Addendum to RFP 092016

(Request for Proposal for Information Security Audit of various IT Services and branches)

Addendum – 1

Revised Annexure 3 – Bidders' scoring chart – Technical Evaluation

Sr. No.	Description	Maximum Score	Scoring Mechanism	Credentials
1	Compliance to Technical requirement	200	The Compliance factor will be scored.	Compliance to Annexure 5
2	Presentation on Project Implementation Methodology,	50		Presentation on Project Implementation and Methodology
	Total	**250**		

Note

1. The cutoff criteria of the above evaluation parameters is minimum 175 marks.
2. This annexure is for bidders' reference and need not be submitted with Bid.
3. Bidders need to provide relevant credentials for all of the above points for scoring.
4. The overall proposal, description of the facilities provided in Technical bid will be evaluated.

Addendum – 2

Under 8.8 Penalties and delays in Service Provider's performance

Revised Clause: Liquidated Damages

The delivery would be treated as incomplete in one/all of the following situations:

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

If the bidder fails to deliver any or all of the Goods or perform the Services within the time period(s) specified in the Contract, the Bank shall, without prejudice to its other remedies under the Contract, deduct from the Contract Price, as liquidated damages, a sum equivalent to 0.50% of the complete contract amount until actual delivery or performance, per week or part thereof (3

days will be treated as a week); and the maximum deduction is 5% of the contract price. Once the maximum is reached, the Bank may consider termination of the contract.

Addendum – 3

The scope given in the RFP is not exhaustive and the Bank reserves the right to add, delete or modify the scope of audit. Bank may ask for additional services such as Forensic Audit, Red Teaming etc. as and when required by the Bank. The fees for additional work may be decided at mutually agreed rates.

Addendum -4

Revised Annexure 5 – Technical Evaluation Criteria

Criteria	Evaluation Parameters	Max Marks	Scoring Methodology
Credentials	The Bidder should have experience in conducting review of IT Infrastructure of Data Centre / Disaster recovery for at least 3 Public Sector Banks/or Equivalent organization. (Bidder should produce relevant Document Proofs)	**40**	• Three or more PSU Banks - 40 marks • Two PSU Banks - 30 marks • One PSU Bank - 15 marks If bidder does not have any references in public sector banks in India, then marks shall be given as follows: For private / foreign bank references (these marks are not in addition to marks for public sector bank references and will be applicable only if bidder does not have PSU bank references in India) • THREE or more private / foreign commercial banks in India – 30 marks • Two private / foreign commercial banks in India – 20 marks • One private / foreign commercial bank in India – 10 marks

	The bidder must have both domain and technical knowledge of Banking and IT areas. The technology area of expertise should include IS Audit of Enterprise Data Centre, hardware and software, Networking and Delivery channels, SDLC, software review, UAT review, BC & DR, vulnerability assessment and risk analysis, expertise in areas related to banking business, outsourcing management, Business Impact Analysis, day-to-day banking operations etc Provide details of 2 references from public sector banks / or equivalent organization. (Bank will conduct the reference check with the references provided. Marks will be awarded based on the satisfactory feedback received from the bank)	**40**	• TWO or more PSU Banks - 40 marks • ONE PSU Bank - 20 marks If bidder does not have any references in public sector banks in India, then marks shall be given as follows for private / foreign bank references (these marks are not in addition to marks for public sector bank references and will be applicable only if bidder does not have PSU bank references in India) • Two or more private / foreign commercial banks in India –20 marks • One private / foreign commercial bank in India – 10 marks
People	The proposed Engagement Manager should have handled at least 3 such projects and should be on the role of the firm/ service provider for at least seven years. **(self-declaration from firm possibly with reference letter from customers is required.)**	**30**	• Handled 3 Information Security Audits or more and on role of the firm for last 7 years: 30 Marks • Handled at least 2 Information Security Audits and on role of the firm for last 5 years: 14 marks: 20 Marks • Handled at least 1 Information Security Audit and on role of the firm for last 3 years: 8 marks: 10 Marks

