


<div>  <div> <b>BOB Financial</b>  <small>CREDIT FINANCER</small> </div> </div> <div> Pre-bid responses - RFP Appointment of consultant for BFSL Information Security Audit (IS Audit).  RFP NO: CO: BFSL/SYS RFP/23-24/08  Dated: 23-12-2023 </div>						
Sr. No.	Pg No	Point No	Tender Original Clause	Clarification	Request for Change / Modification / Addition / Deletion	BFSL Remarks
1	2	Annexure 01-Eligibility Criteria - IS Audit 23 (B) Eligibility Criteria	<b>S.No. 1 - Legal Entity</b> The bidder must be an Indian firm; a public or private firm, registered under Companies Act 1956, a proprietorship firm, or a partnership firm registered under the Partnership Act, 1932 or an LLP. (Consortium of companies not permitted)	N.A.	<b>Request to kindly modify clause as below:</b> The bidder must be an Indian firm; a public or private firm, registered under Companies Act 1956, a proprietorship firm, or a partnership firm registered under the Partnership Act, 1932 or an LLP <b>Act, 2008. (Consortium of companies not permitted)</b>	RFP term cannot be change
2	2	Annexure 01-Eligibility Criteria - IS Audit 23 (B) Eligibility Criteria	<b>S.No. 3 - Business Operation</b> Bidder must have provided/done similar service any 2-3 of the NBFC / Financial Institute or Banks.	N.A.	<b>Request to kindly modify clause as below:</b> Bidder must have provided/done similar service any 2-3 of the NBFC / Financial Institute or Banks/ <b>Insurance Sector/ Govt. sector/ Enterprises in India/Globally</b>	No Change
3	1	Appendix 01 Technical Evaluation	<b>S.No. 1</b> <b>Information Security Audits</b> completed (In the last 5 years) in any Public sector Bank in India, BFSI Sector other than Banks in India.	N.A.	<b>Request to kindly modify clause as below:</b> <b>Information Security Audits</b> completed (In the last 5 years) in any Public sector Bank in India, BFSI Sector other than Banks/ <b>Insurance Sector/ Financial Institutions/ Enterprises/ Govt. sector in India/ Globally</b> .	No Change
4	1	Appendix 01 Technical Evaluation	<b>S.No. 1</b> <b>Documentary proof</b> : Engagement Letters and Purchase orders from all the relevant BFSI Clients.	N.A.	<b>Request to kindly modify clause as below:</b> <b>Documentary proof</b> : Engagement Letters <b>and-OR</b> Purchase orders/ <b>Work order</b> from all the relevant <b>BFSI</b> -Clients.	No Change
5	1	Appendix 01 Technical Evaluation	<b>S.No. 2</b> <b>Infrastructure Audits</b> of Data Centre's completed (In the last 5 years) in any Public sector Bank in India, BFSI Sector other than Bank in India.	N.A.	<b>Request to kindly modify clause as below:</b> <b>Infrastructure Audits</b> of Data Centre's completed (In the last 5 years) in any Public sector Bank in India, BFSI Sector other than Banks/ <b>Insurance/ Financial Institutions/ Corporates/ Govt. sector in India/ Globally</b> .	No Change
6	10	1.1 (b)	IT Infrastructure in DC and DR	N.A.	<b>Request to kindly clarify clause as below:</b> Please clarify the details of work to be performed for the assets defined under this section	The inventory sheet attached.
7	12	1.1 (f)	Network Facility and Equipment Management	N.A.	<b>Request to kindly clarify clause as below:</b> Our understanding is that the review of documentations, process and procedures are to be performed for Network Facility and Equipment Management. Kindly clarify as no other details provided in the RFP	Details mentioned on page no 12 of 47 in RFP document.
8	13	1.1 (g)	Database Management System and Data security.	N.A.	<b>Request to kindly clarify clause as below:</b> Our understanding is that the review of documentations, process and procedures are to be performed for Database Management System and Data Security. Kindly clarify as no other details provided in the RFP	Details mentioned on page no 13 of 47 in RFP document.
9	13	1.1 (h)	Help Desk:	N.A.	<b>Request to kindly clarify clause as below:</b> Our understanding is that the review of documentations, process and procedures are to be performed for Helpdesk. Kindly clarify as no other details provided in the RFP	Details mentioned on page no 13 of 47 in RFP document.
10	Additional clarification required				Request you to kindly provide count and name of Policy, procedures, SOP or any other documents to be reviewed.	Policy, procedures, SOP or any other documents will share with selected bidder for review.
