Request for Quotation (RFQ)
For
Vulnerability Management at IFTAS

RFQ Reference No. IFT/VM/200715-1
RFQ Date: 15-Jul-2020

Table of Contents

1. Introduction 3
1.1 Background 3
1.2 Objective 3
2. Timelines 4
3. Terminology 5
4. Instruction to Bidders 5
5. Purpose of RFQ 6
6. Scope of work 6
6.1 Setting-up of VM Solution 6
6.2 Support During Contract Period 8
6.3 Obsolescence 9
6.4 Training for Vulnerabilities Awareness 9
6.6 Project Timeline 9
7. Eligibility Criteria 10
7.1 Evaluation Process 11
7.2 Technical Evaluation Matrix 11
8. Payment Terms and Conditions 12
8.1 Delivery, Implementation, Training and Support 12
9. Service Level Standards/ Requirements/ Agreement 13
10. Clarification on the Tender Documents 14
11. Performance Bank Guarantee: 14
12. Termination of Purchase Order/Contract: 14
13. Force Majeure 15
14. Governing Law and Disputes 15
15. Disqualification Parameters in Bid Evaluation 16
16. Confidentiality of Information 16
17. Use of Contract Documents and Information 17
18. Indemnification 17
19. Documents 18
Annexure -I: Bidder's Guarantee Certificate 19
Annexure -II: Non-Disclosure Agreement 20
Annexure -III: Conformation to Terms and Conditions 22
Annexure-IV: Performance Bank Guarantee 23
Annexure-V: Technical Specifications of Vulnerability Management 26
Annexure-VI: Commercial Bid format 41
Annexure-VII: Address for locations 42
Annexure-VIII: Response from OEM through Bidder 43
Annexure-IX: Letter of Authority 44
Annexure-X: Indexation Formula 45

1. Introduction

1.1 Background

IFTAS, a wholly owned subsidiary of Reserve Bank of India (RBI). IFTAS, was formed in 2015 as a Section-8, not-for-profit organization, was entrusted with the responsibility of pioneering the use of technology in banking and offering cutting-edge services to financial sector in India. Major technology initiatives from IFTAS include setting up of the Next generation INFINET (INFINET 2.0) network, managing the nationwide communication backbone for the Central Payment System, managing SFMS Central Payment System (Structured Financial Messaging System) and a host of Cloud solutions from IBCC (Indian Banking Community Cloud).

1.2 Objective

Vulnerability Management (VM) as a process will help us identifying, evaluating, treating, and reporting on security vulnerabilities in IT systems and the software that runs on them. As compared to one-time Vulnerability Assessment being carried out, the VM strategy will be an ongoing, comprehensive process that aims at managing our vulnerabilities in a holistic and continuous manner. This, implemented alongside with other security stack, will help in prioritizing possible threats and minimizing the attack surface, proactively finding and fixing potential weaknesses in IT setup. The basic goal is to apply the fixes before an attacker can use vulnerabilities to cause a cybersecurity breach.

IFTAS invites RFQ from eligible bidders for Vulnerability Assessment and Penetration Testing (VAPT) of locally hosted internet, intranet facing applications, servers, Desktops and Network & Security devices placed at IFTAS Datacenters at Hyderabad and Mumbai.

Vulnerability Management Services:

- Define key risk areas.
- Complete visibility of vulnerabilities.
- Analyse scan results with intelligence.
- Customize reporting for clear visibility.
- Prioritized to-do lists that can be put to action straight away.
- Remediation Activities.

2. Timelines

Indicative time frame for the overall process is as shown below

S. No	Particulars	Date
1	Issuance of RFQ document	15-Jul-2020
2	Last date for seeking clarifications on the RFQ	20-Jul-2020
3	IFTAS response to clarifications sought	22-Jul-2020
4	Last date for submission of Technical Bid	27-Jul-2020 before 3:00pm
5	Last date for submission of Commercial Bid	27-Jul-2020 before 3:00pm
6	Opening of Technical Bid	27-Jul-2020 at 3:00pm
7	Technical Presentation	30-Jul-2020
8	Opening of Commercial Bid	To be declared in due course
9	Name and address for Communication	Indian Financial Technology and Allied Services (IFTAS), Unit No. 201, B2 Building, Kanakia Boomerang, Chandivali Farm Road, Chandivali, Andheri (East), Mumbai- 400072, India. (Or) NCC House 4th Floor West wing (near Inorbit Mall) Madhapur, Hyderabad- 500081
10	Bid Related to be mailed to	RFP@iftas.in

3. Terminology

S No	Term	Expansion / Description
1	Bidder/ Vendor/ OEM	Respondent to the RFQ document.
2	RFQ	Request for quotation
3	IFTAS	India Financial Technology & Allied Services
4	RBI	Reserve Bank of India
5	Proposal/Bid/Quotation	Bidder's written reply or submission in response to this RFQ
6	Agreement	The contract signed between the IFTAS and the Selected Bidder and all the attached documents. The "Agreement" includes the RFQ, subsequent modifications to the RFQ, response of the selected vendor to the RFQ and the contract document itself.
7	Authorized Signatory	The person authorized by the company's Board/ Managing Director/ Director for signing the bid documents on behalf of the company. The authorized signatory should give a declaration and through authenticated documentary evidence to establish that he/she is empowered to sign the bid documents and bind the bidder.
8	Incident	Any event / abnormalities in the functioning of the any of the components of the "Total Solution" that may lead to disruption in normal operations
9	VA & PT	Vulnerability Assessment and penetration testing
10	VM	Vulnerability Management

4. Instruction to Bidders

Bidders shall send technical and commercial bids in separate mail with Subject "Technical bid for Implementation of Vulnerability Management Tool - RFQ No. IFT/VM/200715-1" and "Commercial bid for Implementation of Vulnerability Management Tool - RFQ No. IFT/VM/200715-1".

All attachments for "Technical bid" should be in PDF format and "Commercial bid" should be password protected. All the mails to be sent by authorised personnel of the bidder to IFTAS' email address RFP@iftas.in.

All the PDF documents should be digitally signed by the Authorized person of the bidder.

****Bidders should not share the password for commercial bid unless it is requested by RFP@iftas.in**

5. Purpose of RFQ

A. The purpose of this RFQ is to Supply, install, integrate and support the Vulnerability Management tool at IFTAS DC & DR location on subscription basis for 5 years. Vulnerabilities can be discovered with a vulnerability scanner, which analyzes a computer system in search of known vulnerabilities, such as open ports, insecure software configurations, and susceptibility to malware infections.

B. Based on the contents of the RFQ, the selected Bidder shall be required to independently arrive at approach and methodology, based on industry best practices and RBI guidelines, suitable for the IFTAS, after taking into consideration the effort estimate for completion of the same and the resource and the equipment requirements. The approach and methodology will be approved by the IFTAS.

6. Scope of work

6.1 Setting-up of VM Solution

A. Supply, install, integrate and upgrade all the Vulnerability Management technologies together at IFTAS premises for 5 years of on subscription basis for proposed VM infrastructure, which will be upgraded from time to time and all such IT infrastructure which will get added, upgraded etc. at IFTAS during the Contract period.
B. Vulnerability Assessment and Penetration Testing should cover the intranet and internet application and its components including web server, app server, DB Server, Thick client, Thin clients, Mobile applications, Networking systems, Security devices, load balancers etc. , websites maintained at IFTAS's premises in Mumbai and Hyderabad.
C. Vulnerability assessment must be carried out for all the applications/critical devices of the IFTAS on quarterly basis and required 1024 IP/asset's license for Vulnerability.
D. The Bidder shall conduct scheduled penetration testing (i.e. quarterly once) for identified devices / networks to identify security issues/vulnerabilities that could be exploited by remote attackers. The penetration testing exercise must give IFTAS an holistic view of overall infrastructure security of the asset as seen from the Internet/outside organization.
E. VAPT activities: VAPT should be comprehensive but not limited to following activities:
    - Network Scanning
    - Port Scanning
    - System Identification & Trusted System Scanning
    - Vulnerability Scanning
    - Malware Scanning
    - Spoofing
    - Scenario Analysis
    - Application Security Testing & Code Review
    - OS Fingerprinting
    - Service Fingerprinting
    - Access Control Mapping

- Denial of Service (DOS) Attacks
- DDOS Attacks
- Authorization Testing
- Lockout Testing
- Password Cracking
- Cookie Security
- Functional validations
- Containment Measure Testing
- War Dialing
- DMZ Network Architecture Review
- Firewall Rule Base Review
- Server Assessment (OS Security Configuration)
- Security Device Assessment
- Network Device Assessment
- Database Assessment
- Website Assessment (Process)
- Vulnerability Research & Verification
- IDS/IPS review & Fine tuning of Signatures
- Man in the Middle attack
- Man in the browser attack
- Any other attacks

F. Compliance of Regulatory guidelines/Advisories: Successful Bidder shall perform VAPT and ensure that regulatory guidelines issued by various bodies such as RBI, Cert-In, NCIIPC, etc are followed.

