(An ISO-9001-2015 certified)
(CIN: U91110MH1928GAP00)

To, All Prospective Vendors, 21-Aug-2017

Dear Sir/Madam,

Sub: RFP - Information Security Assessment/Audit of IT setup (Ref No: ISAIT-17-18)

This has reference to the written queries received with respect to RFP dated 21st July, 2017 for 'Information Security Assessment/Audit of IT setup (Ref No: ISAIT-17-18)'. The pre-bid meeting was held in this regard on 14th August, 2017.

Appended below is compilation of queries and explanation/responses from IIBF.

Prospective vendors are also requested to note that changes in schedule of activities for RFP as under.

Sr.	Particular	Old date/Time	Changed date/time
1	Proposal submission by vendors	23-Aug-2017 3.00 PM	1-Sep-2017 3.00 PM
2	Technical proposal opening	23-Aug-2017 4.00 PM	1-Sep-2017 4.00 PM

Chief Executive Officer

Responses to queries for - RFP - Information Security Assessment/Audit of IT setup (Ref No: ISAIT-17-18)

Sr. No.	Page No (tender Ref)	Clause(tender Ref)	Description in the tender (tender Ref)	Clarification / Query Sought	IIBF's Response
1		Overall RFP		Please provide below information: 1)Overall IT staff including employees and non employees. 2)Approximate number of IT assets: a)Servers b)Network Devices c)Applications d)Primary data center and location, DR site and location and any other data center and location e) Approximate number of desktops and laptops.	1) 4 employee and 6 non employee in IT Department 2) please refer Annexure VII Existing Hardware/Software details
2		Overall RFP		Apart from IIBF, is there any other entity in scope of this RFP for example group company, subsidiary or JV. If yes, then please provide the name of the entity/company/location	IIBF Only
3		Overall RFP		Apart from Data Centre in Mumbai and DC backup/failover site in Chennai are there any other locations in scope of the audit.	Audit to be performed from one location IIBF central office kurla.
4		Section 7- Scope of work		In scope of work it is specified that *'this assessment/audit is expected to lead to compliance certification like ISO027001, ISO-22301'*. Can you please elaborate on your expectations in this regard. Does it mean that bidder should conduct the audit	Yes
5		Section 7- Scope of work a)IT Risk Assessment(ISO-31000)		1) How many office locations and departments are to be considered in scope of the IT Risk Assessment. Do we need to consider only IT department at Corporate office and backup/failover site in Chennai?	Audit to be performed from one location IIBF central office kurla. All 8 department.
6		Section 7- Scope of work B)Network Security Review		1)What is the expectation from this assessment? 2)Do we have to perform Firewall rule based review? 3)Do we have to perform configuration review of assets given in the RFP? 4) Do we have to perform network architecture review? If so, then for how many locations?	1) please ref to scope 2),3),4) Yes

7		Section 7- Scope of work WLAN Security		1)For WLAN security review, are the 6 Wi-Fo details specified in the RFP are in scope of the audit? Are all of these 6 devices located in Mumbai.	The clause 7 'Indicative Requirement / Scope of Work' , Group I, c - 'WLAN Security' stands deleted.
8		Section 7- Scope of work Operational Security Audit		1) What is the expectation from this assessment? 2) What is the scope for this assessment? Is it related to backup and recovery, log management, incident management)	As per ISO 27001:2013 (Operation Security Control) Class 8.1 to 8.3 and A.12.1 to A.12.7
9		Section 7- Scope of work Physical and environmental audit		1) How many locations needs to be covered under this activity ?	Audit to be performed from one location IIBF central office kurla.
10		Section 7- Scope of work End point security		1)How many end-points are in scope of the audit	please refer Annexure VII Existing Hardware/Software details
11		Section 7- Scope of work Software license audit		1)How many publishers are in scope of the audit. Request you to please provide list of publishers in scope. 2)How many desktops are in scope of review? Is it 106? 3)How laptops are in scope of license audit? Is it 33? 4)Are 14 servers specified in the hardware section of the RFP in scope of the review or there are more servers in scope. 5)Does the organization have Workgroup or Domain Based architecture or both? 6)Is there a single Active Directory domain or multiple domains (part of the AD structure) 7)Does the environment have virtualised instances? 8)Do you have segregated environment for Development, Test and Production? 9)Is there a Software Inventory tool in place in the organization? If yes, list name of tool(s)	1) All publishers mainly MS,Adobe,Oracle,Symentec AV etc. 2) refer Annexure VII Existing Hardware/Software 3) refer Annexure VII Existing Hardware/Software 4) refer Annexure VII Existing Hardware/Software 5) Domain Based architecture 6) Single AD domain 7) no 8) Yes 9) Manual control
12		Section 7- Scope of work APT (IIBF CO-Setup)		1) VAPT is to be performed for all devices specified in the RFP i.e. 50 Hardware devices & 6 Wi-Fi devices? 2) Is there any particular kind of testing which is required (e.g. black box , grey box testing etc.) 3)Is the VAPT assessment internal/external?	1) yes 2) no 3) yes, both

