Replies to the Pre Bid Queries EOI092020 - IS Audit of IT Services and Branches

S N	Page/ Point/ Section	Category	Clarifications/ Query	BOM response
1	2	Invitation to EOI	Will empanelment be a single step or 2 step process I,e 1) Will EOI be followed by RFP for empanelment of service provides or will EOI will lead to shortlisting of services providers for empanelment 2) Will one 1 service provider be shortlisted or multiple service providers will be empanelled	Yes it is two steps process - EOI followed by RFP. Eligible Bidders would be shortlisted through EOI and then Only one service provider will be shortlisted through RFP.
2	2	EOI fees	Is this non-refundable . Apart for EOI fees will there be any EMD fees for RFP	EoI fees is non-refundable and apart from EoI Fees there will be separate EMD.
3	2	EOI response submission	Will only those participating in Prebid be eligible for submission of EOI	Not Necessary
4	7	6. Format and Signing of EOI: a	Considering the pandemic kindly request submission through email in soft copy instead of hard copy. To address size limits on email we can break the EOI proposal files accordingly.	Softcopy submission will be allowed. Refer Corrigendum
5	11	1) The bidder should have conducted at least three Information Security audits of data centres and other IT Infrastructure of PSU banks in India in the past five years	1) Requesting to consider BSFI sector along with PSU Bank. Suggestion to change "PSU banks to PSU banks/ BSFI /Private banks "	The bidder should have conducted at least three Information Security audits of data centres and other IT Infrastructure of PSU/ Scheduled commercial banks in India in the past five years
		2) Reference Letter from Customer/ Document Proof	2) Due to NDA terms we can provide masked copies of PO as required. Detailed information can be	masked copies of POs are allowed.
6	15	Scope of work :Bank is proposing to procure 'CSR Life cycle management Solution 2.1 overview audit management software application.	Please expand CSR . Are service providers required to build reports which can be imported on the tool. With format of reports are expected . The OEM of tool will provide all integration capabilities .please confirm IS CSR referred to audit management software Do Service provider have to provide the CSR tools / Audit management software	Following para is removed: "Bank is proposing to procure 'CSR Life cycle management Solution' for end to processing of Security Review of IT infrastructure and MIS purpose. The selected bidders would be required to furnish the reports as per this solution. Reports would be in □ soft copies, hard copies, copies of screen shots, outputs □ audit evidence □ soft outputs which are importable into a database, spreadsheet, or GRC platform e.g. XML files, CSV files etc."
7	7	The successful bidder(s) through RFP process shall be required to enter into a contract/SLA with the Bank	Can we have a copy of the SA /Contract terms . The SLA and Contract terms will be have to be reviewed by GT legal and risk team and suggestion and changes can be jointly addressed.	The details will be provided in the RFP to the eligible bidders of EoI process
8	7	7.1 Price model /Man-days- Months	Post empanelment will BOM define standard rate card as a baseline of different levels of professional or will it be RFP specific as proposed by Service provider	Clause is removed.

9		2.1 b) Who have solution strictly in line with the technical parameters.	Kindly clarify on point b	Clause is removed.
10		Procurements for MSMEs will be as per the policy guidelines issued by Ministry of Micro, Small and Medium Enterprises (MSME), GOI from time to time. MSMEs registered under the SPRS (Single Point Registration Scheme) of NSIC and complying with all the guidelines thereunder as well as those issued by GOI from time to time shall be eligible.	We are a MSME organisation. We can submit the certificate for the same. Can the clause related to turnover as mentioned on Pg no 10 under Financial Criteria be relaxed?	No Change in EoI clause
11	2.2 Purpose	Bank of Maharashtra is requesting submission of interest for empanelment of Information Security Service Providers (ISSPs).	Is this EOI for the purpose of empanelment or to issue a work order for the scope of work defined in the EOI	This is the EoI for appointment of service provider to conduct Information Security Audit of various IT services and branches
12	A. General Criteria	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	Can this clause be relaxed?	No Change in EoI clause
13	B. Financial Criteria	Shall have a minimum average annual income of Rs.50.00 crores (Rupees Fifty Crores) during last three financial years viz. 2017-18, 2018-19 & 2019-20	We are a MSME organisation. We can submit the certificate for the same. Can this clause be relaxed	No Change in EoI clause
14	C. Technical Criteria	The bidder should have conducted at least three Information Security audits of data centers and other IT Infrastructure of PSU banks in India in the past five years including a) Vulnerability assessment of servers/ security equipment/ network equipment; & b) External attack and penetration test of equipment exposed to outside world through internet	We have conducted audits for banks other than PSU. Can this be considered?	Refer Question No. 5
15	e) Code Review	The code review activity should help the bank in uncovering any vulnerability that an adversary may potentially exploit	1. Which applications are in the scope of the review? 2. For each application in the scope of code review, please share details such as a. no of lines of code. b. Programming language used c. front-end and back-end details	Internal developed applications Bank intend to perform source code audit of inhouse developed software which are mainly in asp, .Net, C#. Approx 30000 to 40000 source code lines are to be analysed per quarter. Front end-ASP .Net and Back end -MS SQL and Oracle

