiday for the Bank, the bids will be received up to the appointed time on the next working day.

2.10.3 The Bank may, at its discretion, extend this deadline for the submission of bids by amending the Bid Documents, in which case all rights and obligations of the Bank and Bidders previously subject to the deadline will thereafter be subject to the deadline as extended.

2.10.4 Any bid received by the Bank after the deadline for submission of bids prescribed by the Bank will summarily be rejected and returned unopened to the Bidder.

2.11 Opening of Bids by Bank

2.11.1 The bids (PART–I) will be opened at 15.30 hours IST on 14/11/2018. Bidder may send their representative during opening of the bid.

2.11.2 The Bidders' names, bid modifications or withdrawals and the presence or absence of the requisite bid security and such other details as the Bank, at its discretion, may consider appropriate, will be announced at the bid opening. No bid shall be rejected at bid opening, except late bids, which shall be returned unopened to the Bidder.

2.11.3 The technically qualified Bidders will be intimated to participate in the reverse auction, to identify Lowest Quoted (L1) Bidder.

2.12 Clarification of Bids

During evaluation of the bids, the Bank may, at its discretion, seek clarification(s) from the Bidder(s). The request for clarification(s) and the response(s) shall be in writing, and no change in the substance of the bid shall be sought, offered, or permitted.

2.13 Evaluation Criteria

2.13.1 General /Technical Evaluation

a) The Bank will examine the bids to determine whether they are complete, whether required sureties have been furnished, whether the documents have been properly signed, and whether the bids are generally in order.

b) The Bank may waive any minor informality, non-conformity, or irregularity in a bid which does not constitute a material deviation, provided such waiver does not prejudice or affect the relative ranking of any Bidder.

c) Prior to the detailed evaluation, the Bank will determine the substantial responsiveness of each bid to the bidding documents. For purposes of these Clauses, a substantially responsive bid is one, which conforms to all the terms and conditions of the Bidding Documents without material deviations.

d) The Bidder should meet all the Qualification Criteria mentioned in Section 5.

e) The Licences offered should meet all the Technical Specifications as stipulated in the bid.

f) The bidder should extend support for the quoted software for a period of three (3) years from the date of delivery.

g) The bidder will be given sample code(s) and asked to do a proof of concept.

2.13.2 Commercial Evaluation

a) Technically qualified Bidders will be intimated to participate in the reverse auction to identify L1 (lowest quoted) Bidder for awarding contract.

b) The comparison shall be between the prices quoted. The price should be

(i) Inclusive of all Duties, Levies, Delivery, installation and support etc.

(ii) Exclusive of Taxes only. TDS, if applicable, will be deducted as per the applicable rates from the payment.

c) Arithmetical errors will be rectified on the following basis.

(i) If there is a discrepancy between the unit price and the total price that is obtained by multiplying the unit price and quantity, the unit price shall prevail and the total price shall be corrected.

(ii) If there is a discrepancy between words and figures, the amount in words will prevail.

If the Supplier does not accept the correction of the errors, such quote will be rejected and they shall forfeit the Bid Security.

d) After the reverse auction, the successful (L1) bidder has to submit the commercial quote as per format provided in section 17.

2.14 Bank's right to accept any bid and to reject any or all bids

The Bank reserves the right to accept or reject any bid/all bids and annul the bidding process at any time prior to awarding contract, without assigning any reason and without thereby incurring any liability to the affected Bidder or Bidders.

2.15 Bank's right to vary quantities

The Bank reserves the right to increase or decrease, by Twenty Five percent (25%), the quantity specified in the schedule of requirements (Section 4) without any change in unit price and other terms and conditions. If Bank decides to procure up to Twenty Five percent (25%) over and above the quantity of Licences mentioned in this RFP from the awardee of the Contract, Repeat Order will be placed within One (1) year from the date of original purchase order at the same price and terms & conditions of this tender/contract.

2.16 Performance Security

On receipt of notification of award from the Bank, the Successful Bidder shall furnish the Performance Security in accordance with the Conditions of Contract, in the Performance Security format provided in section 10.Failure of the Successful Bidder to comply with the requirement of

signing of Contract and Performance Security shall constitute sufficient grounds for the annulment of the award and forfeiture of the Bid Security submitted by the successful bidder.

2.17 Awarding of Contract

The Purchase Order will be issued to lowest quoted (L1) Bidder. Acceptance of Purchase Order should be submitted within Seven (7) days from the date of issue of the Purchase Order along with Authorisation Letter.

2.18 Signing of Contract

Within fifteen (15) days from the date of issue of the Purchase Order, the Successful Bidder shall sign the Contract and return it to the Bank.

2.19 Other Terms and Conditions

2.19.1 The cost of preparing the proposal including visit / visits to the Bank is not reimbursable.

2.19.2 The Bank is not bound to accept any of the proposals submitted and the Bank has the right to reject any/all proposal(s) or cancel the tender without assigning any reason therefor.

2.19.3 The Bank reserves the right to negotiate with the lowest quoted (L1) Bidder under exceptional circumstances.

2.19.4 Either the Agent on behalf of the Principal or the Principal directly could bid in a tender but not both.

2.19.5 All pages of the Bid Document, Clarifications/Amendments if any should be signed by the Authorised Signatory (POA proof to be submitted) and kept with Part-I. A certificate of authorisation should also be attached along with the Part-I.

2.19.6 The supplier has to be provide names of two buyers to whom similar items are supplied in the recent past, as per the format in section 12, and to whom reference may be made by the Bank regarding the bidder's technical and delivery ability:

1. ----------
2. ----------

2.19.7 Bids submitted shall also include the following.
Copies of original documents defining the constitution or legal status, place of registration and principal place of business of the Company.

The Bidder should furnish a brief write-up, backed with adequate data, explaining its available experience (both technical and commercial) for the Supply, Installation, Integration and Maintenance of Application Security Testing solution within the specified time of completion after meeting all their current commitments.

Reports on financial standing of the bidder such as Profit and Loss Statements, Balance Sheet for the past three years.

2.20 SLA, Uptime and Penalty

2.20.1 Service Level Agreement (SLA): Software implementation and maintenance including 24*7 onsite support on call basis. Uptime of 97% to be maintained, calculated on a 24*7 basis per quarter for every installation. The penalty applicable for every 0.1% drop in uptime is 0.1% of the total cost of software whichever is impacted, up to a maximum deduction of Ten percent (10%). This penalty is exclusive of other penalties and reinstatement charges if any, levied by the OEM.

2.20.2 Penalty for non-adherence: If the OEM imposes any reinstatement charges, the same shall be borne by the vendor and the bank shall not be liable to pay any charges to the vendor over and above the order value in this contract.

3. Conditions of Contract

3.1 Definitions

In this contract, the following terms shall be interpreted as indicated:

3.1.1 "The Contract" means the agreement entered into between the Purchaser and the Supplier, as recorded in the Contract Form signed by the parties, including all the attachments and appendices thereto and all documents incorporated by reference therein;
3.1.2 "The Contract Price" means the price payable to the Supplier under the Contract for the full and proper performance of its contractual obligations;
3.1.3 "The Goods" means all of the equipment, machinery, and / or other materials which the Supplier is required to supply to the Purchaser under the Contract;
3.1.4 "The Services" means those services ancillary to the supply of the Goods, such as transportation and insurance, and any other incidental services, such as installation, commissioning, provision of technical assistance, training and other such obligations of the Supplier covered under the Contract;
3.1.5 "The Purchaser" means Indian Bank.
3.1.6 "The Supplier" means the Company supplying the Goods and Services under this Contract.
3.1.7 "The Project Site", where applicable, means the place of installation of item.

3.2 Use of Contract Documents and Information

3.2.1 The Supplier shall not, without the Purchaser's prior written consent, disclose the Contract, or any provision thereof, or any specification, plan, drawing, pattern, sample or information furnished by or on behalf of the Purchaser in connection therewith, to any person other than a person employed by the Supplier in the performance of the Contract. Disclosure to any such employed person shall be made in confidence and shall extend only so far as may be necessary for purposes of such performance.
3.2.2 The Supplier shall not, without the Purchaser's prior written consent, make use of any document or information pertaining to this contract except for purposes of performing the Contract.

3.3 Patent Rights

The Supplier shall indemnify the Purchaser against all third-party claims of infringement of patent, trademark or industrial design rights arising from use of the Goods or any part thereof.