11	Indemnity				Tenderer shall indemnify and hold harmless the bidder for all Losses incurred in connection with any third-party Claim, except to the extent finally judicially determined to have resulted primarily from the fraud or bad faith of such Bidder.	We cannot change / modify the standard clause
12	Limitation of the Bidder's Liability towards the Purchaser				Tenderer (and any others for whom Services are provided) shall not recover from the Supplier, in contract or tort, under statute or otherwise, any amount with respect to loss of profit, data or goodwill, or any other consequential, incidental, indirect, punitive, or special damages in connection with claims arising out of this Agreement or otherwise relating to the Services, whether or not the likelihood of such loss or damage was contemplated. Tenderer (and any others for whom Services are provided) shall not recover from the Supplier, in contract or tort, including indemnification obligations under this contract, under statute or otherwise, aggregate damages in excess of the fees actually paid for the Services that directly caused the loss in connection with claims arising out of this Agreement or otherwise relating to the Services	We cannot change / modify the standard clause
13	Non-solicitation				Bidder shall not hire employees of Tenderer or solicit or accept solicitation (either directly, indirectly, or through a third party) from employees of Tenderer directly involved in this contract during the period of the contract and one year thereafter.	Understanding is correct
14	Force Majeure				1) Bidder shall not be liable for forfeiture of its performance security, Liquidated damages or termination for default, if any to the extent that its delay in performance or other failure to perform its obligations under the contract is the result of an event of Force Majeure. 2) For purposes of this Clause, "Force Majeure" means an event explicitly beyond the reasonable control of the Contractor and not involving the contractor's fault or negligence and not foreseeable. Such events may be due to or as a result of or caused by act of God, wars, insurrections, riots, earth quake and fire, revolutions, civil commotion, floods, epidemics, quarantine restrictions, trade embargos, declared general strikes in relevant industries, satellite failure, act of Govt. of India, events not foreseeable but does not include any fault or negligence or carelessness on the part of the parties, resulting in such a situation. In the event of any such intervening Force Majeure, either party shall notify the other in writing of such circumstances or the cause thereof immediately within five calendar days. 3) Unless otherwise directed by Tenderer in writing, the selected contractor shall continue to perform its obligations under the Contract as far as is reasonably practical, and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event. 4) In such a case the time for performance shall be extended by a period(s) not less than duration of such delay. If the duration of delay continues beyond a period of three months, Tenderer and the bidder shall hold consultations in an endeavour to find a solution to the problem. 5) Notwithstanding above, the decision of Tenderer shall be final and binding on the bidder regarding termination of contract or otherwise	We cannot change / modify the standard clause
15	Termination for Convenience				1) In case of termination, Tenderer shall pay the bidder for all work-in progress, Services already performed, and expenses incurred by the bidder up to and including the effective date of the termination of this Agreement. 2) Tenderer shall be entitled to terminate/cancel the purchase order at any time for the balance order quantity which is within the delivery schedule with no liability on either side and without assigning any reason thereof. However, the purchase order for the quantity which has already been offered for inspection shall not be cancelled and supply of the same shall be availed in due course of time. 3) Bidder may terminate/cancel the contract by giving a written notice of 30 days in case: a) Its invoices are not paid on time b) If Tenderer fails to comply with the terms of agreement	We are okay with Point no. 1 and 2 and Point no. 3 cannot be change.

16	Retention of copies			On payment of all bidder fees in connection with the Contract, Tenderer shall obtain a non-exclusive license to use within its internal business, subject to the other provisions of this Contract, any Deliverables or work product for the purpose for which the Deliverables or work product were supplied, bidder retains all rights in the Deliverables and work product, and in any software, materials, know-how and/or methodologies that bidder may use or develop in connection with the Contract.	Need more clarity or shall discuss with shortlisted bidder only
17	Non-Exclusivity			It is agreed that the services are being rendered on a non-exclusive basis and the bidder shall have the right to pursue business opportunities that it may in its sole discretion deem appropriate.	Understanding is correct
18	5	1.7 - Important Details (Schedule of Events, contact & communication details etc.)	7 - Last date & time for submission of Bids: 15-01-2024 at 3:00 pm	Request you to please consider extending the last of submission by 1-2 weeks	Okay
19	8	2.1 - Intent	The service provider will be required to define, roll-out and support a comprehensive SOC Framework which will effectively and efficiently monitor, respond, and mitigate various threats faced by Bob Financial	Is the requirement for an audit / review of the SOC operations and providing recommendations based on gaps identified or the bidder is expected to provide a policy, procedure / framework document	This is not related to an Audit, this is towards performance review of the shortlisted vendor.