	At least one out of the proposed team members must have experience in executing similar projects in three banks out of which at least one should be a public sector bank **(List of proposed team members possibly with reference letter from customers is required.)**	**30**	• Handled 3 Information Security Audits or more: 30 Marks • Handled at least 2 Information Security Audits: 20 Marks • Handled at least 1 Information Security Audit in Public Sector Bank: 10 Marks
	The firm should have a pool of at least 20 professionals with international accreditation like CISA (Certified Information Systems Auditor), CISSP (Certified Information Security Professional), CEH (Certified Ethical Hacker) and BS7799/ISO27001 trained lead auditors etc. employed with them. **(List of existing (on role of the firm) professionals with their qualifications and certifications is required.)**	**30**	• Firm has 20 professionals or more on role:30 Marks • Firm has at least 15 professionals on role:20 Marks • Firm has at least 10 professionals on role:10 Marks
	The firm proposes to deploy at least 4 professionals of the project **(List of proposed Team members with their qualifications, certifications and age is required)**	**30**	• Firm proposes to deploy 4 or more professionals:30 Marks • **Firm proposes to deploy 3 professionals: 20 Marks** • **Firm proposes to deploy 2 professionals: 10 Marks**
	Total Marks	**200**	**Total score out of Two Hundred**

Addendum – 5

Revised Clause 6.1 Bid Submission Details

The eligibility and technical bids shall be submitted along with demand draft for non-refundable bid amount in three separate sealed envelopes.

Envelope I containing eligibility bid should be superscripted as:

"**Eligibility bid for RFP#092016 - Information Security Audit of Various IT Services and branches"**

Envelope II containing technical bid should be superscripted as:

"**Technical Proposal for RFP#092016 - Information Security Audit of Various IT Services and branches"**

Envelope III containing demand draft for earnest money should be superscripted as:

"**Earnest Money Deposit for proposal for RFP#092016 - Information Security Audit of Various IT Services and branches"**

All these three envelops should be placed in a single envelope and this envelop should be superscripted as

"**Proposal for RFP#092016 - Information Security Audit of various IT Services and Branches"**

Reponses to pre-bid queries - RFP # 092016					
Sr No.	**Page #**	**Point / Section #**	**Clarification point as stated in the tender document**	**Comment/ Suggestion/ Deviation**	**Bank's Remarks**
1	29 of 82 And 59 of 82	4.7 Documentation and Deliverables And Annexure 5 : Technical Evaluation Criteria	Resources as Auditors/Consultant: The bidder shall depute proper resources (resident engineers) in the premises of Bank of Maharashtra. The resources to be deployed at the bank needs prior approval by bank authorities. The resource shall not connect any tool, hardware such as laptop in Bank's network.	In projects which are delivery centric, it is recommended that resources are deployed as per need by the successful bidder and not deputed as what is done in a secondment model. Given that the word 'deputed' is used in the RFP, please clarify whether the payments are linked with the deputation of number of resources or with successful completion of milestones/timelines. Also, please provide the details of the quantity of infrastructure like laptops, etc. to be provided by the bank for the audit purpose (if the resource shall not connect any tool, hardware such as laptop in Bank's network.) Also, please mention the scores to be allotted for proposing to deploy 3 professionals and proposing to deploy 3 professionals as per the technical evaluation criteria. The same is not mentioned.	Refer Addendum - 4 The bidder shall depute minimum 2 resources in the Bank's premise. The emphasis is on achieving milestones. But considering the scope, Bank requires assurance about resources from the bidder.

2	60 of 82 and 61 of 82	Annexure 5 - Technical Evaluation Criteria	The proposed Engagement Manager should have handled at least 3 such projects and should be on the role of the firm/ service provider for at least seven years. (Self-declaration from firm possibly with reference letter from customers is required.) and At least one out of the proposed team members must have experience in executing similar projects in three banks out of which at least one should be a public sector bank (List of proposed team members possibly with reference letter from customers is required.)	Customer Reference letter: Due to NDAs and NDUs signed with the respective customers (such as you), it is very difficult to provide certificates from these customers. Hence, please clarify if the self-declaration will be considered as valid.	Self-declaration is okay
3	14 of 82	4.2 Project Scope	The audit software shall include an industry comparison based on consultancy experience and results from similar previous engagements	Please specify the parameters basis which the industry comparison is to be provided. It will be practically impossible to provide the compliance status/results/ observations details/issue details of the other engagements due to confidentiality issues. Also provide the details and criteria for the evaluation and acceptance of the solution.	Industry standard comparison in terms of compliance level, methods adopted for compliance, time to achieve compliance etc. may be given.

