ANNEXURE-I: COMMENTS ON TERMS & CONDITIONS & SERVICES/ PREBID QUERY FORMAT

Sr. No	RFP Page #	RFP Point/ Section #	Clarification point as stated in the RFP document	Category of Comment/ Suggestion/ Deviation/ Query	Comment/ Suggestion/ Deviation/ Query	Bank's Response
1	19	2.3.4 Locations Covered	Some of the applications and international territories websites are hosted at the Bank's outsourced service provider premises, public/private cloud are also under the scope of VAPT. For such locations VPN/Remote connectivity shall be arranged by the Bank.	Query	i. Total No. of applications for which servers are hosted at vendor locations. ii. Is onsite assessment of such servers required or will BOB provide VPN connectivity for feasibility. (Bank's website or any other such applications)	For remote geographical locations other than Mumbai, Hyderabad and Bangaluru, Bank shall provide VPN connectivity.
2	21	2.3.6 Deliverables	The deliverables for VAPT activity are as follows:- a. Execution of Vulnerability Assessment and Penetration Testing for the identified network devices, security devices, servers, applications, websites, interfaces (part of application), mobile applications, thick/thin clients etc. as per the Scope mentioned in this RFP and Analysis of the findings and guidance for resolution of the same b. Verification of closure of critical vulnerability. c. Perform compliance verification of closure of findings. d. Draft VAPT Report followed by final report. e. Compliance verification (Optional)	Query	Request clarification for point (c) and (e) in the Deliverables section, whether compliance verification will be considered as part of each 1st and 2nd assessment or will it be considered optional.	Compliance verification is optional however commercials need to be submitted as per the Commercial Bid format.
3	24	Legends	No. of integrations (>2)	Query	Define Integration	Integration are the exchange of parameters with different applications other than intra-module/components data/parameters exchange.
4	33	Annexure A: Eligibility Criteria	Documents required: Partnership firm Certified copy of Partnership Deed. Limited Company Certified copy of Certificate of Incorporation and Certificate of Commencement of Business. Reference of Act/Notification For other eligible entities- Applicable documents.	Query	Are all the documents to be attached or submitting any 1 will suffice the requirement.	Documents required: Partnership firm : Certified copy of Partnership Deed OR Limited Company : Certified copy of Certificate of Incorporation and Certificate of Commencement of Business OR Reference of Act/Notification For other eligible entities- Applicable documents.
5	34	Annexure A: Eligibility Criteria	Documents required: Copy of purchase order and Client certificate.	Query	Is client certificate compulsory to be attached or purchase order will suffice the requirement. In case client certificate is compulsory, please provide the certificate format. In case the client certificate is not available, will client contact suffice the requirement?	Copy of purchase order is mandatory and client certificate is non mandatory.
6	37	Annexure B: Technical Evaluation Criteria	Must possess experience in conducting VA & PT of internet facing applications and related infrastructure (Servers, Network devices, Security Devices, Databases) for at least 2 Banks in India in 4 years e.g. 2015-16, 2016-17, 2017-18, 2018-19	Query	Clarification for the evaluation criteria mentioned in point no 1 and 2 and the scoring for the same.	Must possess experience in conducting VA & PT of internet facing applications and related infrastructure (Servers, Network devices, Security Devices, Databases) for at least 2 Banks in India in block of last 4 years (2015 to 2019)
7	38	Annexure B: Methodology & Approach	Demonstration of in-depth understanding of the Bank's project requirements through the technical proposal and presentation.	Query	Tentative date for technical presentation	Tentative dates of presentation, if any, shall be informed in due course of time.