20	9	2.2 - Tenure	The tenure of the contract initially would be for 1 year from the date of the issuance of first purchase order by the Company. Company can further extend at mutually agreed terms	We understand for VA-PT for new/ changes in IT infra / application of the scope of work, the tenure needs to be annually, however, please let us know the tentative period within which the other review needs to be completed	Schedule audit twice in year starting from the issuance of PO. The change management and new project audit will be as on when required.
21	10	1.1 (a)    A- VAPT assessment of IT Infra twice in year	A- VAPT assessment of IT Infra twice in year	Will the tools and systems be facilitated by BFSL? If not, are open-source tools allowed or only commercial tools are expected from bidder?	BFSL will provide Virtual Machine for tool/service installation. Required tools/services and its licenses in bidder scope.
22	10	1.1 (a)    A- VAPT assessment of IT Infra twice in year	A- VAPT assessment of IT Infra twice in year c) Conduct VAPT assessment of internal and external application/URL's d) Conduct VAPT assessment of internal and external API's i) Conduct any additional scope required to comply to regulatory board requirements	What approach the bidder is supposed use to assess vulnerabilities: Black box or Gray box?	Internet facing application/URL - Black Box and Internet application/URL - Graybox
23	10	1.1 (a)    A- VAPT assessment of IT Infra twice in year	a) Network Security review assessment of network equipment i.e. Firewall, LB, WAF, Switch, Access Point etc. b) Conduct security assessment of servers and database infra	Please provide the count for the listed assets to be reviewed: - Firewall - LB -WAF - Switch - Access Point - Servers - Database	Device Inventory Attached
24	10	1.1 (a)    A- VAPT assessment of IT Infra twice in year	e) Conduct security review assessment of BFSL developed applications source codes review	Please share technology (PHP/Java/ASP) used for the assessment.	Inventory Attached
25	10	1.1 (a)    A- VAPT assessment of IT Infra twice in year	g) Conduct rescan of VAPT activity until closer of all findings from above listed VAPT activities	Suggest that we restrict the count to two assessments post the initial assessment	No Change
26	10	1.1 (a)    A- VAPT assessment of IT Infra twice in year	i) Conduct any additional scope required to comply to regulatory board requirements	Please elaborate the requirements or provide an approximate number of requirements	If any new additional regulatory board requirement will be there during contract tenure then bidder has to support for the same.
27	11	1.1 (a)    B- VAPT support for configuration changes and new projects for one year	a) Conduct security assessment of new projects Infra/Application/URL/API etc before production movement.	What approach the bidder is supposed use to assess vulnerabilities: Black box or Gray box?	Internet facing application/URL - Black Box and Internet application/URL - Graybox
28	11	1.1 (a)    B- VAPT support for configuration changes and new projects for one year	a) Conduct security assessment of new projects Infra/Application/URL/API etc before production movement. b) Conduct VAPT of BFSL working Application /URL/API after any changes reported in existing config version.	Please let us know an approximate count of new request / changes based on BFSL's past experience	Unable to predict, its based on business/application requirement
29	10	1.1 (a)    B- VAPT support for configuration changes and new projects for one year	d) Conduct VAPT rescan activity until closer of all observations received after security assessment.	Suggest that we restrict the count to two assessments post the initial assessment	No Change
30	10	1.1 (b) IT Infrastructure in DC and DR	-	1. Is the work expected to be done onsite or remotely? 2. Will BFSL provide the OPEs at actuals or the bidder needs to consider the amount in its commercials?	Bidder has to bear.
31	10	1.1 (b) IT Infrastructure in DC and DR	-	For DR at Hyderabad, we understand that except for physical review, all other review will be done remotely	BFSL DR is in Bangalore an except for physical review, all other review will be done remotely
32	12	1.1 (f) Network Facility and Equipment Management	b) Firewall rule review and optimization c) Review of Network device configurations d) Review of Network device access control m) Review of switches, routers configuration, scalability and port management.	Please provide the count for the listed assets to be reviewed: - Firewall - Network Devices - Switches and Routers	Inventory Attached
33	13	1.1 (f) Network Facility and Equipment Management	u) Hardening of the equipment like Router, Network Switch, IPS, IDS, Firewall, Load Balancer, HSM etc.	Please provide the count for the listed assets to be reviewed: - Router - Network Switch - IPS, IDS - Firewall - Load Balancer - HSM etc.	Inventory Attached
34	13	1.1 (f) Network Facility and Equipment Management	v) Network Vulnerabilities and Threat Management.	Please let us know the exact requirement for the scope. Also is the bidder expected to bring their own tool or do you have any tool to manage this requirement	Requirement details mentioned in RFP on page no 12 of 47. BFSL will provide VM if require and any essential tool for this task is in bidders scope.