4	19 of 82	4.4 (2) Detailed Scope For Activities Covered Under Technology Risks	4. Application Security	Even if the audit involves 10-12 IT services per quarter, please specify the number of large applications, medium applications and small applications (based on criticality and complexity) to be covered under each quarter. Also specify number of pages for each applications	About 40 services of below category Most Critical = 6 Critical = 18 Important = 11 Non-business critical = 5
5	14 of 82 4.3	Brief Scope of Work for Information Security Audit	Review of Risk Assessment and suggest mitigation measures for the identified service	Please mention the details about the risk assessment methodology used by the bank. This will help in effort estimation for the activities involved in the review.	As of now, Bank is using ISO control mapping for risk assessment. Bank wishes to achieve better perfection in risk assessment as mentioned in the RFP.
6	26 of 82	4.4 (15) Source Code Audit	Source Code Audit	Whether the activity will include critical applications like core banking software, net banking etc.? Please specify the detailed list/type of software number of code lines, technologies involved, type of language for which source code review is to be conducted. Also provide an estimate about the details of the softwares to be covered in each cycle in terms of the number of large software applications, medium software applications and small software applications (based on criticality and complexity). As the number of days for which the source code review tool will be used is not specified, request you to please clarify whether the code review tool will be provided by the bank or has to be brought in by the successful bidder.	Bank intends to perform source code audit of in-house developed software which are mainly in asp, aspx, C#. Approximately 30000 to 40000 source code lines are to be analyzed per quarter. Bank has approximately 4-5 critical software, 30-35 medium critical and 55-60 non-critical software developed internally.

7	51 of 82 and 52 of 82	8.16 Termination	1. The Bank shall be entitled to terminate the agreement with the bidder at any time by giving ninety (90) days prior written notice to the bidder. 2. The Bank shall be entitled to terminate the agreement at any time by giving notice if: a. The bidder breaches its obligations under the tender document or the subsequent agreement and if the breach is not cured within 15 days from the date of notice. b. The bidder (i) has a winding up order made against it; or (ii) has a receiver appointed over all or substantial assets; or (iii) is or becomes unable to pay its debts as they become due; or (iv) enters into any arrangement or composition with or for the benefit of its creditors; or (v) passes a resolution for its voluntary winding up or dissolution or if it is dissolved. 3. The bidder shall have right to terminate only in the event of winding up of the Bank.	Clause 8.16 An objective and consultative process should precede before the bank chooses to exercise its termination rights- a mechanism should be put in place to objectively capture service related defaults and allocate the accountability to an appropriate party in a transparent manner. A reasonable "cure" period of 30 days should be provided for service related issues. Upon termination for any reason whatsoever, the service provider should be paid for the services performed by the service provider till the date of termination.	Please refer clause 8.11 - Resolution of dispute
8	11	3.3 RFP validity period	The Bank / its subsidiaries shall have the right at its sole and absolute discretion to continue the assignment / contract on the selected bidder for future requirement on the rates finalized in this	Who will decide on the pricing of future requirements. In case of additional requirements in future will there be second bidding?	Please refer clause no. 8.17 - Effect of Termination

			processing for various items / activities as described in the Price Bid after expiry of current assignment period.		
9	14	4.1 Purpose	The IT infrastructure of the bank of Maharashtra is ISo27001:2013 certified.	What are the locations covered and scope under ISO 27001: 2013 certification?	DC, DR, HO and PMO
10	14	4.1 Purpose	The Bank also has Security Operations Centre (SOC) in place.	Please provide bank's SOC (Security Operation Centre) coverage to monitor's entire three tier such as Branch, Zonal Office, and Head Office.	As of now, Bank covers critical devices placed in DC, DR, HO, PMO, Treasury.
11	14	4.1 Purpose	The Bank also has Security Operations Centre (SOC) in place.	List of devices covered by SOC monitoring. Number of devices and their type will do (ex. Router - 50, Switches - 200)	Total number of routers integrated in SOC= 47 Total number of switches integrated in SOC= 33 Total number of firewalls integrated in SOC= 16 Total number of windows 2008, 2012. linux servers integrated in SOC= 390
12	14	4.1 Purpose	Bank intends to issue this bid document, hereinafter called RFP, to eligible Service Providers, hereafter called as 'SP', to participate in the competitive bidding for appointment of SP for conducting Information Security audit of Bank's	What all IT services are considered to be in-scope and who will decide on scoping of branches?	Please refer 4.4 detailed activities