G. Website/Web/Mobile – Application Assessment: Website/Web- Application/Mobile application assessment should be done as per latest OWASP guidelines including but not limited to the following:

- Injection
- Broken Authentication and Session Management
- Cross-Site Scripting (XSS)
- Insecure Direct Object References
- Security misconfiguration
- Insecure Cryptographic Storage
- Sensitive Data Exposure
- Failure to Restrict URL Access
- Missing Function Level Access Control
- Cross-Site Request Forgery (CSRF)
- Using Known Vulnerable Components
- Un-validated Redirects and Forwards
- Insufficient Transport Layer Protection
- Any other attacks, which are vulnerable to the web sites and web Applications

H. The penetration testing should include testing for information pilferage, denial of service, password cracking, brute force attack etc.
I. Proactively inform about potential security threats/vulnerabilities, new global security threats/ zero-day attacks in circulation and suggest and implement suitable countermeasures to safeguard IFTAS IT assets and data against such evolving threats / attacks along with the analysis.
J. The Dashboard shall Generate Executive Reports in graphical format and Technical Reports in text format for all penetration tests conducted.
K. Assessment document should necessarily contain proof/evidence of the vulnerabilities identified
L. All the licenses provided as part of BoM should strictly adhere to requirements of the RFQ. If during the Contract period, it is observed by IFTAS that provided licenses are not adhering to the RFQ requirements then all the additional hardware/software/licenses should be provided and configured without any additional cost to IFTAS.
M. IFTAS team is going to manage the day to day operations on Vulnerability Management solution. In case of any issue /upgradation/customization on VM tool level, bidder must extend their support to IFTAS team.
N. Vulnerability Management console should run in active & passive mode in DC and DR.

6.2 Support during Contract Period

A. Product licenses should be Enterprise licenses. License date will start after go live sign off from IFTAS.
B. The Bidder further represents and warrants that all licenses delivered /rendered under and in accordance with this Contract shall have no defect, arising from design or from any act, error/defect or omission of the Bidder
C. Any defective equipment /software supplied by Bidder shall be replaced by Bidder at no additional cost to IFTAS, including all incidental cost the upgrades, new releases (Minor/Major) versions; bug fixes etc. for the software will be supplied to IFTAS at no extra cost, with the necessary documentation during the contract period.
D. Bidder shall implement all software updates, new releases & version upgrades on the supplied components during the contract period. Bidder should update and maintain all supplied components to correctly reflect actual state of the setup at any point in time during the contract period.
E. Bidder shall provide and install patches/ updates/ version upgrades of all software provided under this contract at no extra cost to IFTAS during the contract period.
F. In case of deficiency in performance of the Solution, as per the Scope of Work, during the contract period, the successful bidder shall provide additional software as required at his own cost. IFTAS shall not reimburse cost of such software, if any.
G. 24x365 telephonic and online support should be made available by the bidder for online troubleshooting to address any technical issues including configuration and breakdowns.

H. IFTAS should able to log calls directly by web/email or over phone to the bidder/OEM 24x365 during the contract period. Accordingly, escalation matrix of the bidder/OEM and confirmation letter from bidder and OEM should be submitted.
I. IFTAS, initial Support & contract period would be for 5 Years and it may be further extended based on the mutually agreed terms and conditions. Any escalation / increase in the cost will be calculated based on Indexation formula as per Annexure X

6.3 Obsolescence

The Bidder will ensure that the stipulated Support and maintenance facilities on the hardware / software / solution will be available for a contracted period of 5 years. The proposed product should not be under "End of Support" for the next 5 years from the date of final signoff. The vendor will constantly update IFTAS on new technologies that could prove cost effective.

6.4 Training for Vulnerabilities Awareness

The Bidder shall provide a comprehensive training to IFTAS team on Vulnerability management tool and its features twice a year.

6.6 Project Timeline

Delivery and Implementation of the license to be completed within 6 - 7 days from the date of Purchase Order.

7. Eligibility Criteria

S No	Eligibility Criteria	Documentation Required/Compliance/Non-Compliance
1.	Bidder must have registration under companies Act, 1956, also registered with the Goods & Service Tax authorities, and must have completed 3 years of existence as on Bid calling date.	Attested copy of the Certificate of Incorporation/Registration of the Bidder/RoC.
2.	The Bidder should have a minimum annual turnover of at least Rs. 1 Crores in each of the last three financial years. The Bidder should have made positive net worth in each of the last three financial years.	Audited financial statements indicating the net profit and the net worth as required set forth in the eligibility criteria. and Auditor / Chartered Accountant Certificate in support of the criterion
3.	The bidder may be either an OEM or highest-level Authorized Partner of the OEM (Original Equipment Manufacturer) whose product they are proposing. In case the OEM does not deal directly, an OEM may bid through their Authorized Service Partners or System Integrator.	Undertaking from the OEM mentioning a clause that OEM will provide support services during contract period if the bidder authorized by then fails to perform. In case of an authorized representative, a letter of Authority and response from OEM through bidder form original manufacturer must be furnished in original duly signed & stamped (As per Annexure-VIII and Annexure-IX)
4.	The bidder should be currently in the service of providing Vulnerability management/Managed services in Security solutions including at least two Government/public/BFSI in India	Proof of Client Certificate is to be Submitted.
5.	The Vulnerability Management application of the proposed solution must be in the Leaders Quadrant of Gartner's Magic Quadrant 2019 or latest or any other such equivalent.	Bidder should attach copy of the Report.

7.1 Evaluation Process

A. For the purpose of the evaluation and selection of bidder for this project, a two-stage bidding process will be followed. The stages are (1) Technical Bid and (2) Commercial Bid.
B. The Technical bid will contain the exhaustive and comprehensive technical details, whereas the Commercial Bid will contain the pricing information. The Technical Bid shall NOT contain any pricing or commercial information at all and if the Technical Bid contains any price related information, then that Technical Bid would be disqualified and will NOT be processed further. The bidder shall submit the technical and commercial bids separately as per the timelines specified in this RFQ.
C. Technical bid includes eligibility criteria and technical evaluation. Only bids from bidders meeting the eligibility criteria and which are complete and responsive will proceed to the stage of being fully evaluated and compared. Bids qualifying the Eligibility criteria mentioned under Section 7 shall proceed to the next stage of evaluation process i.e. technical evaluation.
D. The objective of technical evaluation stage is to evaluate the bids to select an effective and best fit solution. Evaluation by IFTAS will be undertaken under the guidance of the Procurement Committee formed by the IFTAS which would have IFTAS officials. The decision of the Procurement committee shall be final.
E. Bidders satisfying the Technical evaluation as per the technical evaluation matrix under section 7.2 shall be qualified for commercial evaluation.
F. In the commercial evaluation phase, the lowest commercial bidder (L1) will be identified. Subsequently if necessary further negotiation is possible with other competent bidder to select and award the project as per advice of Procurement committee

7.2 Technical Evaluation Matrix

A. Technical Bids will be opened and evaluated based on the technical bid submissions and presentations.
B. Bidders would be invited to IFTAS to make an exclusive presentation detailing the proposed solution, implementation approach, rollout strategy, for the solution.
C. IFTAS may interact with the Customer references submitted by bidder, if required.
D. An overall cut-off score of 75 marks will be essential for the bidders to be qualified for the next stage of the selection process i.e. commercial evaluation.
E. The bidder is required to present details of the proposed hardware and its related environment, configuration etc. keeping in view of the requirements of the solution.