3.4 Performance Security

3.4.1 Within fifteen (15) days from the date of issue of the Purchase Order, the supplier shall furnish to the Bank the Performance Security equivalent to ten percent (10%) of the Amount quoted for licenses, training and OEM update & support for three (3) years in the form of a Bank Guarantee, valid for thirty nine (39) months with further one (1) month claim period, in the format provided in section 10.
3.4.2 The Performance Security shall be invoked by the Bank as compensation for any loss resulting from the Supplier's failure to complete its obligations under the Contract.

3.4.3 If not invoked, the Performance Security will be discharged by the Bank and returned to the Supplier after expiry of claim period.

3.5 Delivery and Documents

The delivery of the Licence shall be made by the Supplier in accordance with the terms specified in the Schedule of Requirements in Section 4.

The details of documents to be furnished by the Supplier are as follows.

3.5.1 Copy of the Supplier Invoice showing contract number, description, quantity, unit price, total amount;
3.5.2 Delivery Note, acknowledgement of receipt of goods from the Consignee, if any.

3.6 Maintenance and Support (Warranty) Terms

The bidder has to provide support and maintenance (Warranty) for a period of three (3) years from the date of go-live (which is installation, successful demonstration and deployment in production of all software components of the Application security testing tool). The scope of work for the support and maintenance is given separately. The bidder has to quote price for the perpetual Licenses with OEM software update and support for three (3) years.

3.7 Payment

3.7.1 License Cost with ATS covering onsite support and updates:

S.No.	Stage	% of Payment [cost of licenses, training, OEM updates & support, warranty ,onsite support and maintenance cost for three (3) years]	Remarks
1	Delivery	70%	On delivery of all software, licenses, relevant documents and on submission of Performance guarantee, Contract Form, Non-Disclosure Agreement.
2	Installation, configuration, integration, commissioning and training	30%	After successful installation, configuration, integration, commissioning and training of the software as per the scope of work, technical and functional requirements and acknowledged by the bank with a sign off. The invoices and installation report should contain the serial number of the licenses and entitlement.

3.7.2 The payment will be released within 15 days of submission of a request letter along with Invoice, relevant documents and delivery challan duly acknowledged by official of the Bank.
3.7.3 Subsequent ATS Payment: Bank reserves the right to renew the ATS directly with OEM or through the same vendor (successful bidder) or any other partner of the OEM.

3.8 Change Orders

3.8.1 The Bank may at any time, by a written order given to the Supplier make changes within the general scope of the Contract.

3.8.2 If any such change causes an increase or decrease in the cost of, or the time required for, the Supplier's performance of any provisions under the Contract, an equitable adjustment shall be made in the Contract Price or delivery schedule, or both, and the Contract shall accordingly be amended. Any claims by the Supplier for adjustment under this clause must be asserted within thirty (30) days from the date of the Supplier's receipt of the Bank's change order.

3.9 Delays in the Supplier's Performance

3.9.1 Delivery of the Goods and performance of Services shall be made by the Supplier in accordance with the time schedule prescribed by the Bank in the Schedule of Requirements in section 4.

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

3.10 Liquidated Damages

If the Supplier fails to deliver any or all of the Goods or to perform the Services within the period(s) specified in the Contract, the Bank shall, without prejudice to its other remedies under the Contract, deduct from the Contract Price, as liquidated damages, a sum equivalent to 0.5% of the Invoice price for each week or part thereof of delay until actual delivery or performance, up to a maximum deduction of ten percent (10%). If the Licenses are not delivered in time, the Bank may consider termination of the contract.

3.11 Termination for Default

3.11.1 The Bank, without prejudice to any other remedy for breach of contract, by Thirty (30) days written notice of default sent to the Supplier, may terminate this Contract in whole or in part :

a) if the Supplier fails to deliver any or all of the Goods within the period(s) specified in the Contract, or within any extension thereof granted by the Bank;
b) if the Supplier fails to perform any other obligation(s) under the Contract.
c) If the Supplier, in the judgement of the Bank has engaged in corrupt or fraudulent practices in competing for or in executing the Contract.

For the purpose of this clause:
"**corrupt practice**" means the offering, giving, receiving or soliciting of anything of value to influence the action of a public 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 a contract to the detriment of the Bank, and includes collusive practice among Bidders (prior to or after bid submission) designed to establish bid prices at artificial non-competitive levels and to deprive the Bank of the benefits of free and open competition.

3.11.2 In the event the Bank terminates the Contract in whole or in part, the Bank may procure, upon such terms and in such manner as it deems appropriate, Goods or Services similar to those undelivered, and the Supplier shall be liable to the Bank for any excess costs for such similar Goods or Services. However, the Supplier shall continue performance of the Contract to the extent not terminated.

3.12 Force Majeure

3.12.1 The Supplier shall not be liable for forfeiture of its performance security, liquidated damages, or termination for default, if and to the extent that, it's delay in performance or other failure to perform its obligations under the Contract is the result of an event of Force Majeure.
3.12.2 For purposes of this clause, "Force Majeure" means an event beyond the control of the Supplier and not involving the Supplier's fault or negligence and not foreseeable. Such events may include, but are not restricted to, acts of the Bank in its sovereign capacity, wars or revolutions, fires, floods, epidemics, quarantine restrictions, and freight embargoes.
3.12.3 If a Force Majeure situation arises, the Supplier shall promptly notify the Bank in writing of such condition and the cause thereof. Unless otherwise directed by the Bank in writing, the Supplier shall continue to perform its obligations under the Contract as far as is reasonably practical, and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event.

3.13 Termination for Convenience

The Bank, by Thirty (30) days written notice sent to the Supplier, may terminate the Contract, in whole or in part, at any time for its convenience. The notice of termination shall specify that termination is for the Bank's convenience, the extent to which performance of the Supplier under the Contract is terminated, and the date upon which such termination becomes effective.

The Goods that are complete and ready for shipment within thirty (30) days after the Supplier's receipt of notice of termination shall be accepted by the Bank at the Contract terms and prices. For the remaining Goods, the Purchaser may elect:

3.13.1 to have any portion completed and delivered at the Contract terms and prices; and / or
3.13.2 to cancel the remainder and pay to the Supplier an agreed amount for partially completed Goods and Services and for materials and parts previously procured by the Supplier.

3.14 Settlement of Disputes

3.14.1 If any dispute or difference of any kind whatsoever shall arise between the purchaser and the supplier in connection with or arising out of the contract, the parties shall make every effort to resolve amicably such disputes or difference by mutual consultation.
3.14.2 If after thirty(30) days the parties have failed to resolve their disputes or difference by such mutual consultation, then either the purchaser or the supplier may give notice to the other party of its intention to commence arbitration, as hereinafter provided, as to the matter in dispute, and no arbitration in respect of this matter may be commenced unless such notice is given.
3.14.3 Any dispute or difference in respect of which a notice of intention to commence arbitration has been given in accordance with this clause shall be finally settled by arbitration. Arbitration may be commenced prior to or after delivery of the goods under the contract. Arbitration proceedings shall be conducted in accordance with the following rules of procedure. The dispute resolution mechanism to be applied shall be as follows:

a) In case of dispute or difference arising between the Purchaser and a domestic Supplier relating to any matter arising out of or connected with this agreement, such dispute or difference shall be settled in accordance with the Arbitration and Conciliation Act, 1996. The arbitral tribunal shall consist of three (3) arbitrators one each to be appointed by the Purchaser and the Supplier; the third Arbitrator shall be chosen by the two Arbitrators so appointed by the Parties and shall act as Presiding Arbitrator. In case of failure of the two arbitrators appointed by the parties to reach upon a consensus within a period of thirty(30) days from the appointment of the presiding Arbitrator, the Presiding Arbitrator shall be

appointed by the Indian Banks' Association, India which shall be final and binding on the parties.

b) If one of the parties fails to appoint its arbitrator within thirty(30)days after receipt of the notice of the appointment of its Arbitrator by the other party, then the Indian Banks' Association, both in cases of the Foreign Supplier as well as Indian Supplier, shall appoint the Arbitrator. A certified copy of the order of the Indian Banks' Association making such an appointment shall be furnished to each of the parties.
c) Arbitration proceedings shall be held at Chennai, India, and the language of the arbitration proceedings and that of all documents and communications between the parties shall be English.
d) The decision of the majority of arbitrators shall be final and binding upon both parties. The cost and expenses of Arbitration proceedings will be paid as determined by the Arbitral Tribunal. However, the expenses incurred by each party in connection with the preparation, presentation etc. of its proceedings as also the fees and expenses paid to the arbitrator appointed by such party or on its behalf shall be borne by each party itself.
e) Where the value of the contract is Rs. 10 million and below, the disputes or differences arising shall be referred to the Sole Arbitrator. The Sole Arbitrator shall be appointed by agreement between the parties; failing such agreement, by the appointing authority namely the Indian Banks' Association.

