Responses to Pre Bid Queries

RFP-15/2024-25 (GEM/2024/B/5100578) for Appointment of Consultant for Migration Services of Certification from ISO27001:2013 to ISO 27001:2022 of the Bank
(Pre Bid Meeting 05.07.2024 at 15:00 hrs)

बैंक ऑफ महाराष्ट्र
Bank of Maharashtra
भारत सरकार का उद्यम
एक परिवार एक बैंक

Sr no	Page No	Point / Section	Main Section Name	Clarification point as stated in tender document	Comment / Suggestions	Bank Response
1	30	6.3	Conflict of Interest	Bank requires that bidder provide professional, objective, and impartial advice and at all times hold Bank's interest paramount, strictly avoid conflicts with other Assignment(s)/ Job(s) or their own corporate interests and act without any expectations/ consideration for award of any future assignment(s) from Bank. Bidder have an obligation to disclose any situation of actual or potential conflict in assignment/job, activities and relationships that impacts their capacity to serve the best interest of Bank, or that may reasonably be perceived as having this effect. If the Bidder fails to disclose said situations and if Bank comes to know about any such situation at any time, it may lead to the disqualification of the Bidder during bidding process or the termination of its Contract during execution of assignment.	Requirements of this clause to be curtailed to the Engagement Team only. Furthermore, please note that no potential conflict related declaration can be provided, accordingly, we suggest the inclusion of the following disclaimers as part of the proposal: a)'Any conflict related declaration can be given as on the current date only.' b)'All conflict-of-interest confirmations shall be provided for the engagement team members providing the services pursuant to this engagement as per our internal risk management procedures.'	No Change in RFP Clause
2	36,46,47	6. 40 Clause 4	Confidentiality	The Receiving Party who receives the confidential information and materials agrees that on receipt of a written demand from the Disclosing Party: i. Immediately return all written confidential information, confidential materials and all copies thereof provided to, or produced by it or its advisers, as the case may be, which is in Receiving Party's possession or under its custody and control; ii. To the extent practicable, immediately destroy all analyses, compilations, notes, studies, memoranda or other documents prepared by it or its advisers to the extent that the same contain, reflect or derive from confidential information relating to the Disclosing Party; iii. So far as it is practicable to do so immediately expunge any confidential information relating to the Disclosing Party or its projects from any computer, word processor or other device in its possession or under its custody and control; and iv. To the extent practicable, immediately furnish a certificate signed by its director or other responsible representative confirming that to the best of his/her knowledge, information and belief, having made all proper enquiries the requirements of this paragraph have been fully complied with.	"Notwithstanding anything to the contrary, Consultant(s) shall be allowed to retain sufficient documentation as part of its professional records to support and evidence the work performed by the Consultant(s). Such retention shall be subject to obligations of confidentiality mentioned herein."	No Change in RFP Clause
3	40	6.52	Audit and Inspection of Codes / Record	All Bidder records with respect to any matters covered by this tender shall be made available to Bank or its designees, including RBI Inspectors / auditors at any time during normal business hours, as often as Bank deems necessary, to audit, examine, and make excerpts or transcripts of all relevant data. Said records are subject to examination. Bank's auditors or its designees would execute confidentiality agreement with the Bidder, provided that the auditors would be permitted to submit their findings to Bank, which would be used by Bank. The cost of the audit shall be borne by Bank. The scope of such audit would be limited to Levels being covered under the contract, and financial information would be excluded from such inspection, which shall be subject to the requirements of statutory and regulatory authorities. Bank, its representative, RBI and Government Agencies shall have all the rights to carry out the VAPT (Vulnerability and penetration testing) or other system Audit for the service offered under this RFP. The Bidder should comply with the various IS Audit observations raised by the Bank's Audit Team / External Auditor / Regulatory Entity etc. Bank shall conduct Pre on boarding & Post on boarding Risk Assessment of the successful bidder. Bidders are required to cooperate in providing the required support during the process of Pre on boarding & Post on boarding Risk Assessment. Bank reserves its right to cancel the order without assigning any reasons, in the event of one or more of the following situations: a) Non-satisfactory performance of Hardware /solution. b) Delay in delivery beyond the specified period for delivery. c) Delay in installation beyond the specified period for installation from the date of purchase order. d) Serious discrepancy in solution noticed during the pre/post installation. In addition to the cancellation of purchase order, Bank reserves the right to appropriate the damages from the earnest money deposit (EMD) given by the bidder or foreclose the Bank Guarantee given in lieu of EMD and/or foreclose the Bank guarantee given by the supplier against the advance payment.	