35	13	1.1 (g) Database Management System and Data security	r) Audit the data base systems security through automated security scans and manual reviews	Please elaborate on the automated scans to run on database, as this would be risky to use production DB. We recommend manual DB review	OK with recommended manual review as per regulatory guidelines.

36	13	1.1 (h) Help Desk	d) Problems and incidents are resolved, and the cause investigated to prevent any recurrence f) Trend analysis and reporting g) Development of knowledge base		Please elaborate the requirements for review under this requirement	Mentioned details scope on RFP page 13 of 47 in para 1.1(h)
37	15	1.1 (m) Domain Controller / AD (Domestic / International)	-		1. How many AD / Domain Controllers are there 2. Is there a need to review the AD / Domain Controller as well or just the 3 line items that has been asked for	Three domain controller: scope as per mentioned in RFP
38	15	1.1 (n) Staff Training	c) Quality of Human resources /appointment process		We understand the need is to review the HR process - please confirm	Understanding is correct
39	15	2. Business Continuity Plan & Disaster Recovery Planning	a) Review of DRP Process		Specify the count of applications and Infra in scope for DRP	Inventory Attached
40	15	2. Business Continuity Plan & Disaster Recovery Planning	a) Review of DRP Process		What is the status of current ITDR plan implementation?	ITDR plan in place need to review.
41	15	2. Business Continuity Plan & Disaster Recovery Planning	a) Review of DRP Process		Is the mapping and tiering of all applications identified?	understanding is correct
42	15	2. Business Continuity Plan & Disaster Recovery Planning	a) Review of DRP Process		Is RTO and RPO defined in the existing DRP?	Yes
43	15	2. Business Continuity Plan & Disaster Recovery Planning	a) Review of DRP Process		Are applications and infra which is covered in the DRP being tested regularly?	Yes
44	15	2. Business Continuity Plan & Disaster Recovery Planning	a) Review of DRP Process		Do you have DR setup in place for all in scope applications which needed to be covered in IT DRP?	Yes
45	15	2. Business Continuity Plan & Disaster Recovery Planning	a) Review of DRP Process		Is there any automation/orchestration tool in place for seamless switchover and switchback	Yes, it is outsource
46	15	2. Business Continuity Plan & Disaster Recovery Planning	b) Review Business Flows		Provide clarity of what business flows to be covered	understanding is correct
47	15	2. Business Continuity Plan & Disaster Recovery Planning	b) Review Business Flows		Outline the current end to end business flow and highlight the key touchpoints	understanding is correct
48	15	2. Business Continuity Plan & Disaster Recovery Planning	b) Review Business Flows		What are the critical dependencies in current processes and how are they managed?	Will share these details with selected vendor for this activity.
49	15	2. Business Continuity Plan & Disaster Recovery Planning	c) Review of Resource priority for recovery and recovery time objectives		Is the critical resource identification process in place for recovery in the event of disruption?	understanding is correct
50	15	2. Business Continuity Plan & Disaster Recovery Planning	c) Review of Resource priority for recovery and recovery time objectives		Is the critical resource considered to be human resource or IT resource or recovery site?	No Change
51	15	2. Business Continuity Plan & Disaster Recovery Planning	c) Review of Resource priority for recovery and recovery time objectives		Is the resource recovery strategy in place for prolonged disruption?	understanding is correct
52	15	2. Business Continuity Plan & Disaster Recovery Planning	d) Review of Business Continuity Strategy		Is the BCP strategy a separate document apart from BCP Plan?	understanding is correct
53	15	2. Business Continuity Plan & Disaster Recovery Planning	e) Review of adequacy Disaster Recovery Plan and Business Continuity Plan		Is the BCP plan defined as per the BCP strategy and the same is inline with BCP Policy?	understanding is correct
54	15	2. Business Continuity Plan & Disaster Recovery Planning	f) Review of BCP & DRP for DC/DR		Along with ITDR plan do we need to review Runbook application wise	understanding is correct
55	15	2. Business Continuity Plan & Disaster Recovery Planning	g) Review of achieved vs. projected result		Are the projected results part of any plan? And for which process BCP or DR or Both?	understanding is correct
56	15	2. Business Continuity Plan & Disaster Recovery Planning	h) Review of process of business continuity objective		Is the business continuity objective defined in Policy or Plan?	understanding is correct
57	15	2. Business Continuity Plan & Disaster Recovery Planning	i) Review of submission of test result to board		Are you referring to BCP test or ITDR test results? Also clarify if we need to conduct any of these tests or do we need to present results of BCP and ITDR drills already completed in the past	understanding is correct
58	15	2. Business Continuity Plan & Disaster Recovery Planning	j) Identify Individual Point of failure		Specify the identification or SPF of BCP or ITDR process? If it is ITDR then do we need to review architecture diagram for each application in scope?	understanding is correct