S.No	Parameter	Details	Maximum Score
1.	Technical Requirement	Meeting Technical Requirement as per Annexure V	30
2.	Implementation Experience	No of Implementation in Government / Public and BFSI sector	20
3.	Overall solution compatibility	• Suitability and compatibility of solution • Uniqueness of solution approach in design	35

		architecture and understanding of IFTAS requirement. • Integration with existing infrastructure • Implementation Plan & along with offsite support availability.	
4.	Presentation	Technical coverage, solution capabilities, ease of integration, ease of use, quality of reports, etc.	15
Total			100

8. Payment Terms and Conditions

The following are the payment terms and conditions after the contract between IFTAS and the selected bidder is signed:

8.1 Delivery, Implementation, Training and Support

a. 100 % of the implementation cost will be paid on completion of installation and acceptance sign-off from IFTAS.

b. Subscription cost will be paid annually in arrears and for the first year on completion of installation and acceptance sign-off from IFTAS.

Other Payment conditions

a. All payments will be released based on submission of invoices along with necessary SLA evidence/reports of rendering of service as required.
b. Payment will be released within 45 days of receipt of correct invoices along with necessary documents / certificates duly signed by authorized IFTAS official.
c. Prices should be quoted in INR only.
d. Price shall remain fixed during the contract period. There shall be no increase in price for any reason whatsoever and therefore no request for any escalation of the cost / price shall be entertained.
e. The awardee is required to quote GST No. on the invoice submitted for the payment.

9. Service Level Standards/ Requirements/ Agreement

a) Service level requirements

- Service level plays an important role in defining the Quality of Services (QoS). The prime objective of service levels is to ensure high quality of services from selected bidder/authorized partner, in an efficient manner to the identified users under this procurement.
- The service level shall be tracked on a periodic basis and have penalty clauses on non-adherence to any of them. The Bidder shall submit reports on all the service levels to the Purchaser in accordance with the specified formats and reporting periods and provide clarification, if required. The service levels defined below provide for target level of services required, measurements thereof and associated penalties

Sr. No.	Service Area	Service Level- Business Utility (BU)	Penalty (Penalty is percentage of Quarterly charges* except for those items where other percentage has been explicitly mentioned)
1	Vulnerability Assessment	The Vendor is expected to extend support to the provided Vulnerability Management Solution in the event of tool going unresponsive or any software glitches in the tool. An incident needs to be logged for all such identified possibilities and the incident response SLA shall apply for these.	Delay in restoring VM tool beyond notice period of 24 hours will attract penalty of 2% every 8 hours. Any vulnerability which was present in the plugin of the scanner and was not selected/overlooked will lead to penalty of 2% per day. All the above SLA will have cap of 10%.
2	Penetration Testing	The Vendor is expected to provide PT Reports with remediation steps. An incident needs to be logged for all vulnerabilities identified and the incident response SLA shall apply for these.	To be conducted for list of IPs shared by IFTAS. Frequency of PT per quarter or higher frequency as desired by IFTAS. PT should be initiated within 48 hrs from the time of informing to bidder. PT reports to be submitted within 2 days from the date of test completion and any delay beyond that shall incur a penalty of 5% per 12 hours with cap of 10% . Penetration testing - Ad-hoc basis PT as and when required by IFTAS with an advance intimation of 48 hours to the Vendor. In case of urgency, period can be shorter.

10. Clarification on the Tender Documents

A. Written requests for clarification should be submitted to the IFTAS through email / letter and the same should reach IFTAS on or before the dates as given in the time-table section of this RFQ.
B. Both questions and responses will be circulated to all prospective bidders i.e., those that have obtained the tender document after the pre-bid meeting as per the timetable mentioned in this RFQ.
C. Any pre-bid queries can be sent to the designated email id (RFP@iftas.in) as per the timelines mentioned in the timetable in this RFQ. The questions/points of clarification and the responses will be shared with all the bidders. Alternatively, IFTAS may at its discretion, answer all such queries in the Pre-bid meeting. It may be noted that all queries, clarifications, questions, relating to this RFQ, technical or otherwise, should be only to the designated email id as stated earlier. For this purpose, communication to any other email id or through any other mode will not be entertained.
D. The IFTAS reserves the right to pre-pone or post-pone the date as mentioned in the above section 2. The Bidders will be informed of any changes to the date appropriately via designated email id.
E. No queries will be entertained after the last date of receiving clarifications.
F. Bidders must acquaint themselves fully with the conditions of the tender. No plea of insufficient information will be entertained at any time.

11. Performance Bank Guarantee:

The bidder shall at its own expense deposit with IFTAS within thirty (30) working days of the date of notice of award of the tender, a Performance Bank Guarantee from a scheduled commercial bank, payable on demand in terms of Annexure-IV, for an amount equivalent to ten percent (10%) of the contract price for the due performance and fulfillment of the contract.

Performance Bank Guarantee may be discharged by IFTAS upon being satisfied that there has been due performance of the obligations of the bidder under the contract. Performance Bank Guarantee shall be valid for contracted period.

Failure of the bidder to comply with the above requirement, or failure of the bidder to enter into a contract within 30 days or within such extended period, as may be specified by the IFTAS shall constitute sufficient grounds, among others, if any, for the annulment of the award of the tender.

12. Termination of Purchase Order/Contract:

IFTAS by written notice to successful Bidder may terminate the contract in whole or in part at any time for this convenience giving 15 days prior notice. The notice of termination shall specify that the termination is for convenience the extent to which successful Bidder's performance under the contract is terminated and the date upon which such termination become effective.

- The bidder goes into liquidation voluntarily or otherwise.
- The selected Bidder commits a breach of any of the terms and conditions of the bid/contract.

- An attachment is levied or continues to be levied for a period of 7 days upon effects of the bid.
- The progress regarding execution of the contract, made by the selected bidder is found to be unsatisfactory.
- If deductions on account of liquidated Damages exceeds more than 10% of the total contract price.
- After the award of the contract, if the selected bidder does not perform satisfactorily or delays execution of the contract, IFTAS reserves the right to get the balance contract executed by another party of its choice by giving one months' notice for the same. In this event, the selected bidder is bound to make good the additional expenditure, which IFTAS may have to incur to carry outbidding process for the execution of the balance of the contract. This clause is applicable, if for any reason, the contract is cancelled.
- IFTAS reserves the right to recover any dues payable by the selected bidder from any amount outstanding to the credit of the selected bidder, including the pending bills and/or invoking Bank Guarantee, if any, under this contract or any other contract/order. Work, Study Reports, documents, etc. prepared under this contract will become the property of the IFTAS.

The bidder shall deliver all the requirements and complete all necessary documentation as per the requirements mentioned in this RFQ. In the event of an unforeseeable delay, the bidder shall approach IFTAS for an approval extend the timelines with complete justification and reasoning. The discretion to extend the timelines shall rest solely under the discretion of IFTAS, and in the event that extension is provided, the same shall be maintained by the bidder at no extra cost to IFTAS.

13. Force Majeure

The bidder or IFTAS shall not be responsible for delays or non-performance of any or all contractual obligations, caused by war, revolution, insurrection, civil commotion, riots, mobilizations, strikes, blockade, acts of God, plague or other epidemics, fire, flood, acts of government or public enemy or any other event beyond the control of either party, which directly, materially and adversely affect the performance of any or all such contractual obligations.
If a Force Majeure situation arises, the bidder shall promptly notify IFTAS in writing of such conditions and any change thereof. Unless otherwise directed by IFTAS in writing, the bidder shall continue to perform its obligations under the contract as far as possible and shall seek all means for performance of all other obligations, not prevented by the Force Majeure event.

14. Governing Law and Disputes

The bids and any contract resulting there from shall be governed by and construed according to the Indian Laws.
All disputes or differences whatsoever arising between the parties (i.e., the Organization and bidders) out of or in relation to the construction, meaning and operation or effect of this Tender Document or breach thereof, shall be settled amicably. If, however, the parties, as above, are not able to resolve them amicably, the same shall be settled by arbitration in accordance with the applicable Indian Laws, and the award made in pursuance thereof shall be binding on the parties, as above. The Arbitrator/Arbitrators shall give a reasoned award.

The Bidder shall continue work under the Contract during the arbitration proceedings unless otherwise directed in writing by the IFTAS or unless the matter is such that the work cannot possibly be continued until the decision of the arbitrator or of the umpire, as the case may be, is obtained. The venue of the arbitration shall be Mumbai/Hyderabad, India.

