BOB Financial
Credit reimagined

Pre-bid respones towards the RFP
Selection of Agency for IT Risk Assessment and Certification for ISO 27001:2022
RFP NO: CO: BFSL/ IS RFP/2023-24/01, Dated: 22-09-2023

Sr. No.	Pg No	Point No	Tender Original Clause	Clarification	Request for Change / Modification / Addition / Deletion
1	9	2.2	The tenure of the contract initially would be for One year from the date of the issuance of first purchase order by the Company. Company can further extend this at its discretion at mutually agreed terms.	As we understand from the RFP - the engagement is for 1 year. However as per Appendix-2 (Bill of Material) bidder needs to share the costing for the Surveillance audit / Maintenance & Support. Please confirm on the tenure of the project.	Appendix-2 (Bill of Material) modified
2	10	3.1	Development or modification of risk management framework which would ensure that the IT risks are managed as per international best practices.	Is there any existing Risk Management Framework available with BFSL	NO
3	10	3.2	A comprehensive risk assessment of DC/DR operations on yearly basis.	The tenure of the contract initially would be for One year. How yearly basis will apply here	One year only
4	10	3.4	To ensure that the organization maintains ISO 27001 Certification for its DC & DR operations and maintains the same.	Please elaborate what is the expectation from the bidder.	Implementing 27001 controls
5	10	3.6	Perform Risk Assessment and submit Risk Mitigation plan of in scope operations of DC and DR as per Risk Assessment framework for BFSL's review/approval	Does the Risk Assessment Framework already exist or is the bidder expected to create the same.	Yes, to be created
6	10	3.8	Supporting the organization for closure of internal and external audit findings.	Please elaborate what is the expectation from the bidder. As per our understanding Implementation of the controls for closure of the gaps is out of scope .	To be read in continuation of 3.7, Supporting organisation for closure of gaps identified in pre audit / recertification (if contract is renewed after one year) and also support for closure of open points of IS audit (if any).
7	10	3.14	Review based on BFSL appointed IS Auditors Comprehensive Audit reports of IT Infrastructure.	Please elaborate what is the expectation from the bidder.	Review latest IS audit reports
8	10	3.15	Policies for MDM/Work from Home/BYOD etc.	Does the bidder need to create the policies? Or only review of the existing policies?	Yes
9	11	6	Control Implementation & Validation	Please elaborate what is the expectation from the bidder.	Implementing 27001 controls
10	11	7	Internal Audit trainings	Is the bidder expected to perform training and awareness session for the employees	one session
11	12	I	Detailed Scoping of DC and DR operations	Please elaborate what is the expectation from the bidder.	Scope finalizing
12	12	III	Conducting awareness sessions on IT Risk assessment and ISO 27001 standard for DC and DR staff once in a quarter.	How many such sessions will the bidder be required to carry out	once in quarter
13	12	VIII	Review of Policies Standards & Guidelines, Procedures and other subordinate documents.	Please specify what other subordinate documents or the number of policies to be reviewed	ISMS / IS Audit / IT procedures / CCMP/CSRF
14	13		Make/Review of IT/IS governance of the organization.	Does the bidder need to create the policies? Or only review of the existing policies?	Review policy
15	13		Make/Review of Risk Management framework	Does the bidder need to create the framework? Or only review of the existing framework?	Make
16	13		The selected Bidder will also evaluate the third-party relationships and perform risk assessment of the same. Frequency of the Risk Assessment would be on yearly basis.	Please elaborate what is the expectation from the bidder.	Yes
17	13		Review based on BFSL appointed IS Auditors Comprehensive Audit reports of IT Infrastructure.	Please elaborate what is the expectation from the bidder.	only review
18	13		Required awareness training which will include classroom training and, on the job, training would need to be provided by the selected Bidder to BFSL's personnel/BFSL's onsite vendors on quarterly basis to impart proper understanding of ISO 27001 standard and IT Risk Assessment to enable the BFSL personnel/onsite vendors to carry out such assignments independently in future.	1. Number of classroom training is required to be provided in a quarter 2. The classroom training will be for all 4 locations	Physical trainning at Goregoan office, rest location online
19	14		The Selected Bidder will have to hold periodic meetings with the BFSL and the frequency would be quarterly and would spell out a detailed remediation plan meant for various levels such as organization, policies and procedures, devices to facilitate implementation.	. Meetings can be held virtually or onsite presence is mandatory across all 4 locations on every quarter	Quarterly on site mumbai only
20	14		The selected Bidder has to coordinate with the BFSL's system integrator, monitor the progress in risk remediation and provide handholding support to the BFSL till the risk is remediated.	Please elaborate what is the expectation from the bidder.	This will be discuss separately with shortlisted bidder only, with their review.
