SBI RFP - ENGAGING CONSULTANT FIRM FOR ISO 27001:2022 CERTIFICATION - SBI/GITC/ISD/2023-24/ISO/23 (RFP-1336)					
Sr. No	***RFP Page No***	***RFP Clause No***	***Existing Clause***	***Query/Suggestion***	***Response***
1	Part 2 Appendix- B Scope of Work	Scope of Work	Bank is floating this RFP to identify and engage a service provider to review the aforementioned seven applications holistically from an ISO 27001:2022 perspective and do the needful to provide for the ISO 27001:2022 certificates	Protected systems specified as scope of work are ISO 27001:2022 certified? If yes, kindly share the scope statement, scope location and scope departments covered in ISO 27001:2013 certification.	The scope would broadly encompass the activities, processes, human resources, and systems involved in seven CII applications of State Bank of India along with their operations at respective Data Centre ,Disaster Recovery Sites and office locations, same shall be detailed and communicated during the engagement.
2	23. SUB-CONTRACTING	23. SUB-CONTRACTING	As per scope of this RFP, sub-contracting is not permitted.	Since partner is not in certification business, we will have to on board an accredited third party. Hence, request to allow involvements.	Sub contracting is not allowed as per RFP.
3	Part 2 Appendix- B Scope of Work	Scope of Work	Bank is floating this RFP to identify and engage a service provider to review the aforementioned seven applications holistically from an ISO 27001:2022 perspective and do the needful to provide for the ISO 27001:2022 certificates	Please confirm if there are any protected systems for new ISO certifications. OR all the applications enlisted are ISO certified previously.	This is a fresh certification exercise/ cycle.
4	Part 2 Appendix- B Scope of Work	Scope of Work	The scope of ISMS for these applications will include all the documents / activities /procedures relevant for ISMS covering setup across three datacenters viz. DC GITC, DC Rabale, and DR at GDC, Hyderabad, and also include physical and logical boundaries of above referred seven applications including their sub applications at SBI.	Please clarify whether the infrastructure is limited to mentioned DC, DR or involvement of cloud environment too. If cloud, please let us know whether AWS, Azure, GCP in place.	The information will be shared to selected bidder. Infra primarily is on private cloud infra.
5	Part 2 Appendix- B Scope of Work	a. Gap Analysis	The service provider shall handhold Application Owners in preparation of all documents/fine tuning of process etc. which are required for ISO27001:2022 certification ensuring the closure of the audit findings.	We understand that partner is responsible to recommend controls, provide guidance on implementation of controls, validate the closure of any non-conformance and SBI will be responsible for actual implementation and closure. Please confirm implementation of controls shall not be the responsibility of bidder.	Implementation is responsibility of Bank.
6	Part 2 Appendix- B Scope of Work	a. Gap Analysis	The service provider shall handhold Application Owners in preparation of all documents/fine tuning of process etc. which are required for ISO27001:2022 certification ensuring the closure of the audit findings.	Please confirm that partner will not conduct risk assessment, updating of policies and procedures documents, internal audits.	Handholding expected from selected bidder for the activities.
7	Part 2 Appendix- B Scope of Work	d. Impart training to 50 officials	Impart certification training to 50 officials handing these seven applications for ISO 27001:2022 LA/LI certification and award the participation/pass certificate to the participants.	Please clarify training participation certificate to be provided by whom. Is it expected to get the certification from certifying accredited body, please confirm	Training certification has to be provided by accredited body.
8	Part 2 Appendix- B Scope of Work	d. Impart training to 50 officials	Impart certification training to 50 officials handing these seven applications for ISO 27001:2022 LA/LI certification and award the participation/pass certificate to the participants.	Can you please confirm if there are programs in place to increase awareness and competence?	Yes Bank has internal programs for IS Awareness.
9	Part 2 Appendix- B Scope of Work	NA	NA	In case of external certification body to be onboarded by vendor, 1. Should the efforts submitted by partner include the cost of the Certification Body as well? 2. Generally, Certification Body signs the agreement for 3 years, is the agreement with partner is also for 3 years? - Original Certification and ISMS sustenance for next 2 years?	Sub contracting is not allowed. 1. Yes 2. Yes for 3 years
10	Part 2 Appendix- B Scope of Work	NA	NA	We understand that technical assessment such as Source Code Review, VAPT, Application security, configuration review of protected systems will be out of scope. Please confirm	Activities related to ISO certifications are scoped.