Disqualification Parameters in Technical Bid Evaluation

a) IFTAS at its discretion may reject the quotation of the Bidder without giving any reason whatsoever, if in the IFTAS opinion, the quotation was not made appropriately to meet the performance criteria or security requirements as stipulated by IFTAS.
b) IFTAS at its discretion may reject the quotation of the Bidder without giving any reason whatsoever, if in the opinion of IFTAS, the Bidder could not present or demonstrate the skill set as described in the quotation.
c) IFTAS at its discretion may reject the quotation of the Bidder, in case the responses received from the reference sites are negative.
d) IFTAS reserves the right to disqualify any bidder, who is involved in any form of lobbying/ influencing/ canvassing etc., in the evaluation / selection process and any other disqualification criteria mentioned in this RFQ.

15. Disqualification Parameters in Bid Evaluation

a) IFTAS at its discretion may reject the quotation of the Bidder without giving any reason whatsoever, if in the IFTAS opinion, the quotation was not made appropriately to meet the performance criteria or technical requirements as stipulated by IFTAS.
b) IFTAS at its discretion may reject the quotation of the Bidder, in case the responses received from the reference sites are negative.
c) IFTAS reserves the right to disqualify any bidder, who is involved in any form of lobbying/influencing/ canvassing etc., in the evaluation / selection process and any other disqualification criteria mentioned in this RFQ.
d) The commercial bid shall be submitted strictly as per the commercial format enclosed in the RFQ as Annexure VI It shall be submitted in clear printed form. Handwritten bids, any modification in format etc. will be disqualified.

16. Confidentiality of Information

a) Bidder will acknowledge that during the performance of this Agreement, IFTAS may disclose certain confidential information to Bidder to further the performance of this Agreement. For purpose of this Agreement, the term “Confidential Information” means any and all oral or written information that is not generally known and that receiving Party obtained pursuant to this Agreement and the term “Confidential Information” shall include, but shall not be limited to, papers, documents, writings, classified information, inventions, discoveries, know how, ideas, computer programs, source codes, object codes, designs, algorithms, processes and structures, product information, research and development information and other information relating

thereto, financial data and information and processes of a business, commercial, technical, scientific, operational, administrative, financial, marketing or intellectual property nature or otherwise and any other information that Bank may disclose to Bidder, or that Bidder may come to know by virtue of this Agreement.

b) The successful Bidder shall not, without the Bank's prior written consent, disclose the Contract or any provision thereof, or any specification or information furnished by or on behalf of the IFTAS in connection therewith, to any person other than a person employed by the Successful Bidder in the performance of the Contract. Disclosure to any such employed person shall be made in confidence against Non-disclosure agreements completed prior to disclosure and disclosure shall extend only so far, as may be necessary for the purposes of such performance.
c) Any document, other than the Contract itself, shall remain the property of IFTAS and all copies thereof shall be returned to IFTAS on termination of the Contract.
d) The successful Bidder shall not, without the IFTAS's prior written consent, make use of any document or information above except for the purposes of performing the Contract.

17. Use of Contract Documents and Information

The bidder shall not, without prior written consent from IFTAS, disclose the contract or any provision thereof, or any specification or information furnished by or on behalf of IFTAS in connection therewith, to any person other than a person employed by the bidder in the performance of the contract. Disclosure to any such employed person shall be made in confidence against non-disclosure agreements completed prior to disclosure and disclosure shall extend only so far, as may be necessary for the purposes of such performance.
Any document, other than the contract itself, shall remain the property of IFTAS and all copies thereof shall be returned to IFTAS on termination of the contract.
The bidder shall not, without IFTAS's prior written consent, make use of any document or information except for the purposes of performing the contract.
The provisions of Section 14 shall survive termination / expiry of the contract for a period of one year thereafter, and shall not apply to information which:

a) Now or hereafter enters the public domain through no fault of that party.
b) Can be proven to have been in possession of that party at the time of disclosure and which was not previously obtained, directly or indirectly, from the other party hereto; or
c) Otherwise lawfully becomes available to that party from a third party under no obligation of confidentiality.

18. Indemnification

The bidder shall, at its own cost and expenses, defend and indemnify IFTAS against all third-party claims including those of the infringement of Intellectual Property Rights, including patent, trademark, copyright, trade secret or industrial design rights, arising from use of the products or any part thereof in India.

The bidder shall expeditiously meet any such claims and shall have full rights to defend itself there from. If FTAS is required to pay compensation to a third party resulting from such infringement, the bidder shall be fully responsible therefore, including all expenses and court and legal fees.

IFTAS will give notice to the bidder on any such claim and shall provide reasonable assistance to the bidder in disposing of the claim.

The bidder shall also be liable to indemnify IFTAS, at its own cost and expenses, against all losses/damages, which IFTAS may suffer on account of violation by the bidder of any or all national/international trade laws, norms, standards, procedures, etc.

19. Documents

The bidder shall arrange for and provide the following documents during the bidding:

Annexure -I: Bidder's Guarantee Certificate
Annexure -II: Non-Disclosure Agreement
Annexure -III: Conformation to Terms and Conditions
Annexure-IV: Performance Bank Guarantee
Annexure-V: Technical Specifications of Vulnerability Management
Annexure-VI: Commercial Bid format
Annexure-VII: Address for locations
Annexure-VIII: Response from OEM through Bidder
Annexure-IX: Letter of Authority
Annexure-X: Indexation Formula

Annexure -I: Bidder's Guarantee Certificate

(On the letterhead of Bidder)
Place:
Date:

To
Indian Financial Technology and Allied Services (IFTAS),
Unit No. 201, B2 Building,
Kanakia Boomerang,Chandivali Farm Road,
Chandivali, Andheri (East),
Mumbai- 400072, India.

Dear Sir,

Sub: Request for Quotation (RFQ) for Vulnerability Management at IFTAS.

Being duly authorized to represent and act on behalf of …… (hereinafter referred to as "the Applicant") and having reviewed and fully understood all of the qualification requirements and information provided, the undersigned hereby apply Request for Quotation (RFQ) for Vulnerability Management at IFTAS. The details as per the requirements of the RFQ enquiry are enclosed for your consideration.

Yours faithfully,

_____
(Signature of Authorized Signatory) <NAME, TITLE AND ADDRESS>

FOR AND ON BEHALF OF
<NAME OF THE APPLICANT ORGANISATION>

Annexure -II: Non-Disclosure Agreement

(On INR 100 stamp paper)
To
Indian Financial Technology and Allied Services (IFTAS),
Unit No. 201, B2 Building,
Kanakia Boomerang,Chandivali Farm Road,
Chandivali, Andheri (East),
Mumbai- 400072, India.

[Date]
[Salutation]
Confidentiality Undertaking

We acknowledge that during the course of contract period of Vulnerability Management at IFTAS, we may have access to and be entrusted with Confidential Information. In this letter, the phrase "Confidential Information" shall mean information (whether of a commercial, technical, scientific, operational, administrative, financial, marketing, business, or intellectual property nature or otherwise), whether oral or written, relating to IFTAS and its business that is provided to us pursuant this Agreement. In consideration of you making Confidential Information available to us, we agree to the terms set out below:

1. We shall treat all Confidential Information as strictly private and confidential and take all steps necessary (including but not limited to those required by this Agreement) to preserve such confidentiality.
2. We shall use the Confidential Information solely for the preparation of our response to the RFQ and not for any other purpose.
3. We shall not disclose any Confidential Information to any other person or firm, other than as permitted by item 5 below.
4. We shall not disclose or divulge any of the Confidential Information to any other client of [name of product vendor / implementation partner]
5. This Agreement shall not prohibit disclosure of Confidential Information:
   - To our partners/directors and employees who need to know such Confidential Information to assist with the bidding for RFQ floated for deploying Cyber Security consultant at IFTAS location;
   - With your prior written consent, such consent not to be unreasonably withheld;
   - To the extent that such disclosure is required by law;
   - To the extent that such disclosure is required by any rule or requirement of any regulatory authority with which we are bound to comply; and
   - To our professional advisers for the purposes of our seeking advice. Such professional advisors will be informed of the need to keep the information confidential.
6. Upon your request we shall arrange delivery to you of all Confidential Information, and copies thereof, that is in documentary or other tangible form, except:
   - For the purpose of a disclosure permitted by item 5 above; and
   - To the extent that we reasonably require to retain sufficient documentation that is necessary to support any advice, reports, or opinions that we may provide.
7. This Agreement shall not apply to Confidential Information that:
   - Is in the public domain at the time it is acquired by us;
   - Enters the public domain after that, otherwise than as a result of unauthorized disclosure by us;
   - Is already in our possession prior to its disclosure to us; and
   - Is independently developed by us.
8. This Agreement shall continue perpetually unless and to the extent that you may release it in writing.