13		Section 7- Scope of work BCP GAP Assessment		1) How many locations needs to be covered under this activity ?	Audit to be performed from one location IIBF central office kurla.
14		Section 7- Scope of work Source Code Reviews		1) Source code review is to be performed for all 12 application specified in section 12 of the RFP? Are these 12 application developed in-house by IIBF?	Required for all 10 application in-house development
15		Section 7- Scope of work Oracle middleware and database		1)Do we have to perform configuration review in this assessment? If yes, then for how many databases and middleware?	yes. Database and Middleware, Production setup 1 and failover 1 (both onsite)
16		Section 7- Scope of work Change control management & secure coding		1) Is any tool used for the change management process? 2) What are your expectations in secure coding? Does it mean reviewing the secure coding guidelines against industry best practices.	1) no. one inhouse tool is used only for ticketing of change request. 2) yes
17	23	Annexure VIII Commercial Template	h) VAPT (IIBF CO-Setup)	Whether hardware mentioned in (Annexure VII) Location-SZ,EZ,NZ,WZ is not included in the Scope of VAPT	Audit to be performed from one location IIBF central office kurla, all hardware included in scope and mentioned in annexure VII.
18	23	Annexure VIII Commercial Template	f) End point security- no of nodes to be put in annexure	What will be the scope of the End user security.	Annexure VIII Commercial Template, Group I, Sr.no f, 'End point security- no of nodes to be put in annexure' should be read as 'End point security' Number of Client Nodes at corporate office (approx.) o Desktop : 106 o Laptop : 33
19	18	Annexure V Experience Format	Relevant experience (Not more than 3 years old – Government, bank or educational institute organization) (each order value of Rs.20 lac or above)	Is submission of Annexure V mandatory.,Relaxation: No minimum order value for relevant experience.	no change in RFP clause
20				1) IT Risk assessment (ISO-31000) - It already covers risk assessment /Review and update .kindly clarify areas to be covered	Hardware, Applications and clients/nodes ref. Annexure - VII

21				2) Operational Security Audits – what are the areas needs to be covered & Location of audit	As per ISO 27001:2013 (Operation Security Control) Class 8.1 to 8.3 and A.12.1 to A.12.7
22				3) Physical and environmental audit - Locations of the audit	Audit to be performed from one location IIBF central office kurla.
23				4) Endpoint security total of desktop / laptop under this area and locations	please refer Annexure VII Existing Hardware/Software details
24				5) Application security – web application as per OWAPS top or Functionality testing (details required)	As per OWASP top 10, 2017 release.
25				6) Is it a single application with number of modules or list of modules …	it is not single application. Please refer Annexure VII for Existing Application details
26				7) The turnover is too high . Requested to kindly make it 10 crore.	The clause 6 under 'Minimum Eligibility Criteria', Sr.3 'The vendor should have registered a turnover of Rs.15 crore or more in Indian market during each of last three completed financial years. i.e. FY 2014-15, 2015-16 and 2016-17' is modified as 'The vendor should have registered a turnover of Rs.10 crore or more in Indian market during each of last three completed financial years. i.e. FY 2014-15, 2015-16 and 2016-17'
27				8) Is it an one time audit or will it include compliance audit/revalidation/ Retesting	ref. clause 13.d Terms & conditions, revalidation iteration limited to maximum 3.
28				1) IT Risk Assessment(ISO 31000)- Please elaborate if the Risk Assessment methodology of the organization is Asset Based or Process Based and please confirm if the scope of number of applications for Risk Assessment would be the 10 applications listed in the RFP.	Hardware, Applications and clients/nodes ref. Annexure - VII
29				2) Kindly elaborate the expected coverage of the following activities:	

30				i) Software License Audit- Assuming that the coverage is limited to the number of desktops and laptops mentioned in the RFP, kindly provide an indicative number of such licenses to be reviewed.	1) All publishers mainly MS,Adobe,Oracle,Symentec AV etc. 2) refer Annexure VII Existing Hardware/Software
31				ii) Oracle middleware and database- Assuming that the number of databases in scope shall for the 10 applications specified in the RFP, kindly mention the count of middleware. Also, kindly elaborate if the expected coverage is limited to VAPT of the middleware and database.	Database and Middleware, Production setup 1 and failover 1 (both onsite)
32				iii) Change Control Management and Secure Coding- Kindly elaborate the expected coverage of the activity and if the scope shall be limited to the 10 applications listed in the RFP.	scope is limited to 10 application
33				iv) Operational Security Audit- Kindly elaborate the expected coverage of the activity.	As per ISO 27001:2013 (Operation Security Control) Class 8.1 to 8.3 and A.12.1 to A.12.7
34				3) Kindly clarify the locations in Scope of BCP Gap Assessment and Physical and Environmental Audit. From the proposal, we understand that, indicatively, the scope shall be 5 offices and 1 Datacenter. Kindly confirm if the understanding is correct.	Audit to be performed from one location IIBF central office kurla.
35				4) Kindly confirm if the PT needs to be performed internally or externally and if VAPT shall be performed on UAT servers/or production servers/ or both.	yes, both On production setup only
36				5) Kindly elicit if Rule based review is also expected as a part of the Network Security Review.	Yes
37				6) As per the application details provided in Annexure VII, the number of reports per application is also specified. Kindly elicit, as to under which activity the application reports are expected to be covered.	Report Details are for information only
38				For eligibility criteria one of the requirement is Vendor should be Cert-In Empaneled and we are not a Cert-In Empaneled Company, except this we fulfill all the requested criteria so will it be possible to participate in to the same…	no change in RFP clause