We suggest the inclusion of "Any audit shall be subject to the following: (i) the audit shall be restricted to the engagement and shall be conducted with prior reasonable notice (ii) Bank or its authorized representatives shall execute a Non-Disclosure Agreement before such audit which shall govern the conduct of audit and any results thereof; (iii) the auditors or the representatives of Bank for the audit shall not be bidder's competitors; (iv) the audit shall not be conducted more than once in a calendar year and twice in entirety; and (v) any findings during the audit, shall be shared with Bank and be discussed and agreed mutually with Bank and bidder for its closure."	No Change in RFP Clause
4	79	Annexure B: section 4	Technical Evaluation Criteria	Customer reference feedback form	Please Elaborate what exactly should be submitted as a customer reference feedback form.	No document is required to be submitted. Bank obtaining feedback from customer/ client through telephone or site visit.

Sr. No.	General Query related to RFP	Comment / Suggestions	Bank Response
1	The consultant firm will be appointed for the job of migration of certification for the Bank from ISO27001:2013 to ISO27001:2022. The migration is to be completed before August 2024.	Is the "August 2024" a typo error? Can we access the scope statement of previous ISO certification along with the initial issues raised by the auditor? What is the number of employees?	**Please read clause as:** The consultant firm will be aopointed for the job of migration of certification for the Bank from ISO27001:2013 to ISO27001:2022. The consultant shall complete the milestone within 12 weeks from acceptance of purchase order
2	The consultant shall be responsible to coordinate with various departments and offices of the Bank, conduct interviews, conduct sessions to explain the role of the department in achieving and maintaining the certification.	Can we know the departments and offices of the bank that shall be in scope? Can we also know any specific exclusions?	tentatively, departments are DC, DR, HO and PMO primarily.. Additionally we also have Digital Banking Department, IRM, HRM, MIS, security,CISO cell departments; that may play role in achieving the certification.
3	The consultant will understand the current organizational setup and suggest the ISMS scope covering all the relevant standard clauses. Accordingly, the consultant will make changes/ rewrite relevant documents such as Statement of Applicability (SOA), ISMS Scope document, Information System Security Policy (ISSP), Cyber Security policy, CCMP, IS Audit policy etc.	All Bidder records with respect to any matters covered by this tender shall be made available to Bank or its designees, including RBI Inspectors / auditors at any time during normal business hours, as often as Bank deems necessary, to audit, examine, and make excerpts or transcripts of all relevant data. Said records are subject to examination. Bank's auditors or its designees would execute confidentiality agreement with the Bidder, provided that the auditors would be permitted to submit their findings to Bank, which would be used by Bank. The cost of the audit shall be borne by Bank. The scope of such audit would be limited to Levels being covered under the contract, and financial information would be excluded from such inspection, which shall be subject to the requirements of statutory and regulatory authorities. Bank, its representative, RBI and Government Agencies shall have all the rights to carry out the VAPT (Vulnerability and penetration testing) or other system Audit for the service offered under this RFP. The Bidder should comply with the various IS Audit observations raised by the Bank's Audit Team / External Auditor / Regulatory Entity etc. Bank shall conduct Pre on boarding & Post on boarding Risk Assessment of the successful bidder. Bidders are required to cooperate in providing the required support during the process of Pre on boarding & Post on boarding Risk Assessment. Bank reserves its right to cancel the order without assigning any reasons, in the event of one or more of the following situations: a) Non-satisfactory performance of Hardware /solution. b) Delay in delivery beyond the specified period for delivery. c) Delay in installation beyond the specified period for installation from the date of purchase order. d) Serious discrepancy in solution noticed during the pre/post installation. In addition to the cancellation of purchase order, Bank reserves the right to appropriate the damages from the earnest money deposit (EMD) given by the bidder or foreclose the Bank Guarantee given in lieu of EMD and/or foreclose the Bank guarantee given by the supplier against the advance payment.	Bank wishes to achieve ISO certification that helps improve security posture of the Bank. As of now, various departments manage their own policies which are approved by the Baord. The policies related to IT/ DBD/ MIS are managed by IT/ DBD and MIS reaspectively and policies related to Information security are managed by CISO cell.