21	14	7	Control Implementation & Validation	Please specify what control needs to be implemented?	ISO 27001 : 2022 controls and validation
22	14	10	Conduct Risk Assessment for the identified functions & Submit it for review/approval along with Risk Mitigation plan	Please specify the no. of functional units	Mandate Fuctions
23	15	13	All documentation required for ISO 27001 certification process	Please specify what all documentation is being referred to ?	Yes
24	16	3.1.1	Based on the contents of the RFP, the selected vendor shall be required to independently arrive at a Selection of Agency for IT Risk Assessment and Certification for ISO 27001:2022:2022, which is suitable for the Company, after taking into consideration the efforts estimated for implementation of the same and the resource and the equipment requirements.	is the bidder required to select the agency for external certification?	No, to be read as "Based on the contents of the RFP, the selected vendor shall be required to independently arrive at IT Risk Assessment and Certification for ISO 27001:2022:2022, which is suitable for the Company, after taking into consideration the efforts estimated for implementation of the same" and the resource and the equipment requirements.
25	16	3.1.3	The Bidder will be required to fix any vulnerability in the Selection of Agency for IT Risk Assessment and Certification for ISO 27001:2022:2022 at no additional cost during the entire tenure of the contract. These vulnerabilities can be detected by the Company or can be a finding of any internal or external audit conducted by the Company or its auditors on a periodic basis.	What vulnerability needs to be fixed by the bidder? Please elaborate	This will be discuss separately with shortlisted bidder only, with their review.
26	11	3	Following is the list of in-scope business units: 1. BOB Financial Solutions LTD (Head Office) 2. BOB Financial Solutions LTD (BCP Site) 3. NTT Global Data Centers & Cloud Infrastructure India Private Limited. (DC) 4. NTT Global Data Centers & Cloud Infrastructure India Private Limited. (DR)	What are the business functions available for these 4 sites, or number of business functions across 4 sites	1. Card Operations 2. On boarding and card issuance 3. Merchant Management 4. FRM 5. Production Center 6. Customer Experience 7. Finance 8. Support (HR/Admin/ IT Infra)
27	10	7	Perform pre-surveillance/recertification Internal Audit as per ISO 27001 standard	The tenure of the engagement is for 1 year but surveillance audits are performed after the 1st year.	If contract renew for 1 year then surveillance audit to be performed
28	Appendix 2	BOM	Post Certification surveillance audit and training as per scope of work in this RFP (including RCB charges, if any) for first year.	The tenure of the engagement is for 1 year but surveillance audits are performed after the 1st year.	If contract renew for 1 year then surveillance audit to be performed
29	7	11	1.7 Important Details (Schedule of Events, contact & communication details etc.) 11 - Bid Security (EMD) - 3,00,000/-	Is there Exemption for EMD to MSME Certificate Compnay	Yes , bidder has to provide proper MSME certification for the same.
30	16	3.1	Project Scope Based on the contents of the RFP, the selected vendor shall be required to independently arrive at a Selection of Agency for IT Risk Assessment and Certification for ISO 27001:2022:2022, which is suitable for the Company, after taking into consideration the efforts estimated for implementation of the same and the resource and the equipment requirements	Vendor have to deploy resource onsite for conducting the activity	Yes

31	19	5.2	Price Terms of payment as indicated in the Purchase Contract that will be issued by the company on the selected Vendor will be final and binding on the vendor and no interest will be payable by the Company on outstanding amounts under any circumstances.	Could you provide the payment terms for IT Risk Assessment and Certification for ISO 27001 of the project. Will those be a one-time payment or spread out over multiple milestones.	one time after certification
32	1	Appendix A - Technical Bid > Point 1	Experience of providing ISO 27001 consultancy services to the BFSI sector in India leading to successful ISO 27001 certification/recertification in the last 5 years	Request to change the clause to below revised clause: Experience of providing ISO 27001 consultancy services to the BFSI/Financial Instituition (FI) in India leading to successful ISO 27001 certification/recertification in the last 5 years	Yes
33	2	Appendix 2 - Bill Of Materials	Appendix 2 - Bill Of Materials	Cost will be provided for one year or we have to take into consideration certification cost for three years	One year only
34	11	Detailed Deliverable	Control Implementation & Validation	We understand that control implementation recommendation will be provided by us and we will validate the implemented controls. However, BFSL would be responsible for actual control implementation activity. Please confirm	Bidder will be responsible for implentation
35	11	Detailed Deliverable	Internal Audit trainings	Does BFSL expect the bidder organizations to provide Internal Audit trainings for ISO/IEC 27001:2022 along with certifications? - If yes, the responsibility for on-boarding the certification body is with whom? - If no, please elaborate on the training needs in this section	once in quarter
36	11	Following is the list of in-scope business units	-	Is the work expected to be done onsite or remotely?	Onsite
37	12	Scope in Detail	Certification including Recertification should be as per the latest version of ISO 27001 currently being the version 2022	Is BFSL already certifies against the ISO/IEC 27001:2013 as its says 'recertification' or this is for 3 year cycle?	New Certification
