Invitation of bids from eligilible organisations for Creation of IS Policy, Cyber Security Policies & Frameworks.

Dated: 28th July 2020.

BOB Financial Solutions Limited.

303, 3rd Floor, Hallmark Business Plaza,

Near Gurunanak Hospital,

Kalanagar, Bandra East

Mumbai – 400 051

Tel: 022-4208 6613,

Email: rfp@bobfinancial.com

Important Details (Schedule of Events, contact & communication details etc.)

Schedule and Due Dates	**Date**
Release of the request for Proposal Document	28.07.20
share list of queries / clarifications	31.07.20
Response to queries	04.08.20
Commercial & Technical Bid Submission	07.08.20 by 2:00pm IST
Award Letter	14.08.20

BOB Financial
— Credit reimagined —

Scope of Work

BFSL is approachin the selected vendor for Creation of IS Policy, Cyber Security Policies & Frameworks. Formulation and update the existing Information and Cyber Security Policy as per BFSL requirements & Preparation of IT manuals containing Standard Operating Procedures (SOPs), Formulation of Cyber Crisis Management Plan (CCMP), business Continuity plan , Cyber security incident frame work along with how to follow.

	Section/Para	Compliance Requirement
IT Governance	1.1	Constitution of IT Strategy Committee
IT Policy	2	To have a Board-approved IT Policy- Bidder should create an ISMS policy as per PCI-DSS Compliance
	2(c)	To ensure technical competence at senior/middle level management of NBFC, periodic assessment of the IT training requirements should be formulated to ensure that sufficient, competent and capable human resources are available.
Information and Cyber Security	3	Bidder have to create an ISMS Policy with prescribed basic tenets and IS framework which eventually get approved by Board for further distribution
	3.2	Have a Board-approved Cyber security policy with prescribed basic tenets and IS framework
	3.3	Bidder have to create or devise a strategy for managing and eliminating vulnerabilities and such strategy may clearly be communicated in the Cyber Security policy
	3.4	Crate & Development of cyber resilience framework
	3.5	Creation of Cyber Crisis Management Plan (CCMP) which will eventually get approved by Board and will be part of overall Board approved strategy.
	3.7	NBFCs should proactively promote, among their customers, vendors, service providers and other relevant stakeholders an understanding of their cyber resilience objectives, and require and ensure appropriate action to support their synchronised implementation and testing- Creation of User awareness training program for Employee ,Vendor and IT Professionals
	3.9	Bidder has to create an Risk assessment policy which will get used for further audit in BFSL
	3.10	NBFCs that are already using or intending to use Mobile Financial Services should develop a mechanism for safeguarding information assets that are used by mobile applications to provide services to customers. The technology used for mobile services should ensure confidentiality,

		integrity, authenticity and must provide for end-to end encryption.
	3.11	Bidder has to create an Policy which will be followed by BFSL to ensure proper security while using Social Media to market their products should be well equipped in handling social media risks and threats and proper controls, such as encryption and secure connections, should be prevalent to mitigate such risks.
	3.12	There is a vital need for an initial and ongoing training and information security awareness programme. The programme may be periodically updated keeping in view changes in information technology system, threats/vulnerabilities and/or the information security framework. There needs to be a mechanism to track the effectiveness of training programmes through an assessment / testing process. At any point of time, NBFCs need to maintain an updated status on user training and awareness relating to information security.- Bidder has to create and ISMS security awareness traning program for IT , Employee and Vendor and senior management
IT Operations	4.1	NBFCs should identify system deficiencies and defects at the system design, development and testing phases. NBFCs should establish a steering committee, consisting of business owners, the development team and other stakeholders to provide oversight and monitoring of the progress of the project, including deliverables to be realized at each phase of the project and milestones to be reached according to the project timetable.
	4.2	NBFCs should develop, with the approval of their Board, a Change Management Policy that encompasses the following: a) prioritizing and responding to change proposals from business, b) cost benefit analysis of the changes proposed, c) assessing risks associated with the changes proposed, d) change implementation, monitoring and reporting. It should be the responsibility of the senior management to ensure that the Change Management policy is being followed on an ongoing basis.
	4.4	NBFCs may put in place an effective system-generated MIS that assist the Top Management as well as the business heads in decision making and also to maintain an oversight over operations of various business verticals.
	4.5	The MIS that help management in taking strategic decisions shall also assist in generating the required information/returns for the supervisor. All regulatory/supervisory returns should be system driven; there