3.14.4 Notwithstanding any reference to arbitration herein,

a) the parties shall continue to perform their respective obligation under the contract unless they otherwise agree; and
b) the purchaser shall pay the supplier any monies due to the supplier.

Submitting to arbitration may be considered as an additional remedy and it does not preclude Parties to seek redressal/other legal recourse.

3.15 Limitation of Liability

Supplier'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 Supplier's gross negligence. For the purpose for the section, contract value at any given point of time, means the aggregate value of the purchase order placed by bank on the Supplier that gave rise to claim, under this tender.
c) Supplier shall not be liable for any indirect, consequential, incidental or special damages under the agreement/ purchase order.

3.16 Exit Requirements

In the event of Agreement comes to end on account of termination or by the expiry of the term/ renewed term of the Agreement or otherwise, the Successful bidder shall render all reasonable assistance and help to the Bank and to any new vendor engaged by the Bank, for the smooth switch over and continuity of the Services. Self-Declaration to this effect, as per format specified in section 16, should be submitted along with the bid.

3.17 Confidentiality

The Company and its employees either during the term or after the expiration of this contract shall not disclose any proprietary or confidential information relating to the project, the services, this contract, or the business or operations without the prior written consent of the Bank.

3.18 Applicable Law

The Contract shall be interpreted in accordance with the laws of India. Any dispute arising out of this contract will be under the jurisdiction of Courts of Law in Chennai.

4. Schedule of Requirements

4.1 Brief Description

The details of requirement of Licences are as described below. The hardware and the operating system will be provided by the bank.

S. No.	Details of License Required	Quantity
1	Static application security testing (SAST) license	25
2	Dynamic application security testing (DAST) User license	5
3	Concurrent user licenses for DAST	2

4.2 Delivery Locations

The Licences have to be delivered at Indian Bank Head Office, Chennai and shall be installed in the software development machines of Information Technology Department of the Bank as per the requirements.

4.3 Delivery Schedule

4.3.1 The Delivery of the Licenses and software should be made within Four (4) weeks from the date of acceptance of purchase order.

4.3.2 Implementation, configuration of should be completed within Six (6) weeks from the date of acceptance of purchase order.

4.4 Deliverables

4.4.1 Installation, configuration, integration, commissioning

4.4.2 The following documents have to be provided.

a) Implementation/Installation document
b) User manual/Operation manual

4.4.3 All the software shall have the support subscription for a period of three (3) years from the original equipment manufacturer (OEM) from the date of delivery of software to the bank.

4.4.4 If during the subscription period any licenses are found to be defective or not acceptable, they shall promptly be replaced by the supplier at its own cost on the request of the Bank.

4.4.5 Updates Subscription Services: The Updates Subscription Services should be provided with rights to product upgrades, maintenance releases and patches released during the subscription period and distributed on CD/DVD Packs or with option to download from the OEM's website.

4.4.6 Product Support: Product Support services to be offered for direct access via both the telephone and the web to skilled staff of technical analysts for problem resolution, bug reporting, and technical guidance on a 24x7 basis. This service should be provided through telephone, fax, e-mail directly.

4.4.7 Transfer of licenses from one platform to other during contract period as and when required by the Bank.

4.4.8 Training is to be provided to Bank's employees (expected count of 40 members) for three (3) working days from OEM certified trainer. Training should cover on how to install the software in the IDE, how to scan the code, how to scan the application during the run time (DAST), how to generate the report, how to fix the vulnerabilities etc.

4.5 Scope of Work

The supplier should provide support to the Bank on the delivered goods and services for a period of three (3) years from the date of delivery. Scope of work includes, but not restricted to the following:

4.5.1 During the contract period, the bidder is bound to provide the latest version of SAST and DAST. This should include the periodical updating of threat, signature, patches, upgradation etc.
4.5.2 The scope of work is for supply, installation and maintenance of solution and other items
4.5.3 The SAST and DAST solutions should be available in the same environment and SAST should provide static testing of the code and DAST should provide runtime testing.
4.5.4 The bidder should comply with the IT related policies of the bank
4.5.5 The bidder is responsible for installing the solution in the servers/hosts in the bank.
4.5.6 The bidder is responsible for setting up single management console for the related services.
4.5.7 The bidder must engage professional team/services onsite to implement the whole project.
4.5.8 The bidder must provide detailed architecture of the solution along with installation and administration guide
4.5.9 The bidder is responsible to inform if any new version/update/service pack/upgrade of solution is available from OEM, to the bank within seven (7) days of such release and provide the upgrade solution (software) within one month of such releases without any cost to the bank during the period of the contract.
4.5.10 If any additional licenses are procured by the bank, all such licenses are to be maintained by the bidder.
4.5.11 The bidder has to provide escalation matrix for escalating any incidents.
4.5.12 The solution should be free from any kind of vulnerabilities
4.5.13 The bidder should keep the bank explicitly informed of the end of support timelines
4.5.14 OEM and/or the bidder support include to advice and help the bank in implementing controls for the risk advised by regulators/Government of India.
4.5.15 The bidder has to provide all related software for the full functioning of the solution.
4.5.16 The bidder should note that the software and other items being procured shall be delivered at locations as per requirement of the Bank and the bidder will be required to support all such installations. The bank reserves the right to change location by giving prior notice.
4.5.17 The requirements and specifications for the solution must be fully met and functional from day one.
4.5.18 The software installation and configuration for the entire setup must be handled by the qualified/experienced personnel.
4.5.19 All patch update and patch management to be taken care and setup with confirmation as required.
4.5.20 The bidder shall confirm the integrity of the software supplied i.e. the software is free from bugs, malware etc.
4.5.21 The bank will not provide any remote assistance (or session) facility for installation, bug fixing, updates and upgrade during the period of the contract.
4.5.22 The solution should have the ability to freely change forms, fields, workflows, escalations and authorizations structures and reports according to the Bank's process without affecting updates/upgrades and integration with third party software.

4.5.23 The bidder should provide onsite, email and telephonic support.

4.6 SAST - Functional Requirements

4.6.1 The solution should be able to scan different types of source code and pin point different types of vulnerability.

4.6.2 The solution should be able to perform source code analysis in un-compiled form.

4.6.3 The solution should be able to integrate and scan following programming languages

a) .net technologies (C#, J#, VB.NET, ASP.NET, .Net core etc.)
b) Java
c) PHP
d) ASP
e) Python
f) SQL, T-SQL, PL/SQL
g) HTML/HTML 5
h) XML
i) CSS
j) Javascript
k) Jquery
l) C
m) C++

4.6.4 The solution should have integration capabilities which can be integrated in every phase of SDLC. The solution should be capable of integrating with source code repository, IDE, Plugins, build server, build management, bug tracking system and ticketing system. It should be able to integrate with the commercial or free IDEs (the list is not exhaustive rather only indicative) from Day one.

a) Visual Studio 2015/2017
b) Eclipse
c) Android studio

4.6.5 The solution should be able to distinguish the programming language based vulnerabilities

4.6.6 The solution should provide a default prioritization of vulnerabilities according to severity and risk in the code.

4.6.7 The solution should allow the user to drill down and trace through the suspect source code and show the root cause and supporting evidence of vulnerability in textual formats.

4.6.8 The solution should allow for detailed reporting of vulnerabilities found (including vulnerability explanation, recommendations and code snippets) which can be sent to developers, for offline reading and reference.

4.6.9 The solution should provide the developer vulnerability explanation and recommendations to fix issues during the vulnerability remediation process, including line-of-code details and descriptions on how to remediate each vulnerability

4.6.10 The solution should report vulnerabilities that have been fixed, newly introduced or continue to exist across multiple scans. It should also feature compare feature with a line by line review for any two scans of same project.