16	g) Red Teaming exercises.	The bidder shall conduct Red Team Exercise to focus on giving the bank's security teams a practical experience combatting real cyber-attacks to simulate the tools, tactics and procedures (TTPs) of real-world attackers that target our environment, while avoiding business damaging tactics.	1. How many red-team exercises are to be carried out on an annual basis?	Once in a Quarter
17	Page 2 and Page 8	As per page 2: Last Date of submission ofEOI response is mentioned as14/10/2020 14:00 Hours As per page 8: The last date forsubmission of EOI is 07 Oct 2020.	We noted two timelines for EoI submission as per refences mentioned here. Request to confirm deadline i.e. date and time by which EOI needs to be submitted.	Date of submission ofEOI response is:14/10/2020 14:00 Hours
18	Page 11	Table 'List of Resources with Technical qualifications' – Column 'Category of resource'	What is exact expected data in column category of resource? Do we need to provide the same for all the resources?	Category of Resource expected is "Information Security Auditor"
19	Page 14 Point 6	Details of 2019-20	Financial details of 2019-20 are not available yet as the audit is still in progress. Request you to confirm if we can provide these details separately at later date as soon as the financial results are available for the company.	For 2019-20 certified copy of CA will be accepted.
20	Page 15 to Page 27	Appendix I Scope of work	Request you to confirm if we need to submit our detail approach and indicative pricing for services included in this section as part of EoI? Or else EoI Response should include only Annexure A, A1, A2, A3, A4, A5 and Annexure B.	EoI Response should include only Annexure A, A1, A2, A3, A4, A5 and Annexure B.
21	Page 7 Section 6 Point a	EOI should be typed and submitted on A4 size paper, spirally and securely bound and with all pages therein in serial order.	We want to confirm if Is it mandatory to submit EoI in hard copy format? Or Sending EoI in PDF format over email to tanvi.kochhar@mahabank.co.in; akshay.mahajan@mahabank.co.in; ciso@mahabank.co.in is sufficient to consider valid response? Also, can we prepare EoI in landscape mode in A4 format?	EoI submission should be done online. The details of online submission will be shared separately.
22	Point 5 Annexure A – Technical Details- Ability of the ISSP Page 10	Shall have a minimum average annual income of Rs.50.00 crores (Rupees Fifty Crores) during last three financial years viz. 2017-18, 2018-19 & 201920	As this is an EOI for Services, we think that the Average Turnover of Rs. 50 Crores is on higher side. We suggest to relax it to Average Turnover of Rs. 10 Crores in last three financial years.	No change in EoI clause
23	Point f Of Specialized Services Page 21	f) Domain/Channel Process Audit Scope of Work for Code Review: Same as given above for Application Security Assessment	Kindly elaborate the scope of Domain/Channel Process Audit.	The clause "Domain/Channel Process Audit Scope of Work for Code Review: Same as given above for Application Security Assessment" is removed.
24	Page 15 - 27	Appendix – I Scope of work	Kindly provide the details of IT infrastructure under scope of Audit.	The IT infrastructure includes but not limited to Unix/Linux Servers, Windows Servers, Network Devices, Security Devices, etc.