9. We acknowledge that the Confidential Information will not form the basis of any contract between you and us
10. We warrant that we are acting as principal in this matter and not as agent or broker for any person, company, or firm.
11. We acknowledge that no failure or delay by you in exercising any right, power or privilege under this Agreement shall operate as a waiver thereof nor shall any single or partial exercise thereof or the exercise of any other right, power, or privilege.
12. This Agreement shall be governed by and construed in accordance with Indian law and any dispute arising from it shall be subject to the exclusive jurisdiction of the Mumbai courts.

We have read this Agreement fully and confirm our agreement with its terms

Yours sincerely

Signature and Stamp of Company
[Authorized Signatory (same as signing the quotation) – Implementation Partner]
Name:
Position:
Date:

Authorized Signatory Designation Bidder's corporate name

Annexure -III: Conformation to Terms and Conditions
(On letterhead of the Bidder)

To
Indian Financial Technology and Allied Services (IFTAS),
Unit No. 201, B2 Building,
Kanakia Boomerang,Chandivali Farm Road,
Chandivali, Andheri (East),
Mumbai- 400072, India.

Dear Sir,

Sub: Request for Quotation (RFQ) for deploying Vulnerability Management.

Further to our quotation dated _____, in response to the Request for Quotation (RFQ) for Vulnerability Management at IFTAS location issued by IFTAS we hereby covenant, warrant and confirm as follows:

We hereby agree to comply with all the terms and conditions / stipulations as contained in the RFQ and the related addenda, other documents and if required including the changes made to the original bid documents issued by IFTAS, shall form a valid and binding part of the aforesaid RFQ document. IFTAS is not bound by any other extraneous matters or deviations, even if mentioned by us elsewhere either in our quotation or any subsequent deviations sought by us, whether orally or in writing, and IFTAS's decision not to accept any such extraneous conditions and deviations will be final and binding on us.

Yours faithfully,

Annexure-IV: Performance Bank Guarantee

Performance Bank Guarantee

To COO,
Indian Financial Technology and Allied Services,
Unit No. 201, B2 Building, Kanakia Boomerang,
Chandivali Farm Road, Chandivali,
Andheri (East), Mumbai- 400072, India.

Dear Sirs,

PERFORMANCE BANK GUARANTEE – for …….

WHEREAS

M/s. (name of Service Provider), a company registered under the Companies Act, 1956, having its registered and corporate office at (address of the Service Provider), (hereinafter referred to as "our constituent", which expression, unless excluded or repugnant to the context or meaning thereof, includes its successors and assigns), entered into a Purchase Agreement dated.. (Hereinafter, referred to as "the said Agreement") with you (IFTAS) for Vulnerability Management for IFTAS as detailed in the said Agreement.

We are aware of the fact that in terms of sub-para (…), section (…), chapter (…) of the said Agreement, our constituent is required to furnish a Bank Guarantee for an amount Rs……. (in words and figures), being 10% of the Contract Price of Rs. … (in words and figures), as per the said Agreement, as security against breach/default of the said Agreement by our Constituent.

In consideration of the fact that our constituent is our valued customer and the fact that it has entered into the said Agreement with you, we, (name and address of the bank), have agreed to issue this Performance Bank Guarantee.

Therefore, we (name and address of the bank) hereby unconditionally and irrevocably guarantee you as under:

a) In the event of our constituent committing any breach/default of the said Agreement, which breach/default has not been rectified within a period of thirty (30) days after receipt of written notice from you, we hereby agree to pay you forthwith on demand such sum/s not exceeding the sum of Rs…… (in words and figures) without any demur.
b) Notwithstanding anything to the contrary, as contained in the said Agreement, we agree that your decision as to whether our constituent has made any such default/s / breach/es, as afore-said and the amount or amounts to which you are entitled by reasons thereof, subject to the terms and conditions of the said Agreement, will be binding on us and we shall not be entitled to

ask you to establish your claim or claims under this Performance Bank Guarantee, but will pay the same forthwith on your demand without any protest or demur.

c) This Performance Bank Guarantee shall continue and hold good till the completion of the contracted period for the 'Total Solution' i.e. (date), subject to the terms and conditions in the said Agreement.
d) We bind ourselves to pay the above said amount at any point of time commencing from the date of the said Purchase Agreement until the completion of the contracted period for the Total Solution as per said Agreement.
e) We further agree that the termination of the said Agreement, for reasons solely attributable to our constituent, virtually empowers you to demand for the payment of the above said amount under this guarantee and we have an obligation to honour the same without demur.
f) In-order to give full effect to the guarantee contained herein, we (name and address of the bank), agree that you shall be entitled to act as if we were your principal debtors in respect of your claims against our constituent. We hereby expressly waive all our rights of surety ship and other rights, if any, which are in any way inconsistent with any of the provisions of this Performance Bank Guarantee.
g) We confirm that this Performance Bank Guarantee will cover your claim/s against our constituent made in accordance with this Guarantee from time to time, arising out of or in relation to the said Agreement and in respect of which your claim is lodged with us on or before the date of expiry of this Performance Guarantee, irrespective of your entitlement to other claims, charges, rights and relief's, as provided in the said Agreement.
h) Any notice by way of demand or otherwise hereunder may be sent by special courier, telex, fax, registered post or other electronic media to our address, as aforesaid and if sent by post, it shall be deemed to have been given to us after the expiry of 48 hours when the same has been posted.
i) If it is necessary to extend this guarantee on account of any reason whatsoever, we undertake to extend the period of this guarantee on the request of our constituent under intimation to you (IFTAS)
j) This Performance Bank Guarantee shall not be affected by any change in the constitution of our constituent nor shall it be affected by any change in our constitution or by any amalgamation or absorption thereof or therewith or reconstruction or winding up, but will ensure to the benefit of you and be available to and be enforceable by you.
k) Notwithstanding anything contained hereinabove, our liability under this Performance Guarantee is restricted to Rs…… (in words and figures) and shall continue to exist, subject to the terms and conditions contained herein, unless a written claim is lodged on us on or before the afore-said date of expiry of this guarantee.
l) We hereby confirm that we have the power/s to issue this Guarantee in your favour under the Memorandum and Articles of Association/ Constitution of our bank and the undersigned is/are the recipient of authority by express delegation of power/s and has/have full power/s to execute this guarantee under the Power of Attorney issued by the bank in his/their favour.

We further agree that the exercise of any of your rights against our constituent to enforce or forbear to enforce or any other indulgence or facility, extended to our constituent to carry out the contractual

obligations as per the said Agreement, would not release our liability under this guarantee and that your right against us shall remain in full force and effect, notwithstanding any arrangement that may be entered into between you and our constituent, during the entire currency of this guarantee.

Notwithstanding anything contained herein:

a) Our liability under this Performance Bank Guarantee shall not exceed Rs. …. (in words and figures); and
b) this Performance Bank Guarantee shall be valid only up to …….. (date, i.e., completion of contracted period for the Total Solution); and
c) we are liable to pay the guaranteed amount or part thereof under this Performance Bank Guarantee only and only if we receive a written claim or demand on or before …. (date i.e., completion of the contracted period for the Total Solution).

This Performance Bank Guarantee must be returned to the bank upon its expiry. If the Performance Bank Guarantee is not received by the bank within the above-mentioned period, subject to the terms and conditions contained herein, it shall be deemed to be automatically cancelled.

Dated …….. this …….. day …….. 2015.

Yours faithfully,

For and on behalf of the …… Bank,

(Signature)
Designation
(Address of the Bank)

Note:

a) This guarantee will attract stamp duty as a security bond under Article 54(b) of the Mumbai Stamp Act, 1958.
   A duly certified copy of the requisite authority conferred on the official/s to execute the guarantee on behalf of the bank should be annexed to this guarantee for verification and retention thereof as documentary evidence in the matter.