		should be seamless integration between MIS system of the NBFC and reporting under COSMOS. Further, it is essential that "Read Only" access be provided to RBI Inspectors.
IS Audit	5.1	NBFCs shall adopt an IS Audit framework duly approved by their Board. Further, NBFCs shall have adequately skilled personnel in Audit Committee who can understand the results of the IS Audit.
	5.3	IS Audit may be conducted by an internal team of the NBFC. In case of inadequate internal skills, NBFCs may appoint an outside agency having enough expertise in area of IT/IS audit for the purpose.
	5.4	The periodicity of IS audit should ideally be based on the size and operations of the NBFC but may be conducted at least once in a year. IS Audit should be undertaken preferably prior to the statutory audit so that IS audit reports are available to the statutory auditors well in time for examination and for incorporating comments, if any, in the audit reports.
	5.7	NBFCs shall adopt a proper mix of manual techniques and Computer-assisted Audit Techniques (CAATs) for conducting IS Audit. CAATs may be used in critical areas (such as detection of revenue leakage, treasury functions, assessing impact of control weaknesses, monitoring customer transactions under AML requirements and generally in areas where a large volume of transactions are reported) particularly for critical functions or processes having financial/regulatory/legal implications.
Business Continuity Planning	6	NBFC should adopt a Board approved BCP Policy. The functioning of BCP shall be monitored by the Board by way of periodic reports. The Bidder has to create and BCP policy as per PCIDSS compliance and eventually it will get approved by BFSL board for further implementation .
	6.1	Business Impact Analysis- NBFCs shall first identify critical business verticals, locations and shared resources to come up with the detailed Business Impact Analysis. The process will envisage the impact of any unforeseen natural or man-made disasters on the NBFC's business. The entity shall clearly list the business impact areas in order of priority.
	6.2	Recovery strategy/ Contingency Plan- NBFCs shall try to fully understand the vulnerabilities associated with interrelationships between various systems, departments and business processes. The BCP should come up with the probabilities of various failure scenarios. Evaluation of various options should be done for recovery and the most cost-effective, practical strategy should be selected to minimize losses in case of a disaster.

	6.3	NBFCs shall consider the need to put in place necessary backup sites for their critical business systems and Data centers
	6.4	NBFCs shall test the BCP either annually or when significant IT or business changes take place to determine if the entity could be recovered to an acceptable level of business within the timeframe stated in the contingency plan. The test should be based on 'worst case scenarios. The results along with the gap analysis may be placed before the CIO and the Board. The GAP Analysis along with Board's insight should form the basis for construction of the updated BCP.
	7.1	The terms and conditions governing the contract between the NBFC and the IT Outsourcing service provider should be carefully defined in written agreements and vetted by NBFC's legal counsel on their legal effect and enforceability. The contractual agreement may have the prescribed provisions

Bidder Eligibility criteria:-

- Should be either an Government Organization/PSU/PSE/ partnership firm/LLP or a limited Company under Indian Laws or / an autonomous Institution approved by GOI/RBI promoted. Document proof - Copy of Certificate of Incorporation self attested.
- Should have been in existence in India for five years as on 28/07/20
- Should have a minimum average annual turnover of Rs.10.00 crores (Rupees Ten Crores) during last three financial years viz. 20017-18, 2018-19 and 2019-20 and at least 20% revenue must have come from the Security testing & Consulting services. Document proof –Self Declaration and Copies of Annual Reports in case of listed companies and copies of audited balance sheets and P&L statements in case of others

Technical Evaluation Criteria

In order to determine whether the bidders are qualified and whether the technical aspects are substantially responsive to the requirements set forth in the bidding documents, the Tendering Authority will examine the information supplied by the Bidders and shall award points to the bidders on the basis of the following parameter.

#	Parameter	Maximum Score
1	B.E. / B.Tech. / with minimum 15 years of experience	20

	>=15 years : 20 marks >=10 and <15 Resource : 10 marks <=5 and <10 Resource : 5 marks (Self-Declaration on company letter head with experience details)	
2	MBA/MCA with minimum 15 years of experience in conducing IT/IS Audit >=15 years : 20 marks >=10 and <15 Resource : 10 marks <=5 and <10 Resource : 5 marks (Self-Declaration on company letter head with experience details)	20
3	**Certifications** – Certified Information Security Auditor (CISA) & ISO 27001 Lead Auditor CISA & ISO 27001 LA: 20 Marks ISO 27001 LA : 10 Marks CISA : 5 marks	20
4	**Experience -** • Experience on preparing & Executing the CCMP Plan for banks or regulatory bodies (05 Markks) • Experience in conducting IS Audit/Similar assignment. (05 Marks) • (Self- declaration & Relevant supporting documents)	10
5	Technical Approach/Methodology/Presentation basis scope of work	30

Based on the submission of documents. Bidder must get a minimum score of 70 Marks to qualify for commercial bid opening.

Qualified Bidder will be called for a discussion about the assignment.
Commercial score will be for 30 marks.

Bidder will be finalized on Tehno-commercial basis, which is H1 L1.