59	15	3. Security Operations Centre	a) Review of SOC infrastructure / implementation of Security Tools		Please provide the count and list of security tools currently implemented at BFSL	Inventory Attached
60	15	3. Security Operations Centre	f) People Management		Please elaborate the requirements for review under this requirement	policy in place need to review
61	16	4. Application Audit	-		Please let us a range of applications that would be part of the review	Inventory Attached
62	16	4. Application Audit	f) Audit of management controls including system configuration/ parameterization development. Complete Review of Application Parameterization		Please elaborate the requirements for 'Application Parameterization'	complete review of application
63	16	4. Application Audit	h) Interface controls - Application interfaces with other applications and security in their data communication. Whether the interface access is secure enough from penetration by internal / external users		We understand that bidder will additionally be required to check on sample basis the output for application interface - please confirm	Understanding is correct
64	16	4. Application Audit	i) Adherence to Legal & Statutory Requirements		Please provide the list of applicable laws and the regulatory requirements	RBI, SEBI and NPCI regulatory guidelines.
65	16	4. Application Audit	t) Source Code Review for in house developed applications		Is the bidder expected to conduct Source Code Review or just review the existing process and what will be range of such applications	Bidder has to conduct Source code review
66	16	5. Migration Audit of Infrastructure & Applications	a) Review of Migration activities with respect to Migration plan of BFSL. Ensure consistent, methodical approach adopted for migration of Data or Application		Please provide the count of migration plans / activities to be reviewed	discuss with selected bidder
67	17	6. Regulatory Compliance Audit	Scope will be as per Regulatory guidelines given by Regulatory Authority		1. What other regulators will be included: SEBI, NCIPC, etc. 2. We understand the bidder is expected to perform these regulatory audits - please confirm what is the requirement 3. How many such audits will be required to be conducted	RBI, SEBI and NPCI regulatory guidelines.
68	17	7. Consulting Services	Audit Related Consulting Services on need basis throughout the audit.		Please elaborate the requirements for this scope of work	If any new additional regulatory board requirement will be there during contract tenure then bidder has to support for the same.

69	17	Deliverables	b) Provide re-designed network & security architecture along with technical specifications of network & security solutions based on the operational and business requirements of the BFSI.		We understand that bidder is expected to provide a new network & security architecture diagram - please confirm	Review existing network & security architecture as per regulatory guideline and suggest/recommend changes in existing architecture if observe any gap in the assessment.
70	17	Deliverables	g) Reports will be submitted as soft copy (password protected) in doc and pdf format as well as in signed hard copy.		Is signed copy required to be submitted?	Yes
71	18	4.2. Price	VII. Terms of payment as indicated in the Purchase Contract...		Please provide the payment milestones / schedule or the bidder can provide the payment milestone / schedule	Standard payment terms are 30 Days from the date of Invoice or same will be discuss separately or on mutually agreed terms with shortlisted bidder.
72	18	4.2. Price	VIII. The Company will consider the Total Cost of Ownership (TCO) over a [Three year period]		Please explain this	Please ignore this point.
73	23	4.5. Other RFP Requirements	14. Selected Bidder shall inform their readiness for the pre-delivery/post-delivery inspection at least 15 days in advance. Inspection of the centralized application and data base servers, etc. will be carried out at the Vendor's Data Centre/DRC..... 15. There will be an acceptance test by Company or its nominated representatives after installation of the Solutions..... 17. However, the selected Bidder shall install and commission the solution, in terms of this RFP, at locations designated by Company or at such Centers as....		We understand that this is not applicable to this RFP as the bidder will not be submitting any product / application - please confirm	Understanding is correct
74	25	5.2. Authorized Signatory	The Bidder shall submit the bid authenticated by an authorized person from any of their offices in India. The Bidder's authorized signatory shall authenticate by sign and seal, each page of the bid in original and photocopies including brochures/ pamphlets/ write-up etc.		In-case the bid documents are signed using digital signature can this requirement be waived off?	RFP term cannot be change
75	27	5.8. Integrity Pact	All bidders will be required to enter into an integrity pact with the Company as per the CVC guidelines. Please refer Annexure 08.		Is this document to be submitted along with the bid or only successful bidder needs to be submit this?	All participants has to share.