Annexure-V: Technical Specifications of Vulnerability Management

Vulnerability Management Specifications:

Sr No	Specifications	Mandatory (M) / Optional (O)	Comply / Partial / No	Variations/ Remarks, if any
	ARCHITECTURE, PERFORMANCE AND SCALABILITY			
1	The proposed solution must be able to operate 100% on-premise. Scan results should always be available on premise. Describe the solution's architecture. Detail all components and modules required to deliver the complete solution.	M		
2	The proposed solution must be offered as either Software Product or Software as a Service	M		
3	The proposed solution must support at least the below mentioned supported platforms as OS. - Ubuntu Linux LTS - Microsoft Windows Server - Microsoft Windows - Red Hat Enterprise Linux Server	M		
4	The proposed solution must offer both the console and scanner engines available as a hardware appliance.	O		
5	The proposed solution's hardware appliance or any equivalent technology (if proposed) must run off 64-bit OS architecture and must be able to utilize resources going beyond 4GB RAM.	O		
6	The proposed solution must not have any limit in terms of CPU & memory fetch. Deployed scanner to provide higher performance or handle more concurrent scans.	M		
7	The proposed solution must have the capability to perform both internal and external scanning.	M		
8	The proposed solution must be able to be deployed in different ways and in hybrid mode (appliance, software-based, etc.)	O		
9	The proposed solution must be able to support for centralized management of distributed scanners. Solution must be able to scan multiple network segments. No licensing cost should be imposed due to need for reporting task, user access, configuration, administration, and additional distributed on-premise scanners.	M		

10	The proposed solution must be able to scale beyond its initial deployment of 1500 devices. Describe how the product's architecture scales in larger deployments. Indicate if any additional modules or components must be purchased for deployments larger than 1500, IP addresses.	M		
11	The proposed solution must support having scan engine pooling with multiple engines grouped together to run any single scan to reduce and improve scanning time by load sharing	O		
12	The proposed solution must be able to scan with minimum performance impact on the Virtual Machines. It shall have the functionality to granular controls for managing scan speed and resource usage: - Maximum retries - Timeout Interval - Scan Delay - Packet-Per-Second Rate - Parallelism	M		
	ADMINISTRATION			
13	The proposed solution must include web-based management user interface over encrypted traffic. It must not be accessed in clear text.	M		
14	The proposed solution must support command line console within web GUI.	O		
16	The proposed solution must be able to manages multiple scanners and collect scan data from within the management user interface	M		
17	The proposed solution must support role-based access with both pre-defined and custom roles on a per user basis to allow granular controls and/or extend/restrict user permissions.	M		
18	The proposed solution must allow approval permissions to be assigned to user for vulnerability exclusions or exceptions.	M		
19	The proposed solution must support integration with Active Directory, Kerberos, or any LDAP compliant directory. LDAP must support bind credential for LDAP authentication lookups.	M		
20	The proposed solution must not impose limitation in term of number of user accounts it can create in the solution.	O		
21	Describe whether the solution provides scan scheduling, scan event and vulnerability alerts, and report generation and distribution capabilities.	M		

22	The proposed solution must support automatic vulnerability coverage updates without restart	M		
23	The proposed solution must be able to update coverage in environments where no network or internet access is available.	M		
24	The proposed solution must be able to track devices that have been virtualized and may have common MAC and/or Hostnames.	M		
25	The proposed solution's scans shall be user controllable, i.e. able to be started, stopped, paused and resumed at any time per user requirements.	M		
26	The proposed solution shall be able to schedule scans at specific starting dates and time, frequencies and maximum scan durations.	O		
27	The proposed solution shall be able to automatically pause scheduled scans if unable to complete within the predefined durations.	M		
28	The proposed solution's unfinished scheduled scans shall be able to automatically continue the scan where it previously stopped on the next scheduled session.	M		
29	The proposed solution's scheduled scans must support repeatable scans across specific time windows and intervals. Describe what happens in the event a scheduled scan is incomplete.	M		
30	The proposed solution must provide the ability to blackout times in which scans can never be run.	O		
31	The proposed solution must provide a bi-directional API access. API usage should not require additional fees.	M		
32	The proposed solution must support monitoring of active scans and automated notification when scans are complete/incomplete	M		
33	The proposed solution must support the following minimum three alerting types out of the box: - SMTP - SNMP - Syslog	M		
34	The proposed solution must include built-in diagnostic tools to display system status. Diagnostic tools shall be able to upload log files through encrypted channels to support for analysis.	O		

35	The proposed solution must be able to perform backup and restore of database, configuration files, reports, scan logs, etc.	M		
36	The proposed solution must provide secure restoration method for its backups. Describe how can this is achieved.	M		
37	The proposed solution must have built-in features to perform an export of data to an external system. The export must support a highly-optimized, indexed and efficient dimensional model that any business intelligence (BI) tool can easily connect to.	M		
	VULNERABILITY ASSESSMENT AND COVERAGE			
38	The proposed solution shall have a vulnerability database of at least 150,000 vulnerabilities checks.	O		
39	The proposed solution shall perform more than 60,000 vulnerability checks across network, operating systems, web applications and databases.	M		
40	The proposed solution must be able to discover new hosts, including default port scan settings. Describe the methods used.	M		
41	The proposed solution must be able to allow the list of default ports used for scanning to be modified (default ports excluded, or additional ports included)	M		
42	The proposed solution must be able to perform discovery, vulnerability scanning, web scanning, and compliance assessment in a single scan.	M		
43	The proposed solution must be able to perform TCP scanning in full connection scan and stealth scan, including but not limited to SYN, SYN+FIN, SYN+RST, SYN+ECE.	M		
44	The proposed solution must provide pre-configured scan templates and the ability to customize them. Describe how to configure your solution to scan for a particular vulnerability or set of vulnerabilities.	M		
45	The proposed solution must support automatic scanning for specific vulnerabilities and browse the vulnerability database by category and type.	M		
46	The proposed solution must label unsafe checks and allow users to disable these on a per-scan basis. The proposed solution must include scan templates designed to limit the impact on target assets.	M		
47	The proposed solution must have the capability to perform agentless scanning	O		

48	The proposed solution must be able to exclude vulnerabilities and assets from scans and reports.	M		
49	The proposed solution must be able to support both credentialed and non-credentialed scans which include but is not limited to: - File Transfer Protocol (FTP) - IBM AS/400 - Lotus Notes/Domino - Microsoft Windows/Samba (SMB/CIFS) - Microsoft Windows/Samba LM/NTLM Hash (SMB/CIFS) - Oracle - Post Office Protocol (POP) - Remote Execution - Simple Network Management Protocol (SNMP) - Secure Shell (SSH) - Secure Shell (SSH) Public Key - Telnet	M		
50	The proposed solution must be able to support credentials login to database including but not limited to : - DB2 - Microsoft SQL - MySQL Server - Oracle - PostgreSQL - Sybase SQLSever	M		
51	The proposed solution must be able performs local checks with credentials. Describe the ability of your product to manage credentials for hosts in a large enterprise.	M		
52	The proposed solution must support the ability to scan with a hash value to identify password reuse.	M		
53	The proposed solution must be able to provide a holistic view of the environment where users can drill down at any stage to explore, including but not limited to: - Sites - Assets - Vulnerabilities - Exploits - Malwares - Policies - Installed Software - Services	M		

	- Users & Groups - Databases - Files & Directories Listing			
54	The proposed solution must have the functionality to build a database of discovered assets and detected vulnerabilities without relying on any third party tools. - Independently of scanning frequency - Independently of scanning type - Providing real time up-to-date security posture of the environment	O		
55	The proposed solution must be able to support both IPv4 and IPv6 in the same installation.	M		
56	The proposed solution must be able to supply reference IDs from vulnerability databases such as NVD, CERT, SANS, etc.	M		
57	The proposed solution vendor must develop their own vulnerability checks. Describe internal vulnerability development. Include any internal 0-day exploit development.	M		
58	The proposed solution vendor must maintain a fixed coverage updates to all deployed consoles. Describe release cycles for newly developed coverage, including attached service-level agreements.	M		
59	The proposed solution must be able to perform both automatic & manual (i.e. online & separate offline) updates. Updating interval must be customizable within the solution.	O		
60	The proposed solution must be able to display suggested vulnerability remediation solution or reference links for each discovered vulnerability within the web interface without online/internet access (with exception to respective knowledge base for each affected product/OS/application/devices vendor).	M		
61	The proposed solution must be able to support for user-defined vulnerability signature and check creation.	M		
62	The proposed solution must have the functionality to create dynamic groups by setting conditions including but not limited to asset name, asset risk score, CVSS, host type, IP range, Operating System (OS) name, PCI compliance status, service name, site name, software name and vulnerability type.	M		
63	The proposed solution must support automatic asset discovery and inventory. Explain how the solution handles systems with changing IP addresses.	M		
64	The proposed solution must automatically discover and tag assets as they come onto the network.	O		