Deliverables & Payment Terms –

#	Deliverables	Payment Terms
1	Submission of Gap Assessment Report	20%
2	Submission of IS Policy documentation	20%
3	Submission of SOPs	20%
4	Submission of BCP & CCMP Documentation	30%
5	Final Sign Off	10%

BOB Financial
— Credit reimagined —

Price Bid Format

Sr. No	Description	Professional Fee	Tax	Total
1	**Conducting Security Gap Assessment, Creation of IS Policy, Cyber Security Policies & Frameworks**			
	Total			

Techno-commercial Proposal Evaluation Criteria:

Fixed cost bids would be evaluated on techno commercial basis.

In techno commercial evaluation the Technical Proposal will have 70% weightage and Financial Proposal shall have 30% weightage. These weightages shall be taken into consideration for arriving at the successful firm. The evaluation methodologies vis-a-vis the weightage are as under: Score will be calculated for all empanelled firms who have submitted their application using the following formula:

S = (T/T High x 70) + (C Low/C x 30)

Where: S = Score of the Firm

T =Technical score of the firm

T High = Highest Technical score among the firms

C = Quote as provided by the firm

C Low = Lowest Quote of C among the firms

The firm securing the highest score becomes the successful firm For example – There are three bidders A, B and C. Technical score will be arrived at treating the marks of the bidder scoring the highest marks (A) in Technical evaluation as 100. Technical score for other bidders (B, C, etc.) will be computed using the formula Marks of B / Marks of highest scorer A*100. Similarly Commercial Score of all technically cleared bidders will be arrived at taking the cost quoted by L1 bidder i.e., the lowest quote from all technically qualified bidder (say C) as 100. Marks for other bidders will be calculated using the formula Commercial Score = Cost of L1 bidder / Cost quoted by bidder * 100.

A “Combined score” will be arrived at, taking into account both marks scored through Technical Proposal evaluation and the nominal commercial quotes with a weightage of 70% for the Technical Proposal and 30% for the Financial Proposal as described below. The combined score is arrived at by adding Technical Score and Commercial Score. The successful bidder will be the one who has highest Combined Score.

Sr.No.	Empanelled Firm	Technical Evaluation marks (T)	Commercials in INR(C)	Technical Score	Commercial Score	Combined Score (out of 100)
1	A	95	71	95/95*70 = 70.0	60/71*30 = 25.35	70.0+25.35 =95.35
2	B	85	65	85/95*70 = 62.63	60/65*30 = 27.69	62.63+27.69 = 90.32
3	C	90	60	90/95*70 = 66.32	60/60*30 = 30.0	66.32+30.0 = 96.32

In the above example Empanelled Firm C with highest score becomes the successful winner for this mandate.

Proposal submission : -

1. The quotation in a sealed envelope to be submitted at Hallmark Business Plaza office address mentioned above , If physical submission is not possible due to current situation of Lockdown , than would request you to submit proposal in password protected pdf format to rfp@bobfinancial.com
2. Technical documents must be submitted and commercial bid must be password proctected at the time of bid submission.
3. Only once the presentation is done and BFSL will carry out commercial bid opening only for technically qualified bids , that's when we request all the bidders to share the commercial bid password at the above email ID.

Terms & Conditions:

BFSL reserves the right to at any point:

- Reject any and all proposal received in response to the Terms of Reference.
- Waive or Change any responsibility in the proposal.
- Negotiate any aspect of proposal with final shortlisted proposer.
- Extend the time for submission of all proposals.
- Select the most responsive proposer as deemed suitable.
- Share the information/ clarifications provided in response to the Terms of Reference by any proposer, with any other proposer(s) /others, in any form.
- Cancel the Terms of Reference at any stage, without assigning any reason whatsoever.
- Bidders will be selected basis techno-commercial (documents submitted) proposed.

ANNEXURE -I

UNDERTAKING FOR NON- BLACKLISTED

(To be provided on letter head of the Bidder's Company)

AVP Procurement
BOB Financial Solutions Ltd.
303, 3rd Floor,
Hallmark Business Plaza,

Near Gurunanak Hospital,

Kalanagar, Bandra East

Mumbai – 400 051

Tel: 022-4208 6613,

Dear Sir,

We, M/s_____, do hereby confirm that we have not been blacklisted/banned/ declared ineligible for corrupt and fraudulent practices by any Govt. Financia Institutions/Banks/ Government/ RBI/ ICAI/ Semi Government Departments/ PSUs in India and haveno disciplinary proceedings pending against the applicant firm or any of the partners.

This declaration is been submitted and limited to, in response to the tender reference mentioned in this document

Dated at __day of_____2018.

Thanking You,

Yours faithfully,

Signature of Authorized Signatory

Name of Signatory:

Designation:

Seal of Firm/LLP