76	47	Annexures & Appendices	Appendix 01 Technical Evaluation - Infrastructure Audits of Data Centre's completed (In the last 5 years) in any Public sector Bank in India, BFSI Sector other than Bank in India. - <b>Assignments completed in NBFC</b>		Generally the Information Security or any other cybersecurity audit covers Data Centre Infrastructure as a scope, hence it would be difficult to demonstrate the exact mentioned scope requirement in PO for all clients and hence consider the broad coverage of the audit	No Change
77	47	Annexures & Appendices	Appendix 02 - Bill of Materials IS		Unit price is asked, is the complete cost for the full scope of work not required to be submitted	Complete cost for full scope of work required to be submitted in front of respective sections as per mentioned in "Bill of Material" sheet.
78	47	Annexures & Appendices	-		The Appendix 3, 4, 5 are required on Bidder's letter head - please confirm	Yes
79	Page 9	3.0.	1. IT Infrastructure (Data Centre, Disaster Recovery Centre)	Total number of Network/Security devices Total Number of Server and Database server Total Number of API(Internal/External) and its number of method Total Number of Application(Internal/External) and its Size(Big/medium/small) Total Number of application for Source code: Line of code Total Number of source code: certificate to be reviewed Conduct rescans of VAPT activity until closer of all findings from above listed VAPT activities: Kindly confirm iteration Are all devices accessible from 1 single location		Inventory attached
80	Page 9	3.0.	Scope of Work -	Location of Audit for Technical & Process audit both		Mumbai, Bangalore and Delhi.
81	Page 9	3.0.	Scope of Work - Change Management Audit	What would be the total count of the application.		Inventory Attached
82	Page 11	1.1 C	1.1 (c) Review of outsource of IT Operation (DC & DR) in compliance with IS Policy.	Total number of vendors to be covered under the scope/ Can I be done remotely . If not then what be the location of audit		Vendor list will provide during assessment. Activity will conduct physically from BFSI Goregan Office.
83	Page 15	3	Security Operations Centre	what is the location of SOC.		It is on Cloud
84	Page 16	4	Application Audit	What would be the total count of the application.		Inventory Attached
85	Page 17	6	Regulatory Compliance Audit	kindly provide the details of the guidelines to be reviewed as part of audit scope		RBI, SEBI and NPCI regulatory guidelines.
86	Page 2	Eligibility criteria	Bidder must have provided/done similar service any 2-3 of the NBFC / Financial Institute or Banks.	Kindly confirm us total number of work order to be submitted and for which year		Kindly go through technical evaluation file.
87	Pg 2	Eligibility criteria	CERT-IN Empanelment	As per the RFP there is no cert-In empanelled Organisation is mentioned - Kindly confirm if this tender is applicable for NON- CERT-In empanelment vendors also. If not then we request you to add this clause and mention ( The Bidder should be CERT-In empanelled continuously for last 12 years)		No Change
88	Pg1	INTEGRITY PACT	INTEGRITY PACT	Do we need to submit along with the bid or once the Bidder is awarded - Kindly confirm		Needs to discuss
89	10	1.1 (a) Conduct VAPT for IT Infra, Application and APIs.	a) Network Security review assessment of network equipment i.e. Firewall, LB, WAF, Switch, Access Point etc.	Can you provide more details about the specific components under "network equipment" (Firewall, LB, WAF, Switch, Access Point) as well as count of devices that need to be assessed for network security?	NA	Inventory Attached

90	10	1.1 (a) Conduct VAPT for IT Infra, Application and APIs.	i) Conduct any additional scope required to comply to regulatory board requirements	Are there specific regulatory board requirements that need to be addressed, and could you provide details on the additional scope required for compliance?	NA	RBI, SEBI and NPCI regulatory guidelines.