4.6.11 The solution should be able to scan web, windows and mobile applications.

4.6.12 The solution should be able to detect OWASP threats.

4.6.13 The solution should be compatible to install virtual/physical machines (Server client architecture)

4.6.14 The solution should have capability to add custom rules as required

4.6.15 The solution should have API support for easy integration

4.6.16 The solution should be able to integrate with Active Directory

4.7 DAST - Functional Requirements

4.7.1 Core technical capabilities

4.7.1.1 The solution should detect web application vulnerabilities and generate reports

4.7.1.2 The solution should perform vulnerability checks for the following technologies

a) REST
b) WSDL
c) JSON
d) GWT
e) JavaScript
f) AJAX
g) HTML 4 and 5
h) SOAP
i) .Net
j) Silverlight
k) PHP
l) ASP

4.7.1.3 The solution should detect the following class of security vulnerabilities

a) Apache struts 2 framework checks
b) Apache struts detection
c) Arbitrary file upload
d) Autocomplete attribute
e) Brute force (Form auth& HTTP auth)
f) Business logic abuse attacks
g) Cookie attributes
h) Credentials stored in clear text in cookie
i) Cross-site request forgery (CSRF)
j) Cross-site scripting (XSS)
k) Cross-site tracing (XST)
l) Directory indexing
m) Email disclosure
n) Force browsing
o) Form session strength
p) HTTP response splitting
q) HTTP strict transport security
r) HTTPS downgrade
s) Information disclosure
t) Information leakage
u) Java grinder
v) OS commanding
w) Parameter fuzzing
x) Predictable resource location
y) Privacy disclosure
z) Reflection
aa) Remote file include
bb) Reverse proxy
cc) Secure and non-secure content mix
dd) Server configuration
ee) Session fixation
ff) Session strength
gg) Source code disclosure

hh) SQL injection
ii) SSL Strength
jj) Un-validated redirect
kk) URL rewriting
ll) Web beacon
mm)Web service parameter fuzzing
nn) X-Frame options missing HTTP header
oo) X-XSS protection missing header
pp) Z-customer created attacks

4.7.1.4 The solution should support scanning of vulnerabilities in custom developed applications.
4.7.1.5 The solution should support testing web application for data injection and manipulation
4.7.1.6 The solution should support testing flow control vulnerabilities, such as forceful browsing and cross site request forgery.
4.7.1.7 The solution should support testing general vulnerabilities, such as directory indexing and enumeration, file enumeration, directory and path traversal.
4.7.1.8 The solution should support testing other vulnerabilities and flaws, such as session strength analysis and remote active content analysis.
4.7.1.9 The solution should support reducing the overall testing time of big applications by reducing duplicate attacks.
4.7.1.10 The solution should support testing an application with multiple user/role perspectives
4.7.1.11 The solution should have capabilities for human-assisted crawling of the application so the scanner can better understand authentication flow.
4.7.1.12 The solution should support selenium or other web scripting/automation tools.
4.7.1.13 The solution should support testing applications that extensively use client-side Javascript and ability to understand what the Javascript code is doing.
4.7.1.14 The solution should support detection of hostile client-side Javascript code.
4.7.1.15 The solution should support detection of client-side Javascript vulnerability.
4.7.1.16 The solution should support detection of client-side Javascript XSS issue
4.7.1.17 The solution should support testing Rich internet application based on Adobe flash and flex.
4.7.1.18 The solution should support automatically or programmatically generated URLs to crawl auto generated web pages.
4.7.1.19 The solution should prevent the scanner from entering an infinite loop scanning auto-generated web pages.
4.7.1.20 The solution should be able to test HTML 5 applications.
4.7.1.21 The solution should have the ability to create custom attacks.

4.7.2 Web Service Testing

4.7.2.1 The solution should support testing web service enabled using SOAP, WSDL and UDDI
4.7.2.2 The solution should support auto discover and test the web service interfaces.

4.7.3 XML APIs and Fuzz testing

4.7.3.1 The solution should support testing RESTful applications using XML based protocol fuzzing.
4.7.3.2 The solution should provide generic XML based protocol fuzzing and/or testing.
4.7.3.3 The solution should provide JSON testing.

4.7.4 Solution Capabilities

4.7.4.1 The solution should have options to reduce the risk that minimum disruptions to service are caused when testing/performed against production applications.

4.7.4.2 The solution should have the ability to execute retests of single vulnerabilities against previously discovered items once they are believed to have been remediated.

4.7.4.3 The solution should allow developers quickly replicate discovered vulnerability without retesting the entire application.

4.7.4.4 The solution should provide a record or replay capability of vulnerabilities discovered so that the exploitation of a vulnerability can be replayed by the developer investigating the issue or later by auditors to ensure the vulnerability has been addressed when retesting.

4.7.5 Mobile application security testing

4.7.5.1 The solution should have ability to test web applications designed for use on mobile device.

4.7.5.2 The solution should have ability to analyse traffic between the mobile application and web server and/or ability to analyse web application/service that communicates with mobile application.

4.7.5.3 The solution should have ability to integrate with IPS or Web Application Firewall (WAF) vendors so that knowledge of web vulnerabilities may be used to automatically generate the necessary rules for WAF protection.

4.7.5.4 The solution should have the ability to test WAF/IPS rules generated by the solution to make sure good traffic is allowed to pass and bad traffic is blocked.

4.7.6 Management reporting and analysis

4.7.6.1 The solution should support floating licenses between users (not locked to an individual user or machine).

4.7.6.2 The solution should provide a rating scale and rating mechanism for detected vulnerabilities. The solution should provide the ability to manually assign/reassign the priority or severity rating that the scanner has automatically assigned.

4.7.6.3 The solution should provide report that can help developer quickly focus on the highest severity issues.

4.7.6.4 The solution should identify the relevant web page and URL where the vulnerability is detected.

4.7.6.5 The solution should have ability to generate reports for regulatory compliance.

4.7.6.6 The solution should have ability to integrate with security information and event management (SIEM) system.

4.7.7 Remediation advice, examples and guidance

4.7.7.1 The solution should provide (or link to) remediation advice.

4.7.7.2 The solution should follow specific source of advisory (like OWASP) to determine the vulnerabilities

4.7.8 System requirement and maintenance

4.7.8.1 The solution should have the ability to perform testing on unlimited web applications within the same engine/installation.

4.7.8.2 The solution should have all its technical updates included as part of the maintenance.

4.7.8.3 The solution should have access to new updates and releases.

4.7.8.4 The solution should provide support for technical issues.

4.7.9 Training

4.7.9.1 The bidder should provide training to the Bank's officials on how to use the solution. The solution should be customizable as per the needs of the bank without any extra cost to the bank.

4.7.10 Reports

The solution must have a provision to provide the reports noted below. All reports should be available for pulling from the system.

4.7.10.1 Summary of support status

4.7.10.2 Significant incidents raised by the bank in the month. These include all priority observations and any other incidents reducing the quality of service.

4.7.10.3 Number of support calls closed during the month, by priority

4.7.10.4 Number of support calls open at the end of the month, by priority

4.7.10.5 Patch, Fixes, update reports

4.7.10.6 Application bugs/Issue call analysis

4.7.10.7 Proactive monitoring and preventive maintenance report.

5. Qualification Criteria

S.No.	Qualification Criteria	Documents Required
1	The Bidder should be a registered company in India (as per Indian Companies Act, 1956 or Indian Companies Act, 2013) and should be in existence in India for the last five (5) years (as on 31.03.2018).	Copy of certificate of incorporation issued by Registrar of companies.
2	The bidder should be a Original Software Developer (OSD) of the application security testing solution or an authorized partner/distributor of OSD	(a) If the bidder is authorized partner/distributor Manufacturers' Authorization Form is to be produced. (b) If the bidder is an OSD, an undertaking letter has to be submitted.
3	The Bidder should be Net profit earning organization in the last two (2) financial years (2016-17,2017-18)	Audited balance sheets for the last two (2) financial years (2016-17, 2017-18) have to be produced.
4	The Annual turnover should be more than Rs.2 Crores in last three (3) financial years (2015-16,2016-17,2017-18)	Audited balance sheets for the last three (3) financial years (2015-16,2016-17,2017-18) have to be produced.
5	The Bidder should not have been blacklisted currently by any Government Department/PSU/Banks.	The bidder should provide self-declaration as per section 7.
6	The bidder should have a team of well qualified and experienced staff in India, who will be able to attend the calls in person/provide onsite support, respond to the issues at a very short notice and they should have the knowledge to extend support to the bank for the in-scope activities on a need basis.	The bidder should provide the details as per section 18 and a proof of address for the branch.
7	The bidder should have implemented the solution in at least two (2) Scheduled Commercial Bank/National Informatics Center/Corporates in India during the period from 1/1/2015 to 31/09/2018.	The bidder must produce purchase order/ reference letter from their customer duly mentioning the solution name. The bidder should also furnish the details as per section 12.