65	The proposed solution must provide continuous monitoring and support automated actions for a variety of criteria, including when new assets are discovered, and new vulnerability coverage is released. It had to run without automatically without human user intervention.	M		
66	The proposed solution must provide the ability to inventory all external devices associated with a given domain.	M		
67	The proposed solution must be able to integrate native exploit information from well-known sources.	M		
68	The proposed solution must be able to identify known exploits and malware kits associated with detected vulnerabilities.	M		
69	The proposed solution must provide a correlated list of: - Exploit modules available for each vulnerability - malware kits available for each vulnerability - automatic workflow to validate vulnerabilities	M		
70	The proposed solution must be able to demonstrate threat data by correlating known exploits with vulnerability found.	M		
71	The proposed solution must be able to provide information on how to develop exploit(s) to demonstrate and validate the vulnerability found.	O		
72	The proposed solution must correlate vulnerabilities across multiple tiers of the IT stack.	M		
73	The proposed solution must have functionality to pull asset inventory and publish asset risk scores to and from existing endpoint management system.	O		
74	The proposed solution must be able to connect to and scan for machines within hosted environment.	M		
76	The proposed solution must display certainty level or confidence of OS fingerprints.	M		
77	The proposed solution must be able to detect vulnerabilities in databases, network infrastructure, middleware. Describe the capability on how it works.	M		
	POLICY COMPLIANCE & CONFIGURATION MANAGEMENT			
78	The proposed solution must be able to determine if your systems comply with corporate or regulatory policies such as PCI, HIPAA, NERC, or FISMA.	M		

79	The proposed solution must include built-in compliance checks, including but not limited to CIS Hardening Guidelines, FDCC Policies and USGCB Standards.	M		
80	The proposed solution must support SCAP compliance policy checks and customized SCAP policy uploads.	M		
81	The proposed solution must include configuration and compliance assessment as part of vulnerability assessments in a single scan. Indicate if this offering is a separately installed product or module.	M		
82	The proposed solution must provide pre-packaged templates for systems in scope for ISO compliance. Describe ISO coverage.	M		
83	The proposed solution must provide a policy editor for custom configuration policy scans.	M		
84	The proposed solution must provide the ability to customize policies within the UI.	O		
85	The proposed solution must provide the ability to accept risk on individual configuration on an individual asset level.	M		
86	The proposed solution must have the ability to prioritize solutions for failures to show quickest path to remediation.	M		
87	The proposed solution must centrally manage and modify policies and easily detect misconfigurations in scan environments and must be able to highlight hosts that do not match configuration policy settings by asset, policy, and policy element.	M		
	WEB SCANNING			
88	The proposed solution must include built-in web application scanning capabilities against web technologies including but not limited to AJAX, ASP.NET 2.0 and Flash-based sites.	M		
89	The proposed solution must have the ability to correlate discovered information between web application and network/operation system scan results to uncover vulnerabilities.	O		
90	The proposed solution must support coverage of OWASP Top Ten (at least 2013) and having the ability to import from a external DAST solution(s) and display aggregated risk within the solution.	M		
91	The proposed solution must support credential login through HTTP Form and Basic Digest authentication for scanning.	M		

92	The proposed solution must support web spidering/crawling to gather security related information such as directory structures, files and applications running on the web servers.	M		
93	The proposed solution must have the functionality to set scan rate such as thread per web server and spider request delay to control bandwidth consumption and scanning time.	M		
94	The proposed solution must have the functionality to set limit of maximum foreign host to resolve, maximum directory level, maximum spidering/crawling time, maximum pages and maximum link depth.	O		
95	The proposed solution must have the functionality to exclude scan by HTTP daemon and path.	O		
	REPORTING			
96	The proposed solution must support for consolidated reporting in large deployments without any additional add-ons or fees required.	M		
97	The proposed solution must include pre-configured report templates. Provide samples of your solution's standard reports.	M		
98	The proposed solution must support report template customization from default available ones.	M		
99	The proposed solution must provide customized reports that allow at least 4 technical detail level options.	O		
100	The proposed solution must provide customized reports that allow creation of new templates and inclusion of customized logo and title.	M		
101	The proposed solution must be able to generate report based on scan groups (site), asset group (static or dynamic), tags (default and customized) and individual asset(s).	O		
102	The proposed solution must support report scheduling capabilities. Solution must be able to automatically send reports when scans are completed.	O		
103	The proposed solution must be able to distribute reports to external recipient at least in the form of email and support report scheduling capabilities. Solution should be able to automatically generate and send reports when scans are completed.	M		
104	The proposed solution must support report distribution options within the interface and via email.	O		

105	The proposed solution must support filtering vulnerabilities included in reports by category and severity.	M		
106	The proposed solution must be able to export reports in various formats such as but not limited to CSV, PDF, RTF, HTML, Text and XML.	M		
107	The proposed solution must be able to export scan data in format including but not limited to ARF, CSV, CyberScope XML, Simple, XML 1.0 and 2.0, SCAP XML, SQL Query Export and XCCDF.	M		
108	The proposed solution must include access controls to reports based on user roles.	O		
109	The proposed solution must allow SQL queries should be able to be run against reporting data model, without using third-party tools, within the solution.	O		
110	The proposed solution must provide built-in reports including but not limited to audit, baseline comparison, executive summary, PCI, policy compliance, policy details, remediation plan, top remediation, top policy remediation and vulnerability exception report.	O		
111	The proposed solution's base-line comparison reports shall include risk trend, newly added or missed assets, newly added or missed service between current and previous scans, first scan or any specific scans performed previously.	O		
112	The proposed solution must track the state of each device in order to predict which devices might be vulnerable to new 0-day attacks	M		
113	The proposed solution's reports must be prioritized according to asset or group of assets risk.	O		
	RISK AND REMEDIATION MANAGEMENT			
114	The proposed solution must calculate risk for each detected vulnerability. Risk scoring must include CVSS scoring, asset exploitability, and susceptibility to malware kits.	M		
115	The proposed solution must support CVSSv2 and CVSSv3 scoring	M		
116	The proposed solution must have at least 4 types of criticality rating to calculate risk score.	O		
117	The proposed solution must provide granular risk scoring	O		

118	The proposed solution's risk score shall include but not limit to vulnerability impact, likelihood of compromise, date of disclosure, exploit exposure and malware exposure.	O		
119	The proposed solution must provide both Quantitative (i.e.0-1000) Metrics as well as Qualitative (i.e. High,Med,Low) Metrics	O		
120	The proposed solution must have the functionality to set asset and site importance level to allow user to scale up or down the risk.	M		
121	The proposed solution must have prioritization capabilities with respect to vulnerabilities and remediation tasks. Describe how this is achieved in the solution.	M		
122	The proposed solution must provide capabilities to focus remediation efforts on critical business assets.	M		
123	The proposed solution must indicate vulnerabilities that are targeted by malware.	M		
124	The proposed solution must have ability to display suggested vulnerability remediation solution or reference links for each discovered vulnerability within the web interface without online/internet access (with exception to respective knowledge base for each affected product/OS/application/devices vendor).	M		
125	The proposed solution must provide remediation reports including engineer level instructions and cross linking to external databases for patches, downloads and references.	M		
126	The proposed solution's remediation reports must provide step-by-step guide for administrators to fix the vulnerabilities found. Steps shall be well organized with correct orders without duplicates. Steps shall also include estimated down time as a reference for the administrators.	M		
127	The proposed solution must be able to create reports that identify the top steps to reduce the risk of (a user defined) group of devices.	M		
128	The proposed solution must be able to create reports that aggregate common remediation steps across patches and other remediation steps, such as configuration changes.	M		
129	The proposed solution must support identification and management of vulnerability exceptions. Exceptions should support an approval workflow.	M		
	INTEGRATION			

130	The proposed solution must support other technology alliance partners to which it can leverage on discovered vulnerability findings to extend the value within the organization. List and describe the solution's relationships with security technology partners.	M		
131	The proposed solution must have integration with existing PIM solution at IFTAS. Details will be provided to the successful bidder.	M		
132	The proposed solution must support integration with virtual environments.	M		
133	The proposed solution must support the automatic discovery of virtual assets on: - Vmware vCenter - Vmware ESX/ESXi -KVM	O		
134	The proposed solution must have ability to identify virtual devices that are in a suspended or off state.	O		
135	The proposed solution must support integration with network topology and risk analysis products.	M		
136	The proposed solution must support integration with IDS/IPS products.	M		
137	The proposed solution must support integration with IT GRC products.	M		
138	The proposed solution must support integration with any NGSOC Solutions	M		
139	The proposed solution must support integration with external penetration testing platforms to perform and automatic vulnerabilities exploitation without running any manual imports to confirm that vulnerabilities can be exploited.	M		
140	The proposed solution must be able to automatically exclude vulnerabilities that cannot be exploited by integration with penetration testing platform.	M		
141	The proposed solution must be able to integrate with tools that provide KPIs and guidance to improved defenses on your endpoints.	M		
142	The proposed solution must be able to offer an API capability. Describe how the API is accessed, and what functions are available. Are there any additional modules or fees associated with the API?	M		
	VENDOR VIABILITY & PRODUCT STRATEGY			