91	16	4. Application Audit from Scope of Work	t) Source Code Review for in house developed applications	Do we need to conduct the IS audit on samplert basis for the applications or please share the total number of in house developed applications in case all the in house developed application needs to be considered for IS Audit	NA	Inventory Attached
92	NA	Point No. 1 of Appendix 01 Technical Evaluation	Information Security Audits completed (In the last 5 years) in any Public sector Bank in India, BFSI Sector other than Banks in India.	NA	Request you to modify the clause to below: Information Security Audits completed (in the last 5 years) in any Public/Private sector Bank in India, BFSI/FI Sector other than Banks in India.	No Change
93	NA	Point No. 2 of Appendix 01 Technical Evaluation	Infrastructure Audits of Data Centre's completed (In the last 5 years) in any Public sector Bank in India, BFSI Sector other than Bank in India.	NA	Request you to modify the clause to below: Information Infrastructure Audits of Data Centre's completed (In the last 5 years) in any Public/Private sector Bank in India, BFSI/FI Sector other than Bank in India.	No Change
94	NA	1	NA	NA	As per our assumption the DC location will be as per mentioned on page no. 1. Along with these locations, Kindly confirm whether the activity were onsite or offsite.	DC Location is in mumbai Chandivali. Activity should be onsite.
95	3	10	1.1 (A)	1.1 (a) Conduct VAPT for IT Infra, Application and APIs's	Kindly share the below details, 1. Quantity of network devices to be reviewed under VAPT activity. 2. No. of internal and external web applications w.r.t. type and Size of the web application (Small, medium, large), thin client, thick client, mobile application- Android, IOS) 3. Kindly confirm total No. of APIs? count of integrated & non-integrated web APIs's. 4. Source code review (please share the tentative No. of lines for source code for review)	Summary count will share with inventory sheet and details will share during assesment.
96	3	11	1.1 (C)	Review of outsource of IT Operation (DC & DR) in compliance with IS Policy.	Kindly confirm whether it comes under Vendor/third party audit.	It come under vendor audit
97	3	11	1.1 (D)	Management of Hardware in compliance with IT Policy	The below-mentioned clause comes under as per OEM requirement, kindly share the exact requirement from audit perspective. a) Acquisition in DC/DR, installation, Upgradation b) Server sizing processes - hard disk capacity, RAM, Processing power etc. as per requirements	Details scope mentioned in RFP on pafe 11 of 47 in section 1.1(d)
98	3	13	1.1 (h)	Help Desk	Kindly confirm whether this comes under Vendor/third party audit.	It come under vendor audit
99	3.2	18	3	The Bidder will be required to fix any vulnerability in the Appointment of consultant for BFSI. Information Security Audit (IS Audit) 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.	Kindly confirm whether the detected vulnerability has to be fixed/remediated by the appointed consultant? As per our understanding & industry practice, the respective application developer will be responsible for fixing the vulnerabilities identified by bidder.	Appointed consultant will share observation and the respective application developer will be responsible for fixing the vulnerabilities identified by bidder.
100	1	9	1.1(a)	A- VAPT assessment of IT Infra twice in year	Count of Firewall, Load balancer, Web Application Firewall, Switches, and Access Points Count of Servers and DB Instances along with flavours Count of pages per application Count of API endpoints Total count of Line of code for source code review	Inventory Attached
101	2	9	1.1(a)	VAPT support for configuration changes and new projects for one year	Count of Server racks Count of UPS Systems Count of CCTV Count of physical security personnel Count of users for Privileged Identity Management	Inventory Attached
102	3	11	1.1 (c)	Review of outsource of IT Operation (DC & DR) in compliance with IS Policy.	Could you please share with us the guidelines for carrying out a compliance audit of an outsourced IT service provider or do we conduct as per Industry Standard, ISO, CERT-In Guidelines etc	RBI, SEBI and NPCI regulatory guidelines.
103	4	11	1.1 (c)	Review of outsource of IT Operation (DC & DR) in compliance with IS Policy.	We have to perform this activities onsite and if Yes, (Kindly share the Locations)	BFSI Goregaon and Gurugram office, and DC, DR locations i.e. Chandivali Mumbai and Bangalore respectively.
104	5	12	1.1 (f)	Network Facility and Equipment Management	Count of VPN tunnels Count of IPS, IDS and HSM	Inventory Attached
105	6	14	1.1 (i)	Process Management Review	No.of Policy	Will share these details with selected vendor for this activity.
106	7	15	3	Security Operations Centre	How many Servers in consideration - Windows, Linux, Unix, AIX etc. All Physical, Virtual (VM), IaaS (AWS, Azure etc), across all environments - Prod, Dev, UAT, DR etc	Inventory Attached
107	8	15	3	Security Operations Centre	Number of locations from where logs will be collected. Log Retention Ratio - 3 month online, 9 months offline	Three locations, As per regulatory guidelines
108	9				No.of Architecture Network Diagram	Will share these details with selected vendor for this activity.