			various IT services and Branches.		
13	14	4.2 Project Scope	The scope of work includes regular Information Security audits for various IT services of Bank. It also includes audit of critical infrastructure of the Bank	Please list of critical infrastructure of Bank be covered as part of this audit (number of devices and their type will do)	Approximately Routers= 50 Switches = 35 Firewall = 16 Servers = 400
14	14	4.2 Project Scope	Entire audit activities should be automated using audit management software application.	Who is responsible for implementing, configuring and bearing the cost for implementation of the audit management software	The bidder is responsible for implementing, configuring and managing the Audit software. Bank will provide necessary infrastructure. In case bidder uses third party services for the same, that party will have to sign NDA, NDU with the Bidder and the Bank.
15	14	4.2 Project Scope	The requirements of this software application are provided later in this section.	Will the Bank assess audit software application as part of bidding process to decide upon suitability of the software?	Bidder is expected to explain the suitability of the software during technical bid evaluation as a part of project implementation methodology
16	14	4.3 Brief scope of work for Information Security Audit	Review of Risk Assessment and suggest mitigation measures for the identified service	Two points are mentioned regarding review and conduct risk assessment exercise; would SP be required to conduct entire risk assessment exercise or only review of the exercise?	Please refer detailed scope in the RFP.
17	15	4.3 Brief scope of work for Information Security Audit	Configuration review of components for the service	Who will decide on sample size of servers, network devices and database for configuration review	Please refer the scope in the RFP

18	16	4.3 Brief scope of work for Information Security Audit	Review of user friendliness of the service provided	What are the parameters / aspects on which bank is looking to monitor “user friendliness of the service provided”.	Bidder is expected to use its experience and the inputs from the users to decide on "User Friendliness"
19	15	4.3 Brief scope of work for Information Security Audit	Review of the vendor risk assessment measures implemented by the bank	How many vendors will be covered by SP under “Conduct risk assessment of the Bank’s vendors in their premises for part of the implementation of the Bank’s project	Review of vendor risk assessment is part of service to be audited.
20	15	4.3 Brief scope of work for Information Security Audit	Application Security	How many applications would be considered for application security? Please provide overall number of apps/devices to be covered in 3 years and each cycle of testing also	Application security testing is a part of service audit.
21	15	4.3 Brief scope of work for Information Security Audit	Conduct vulnerability assessment for the devices for the service. Conduct penetration testing of the applications used for the service	How many applications/devices would be considered for VA and PT? Please provide overall number of apps/devices to be covered in 3 years and each cycle of testing also	The bidder has to decide based on the service. Count of devices is already provided.
22	15	4.3 Brief scope of work for Information Security Audit	Conduct vulnerability assessment for the devices for the service. Conduct penetration testing of the applications used for the service	Which all external and internal sites would be considered for VAPT? Please provide overall number of apps/devices to be covered in 3 years and each cycle of testing also	About 5-6 Internal sites and 5-6 external sites to be covered in each quarter
23	15	4.3 Brief scope of work for Information Security Audit	Develop indicators for Cyber Security Audit and conduct Cyber Security Audit of Critical Infrastructure of the Bank.	Who will decide critical infrastructure for cyber security audit?	Bank

24	15	4.3 Brief scope of work for Information Security Audit	Source code Audit of In-house developed software. (once in 3 months)	Will the source code audit be performed on all in-house applications or on sample basis? Please provide overall lines of codes to be covered in 3 years and each cycle of review also	Bank intends to perform source code audit of in-house developed software which are mainly in asp, aspx, C#. Approximately 30000 to 40000 source code lines are to be analysed per quarter. Bank has approximately 4-5 critical software, 30-35 medium critical and 55-60 non-critical software developed internally.
25	16	4.4 Detailed Scope	Review of Risk Assessment and suggest mitigation measures for the identified service	Please provide sample size to select for the number of branches and for each type of devices/app in branch	Around 25 branches will be considered for audit per quarter. The detailed scope of audit at branch is already described in the RFP.
26	17	13. Risk assessment of Bank's vendors	Review of the vendor risk assessment measures implemented by the bank	What all needs to be assessed from privacy and data protection perspective at vendor premises	The clause is clear. Further discussion will be done with successful bidder
27	17	13. Risk assessment of Bank's vendors	Review of the vendor risk assessment measures implemented by the bank	How many vendors needs to be considered for such testing	Review of vendor risk assessment is part of service to be audited.
28	25	16. Advisory and Training	Monthly Advisory and Training	Would the training need to be conducted at all zonal offices or on sample basis?	Training to be conducted at all zonal offices under audit during the quarter. Bank has in all 34 zones which are to be covered in a year.
29	25	4.7 Documentation	Security Profile of a Service.	What will be covered as part of security profile for a service?	The clause is clear. Further discussion will be done with successful bidder