143	The proposed solution vendor must be PCI ASV, that able to execute with a set of security services and tools ("ASV scan solution") to conduct external vulnerability scanning services to validate adherence with the external scanning requirements of PCI DSS Requirement 11.2.2. The scanning vendor's ASV scan solution is tested and approved by PCI SSC before an ASV is added to PCI SSC's List of Approved Scanning Vendors.	M		

Penetration Testing Requirements				
S.No	Specifications	Mandatory (M) / Optional (O)	Comply / Partial / No	Variations/ Remarks, if any
1	Solution must be able to support installation on 64-bit Linux and Windows (64-bit).	O		
2	PT shall be conducted with latest updates (e.g. exploit module)	M		
3	Must be able to perform full backup to prevent data loss and enable to easily migrate data.	M		
4	Solution must be able to integrate with VA SCANNING TOOLS to discover host's OS, running services and vulnerabilities via existing scan results or new scans.	M		
5	Solution must support importing of scan result from external solutions including but not limited to Nexpose, Metasploit, Foundstone, Microsoft, nCircle, NetSparker, Nessus, Qualys, Burp, Acunetix, AppScan, Nmap, Retina, Amap, Critical Watch, IP Address List, Libpcap, Spiceworks and Core Impact.	M		
	System Exploitation			
6	Solution shall be able to apply exploits on individual IP or multiple IPs.	M		
7	Solution shall work on exploit modules based on OS, service and vulnerability references.	M		
8	Solution shall support replay of exploitation tasks or equivalent	M		
9	Solution shall support automation of Security tests that provide a more efficient way to get specific jobs done or equivalent	M		
10	Solution shall support the reuse of manually added or captured credentials within a project to validate specified credentials on additional hosts in the target network.	M		
	Bruteforcing			
11	Solution shall support bruteforce testing on services including but not limited to AFP, SMB, Postgres, DB2, MySQL, MSSQL, HTTP, HTTPS, SSH, SSH PUBKEY, Telnet, FTP, POP3, VNC, SNMP, WinRM.	M		
12	Solution shall provide password references for factory default logins.	M		
13	Solution shall support customized credentials and dictionary import for bruteforce.	M		

14	Solution shall support credential mutation to create multiple permutations of a specified password, which enables building of a larger list based on a defined set of passwords.	M		
	Post Exploitation Action And Evidence Collection			
15	Solution must support post exploitation actions including but not limited to collect system data (screen capture, password, system information), build a virtual desktop connection, access file system, search the file system, run a command shell, create proxy pivot, create VPN pivot.	M		
	Social Engineering Campaign			
16	Solution must support web campaign, Email campaign and USB campaign.	M		
17	Solution must allow web campaign customized with http/https, IP address, port and path (e.g. https://www.abc.com:1234/abcd).	M		
18	Solution must support web content to be cloned from another web site (e.g. www.google.com).	M		
19	Solution must support email campaign content customization to include a specific URL or an agent attachment.	M		
20	Solution must support USB campaign that generates an agent deployment .exe file.	M		
	Web Application Exploitation			
21	Solution must be able to test web crawling on IPv4 and IPv6 web sites.	M		
22	Solution must test web crawling applied on a web site (e.g. http://www.abc.com) or started from a specific point (e.g. http://www.abc.com/path/starthere/).	M		
23	Solution must support detection of vulnerable URLs and parameters such as SQL Injection and Cross Site Scripting.	M		
	Report and Data Export			
24	Solution must provide standard reports and support customization if required.	M		

Annexure-VI: Commercial Bid format

Commercial Bid format for IFTAS

(On the letterhead of Bidder)

Table 1: Proposed solution					
S.No	**Description**	**Assets**	**Unit Price per asset per year**	**Total Price per year in INR**	**Total price for 5 years in INR**
		(A)	(B)	(C) =AxB	(D) = C x 5
1	Vulnerability Management Tool	1024			
2	Penetration testing as a service	50			
3	One-time Installation charges for VM Tool	-	-	-	
Total Amount (E)					
Total Applicable Tax Amount (F)					
Total Amount including Taxes (E+F= G)					

**Its Mandatory to abide on below mentioned format else it can be termed on disqualification in bidding.

Note:

1. The quantity mentioned from the perspective of arriving at TCO. Bidder is required to provide the materials as required, and as per the unit rates mentioned therein.
2. IFTAS reserves the right to select any vendor as per its requirements, and the decision of IFTAS on this matter shall be final.
3. The commercial bids shall be password protected. Passwords will be shared by the bidder by email at rfp@iftas.in strictly after email intimation from the procurement team of IFTAS. Any violation of this process will lead to rejection of bid.

Annexure-VII: Address for locations

S. No	Location	Address
1	IFTAS DC	IFTAS,Reliance Data Centre,Survey No:64,Madhapur, Hyderbad -22,Hyderbad-500019,Telangana
2	IFTAS DC(Mumbai GPX)	IFTAS GPX, Mumbai DC,GPX India Pvt Ltd. Boomerang, Chandivalli Farm Road, Near Chadivalli Studio, Andheri East, Mumbai-400072

Annexure-VIII: Response from OEM through Bidder

[On the Letter head of the OEM]

All eligibility criteria as described in the respective Annex are satisfied by the OEM M/s ……. of the product …….. The details provided in this document are correct and submitted in the below format:

Discloser and declaration

S.no	Description	Response from OEM
1	Name of the OEM	
2	Name of the product	
3	Product Category	
4	Product Name	
5	Product Version	
6	Date of the release version	
7	Appliance-Based/Software-Based solution	
8	Road Map of product including EOS and EOL	
9	Number of certified engineers giving technical support for the product in India	
10	Architectural diagram of the product	
11	Head Quarters address	
12	Address in India & Date of Incorporation in India	
13	Address of Product Development Centre	
14	Address of Product Service Centre	
15	Communication Details of Contact Official(s) – Name, Designation, Phone & Fax Number (with STD/ISD code), Mobile No. & E-mail Address	

*Same format to be used for the Anti-phishing services suitably replacing the product with services.

Annexure-IX: Letter of Authority

(This 'Letter of Authority' should be issued on the letterhead of the OEM)

Place:
Date:

To,
Indian Financial Technology and Allied Services (IFTAS),
Unit No. 201, B2 Building,
Kanakia Boomerang, Chandivali Farm Road,
Chandivali, Andheri (East),
Mumbai- 400072, India.

Dear Sir,

Sub: Request for Proposal (RFQ) for Vulnerability Management.

Dear Sir,

Subject: Letter of Authority

We have been approached by M/s_____ in connection with your RFQ name _____with No._____dated_____.

We confirm having offered to them the required software in line with your requirement. Our offer to them is for the following software/hardware for which we are the OEM and have back to back support agreement with the bidder. We confirm that we will make available all necessary components/sub-components required for providing seamless service during the tenure of the service as required in the RFQ. In case if the required components/sub-components are not available, alternate and compatible components will be made available for smooth functioning of the equipment's, as required by IFTAS.

1._____ 2._____
3._____ 4._____
5._____ . . .

The authorized agency would independently support and service the above-mentioned software / hardware during the contract period.

(Authorized Signatory) For _____

Annexure-X: Indexation Formula

Indexation Formula.

A = B {15 + 45 x (WPIc / WPIp) + 40 (CPIc / CPIp)} * 1/100

Where,

A = The contract amount for the current year

B = The contract amount for the previous year

WPIc=WholeSale price Index for Electrical Products 6 months prior to the Commencement date of contact for the current year

WPIp=WholeSale Price Index for Electrical Products 6 months prior to the Commencement date of contact for the previous year

CPIc= Consumer Price Index for industrial workers for Mumbai City 6 months prior to the commencement date of contract for the current year

CPIp= Consumer Price Index for industrial workers for Mumbai City 6 Months prior to the commencement date of contract for the previous year