109	10	9	3.0	Scope of Work - SP=Service Provider	Should SP be an CERT-In Empanniled	Yes
110	11	32	7	Payment Terms	Could share what will be payment terms	Standard payment terms are 30 Days from the date of Invoice or same will be discuss separately or on mutually agreed terms with shortlisted bidder.
111	9	3		1. IT Infrastructure (Data Centre, Disaster Recovery Centre) 2. Business Continuity Plan & Disaster Recovery Planning 3. Security Operation Centre (SOC) 4. Application Audit 5. Change Management Audit 6. Regulatory Compliance Audit 7. Consulting Services a need basis throughout the audit.	We request you to please provide the Infra details and Number of application for the effort estimation	Inventory attached

112			<p>Bob Financial is inviting bids from Service Providers (SP) to define, roll-out and support a comprehensive Security Operations Center (SOC) Framework which will provide assurance on the security posture and enhance Bob Financials capabilities to monitor, respond and mitigate threats against Bob Financial.</p> <p>Bob Financial intends to remodel its existing Security Operations Center (SOC) by engaging with a Service Provider (SP) which has a sustainable and proven business model, recognized accreditation, established customer-base, distinguishable solution accelerators and enablers, high-performance personnel, while maintaining the ability to support Bob Financials evolving requirements.</p> <p>The service provider will be required to define, roll-out and support a comprehensive SOC Framework which will effectively and efficiently monitor, respond, and mitigate various threats faced by Bob Financial.</p>	<p>Information Security Audit (IS Audit)"</p> <p>Is the setup of the SOC also part of the above scope?</p> <p>293Scope of Work</p> <p>Broad Scope given as under however detailed / Final scope will be given at the time of actual allocation of Work:</p> <ol style="list-style-type: none"> <li>1. IT Infrastructure (Data Centre, Disaster Recovery Centre)</li> <li>2. Business Continuity Plan &amp; Disaster Recovery Planning</li> <li>3. Security Operation Centre (SOC)</li> <li>4. Application Audit</li> <li>5. Change Management Audit</li> <li>6. Regulatory Compliance Audit</li> <li>7. Consulting Services a need basis throughout the audit</li> </ol> <p>Out of these 7 areas to be audited</p> <ol style="list-style-type: none"> <li>1. What are the regulatory compliance audits and how often do we need to conduct the audit?</li> <li>2. How many applications are in the scope of the audit? Does it cover WebApp audit as well as application security assessment?</li> <li>3. Can you elaborate on the consulting services requirements?</li> </ol> <p>31011. IT INFRASTRUCTURE</p> <p>SP shall carry out a review to ensure IT Infrastructure compliance with IT Policy of BFSL. Will this</p>		RFP term cannot be change
113			<p>Scope of Work</p> <p>Broad Scope given as under however detailed / Final scope will be given at the time of actual allocation of Work:</p> <ol style="list-style-type: none"> <li>1. IT Infrastructure (Data Centre, Disaster Recovery Centre)</li> <li>2. Business Continuity Plan &amp; Disaster Recovery Planning</li> <li>3. Security Operation Centre (SOC)</li> <li>4. Application Audit</li> <li>5. Change Management Audit</li> <li>6. Regulatory Compliance Audit</li> <li>7. Consulting Services a need basis throughout the audit</li> </ol>	<p>Out of these 7 areas to be audited</p> <ol style="list-style-type: none"> <li>1. What are the regulatory compliance audits and how often do we need to conduct the audit?</li> <li>2. How many applications are in the scope of the audit? Does it cover WebApp audit as well as application security assessment?</li> <li>3. Can you elaborate on the consulting services requirements?</li> </ol>		RBI, SEBI and NPCI regulatory guidelines. The device inventory details attached
114			<p>1. IT INFRASTRUCTURE</p> <p>SP shall carry out a review to ensure IT Infrastructure compliance with IT Policy of BFSL.</p>	<p>Will this assessment cover HO + 38 locations mentioned in the RFP?</p>		DC, DR, BCP and HO Location.
115			<p>1.1 (a) Conduct VAPT for IT Infra, Application and API's:</p>	<p>Can you please give the count of the IT infrastructure components and applications within the scope of the VAPT Activity</p> <ol style="list-style-type: none"> <li>1. Servers</li> <li>2. Network Devices</li> <li>3. Security Devices</li> <li>4. Endpoints</li> <li>5. Applications</li> <li>6. APIs</li> <li>7. Databases</li> </ol>		Inventory Attached