25	Page 15 - 27	Appendix – I Scope of work	Kindly confirm whether the web application audit / Mobile application Audit is to be conducted on site of Offsite. Also, please provide the details like number of Input forms, input fields etc. of application under scope of work	The web application audit/Mobile application audit can be conducted on-site or off-site. These are standard applications such as Internet Banking, Mobile Banking, etc. the details will be provided to the successful bidder.
26	Page 7	7.2 Man-days Hire model: For given N man-days / man-months, resource cost will be arrived based on the discovered prices through a RFP, say the cost is Y. Vendors will be asked to quote the discount percentage on Y in sealed cover. Whoever offers maximum discount on Y will be awarded the contact.	Will the deployment of man power will be for entire 3 years at Bank Premises for Technical and Process Audit Kindly confirm	Clause NO 7 will be removed
27	Page 10	Annexure A – Technical Details-Ability of the ISSP B. Financial Criteria Shall have a minimum average annual income of Rs.50.00 crores (Rupees Fifty Crores) during last three financial years viz. 2017-18, 2018-19 & 2019-20	The turnover figure is very high and may not involve much participation. Several banks in RFP for Empanelment of Service Provider for Information Security Audit had a turnover criteria of Rs. 10 Crores in each of the last three years. Hence, we request you to modify the clause accordingly to have turnover of Rs. 10 Crores or above (from Indian Operations Only) in each of the last three years. And also we are Micro and Small Enterprise (MSE) requested to kindly consider the same	No change in RFP
28	Page 11	C. Technical Criteria point number 7 Bidder should be CERT-IN empaneled as on the date of submission of bid	Currently the CERT In empanelment is upto 31st October 2020 for all empaneled audit firms mentioned on the website . The results will be declared in due course on CERT-IN website	In case the firm is qualified through this process, is discontinued from Cert-In empanelment after 31st Oct 2020, then the said firm will be disqualified for further participation in the RFP process.
29		Annexure A – Technical Details-Ability of the ISSP C. Technical Criteria Reference Letter from Customer/ Document Proof	3 work order should be sufficient in Last 5 years Kindly confirm	Yes
30	Page 12	Annexure A2 Specific Work Experience of Vendor in Bank (Please write 'Yes' or 'No' in the box + Bank Name (Blank means 'No')	As per the activity mentioned in an Single many of the activities are been covered . Kindly confirm number of PO to be submitted to qualify	As per the annexure only "Yes" or "No" + "Bank name" to be filled. The Bank may ask for submission of PO/s as and when required.
31	Page 13	Annexure A5 Mandatory Services Capability List for eligibility	Out of 24 activity kindly confirm number of activity to qualify	All are mandatory

32	Page 17 to 27	Scope work Service Types: Services are categorized into two areas viz. a) Standardized b) Specialized.	Following are the details required I. Total Number of Server II. Total Number of OS & Database III. Network and Security Device IV. Total Number of Internal and External Application with number of ststic pages/ Dynamic pages/ types of user and Roles of each user V. Total Number of Mobile Application (Platform required/ Dynamic pages and number of screens required.	it will be part of RFP document
33	Page - 17	c) Technical standard creation Creating – The ISSP is expected to create a base document with parameters, values etc. and descriptions of risks to enable an OS, system, platform, application, database etc. to be securely configured for use in the Bank.	Do we need to Review / Or It is Created or Do we need to Create- Kindly confirm what is expected from auditors	It is required to review the existing documents and provide recommendation for creation of document if any.
34	Page 18	IT General Controls Audit	Kindly confirm us the number of application and audit location – can we audit from one centralized location	Bank has approximately 23-25 high important software, 26-30 medium importante software, and 15 Low important software developed internally. The audit can be done from one cetralized location. The audit location would be Pune in most of the cases, however in some cases this location can be changed.
35	Page 18	ISO 27001 Consulting	Kindly confirm us the Location and the total number of departments	Audit location can be Pune or Hyderabad
36	Page 19	Point e) Vendor Risk Assessment	Number of Vendors and their locations	Review of Vendor Risk assessment is part of service to be audited
37	Page 19	Specialized Services 1) IS Program Management 2) Log Monitoring 3) Information Security Awareness 4) Application Security	1. IS Program Management – What is Expected from Audit firm	It is expected that the bidder may provide consultancy services related to the scope
			2. Log Monitoring - What is Expected from Audit firm	It is expected that the bidder may provide consultancy services related to the scope
			3. Information Security Awareness – Number of secession and number person in one batch and its location	It will be provided in the RFP document
			4. Application Security - § Name of modules/ number of modules § Functionality of modules § Process flow § Any other application integrated with the application	It will be provided in the RFP document
38	Page 21	Point Nos. e) Code Review	Number of application required and total number of line of code for each application	Bank has approximately 23-25 high important software, 26-30 medium importante software, and 15 Low important software developed internally. Approx 30000 to 40000 source code lines are to be analysed per quarter.
39	Page 21	Point Nos. g) Red Teaming exercises.	Frequency of audit	Quarterly
40	Page 22	Point Nos. h) BCP / DRP	What is expected by Audit firm – Kindly clarify	Audit of DR drill to be conducted which happens on quarterly basis. Details will be shared in the RFP document. Review of BCP/DR while auditing the said system.