



Small Industries Development Bank of India

Purpose	Request for Proposal for Appointment of Consultant for ISO 27001 Certification of Data Centre and Disaster Recovery Site.
Tender No.	400/2016/1145/BYO/ITV Dated February 18, 2016
Pre-bid Meeting	February 24, 2016, 1100 hours

Pre-Bid Clarifications

. N.	Page No.	Section No.	Clarification point as stated in the tender document	Deviation	SIDBI Response
1.	36	6.5 (3)	The details and number of personnel deployed, qualification, experience etc to be clearly given in the technical bid response.	Please confirm if dedicated team needs to be deployed at DC & DR.	SIDBI is not expecting full time on-site resource for the project. However consultant should ensure that resource assigned for the project is engaged throughout its life cycle till its completion.
2.	52	9.16	If the selected bidder fails to complete the project within stipulated time, SIDBI will impose a penalty of 0.5% of the order value for each weeks delay or part thereof attributable to the bidder, subject to maximum of 10% of the order value. Fraction of week is to be construed as one full week for arriving at the delay in terms of weeks.	We request to limit the damages till 5%	No Change
3.	N/a	N/a	The payment terms are: <ul style="list-style-type: none"> • Completion of phase1 and 	The payment details should be: <ul style="list-style-type: none"> • 40% in Advance 	No Change

. N.	Page No.	Section No.	Clarification point as stated in the tender document	Deviation	SIDBI Response									
			phase2: 30% <ul style="list-style-type: none"> • Phase3 :30% • Phase 4: 40% • Surveillance audit :on completion of activity in respective years. 	<ul style="list-style-type: none"> • 20% on Phase 1 and Phase 2 • 20% on Phase 3 • 20% on Phase 4 										
4.	N/a	N/a	Clarification	What is the scope of the project in terms of no. of departments / business processes?	<ul style="list-style-type: none"> • Scope of project is ISO 27001 Certification of Data Center, Mumbai and DR Site, Chennai and its associated processes. • As per ISO 27001 all process needs to be reviewed and implemented. • The department coordinating the ISO 27001 consultancy would be Information Technology Vertical (ITV). • However, in case consultant need to interact with any other department during the course of consultancy, the same would be arranged by ITV 									
5.	N/a	N/a	Clarification	What is the count of employees in the scope of the project?	The count of employees, including outsourced partners managing DC and DR is: <table border="1" data-bbox="1556 1230 1906 1401" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th data-bbox="1556 1230 1619 1300">S. N.</th> <th data-bbox="1619 1230 1799 1300">Details</th> <th data-bbox="1799 1230 1906 1300">No.</th> </tr> </thead> <tbody> <tr> <td data-bbox="1556 1300 1619 1336">1</td> <td data-bbox="1619 1300 1799 1336">SIDBI Staff</td> <td data-bbox="1799 1300 1906 1336">10-15</td> </tr> <tr> <td data-bbox="1556 1336 1619 1401">2</td> <td data-bbox="1619 1336 1799 1401">Outsource d partner</td> <td data-bbox="1799 1336 1906 1401">25-30</td> </tr> </tbody> </table>	S. N.	Details	No.	1	SIDBI Staff	10-15	2	Outsource d partner	25-30
S. N.	Details	No.												
1	SIDBI Staff	10-15												
2	Outsource d partner	25-30												

. N.	Page No.	Section No.	Clarification point as stated in the tender document	Deviation	SIDBI Response
6.	N/a	N/a	Clarification	Is the scope of the project within one geographical location or multiple locations?	Two locations viz., Data Center, Mumbai and DR Site, Chennai
7.	N/a	N/a	Clarification	How many teams / people are currently responsible for Information Security Management?. Please provide the team names.	<p>Currently, teams from SIDBI responsible for IS management are.</p> <ul style="list-style-type: none"> • Information Technology Vertical : <ul style="list-style-type: none"> ➤ Network and Security team consisting of 4 people and ➤ Data Center team consisting of 4 people. • Risk Management Vertical <ul style="list-style-type: none"> ➤ CISO • Besides SIDBI teams mentioned above, personnel from outsourcing partner who are managing the Data Center and DR site are also responsible for IT and IS management.
8.	N/a	N/a	Clarification	Please provide count of total information assets to be covered as part of ISO 27001 risk assessment activity. Rough count is sufficient.	<p>All the assets at Data Center and DR site as given in the tender are required to be covered under the scope of ISO 27001 risk assessment.</p> <p>Rough count of some of the assets at DC and DR is:</p> <ul style="list-style-type: none"> • Servers (including physical and virtual): 90-120