38	12	Scope in Detail	-	Can you please provide the details of department / key business and support functions which needs to covered under the scope for certification	Overall BFSL
39	13	Policy & Procedures Review	....Compliance to RBI / Other Regulatory Guidelines etc.'	What other regulators will be included: SEBI, NCIIPC, etc.	RBI / SEBI /NPCI
40	13	Training	Required awareness training which will include classroom training and, on the job, training would need to be provided by the selected Bidder to BFSL's personnel/BFSL's onsite vendors on quarterly basis to impart proper understanding of ISO 27001 standard and IT Risk Assessment to enable the BFSL personnel/onsite vendors to carry out such assignments independently in future	Request you to confirm that how many training sessions would be required to conduct per quarter	once in quarter
41	13	Risk Assessment and Risk mitigation	Risk Assessment and Risk mitigation	Can you please provide the number of customer facing and internal applications that needs to be covered in the scope of ISO 27001:2022	All the applications
42	13	Risk Assessment and Risk mitigation	The selected Bidder will also evaluate the third-party relationships and perform risk assessment of the same	Can you please elaborate the same. Do you want bidder organizations to perform third party security risk assessment for vendors of BFSL? If yes, request you to provide the number of vendors to be covered	2 samples
43	15	DETAILS OF INFRASTRUCTURE AT BFSL'S DC/DR	Details of infrastructure at BFSL's DC/DR	Request you to provide counts for following IT devices installed at DC and DR 1. Servers 2. Databases 3. Network devices (Switches, Router, etc.) 4. Firewall 5. Any other security tools or devices	Inventory will be share ones the bidder will get selected
44	16	3.1 Project Scope	Point 3 - The Bidder will be required to fix any vulnerability in the Selection of Agency for IT Risk Assessment and Certification for ISO 27001:2022:2022 at no additional cost during the entire tenure of the contract. These vulnerabilities can be detected by the Company or can be a finding of any internal or external audit conducted by the Company or its auditors on a periodic basis.	We understand that we shall not be responsible for control implementation against any vulnerability identified. Hence, requesting you to remove this clause	As requested by bidder, this point will be removed.
45	16	3.1 Project Scope	The Bidder has to size the Selection of Agency for IT Risk Assessment and Certification for ISO 27001:2022:2022 covering hardware, software & services to ensure availability, scalability, redundancy and performance of the Selection of Agency for IT Risk Assessment and Certification for ISO 27001:2022:2022, and to meet technical and functional requirements as per the terms of the RFP within the timeframe prescribed by the Company	Request you to elaborate the same	Inventory will be share ones the bidder will get selected
46	17	3.3	The FRSM (Functional Requirements Specification Manual) would be reviewed by the Company and the selected bidder is expected to remediate all gaps identified by the Company	Request you to elaborate the requirement here	Suggessions to mitigate current gaps
47	17	3.3 and 3.4	Functional Requirements specifications study : The selected bidder will conduct a detailed systems requirements study and provide a solution specific FRSM for solutions relating to the functionalities as required supporting the various processes within the Company as responded by the Bidder	We understand that the main scope of this RFP to perform risk assessment, internal audit and assist BFSL to get certified against ISO 27001:2022. Hence, we could not understand the requirement of FRSM for solutions in this scope. Request you to elaborate the same	Suggessions to mitigate current gaps
48	17	3.4 (point 3)	Bidder is expected to prepare detailed documentation, presentation, workflows for the business processes affected due to implementation of the Selection of Agency for IT Risk Assessment and Certification for ISO 27001:2022:2022.	Can you please elaborate this requirements	Review and modifications in current policy and procedure
49	28	Part - II Technical Bid	g. Product roadmap of the proposed solution for the next three years	As scope of work under this RFP is only for one year (including first surveillance audit), requesting you to change this for one year instead of three years	1 year only
50	18	3.5	Business Process Definition (BPD)/Parameterization The selected bidder is expected to help the Company to parameterize the product and provide valuable inputs at the time of system parameterization based on the current state assessment undertaken by the selected bidder. Also, the core team training conducted by the selected bidder should reflect the understanding of the Company's current processes as a result of conducting the current assessment. The selected bidder would be responsible for ensuring that the BPD/Parameterization exercise is as per the plan.	We understand that key security controls to be suggested on each process or application of BFSL. Please confirm the same and request you to elaborate the requirement under Business process definition or parameterization	Security Controls suggestions and recommedations
51	28	-	Is there any requirement where the Bidder organizations are required to perform technical assessment such as conducting vulnerability assessment, penetration testing, configuration review, AppSec, etc. for selected infrastructure / applications? If yes, please provide the count of applications and infrastructure components such as servers, network and security devices (routers, switch, firewall,), etc.		not in scope