6. Bid Form

(Bidders are required to furnish the Bid Form)

Date: _____

To

Indian Bank Corporate Office,
Information Technology Department
254-260, Avvai Shanmugam Salai,
Royapettah, Chennai, India - 600014

Sub: Supply and Maintenance of Application Security Testing Solution

Ref: Bid Document No. CO:ITD:CDC:1049/R1:2018-19 dated 24/10/2018.

Having examined the Bidding Documents including Addenda Nos._____(Insert numbers), the receipt of which is hereby duly acknowledged, we, the undersigned, offer to supply, install and maintain the following licences in conformity with the said bidding documents:

S. No.	Details of License Required	Quantity
1	Static Application Security Testing	25
2	Dynamic Application Security Testing	5

We undertake, if our bid is accepted, to deliver the goods in accordance with the delivery schedule specified. If our bid is accepted, we will obtain the Guarantee of a Bank in a sum equivalent to ten percent (10%) of the amount quoted for Licences, training and OEM update & support for three (3) years for the due performance of the Contract, in the form prescribed by the Bank. We agree to abide by this for the bid validity period specified and it shall remain binding upon us and may be accepted at any time before the expiration of that period. We agree to extend the Bid Validity Period and Bank Guarantee towards Earnest Money Deposit, if required. Until a formal contract is prepared and executed, this bid, together with your notification of award, shall constitute a binding Contract between us. We undertake that, in competing for (and, if the award is made to us, in executing) the above contract, we will strictly observe the laws against fraud and corruption in force in India. We understand that bank is not bound to accept the lowest or any bid bank may receive. We confirm that we comply with the qualification criteria of the bidding documents and are submitting proof of the same along with bid.

Dated this _____ day of _____ 201_____.

_____
Signature

_____
(In the Capacity of)

Duly authorised to sign bid for and on behalf of

(Name & Address of Bidder) _____

_____

Phone:
Email:

7. Self-Declaration – Non Blacklisting

To

The Assistant General Manager,
Indian Bank Corporate Office,
Information Technology Department,
254-260, Avvai Shanmugam Salai,
Royapettah, Chennai, India - 600014

Dear Sir,

Sub: Supply and Maintenance of Application Security Testing Solution

Ref: Bid Document No. CO:ITD:CDC:1049/R1:2018-19 dated 24/10/2018.

We hereby certify that, we have not been blacklisted currently by any Government Department / Public Sector Undertakings / Banks.

Signature of Authorized Official

Name:

Designation:

Place:

Date:

Office Seal

8. Bid Security Form

Whereas_____(Hereinafter called "the Bidder") who intends to submit bid dated_____ (date of submission of bid) for the Supply and Maintenance of Application Security Testing Solution(Hereinafter called "the Bid).

KNOW ALL PEOPLE by these presents that We_____(Name of Bank) of_____ (Name of Country), having our registered office at_____(address of Bank) (hereinafter called "the Bank"), are bound unto Indian Bank in the sum of _____for which payment well and truly to be made to the said Purchaser, the Bank binds itself, its successors, and assigns by these presents. Sealed with the Seal of the said Bank this _____day of _____2018.

THE CONDITIONS of this obligation are:

1. If the Bidder
   a) withdraws its Bid during the period of bid validity
   or
   b) does not accept the correction of errors in accordance with the Instructions to Bidders; or
2. If the Bidder, having been notified of the acceptance of its bid by the Purchaser during the period of bid validity:
   a) fails or refuses to execute the Contract Form if required;
   or
   b) fails or refuses to furnish the performance security, in accordance with the Instruction to Bidders.

We undertake to pay the Purchaser up to the above amount upon receipt of its first written demand, without the Purchaser having to substantiate its demand, provided that in its demand the Purchaser will note that the amount claimed by it is due to it, owing to the occurrence of one or both of the conditions, specifying the occurred condition or conditions. This Guarantee will remain in force up to _____and any demand in respect thereof should reach the Bank not later than _____.

(Signature of the Authorised Official of Bank)

NOTE:

1. The bidder 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 and shall be on a Non-Judicial Stamp Paper of requisite value.

9. Contract Form

THIS AGREEMENT made the _____day of_____2018 Between Indian Bank, having its Corporate Office at 254-260, Avvai Shanmugam Salai, Royapettah, Chennai 600014 (hereinafter called "the Purchaser") of the one part and _____(Name of Supplier) having its Registered Office at _____(City and Country of Supplier) (hereinafter called "the Supplier") of the other part:

WHEREAS the Purchaser invited bids vide RFP No. CO:ITD:CDC:1049/R1:2018-19 dated 24/10/2018 for certain Goods and ancillary services viz., Supply and Maintenance of Application Security Testing Solution and has accepted a bid by the Supplier for the provision of those goods and services for the sum of _____(Contract Price in Words and Figures) (hereinafter called "the Contract Price").

NOW THIS AGREEMENT WITNESSETH AS FOLLOWS:

1. In this Agreement words and expressions shall have the same meanings as are respectively assigned to them in the Conditions of Contract referred to.
2. The following documents shall be deemed to form and be read and construed as part of this Agreement, viz.:
   a) the Bid Form and the Price Schedule submitted by the Bidder;
   b) the Schedule of Requirements;
   c) the Scope of Work;
   d) the Conditions of Contract;
   e) the Purchaser's Notification of Award.
3. In consideration of the payments to be made by the Purchaser to the Supplier as hereinafter mentioned, the Supplier hereby covenants with the Purchaser to provide the goods and services and to remedy defects therein in conformity in all respects with the provisions of the Contract.
4. The Purchaser hereby covenants to pay the Supplier in consideration of the provision of the goods and services and the remedying of defects therein, the Contract Price or such other sum as may become payable under the provisions of the Contract at the times and in the manner prescribed by the Contract.

Brief particulars of the goods and services which shall be supplied / provided by the Supplier are as under:

S. No.	Details of License Required	Quantity
1	Static application security testing (SAST) license	25
2	Dynamic application security testing (DAST) User license	5
3	Concurrent user licenses for DAST	2

Scope of Work

The supplier should provide support to the Bank on the delivered goods and services for a period of three (3) years from the date of delivery. Scope of work includes, but not restricted to the following:

1. During the contract period, the bidder is bound to provide the latest version of SAST and DAST. This should include the periodical updating of threat, signature, patches, upgradation etc.
2. The scope of work is for supply, installation and maintenance of solution and other items
3. The SAST and DAST solutions should be available in the same environment and SAST should provide static testing of the code and DAST should provide runtime testing.
4. The bidder should comply with the IT related policies of the bank
5. The bidder is responsible for installing the solution in the servers/hosts in the bank.
6. The bidder is responsible for setting up single management console for the related services.
7. The bidder must engage professional team/services onsite to implement the whole project.
8. The bidder must provide detailed architecture of the solution along with installation and administration guide
9. The bidder is responsible to inform if any new version/update/service pack/upgrade of solution is available from OEM, to the bank within seven (7) days of such release and provide the upgrade solution (software) within one month of such releases without any cost to the bank during the period of the contract.
10. If any additional licenses are procured by the bank, all such licenses are to be maintained by the bidder.
11. The bidder has to provide escalation matrix for escalating any incidents.
12. The solution should be free from any kind of vulnerabilities
13. The bidder should keep the bank explicitly informed of the end of support timelines
14. OEM and/or the bidder support include to advice and help the bank in implementing controls for the risk advised by regulators/Government of India.
15. The bidder has to provide all related software for the full functioning of the solution.
16. The bidder should note that the software and other items being procured shall be delivered at locations as per requirement of the Bank and the bidder will be required to support all such installations. The bank reserves the right to change location by giving prior notice.
17. The requirements and specifications for the solution must be fully met and functional from day one.
18. The software installation and configuration for the entire setup must be handled by the qualified/experienced personnel.
19. All patch update and patch management to be taken care and setup with confirmation as required.
20. The bidder shall confirm the integrity of the software supplied i.e. the software is free from bugs, malware etc.
21. The bank will not provide any remote assistance (or session) facility for installation, bug fixing, updates and upgrade during the period of the contract.
22. The solution should have the ability to freely change forms, fields, workflows, escalations and authorizations structures and reports according to the Bank's process without affecting updates/upgrades and integration with third party software.
23. The bidder should provide onsite, email and telephonic support.