11	General	General	NA	Have we performed asset based risk assessment or process based risk assessment?	Information will be shared with selected bidder

12	General	General	NA	Can you please provide approx.. Count of following devices for all seven applications 1. Servers 2. Databases 3. Network devices (Switches, Router, etc.) 4. Firewall 5. Any other security tools or devices	Information will be shared with selected bidder. Applications are 7.
13	General	General	NA	Are security tools such as SIEM, DLP, EDR, Antivirus, etc. common for all protected systems?	Yes
14	General	General	NA	Do we have central domain controller for seven applications and underlying processes? Or decentralized access management is implemented	Domain controllers are centralised with a mix of authentication for various applications.Detailed information will be shared with selected bidder.
15	General	General	NA	Are the new considerations for addressing the effects of climate change within the scope of ISMS?	ISO 27001:2022 scope to be covered.
16	General	General	Last date and time for Bid submission - Up to 12.00 P.M. on 11.11.2024	Request to increase the time duration to submit the proposal considering Diwali/Chhatt Pooja festivals, by at least 1-2 week	Please adhere to published timelines.
17	74 102	Clause 13.10 on Page 74 and clause (b) on page 102	a. Any document received from the Bank shall remain the property of the Bank and shall be returned (in all copies) to the Bank on completion of Service Provider's performance under the Agreement. b. Receiving Party shall return all originals, copies, reproductions and summaries of Confidential Information or Confidential Materials at Disclosing Party's request, or at Disclosing Party's option, certify destruction of the same.	We propose the below disclaimer: The Bidder shall be allowed to retain sufficient documentation as part of its professional records to support and evidence the work performed by it. Such retention shall be subject to obligations of confidentiality mentioned in the RFP.	Please adhere to published RFP guidelines.
18	Page 33	Clause 48. "Conflict of Interest"	48. CONFLICT OF INTEREST:	Please note that the provisions of this clause would be limited to the members of the engagement team of the consultant who are engaged in performing the services. Further, the terms "Members / Associates / Affiliates" as used in this clause would be limited to "Members / Associates / Affiliates" in India only. Request confirmation	Please adhere to published RFP guidelines.
19	Page 86	Annexure Penalty	If the Service Provider fails to deliver the report within stipulated time schedule, the Bank shall, without prejudice to its other remedies under the contract, deduct from the order price, as liquidated damages, a sum equivalent to 3% of the total order price for delay of each week or part there of maximum up to 15% of order price. Once the maximum penalty is reached, Bank may consider for termination of contract and initiate other appropriate action.	Request you to cap the overall penalties and liquidated damages of the Bidder under this RFP to 10% of the total contract value.	Please adhere to published RFP guidelines.
20	General	Overall RFP		Notwithstanding anything to the contrary, kindly note that we do not provide any legal services directly or indirectly since we are not permitted to provide the same. Our scope is limited to technical/commercial aspect and our services will not include provision of any legal services or legal advice. No work performed by our employees shall be construed as legal service/legal advice. Please confirm	Please adhere to published RFP guidelines.
21	9	6 : SKILL SET AND EXPERIENCE REQUIREMENTS OF RESOURCES	subcontracting/hiring of external resources is not permitted	The section states that sub contracting/ external hiring is not permitted. We being consulting firm is not allowed to perform external audit and provide certification. Can we get an external agency to support for certification	Sub contracting is not allowed.
22	9	6 : SKILL SET AND EXPERIENCE REQUIREMENTS OF RESOURCES	subcontracting/hiring of external resources is not permitted	If we can bid with auditing agency is there any preffered audit partner	Sub contracting is not allowed.

23	53	Appendix E	Bank Guarantee Format	Do we need to provide bank guarntee at the time of bid submission or it is only to be provided by successful bidder	Bank guarantee to be provided by successful bidder but EMD to be provided at the submission of bid.
24	56	Appendix F	Format for submission of client refrence	If we participate with external audit agency cleint refrence are to be provided of the agency or deloitte for similar work done with client	Sub contracting is not allowed.
25	8	Eligibility criteria	Eligibility criteria	In case of external agency wil qualificaation of eligibility criteria apply only to the bidding entity	Sub contracting is not allowed.