ANNEXURE-I: COMMENTS ON TERMS & CONDITIONS & SERVICES/ PREBID QUERY FORMAT

Sr. No	RFP Page #	RFP Point/ Section #	Clarification point as stated in the RFP document	Category of Comment/ Suggestion/ Deviation/ Query	Comment/ Suggestion/ Deviation/ Query	Bank's Response
8	43	Annexure D: Technical Bid Format	Details of the similar assignments on hand as on date (Name of the Bank, time projected for execution of the assignment and documentary proofs such as work order are to be furnished)	Query	Is there any minimum number requirement of assignments to be listed?	Please provide details of similar assignments on hand as on 31/03/2019.
9	50	Annexure J	Commercial Bid Format	Query	Repeat assessment consists of only compliance of observations reported in 1st Assignment or is complete assessment of the application is expected.	Repeat assessments shall be complete re assessments of application whereas compliance testing is limited to verification of closure of observations.
10	50	Annexure J	Commercial Bid Format	Query	Define Notional Count	Notional count is for Bids evaluation purpose only. Actual numbers of High, Medium, Low may vary depending upon the Bank's requirement from time to time.
11	14	2.3 Project Scope	Vulnerability Assessment and Penetration Testing should cover the application and its components including web server, app server, DB Server, Thick client, Thin clients, Mobile applications, Networking systems, Security devices, load balancers etc. accessible with public IP's, websites maintained at Bank's premises in Mumbai, Hyderabad and Bangaluru including Bank's website hosted at the Service Provider's Data Centre.	Query	Please share the total no of assets to be assessed as part of VAPT activity for below mention IT components: a. Number of application servers (shared, non shared) b. Numbe rof Web servers (shared, non shared) c. Number of DB Servers (Shared, non Shared) d. Number of Thin clients to assess e. Numbe rof Thick clients to assess f. Numbe rof Networking devices to assess along with type of devices g. Number of securty devices to assess	Shall be provided to successful bidder.
12	40	Annexure J - Commercial Bid	Please also furnish the following: 1. Average cost per man-day (in Rupees): 2. Rate per man-day for Senior Resource (in Rupees): 3. Rate per man-day for other Resources (in Rupees): 4. Rate per man-day external site duty (Composite Rate):	Query	Do we need to incorporate the per man day cost as part of commercial bid ? OR its ok to submit the separate rate card for per man day cost attaching to commercial bid document along with seal and signature	Submit the details as per RFP Annnexure J only.
13	14	Project Scope / 2.3	Project Scope	Scope of Work	Do we need to perform re-compliance verification for all the issues reported? How many rounds of compliance verification is expected?	In case of any critical findings during VAPT, the same should be immediately brought to the notice of the Bank without waiting for the formal VAPT draft report, and in such cases, compliance verification of only critical findings will need to be performed immediately on confirmation by the Bank at no extra cost to the Bank. Compliance verification need to be carried out for all the issues reported during VAPT assessments on placement of explicit PO for compliance verification.
14	15	Project Scope / 2.3.1	VAPT Activities : System Identification & Trusted System Scanning	Scope of Work	Do we need to perform network mapping of the entire bank network?	No.

ANNEXURE-I: COMMENTS ON TERMS & CONDITIONS & SERVICES/ PREBID QUERY FORMAT

Sr. No	RFP Page #	RFP Point/ Section #	Clarification point as stated in the RFP document	Category of Comment/ Suggestion/ Deviation/ Query	Comment/ Suggestion/ Deviation/ Query	Bank's Response
15	15	Project Scope / 2.3.1	VAPT Activities : Application Security Testing & Code Review	Scope of Work	Do we need to perform source code review for all in-scope application? What is the coding language and no. of lines of code for each applications?	Review of source codes/scripts which are available at the client side.
16	15	Project Scope / 2.3.1	VAPT Activities : Denial Of Service (DOS) Attacks and DDOS Attacks	Scope of Work	Do we need to perform DOS testing scenario?	It's part of application security testing.
17	15	Project Scope / 2.3.1	VAPT Activities : DMZ Network Architecture Review	Scope of Work	Do we need to perform network architecture review? How many locations/branches/departments in-scope?	Network architecture of application components will need to be reviewed and findings should form part of the VAPT report as per international best practices. Please refer to RFP document.
18	15	Project Scope / 2.3.1	VAPT Activities : Firewall Rule Base Review	Scope of Work	Do we need to perform firewall-rule base review? How many firewalls in-scope? What are the firewall type and number of rules in each ruleset?	Application specific details shall be shared at the time of VAPT assessment.
19	15	Project Scope / 2.3.1	VAPT Activities : Server Assessment (OS Security Configuration) Security Device Assessment Network Device Assessment Database Assessment	Scope of Work	Do we need to perform configuration review for servers and databases and network and security devices? Is there a secure configuration document for all databases and operating system?	Configuration review of servers, databases, network and security devices is part of the scope. Secure configutation document shall be provided.
20	15	Project Scope / 2.3.1	VAPT Activities	Scope of Work	Number of IP's, OS and DB per application is in scope for the assessment?	Application specific details shall be shared at the time of VAPT assessment.
21	15	Project Scope / 2.3.1	VAPT Activities : IDS/IPS review & Fine tuning of Signatures	Scope of Work	What are the IDS/IPS type and count? Do we need to assist in implementation of recommendations?	Application specific details Shall be provided at the time of assessment. Implementation of recommendations is not part of the scope, however in case of any technical issues in implementation of recommendation, alternative approach will need to be suggested by the successful Bidder.
22	18	Project Scope / 2.3.3	Indicative List of Applications and Efforts estimate	Scope of Work	What is effort estimate value for item number **38.0** mentioned in the application list? Currently the country name is written	Efforts estimate value for item number 38.0 Baroda Connect (Internet Banking) Tanzania Territory application is **Medium.**
23	19	Project Scope / 2.3.4	Locations covered	Scope of Work	How many applications are hosted in Mumbai, how many in Bengaluru and how many in Hyderabad?	Please refer to RFP document Part No. 2.3.4
24	23	Effort Estimate/2.4	Effort Estimation Criteria on High Medium Low Parameters	Effort Estimation	Kindly share the basis for the effort estimate for all applications in scope?	Please refer to point no 2.4 and Indicative List of Applications and efforts estimates at part no. 2.3.3
25	23	Effort Estimate/2.4	Effort Estimation Criteria on High Medium Low Parameters	Effort Estimation	Will all the applications be awarded to a single or multiple contractor?	Applications VAPT shall be awarded to the successful Bidder.