TOTAL VALUE: Total value of the contract is the sum of the below:

S.No.	Particulars
1	Cost of Licenses
2	Cost of OEM Update & Support for the three (3) years
3	Cost of training

DELIVERY SCHEDULE:

IN WITNESS whereof the parties hereto have caused this Agreement to be executed in accordance with their respective laws the day and year first above written.

Signed, Sealed and Delivered by the

said_____(For Indian Bank)

in the presence of:

1. _____

_____

_____

2. _____

_____

_____

Signed, Sealed and Delivered by the

said_____(For the Supplier)

in the presence of:

1. _____

_____

_____

2. _____

_____

_____

10. Performance Security Form

Bank Guarantee No. Date: _____

To

Indian Bank, Chennai, India.

WHEREAS_____(Name of Supplier) hereinafter called "the Supplier") has undertaken, in pursuance of Contract No_____ _____dated_____to supply and maintain _____(Description of Goods and Services) (hereinafter called "the Contract").

AND WHEREAS it has been stipulated by you in the said Contract that the Supplier shall furnish you with a Bank Guarantee by a Scheduled Commercial Bank for the sum specified therein as security for compliance with the Supplier's performance obligations in accordance with the Contract including Maintenance.

AND WHEREAS we have agreed to give the Supplier a Guarantee:

THEREFORE WE hereby affirm that we are Guarantors and responsible to you, on behalf of the Supplier, up to a total of _____(Amount of the Guarantee in Words and Figures) and we undertake to pay you, upon your first written demand declaring the Supplier to be in default under the Contract and without cavil or argument, any sum or sums within the limit of _____(Amount of Guarantee) as aforesaid, without your needing to prove or to show grounds or reasons for your demand or the sum specified therein.

This guarantee is valid until the _____day of_____, 2018 and claim period is valid up to_____.

Signature of Authorised Official with Seal _____

Date_____/_____/2018

Address: _____

_____

NOTE:

1. The Supplier should ensure that 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 and shall be on a Non-Judicial Stamp Paper of requisite value.

11. Manufacturers' Authorization Form

No. Date: _____

To

The Assistant General Manager,
Indian Bank Corporate Office,
Information Technology Department,
254-260, Avvai Shanmugam Salai,
Royapettah, Chennai, India - 600014

Dear Sir,

Sub: Supply and Maintenance of Application Security Testing Solution

Ref: Bid Document No. CO:ITD:CDC:1049/R1:2018-19 dated 24/10/2018.

We who are established and reputable manufacturers of _____(name & descriptions of goods offered) software and Licenses do hereby authorize, M/s _____ (Name and address of Agent) to submit a bid, and sign the contract with you for Application Security Testing software and Licenses against the above RFP. We duly authorise them to act on our behalf in fulfilling all installation, technical support and maintenance obligations required by the Contract.

Yours faithfully,

(Name of Manufacturer)

12. Proof of Application Security Testing software Licenses supplied and maintained by the Bidder

(Please attach a copy of the purchase order)

S.No.	Order placed by	Order No. and Date	Quantity supplied	Value of Order (Optional)	Date of completion of delivery		Remarks indicating reasons for late delivery, if any
	Full address of Purchaser				As per Contract	Actual	

Date:

Signature of Authorised Official with Seal

13. Proforma of Installation Certificate for Issue bythe Bank after Successful Commissioning

Date: _____

Sub: Certificate of commissioning of Application Security Testing Solution.

Ref: Purchase Order No.

1. This is to certify that the Licenses as detailed below has/have been delivered, installed and commissioned.
   Contract No._____ dated _____
   Description of the Licenses _____
   Quantity _____
   Date of delivery_____
   Date of commissioning _____
2. The proving test has been done to our entire satisfaction and operators have been trained as per contract terms
3. The supplier has fulfilled its contractual obligations satisfactorily* Or
4. The supplier has failed to fulfil its contractual obligations with regard to the following:
   (a)
   (b)

Signature _____

Name _____

Designation with date and stamp _____

Explanatory notes for filling up the certificates:

(a) The Supplier has adhered to the time schedule specified in the contract in dispatching the documents pursuant to Technical Specifications.

(b) The Supplier has supervised the commissioning of the software in time i.e. within the period specified in the contract from the date of intimation by the Purchaser in respect of the installation of the system.

(c) In the event of documents having not been supplied or installation and commissioning of the softwarehave been delayed on account of the supplier, the extent of delay should always be mentioned.

14. Non-Disclosure Agreement

THIS AGREEMENT made and entered into at _____on this the_____day of_____, 2018 between **INDIAN BANK**, a body corporate constituted under the Banking Companies (Acquisition & Transfer of Undertakings) Act 1970, having its Corporate Office at No.254-260, Avvai Shanmugam Salai, Royapettah, Chennai – 600014, hereinafter called the **"Bank"** which term shall wherever the context so require includes its successors and assigns

AND

M/s._____ limited a company registered under the Companies Act having its registered office at_____ hereinafter called the **"supplier"** which term shall wherever the context so require includes its successors and assigns, **WITNESSETH**:

WHEREAS

The Bank is interalia engaged in the business of banking and hasbeen procuring computer systems, M/s_____Limited has been engaged in the business of supply and installation of Application Security Testing solution.

The parties intend to engage in discussions and negotiations concerning establishment of business relationship between them. In the course of discussions and negotiations, it is anticipated that the parties may disclose or deliver to the other certain or some of its trade secrets or confidential or proprietary information for the purpose of business relationship.

NOW THERFORE THIS AGREEMENT WITNESSETH and it is hereby agreed by and between the parties hereto as follows:

1. Confidential information

Confidential information means all information disclosed/furnished by either party to another party in connection with the business transacted/ to be transacted between the parties. Confidential information shall include any copy, abstract, extract, sample, note or module thereof and electronic material or records. Receiving party may use the information solely for and in connection with the Purpose.

2. Use of Confidential Information

Each party agrees not to use the other's confidential information for any purpose other than for the specific purpose. Any other use of such confidential information by any party shall be made only upon the prior written consent from the authorized representative of the other party or pursuant to subsequent agreement between the Parties hereto. The receiving party shall not commercially use or disclose for commercial purpose any confidential information or any materials derived there from, to any other person or entity other than persons in the direct employment of the Receiving Party who have a need to access to and knowledge of the confidential information solely for the purpose authorized above. The Receiving Party may disclose confidential information to consultants only if the consultant has executed non-disclosure agreement with the Receiving Party that contains terms and conditions that are no less restrictive than these and such consultant should also be liable to the original disclosing party for any unauthorized use or disclosure. The Receiving party shall take appropriate measures by instruction and written agreement prior to disclosure to such employees to assure against unauthorized use or disclosure. The Receiving Party agrees to notify the Disclosing Party immediately if it learns of any use or disclosure of the Disclosing party's confidential information in violation of the terms of this Agreement. Neither party shall make news release, public announcements, give interviews, issue or publish advertisements or Agreement, the contents/provisions thereof, other information relating to this

agreement, the purpose, the Confidential information or other matter of this agreement, without the prior written approval of the other party.

3. Exemptions

The obligations imposed upon either 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 any 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 used only for the purposes for which the order was issued.

4. Term

This agreement shall be effective from the date of the execution of this agreement and shall continue till expiration or termination of this agreement due to cessation of the business relationship between the parties. Upon expiration or termination as contemplated herein the Receiving party shall immediately cease any or all disclosures or uses of confidential information and at the request of the disclosing party, the receiving party shall promptly return or destroy all written, graphic or other tangible forms of the confidential information and all copies, abstracts, extracts, samples, note or modules thereof.The obligations of the receiving party respecting disclosure and confidentiality shall continue to be binding and applicable without limit until such information enters the public domain.

5. Title and Proprietary rights

Notwithstanding the disclosure of any confidential information by the disclosing party to the receiving party, the disclosing party shall retain title and all intellectual property and proprietary rights in the confidential information. No license under any trademark, patent or copyright or application for same which are or thereafter may be obtained by such party is either granted or implied by the conveying of confidential information.

6. Return of confidential information

Upon written demand of the disclosing party, the receiving party shall (I) cease using the confidential information (ii) return the confidential information and all copies, abstracts, extracts, samples, note or modules thereof to the disclosing party within seven (7) days after receipt of notice and (iii) upon request of the disclosing party, certify in writing that the receiving party has complied with the obligations set forth in this paragraph.

7. Remedies

The receiving party acknowledges that if the receiving party fails to comply with any of its obligations hereunder, the disclosing party may suffer immediate, irreparable harm for which monetary damages may not be adequate. The receiving party agrees that, in addition to all other remedies provided at law or in equity, the disclosing party shall be entitled to injunctive relief hereunder.