		and Deliverables			
30	26	4.7 Documentation and Deliverables	A selected bidder should provide a centralized audit tracking software.	Is it require to provide Audit Tracking software source code to the bank? Or executable files are sufficient?	Executable files and license is sufficient
31	29	4.7 Documentation and Deliverables	At the end of three-year audit cycle this software will remain with Bank of Maharashtra.	What will agreement between bank and audit tracking software provider post 3 years?	The bidder has to provide audit tracking software with license in the name of the Bank. Post contract, the license remains with the Bank.
32	29	4.7 Documentation and Deliverables	Each resource involved shall sign NDU as per Bank's format and shall abide by the Information System Security Policy of the Bank.	Whether each resource need to sign NDU on individual capacity or bidder can sign on NDU which will cover all resources	Each individual will need to sign NDU, in the format provided by the Bank
33	29	4.7 Documentation and Deliverables	The resource shall not connect any tool, hardware such as laptop in Bank's network.	If resources are not allowed to connect any tool, hardware to Bank's network would the Bank be providing necessary tools for VAPT testing?	Bank will provide necessary infrastructure. Bidder may use their tools on the machines provided by the Bank whenever needed.
34	29	7.2.3	The Price offer shall be on a fixed price basis and should include: All taxes, duties and levies of whatsoever nature if any except Service Tax and Octroi; and Services which are required to be extended by the bidder in accordance with the terms and conditions of the contract.	If the government cess / services tax changes during the course of the project, whether bidder can bill accordingly or the bidder will have to stick to the current cess / service tax.	Bidder can bill accordingly

35	29	7.2.4 Performance Guarantee	The software will be subjected to acceptance testing by the Bank.	In case software does not satisfy acceptance criteria of the Bank then what would be next steps?	Bank expects the bidder to do necessary modifications till the satisfaction of the Bank. Any delay on the part of the bidder would attract penalty.
36	43	8.2 Contract Extension	Upon satisfactory completion of work, bank reserves right to extend the contract by another one year or as per the banks discretion on the same terms and conditions.	If bank extend the contract by one year, will it be on the same fees or bidder can charge additional fees for the extended one year	Please refer Clause 8.2 - Contract Extension.
37	57	Annexure 4 – Eligibility Criteria B. Financial Criteria	Copy of audited Balance Sheet and P&L statement for the financial years. 2013-14, 2014-15 and 2015-16.	The P&L statement is not yet out/available, hence we would like to know the alternative document expected for qualifying the financial eligibility criteria.	Provisional balance sheet and P&L statement signed by the company secretary.
38	59	Page 59 of 82 Annexure 5 - Technical Evaluation Criteria	The Bidder should have experience in conducting review of IT Infrastructure of Data Centre / Disaster recovery for at least 3 Public Sector Banks/or Equivalent organization.	Do we have extra marks if the credentials has work done in more than 3 Public Sector Banks/ Equivalent organization?	No
39	17	4.3 Brief Scope of work for Information Security Audit	Review of IT Security policies, procedures and frameworks in terms of adequacy of its coverage of Information Security. Suggest scope for improvement in the documents considering RBI compliance, IT Act and other applicable regulations and standards.	Number of IT Security policies, procedures and frameworks to be reviewed.	Bank is ISO27001:2013certificate.Accordingly, Bank has all those documents and some few more policies and procedures.
40	--	--	-	Location of DC and DR	DC is in Pune and DR is in Hyderabad

41	45	4.5 Details of Audit Frequency	About 5-6 Internal sites and5-6 external sites tobe covered	We understand that About 5-6 Internal applications and 5-6 external application to be covered	Your understanding is correct.
42	--	--	--	Will the Audit frequency will be the same after for the 2nd and 3rd year as that of the 1st year?	Yes

***** ALLL OTHER TERMS AND CONDITIONS OF THE RFP#092016 REMAIN UNCHANGED.**