. N.	Page No.	Section No.	Clarification point as stated in the tender document	Deviation	SIDBI Response
					<ul style="list-style-type: none"> • Network hardware (routers, switches, load balancers etc): 25-30 • Security devices :7-10 • Applications (internal): 35-40. • Applications (web facing): 5-10 • Backup and Storage: 5-10. • VC equipment:7-10 etc.
9.	N/a	N/a	Clarification	<p>Please provide the list of information security policies and procedures which are to be reviewed and updated.</p> <p>Please provide a list of IT & IS processes that are already implemented.</p>	<p>Bank has in place IT Security Policy, IT Procedure manual, Backup Policy and Email policy.</p> <p>Any gaps in the above policies which are required for getting ISO certification of Data Center and DR Site needs to be identified.</p> <p>In addition all other policies / procedures and process as required for ISO 27001:2013 certification are to be developed by the Consultant.</p>
10.	N/a	N/a	Clarification	Please provide a list of IT & IS processes that are already implemented.	The policies as mentioned in S.N.9 are implemented.
11.	N/a	N/a	Clarification	Please provide a list of current IT security technologies already implemented.	<ul style="list-style-type: none"> • Firewalls • Intrusion Prevention System • Web Gateway Security • Antivirus

. N.	Page No.	Section No.	Clarification point as stated in the tender document	Deviation	SIDBI Response												
					Refer to Section 5.5 [(v)g] on page 23 or RfP for the details.												
12.	N/a	N/a	Clarification	Does the organization already have any other standard certifications?	No												
13.	N/a	N/a	Clarification	Do you want to conduct technical security assessments also? If please provide details below: <ul style="list-style-type: none"> • No. of IP for penetration testing. • No. of devices for configuration review. • No. of application for security testing. 	Yes Based on the applications hosted at data center for public access, the details are: <table border="1" data-bbox="1495 578 1915 786"> <thead> <tr> <th>S. N.</th> <th>Details</th> <th>No.</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>No of IPs</td> <td>10-16</td> </tr> <tr> <td>2</td> <td>No of Devices</td> <td>10-12</td> </tr> <tr> <td>3</td> <td>No of applications</td> <td>5-7</td> </tr> </tbody> </table>	S. N.	Details	No.	1	No of IPs	10-16	2	No of Devices	10-12	3	No of applications	5-7
S. N.	Details	No.															
1	No of IPs	10-16															
2	No of Devices	10-12															
3	No of applications	5-7															
14.	N/a	N/a	Clarification	Is there any expected date to achieve the ISO 27001 compliance?	December' 2016												
15.	N/a	N/a	Clarification	Should the ISMS maintenance include one round of gap assessment, risk assessment, documentation review, training and internal audit or should we consider only the surveillance audit cost and engagement during the surveillance audit?	Yes												
16.	N/a	N/a	Clarification	What is the count of participants for ISO 27001 Lead auditor training?	5												
17.	N/a	N/a	Clarification	What is the number of posters and emailers expected for a year?	Posters: 15-20 Emailers:25-30												
18.	40	7(6)	The bidder should have executed at least one order of Rs.20 lakh	The bidder should have executed atleast two orders total worth of	No Change.												

. N.	Page No.	Section No.	Clarification point as stated in the tender document	Deviation	SIDBI Response
			for ISO27001 consultancy (includes two surveillance audits for a period of two years) in at least one organization in BFSI sector.	Rs.20 lakh for ISO 27001 consultancy out of which atleast one should be in BFSI Sector.	

All other terms and conditions of the RfP remain unchanged.