8. Entire agreement

This agreement constitutes the entire agreement between the parties relating to the matter discussed herein and supercedes any and all prior oral discussion and/or written correspondence or agreements between the parties. This agreement may be amended or modified only with the mutual written consent of the parties. Neither this agreement nor any rights, benefits and obligations granted hereunder shall be assignable or otherwise transferable.

9. Severability

If any provision herein becomes invalid, illegal or unenforceable under any law, the validity, legality and enforceability of the remaining provisions and this agreement shall not be affected or impaired.

10. Dispute resolution mechanism

In the event of any controversy or dispute regarding the interpretation of any part of this agreement or any matter connected with, arising out of, or incidental to the arrangement incorporated in this agreement, the matter shall be referred to arbitration and the award passed in such arbitration shall be binding on the parties. The arbitral proceeding shall be governed by the provisions of Arbitration and Conciliation Act 1996 and the place of arbitration shall be Chennai. Submitting to arbitration may be considered as an additional remedy and it does not preclude Parties to seek redressal/other legal recourse.

11. Jurisdiction

The parties to this agreement shall submit to the jurisdiction of courts in Chennai.

12. Governing laws

The provisions of this agreement shall be governed by the laws of India.
In witness whereof, the parties hereto have set their hands through their authorised signatories

Signed, Sealed and Delivered by the
said_____ (For Indian Bank)
in the presence of:
1. _____
_____

2. _____
_____

Signed, Sealed and Delivered by the
said_____ (For the Supplier)
in the presence of:
1. _____
_____

2. _____
_____

15. Undertaking of authenticity

Sub: Supply and Maintenance of Application Security Testing Solution

Ref: Bid Document No. CO:ITD:CDC:1049/R1:2018-19 dated 24/10/2018.

This has reference to Application Security Testing Solution Licenses being quoted to Indian Bank vide our Quotation No. _____ Dated _____.

We undertake that in respect of Application Security Testing Solution licenses asked by Indian Bank shall be supplied along with the authorised license certificate and also that it shall be sourced from the authorised source. Should Indian Bank require, we shall produce certificate from our OEM supplier in support of above undertaking at the time of delivery/installation. It will be our responsibility to produce such letter from our OEM supplier's at the time of delivery or within a reasonable time. In case of default and we are unable to comply with above at the time of delivery or during installation or support, for the licenses already billed, we agree to return the money if any paid to us by Indian Bank in this regard and our Earnest Money Deposit/Bank Guarantee get forfeited. We also take full responsibility as per the content even if there is any defect by Authorised Reseller etc.

Signature of Authorized Official

Name:

Designation:

Place:

Date:

Office Seal

The above declaration has to be given by the company secretary dulySigned on the Letter Head of the Company

16. Self-Declaration – Exit Requirements

To

The Assistant General Manager,
Indian Bank Corporate Office,
Information Technology Department,
254-260, Avvai Shanmugam Salai,
Royapettah, Chennai, India - 600014

Dear Sir,

Sub: Supply and Maintenance of Application Security Testing Solution

Ref: Bid Document No. CO:ITD:CDC:1049/R1:2018-19 dated 24/10/2018.

We hereby certify that in the event of Agreement comes to end on account of termination or by the expiry of the term / renewed term of the Agreement or otherwise, we shall render all reasonable assistance and help to the Bank and to any new vendor engaged by the Bank, for the smooth switch over and continuity of the Services.

Signature of Authorized Official

Name:

Designation:

Place:

Date:

Office Seal

17. Commercial Bid (Part-II)

To

The Assistant General Manager,
Indian Bank Corporate Office,
Information Technology Department,
254-260, Avvai Shanmugam Salai,
Royapettah, Chennai, India - 600014

Dear Sir,

Sub: Supply and Maintenance of Application Security Testing Solution

Ref: Bid Document No. CO:ITD:CDC:1049/R1:2018-19 dated 24/10/2018.

We submit hereunder the price details of SAST and DAST Licences with support and maintenance as per the requirement of the tender.

S.No	Details of License	One time License Cost (A)	OEM update & Support cost for three (3) years(B)	Unit Price C = A+B	Quantity (Q)	Total Price = Q * C (#)
1	SAST				25	
2	DAST				5	
Total License Cost (D)						
One time training cost for Application Security Testing Solution (E)						
Total Cost for 3 years = (D) + (E)						

Price in words: Rupees _____

- Inclusive of all duties, levies, delivery, installation, support etc. and exclusive of taxes. TDS if applicable will be deducted as per the applicable rates from the payment.

We submit that we shall abide by the details given above and the conditions given in your above tender.

Signature of Authorized Official

Name:

Designation:

Place:

Date:

Office Seal

18. Service Support Details

To

The Assistant General Manager,
Indian Bank Corporate Office,
Information Technology Department,
254-260, Avvai Shanmugam Salai,
Royapettah, Chennai, India - 600014

Dear Sir,

Sub: Supply and Maintenance of Application Security Testing Solution.

Ref: Bid Document No. CO:ITD:CDC:1049/R1:2018-19 dated 24/10/2018.

The information of our branches and the support engineers stationed at those branches are produced below.

S.No.	Location	Postal Address	Landline Phone No.	Email ID	No. of Engineers/Service staff
1					
2					
3					

Signature of Authorized Official

Name:

Designation:

Place:

Date:

Office Seal

19. Check List (Part-I)

S.No.	Qualification Criteria	Documents Required
1	The Bidder should be a registered company in India (as per Indian Companies Act, 1956 or Indian Companies Act, 2013) and should be in existence in India for the last five (5) years (as on 31.03.2018).	Copy of certificate of incorporation issued by Registrar of companies.
2	The bidder should be a Original Software Developer (OSD) of the application security testing solution or an authorized partner/distributor of OSD	(c) If the bidder is authorized partner/distributor Manufacturers' Authorization Form is to be produced. (d) If the bidder is an OSD, an undertaking letter has to be submitted.
3	The Bidder should be Net profit earning organization in the last two (2) financial years (2016-17,2017-18)	Audited balance sheets for the last two (2) financial years (2016-17, 2017-18) have to be produced.
4	The Annual turnover should be more than Rs.2 Crores in last three (3) financial years (2015-16,2016-17,2017-18)	Audited balance sheets for the last three (3) financial years (2015-16,2016-17,2017-18) have to be produced.
5	The Bidder should not have been blacklisted currently by any Government Department/PSU/Banks.	The bidder should provide self-declaration as per section 7.
6	The bidder should have a team of well qualified and experienced staff in India, who will be able to attend the calls in person/provide onsite support, respond to the issues at a very short notice and they should have the knowledge to extend support to the bank for the in-scope activities on a need basis.	The bidder should provide the details as per section 18 and a proof of address for the branch.
7	The bidder should have implemented the solution in at least two (2) Scheduled Commercial Bank/National Informatics Center/Corporates in India during the period from 1/1/2015 to 31/09/2018.	The bidder must produce purchase order/ reference letter from their customer duly mentioning the solution name. The bidder should also furnish the details as per section 12.
8	Bid Security of required amount	As per the format provided in section 8
9	Bid Form	As per the format provided in section 6
10	Undertaking of Authenticity	As per the format provided in section 15
11	Exit Requirements	As per the format provided in section 16
12	Copy of the RFP document and all Clarifications/amendments signed with seal on all pages.	
13	Requirement Compliance matrix	As per format specified in section 20
14	Certificate of authorization for authorized signatory as required in section 2.19.5	
15	An undertaking from the bidder that the bidder will extend support for a period of three (3) years from the date of delivery as required in section 2.4.1 (e)	

20. Compliance Matrix

To

The Assistant General Manager,
Indian Bank Corporate Office,
Information Technology Department,
254-260, Avvai Shanmugam Salai,
Royapettah, Chennai, India - 600014

Dear Sir,

Sub: Supply and Maintenance of Application Security Testing Solution.

Ref: Bid Document No. CO:ITD:CDC:1049/R1:2018-19 dated 24/10/2018.

The compliance of the proposed solution to the requirements specified in the RFP is produced below.