4	The consultant should help the Bank develop risk assessment format specific to the particular functionality/ implementation and ultimately suggest to improve on risk score. The consultant should help the departments to develop and automate their processes such that the departments achieve their business objectives by managing the associated risks; at the same time, achieve the compliance to the regulatory guidelines.		Consultant shall consider all the controls as mentioned in the ISO27001:2022 strandard while developing formats for risk assessment. Bank will provide necessary data/ information to finalize risk assessment of the funcationality through the consultant.
5	The consultant should develop Balance Scorecard and effectiveness matrix indicating the security posture of the Bank.	Can you please elaborate on the requirement? Is a scorecard in place currently?	The consultant shall prepare balance score card by mapping each ISO controls to the perspectives of Balance score card indicating security posture of the Bank
6	The consultant should develop various senior and middle management level reports, which should provide clear picture of residual risk for that particular service/ implementation. These formats should be self-explanatory and evolving such that they reflect new requirements. The consultant may have to develop various formats suitable to department in-charge, IRM and Inspection department, IT Head, CISO, CTO, Audit Committee of the Board and Strategy Committee of the Board. The consultant shall submit Executive summary and detailed Risk Assessment Reports for Management review and acceptance.	Can the management throw some light on what kind of reports? Will it be for internal consumption or may be shared with external parties?	The consultant should prepare comprehensive formats for reporting to the management about security posture for each IT/ security funcationality that includes relevant KPIs, risk register with residual risk, analysis and action plan etc. The formats/ reprots/ any other material developed will be owned by the Bank and the Bank reserves the rights to use the material at its discretion.
7	Bank expects L1 and L2 resources to be deployed at Bank's head office and another senior specialist resource guiding them from consultant's office. The senior resource should participate in any meeting the Bank has called him for.	Does the bank need the consultants be available at the HO full time during the course of project?	Bank require the presence of consultants at the HO since it will help roll out the project within timeline.
8	Certification Body	The certification body shall be on-boarded by the bank itself and the consultant's scope shall be limited to assistance. Is the understanding correct?	Bidder's understanding is correct
9	Technical Assessment	We understand that technical aspects like VAPT etc is not in scope for this project. Red team and Blue team requirement is only limited to the training? Is the understanding correct?	Bidder's understanding is correct
10	The Bidder should have experience of completing at least 1 project for consultation services for ISO27001:2022 audit in at least one scheduled Commercial Bank/Financial Institution/Foreign Bank in India..	Considering that the standard is relatively new, can this requirement be widened to assistance in other industries as well?	**Please read clause as:** The Bidder should have experience of completing at least 1 project for consultation services for ISO27001:2022 audit in at least one scheduled Commercial Bank/Financial Institution/Foreign Bank/ RBI regulated entities having substantial presence in India.
11	Resilience	Is the resilience be centrally managed? No drills have to be conducted as a part of this project. Is this understanding correct?	Bank has various tools for central management of cyber security. The consultant shall conduct necessary training, knowledge transfers and handholding for establishing resiliency. The goal is to establish cyber security practices as per ISO standard.