Requirement	Complied (Yes/No)
4.1 Static application security testing (SAST) license - 25 Nos. Dynamic application security testing (DAST) User license - 5 Nos. Concurrent user licenses for DAST - 2 Nos.	
4.6.1 The solution should be able to scan different types of source code and pin point different types of vulnerability.	
4.6.2 The solution should be able to perform source code analysis in un-compiled form.	
4.6.3 The solution should be able to integrate and scan following programming languages a) .net technologies (C#, J#, VB.NET, ASP.NET, .Net core etc.) b) Java c) PHP d) ASP e) Python f) SQL, T-SQL, PL/SQL g) HTML/HTML 5 h) XML i) CSS j) Javascript k) Jquery l) C m) C++	
4.6.4 The solution should have integration capabilities which can be integrated in every phase of SDLC. The solution should be capable of integrating with source code repository, IDE, Plugins, build server, build management, bug tracking system and ticketing system. It should be able to integrate with the commercial or free IDEs (the list is not exhaustive rather only indicative) from Day one. a) Visual Studio 2015/2017 b) Eclipse c) Android studio	
4.6.5 The solution should be able to distinguish the programming language based vulnerabilities	

4.6.6 The solution should provide a default prioritization of vulnerabilities according to severity and risk in the code.	
4.6.7 The solution should allow the user to drill down and trace through the suspect source code and show the root cause and supporting evidence of vulnerability in textual formats.	
4.6.8 The solution should allow for detailed reporting of vulnerabilities found (including vulnerability explanation, recommendations and code snippets) which can be sent to developers, for offline reading and reference.	
4.6.9 The solution should provide the developer vulnerability explanation and recommendations to fix issues during the vulnerability remediation process, including line-of-code details and descriptions on how to remediate each vulnerability	
4.6.10 The solution should report vulnerabilities that have been fixed, newly introduced or continue to exist across multiple scans. It should also feature compare feature with a line by line review for any two scans of same project.	
4.6.11 The solution should be able to scan web, windows and mobile applications.	
4.6.12 The solution should be able to detect OWASP threats.	
4.6.13 The solution should be compatible to install virtual/physical machines (Server client architecture)	
4.6.14 The solution should have capability to add custom rules as required	
4.6.15 The solution should have API support for easy integration	
4.6.16 The solution should be able to integrate with Active Directory	
4.7.1.1 The solution should detect web application vulnerabilities and generate reports	
4.7.1.2 The solution should perform vulnerability checks for the following technologies a) REST b) WSDL c) JSON d) GWT e) JavaScript f) AJAX g) HTML 4 and 5 h) SOAP i) .Net j) Silverlight k) PHP l) ASP	

4.7.1.3 The solution should detect the following class of security vulnerabilities a) Apache struts 2 framework checks b) Apache struts detection c) Arbitrary file upload d) Autocomplete attribute e) Brute force (Form auth& HTTP auth) f) Business logic abuse attacks g) Cookie attributes h) Credentials stored in clear text in cookie i) Cross-site request forgery (CSRF) j) Cross-site scripting (XSS) k) Cross-site tracing (XST) l) Directory indexing m) Email disclosure n) Force browsing o) Form session strength p) HTTP response splitting q) HTTP strict transport security r) HTTPS downgrade s) Information disclosure t) Information leakage u) Java grinder v) OS commanding w) Parameter fuzzing x) Predictable resource location y) Privacy disclosure z) Reflection aa) Remote file include bb) Reverse proxy cc) Secure and non-secure content mix dd) Server configuration ee) Session fixation ff) Session strength gg) Source code disclosure hh) SQL injection ii) SSL Strength jj) Un-validated redirect kk) URL rewriting ll) Web beacon mm) Web service parameter fuzzing nn) X-Frame options missing HTTP header oo) X-XSS protection missing header pp) Z-customer created attacks	
4.7.1.4 The solution should support scanning of vulnerabilities in custom developed applications.	
4.7.1.5 The solution should support testing web application for data injection and manipulation	
4.7.1.6 The solution should support testing flow control vulnerabilities, such as forceful browsing and cross site request forgery.	

4.7.1.7 The solution should support testing general vulnerabilities, such as directory indexing and enumeration, file enumeration, directory and path traversal.	
4.7.1.8 The solution should support testing other vulnerabilities and flaws, such as session strength analysis and remote active content analysis.	
4.7.1.9 The solution should support reducing the overall testing time of big applications by reducing duplicate attacks.	
4.7.1.10 The solution should support testing an application with multiple user/role perspectives	
4.7.1.11 The solution should have capabilities for human-assisted crawling of the application so the scanner can better understand authentication flow.	
4.7.1.12 The solution should support selenium or other web scripting/automation tools.	
4.7.1.13 The solution should support testing applications that extensively use client-side Javascript and ability to understand what the Javascript code is doing.	
4.7.1.14 The solution should support detection of hostile client-side Javascript code.	
4.7.1.15 The solution should support detection of client-side Javascript vulnerability.	
4.7.1.16 The solution should support detection of client-side Javascript XSS issue	
4.7.1.17 The solution should support testing Rich internet application based on Adobe flash and flex.	
4.7.1.18 The solution should support automatically or programmatically generated URLs to crawl auto generated web pages.	
4.7.1.19 The solution should prevent the scanner from entering an infinite loop scanning auto-generated web pages.	
4.7.1.20 The solution should be able to test HTML 5 applications.	
4.7.1.21 The solution should have the ability to create custom attacks.	
4.7.2.1 The solution should support testing web service enabled using SOAP, WSDL and UDDI	
4.7.2.2 The solution should support auto discover and test the web service interfaces.	
4.7.3.1 The solution should support testing RESTful applications using XML based protocol fuzzing.	
4.7.3.2 The solution should provide generic XML based protocol fuzzing and/or testing.	
4.7.3.3 The solution should provide JSON testing.	
4.7.4.1 The solution should have options to reduce the risk that minimum disruptions to service are caused when testing/performed against production applications.	
4.7.4.2 The solution should have the ability to execute retests of single vulnerabilities against previously discovered items once they are believed to have been remediated.	
4.7.4.3 The solution should allow developers quickly replicate discovered vulnerability without retesting the entire application.	

4.7.4.4 The solution should provide a record or replay capability of vulnerabilities discovered so that the exploitation of a vulnerability can be replayed by the developer investigating the issue or later by auditors to ensure the vulnerability has been addressed when retesting.	
4.7.5.1 The solution should have ability to test web applications designed for use on mobile device.	
4.7.5.2 The solution should have ability to analyse traffic between the mobile application and web server and/or ability to analyse web application/service that communicates with mobile application.	
4.7.5.3 The solution should have ability to integrate with IPS or Web Application Firewall (WAF) vendors so that knowledge of web vulnerabilities may be used to automatically generate the necessary rules for WAF protection.	
4.7.5.4 The solution should have the ability to test WAF/IPS rules generated by the solution to make sure good traffic is allowed to pass and bad traffic is blocked.	
4.7.6.1 The solution should support floating licenses between users (not locked to an individual user or machine).	
4.7.6.2 The solution should provide a rating scale and rating mechanism for detected vulnerabilities. The solution should provide the ability to manually assign/reassign the priority or severity rating that the scanner has automatically assigned.	
4.7.6.3 The solution should provide report that can help developer quickly focus on the highest severity issues.	
4.7.6.4 The solution should identify the relevant web page and URL where the vulnerability is detected.	
4.7.6.5 The solution should have ability to generate reports for regulatory compliance.	
4.7.6.6 The solution should have ability to integrate with security information and event management (SIEM) system.	
4.7.7.1 The solution should provide (or link to) remediation advice.	
4.7.7.2 The solution should follow specific source of advisory (like OWASP) to determine the vulnerabilities	
4.7.8.1 The solution should have the ability to perform testing on unlimited web applications within the same engine/installation.	
4.7.8.2 The solution should have all its technical updates included as part of the maintenance.	
4.7.8.3 The solution should have access to new updates and releases.	
4.7.8.4 The solution should provide support for technical issues.	
4.7.9.1 The bidder should provide training to the Bank's officials on how to use the solution. The solution should be customizable as per the needs of the bank without any extra cost to the bank.	
The solution must have a provision to provide the reports noted below. All reports should be available for pulling from the system.	
4.7.10.1 Summary of support status	

4.7.10.2 Significant incidents raised by the bank in the month. These include all priority observations and any other incidents reducing the quality of service.	
4.7.10.3 Number of support calls closed during the month, by priority	
4.7.10.4 Number of support calls open at the end of the month, by priority	
4.7.10.5 Patch, Fixes, update reports	
4.7.10.6 Application bugs/Issue call analysis	
4.7.10.7 Proactive monitoring and preventive maintenance report.	

Signature of Authorized Official

Name:

Designation:

Place:

Date:

Office Seal