40	6	**Minimum Eligibility Criteria** The vendor should be a company registered under Companies Act, 1956, having its Registered Office in India and in existence for at least 5 years .(As of 1st April 2017)	Query	The eligibility criteria mentions vendor should be a 'Company'. What about Limited Liability Partnership (LLP) firms?	The clause 6 under 'Minimum Eligibility Criteria', Sr.1, 'The vendor should be a company registered under Companies Act, 1956, having its Registered Office in India and in existence for at least 5 years.(As of 1st April 2017)' is modified as 'The vendor should be a company registered under Companies Act, having its Registered Office in India and in existence for at least 5 years .(As of 1st April 2017)'
41	7	**Indicative Requirement / Scope of Work**: Assessment/audit to be conducted in the following areas: <u>Group I</u> a) IT Risk assessment (ISO-31000) b) Network Security Review c) WLAN Security d) Operational Security Audits e) Physical and environmental audit f) End point security g) **Software license audit** h) VAPT (IIBF CO-Setup) i) BCP GAP Assessment	Query	Please specify the names of software publishers (like Microsoft, Oracle, etc.) for which software license review is to be performed	1) All publishers mainly MS,Adobe,Oracle,Symentec AV etc. 2) refer Annexure VII Existing Hardware/Software
42	7	**Indicative Requirement / Scope of Work:** The assessment/audit scope also includes a correction report, so that the identified security gaps can be plugged in as per advice and a final assessment/audit review should result in **no-serious-security-lapses** outstanding at the end of the exercise.	Query	What if IIBF is unable to pug the gaps completely and the residual gap is serious in nature?	management will take call on such gaps which is serious in nature.
43	6		Comment	For the Year 16-17 .... will not be able to provide Self certified copies of the audited balance sheet since the audit is under progress.	vendor may submit the 2016-17 audited balance sheet on or before technical evaluation stage - II.

44	Indicative Requirement / Scope of Work:	Group 1	Information Asset Listing	Is information Asset Listing done centrally at an institute level or per process/function level. If done per process/function level, please indicate the number of Information Asset listing.	no change in RFP clause
45	Indicative Requirement / Scope of Work:	Group 1	Risk Assessment	Is risk assessment for information assets done centrally at an institute level or per process/function level. If done per process/function level, please indicate the number of Risk assessments.	no change in RFP clause
46	Present IT Setup	Annexure 1 - locations	Centralised & Decentralised Activities	We understand from the RFP that there are 5 physical locations of the institute. Please provide list of functions conducted centrally and those conducted locally at each of these locations.	Major administrative activities are conducted at Co.(kurla and cuffeparade office) (EZ,SZ,NZ offices are extended training arm of the institute.
47	2. Purpose	The purpose of this document is to select an agency for conducting Information Security Assessment/Audit of institute's IT setup/infrastructure, submit reports & assist in implementing suggestions.	Comment + Query	The recommendations would be provided to the teams who would do the implementation. .... can provide guidance to the implementation team but would not be directly involved in the implementation. Please confirm	refer clause 13.d Terms & conditions
48	1. About IIBF	IIBF (www.iibf.org.in) is an ISO 9001-2015 certified organization with its Corporate Office in Mumbai and Professional Development Centre's located at	Query	How many locations are to be covered from Offices and Development centres	Audit to be performed from one location IIBF central office kurla. All location covered.
49	4. Present IT setup	IIBF has established its Data Centre (DC) at its corporate office Mumbai. Apart from this DC Institute has Backup/failover site at Chennai office. All offices are connected to DC through lease line with backup ISDN line. IIBF Data Centre is operated on 24x7 basis	Query	Please confirm If DR site is included in the scope of work.	Audit to be performed from one location IIBF central office kurla. All location covered.

50	4. Present IT setup	IIBF has established its Data Centre (DC) at its corporate office Mumbai. Apart from this DC Institute has Backup/failover site at Chennai office. All offices are connected to DC through lease line with backup ISDN line. IIBF Data Centre is operated on 24x7	Query	Please confirm whether Data center is managed by in-house teams or third party	in-house and third party is engaged for AMC and available on call basis
51	1. About IIBF	IIBF (www.iibf.org.in) is an ISO 9001-2015 certified organization with its Corporate Office in Mumbai and Professional Development Centre's located at Delhi, Chennai and Kolkata (Annexure I).	Query	Can the testing be done centrally from Mumbai location, or it is required to travel to other offices	Audit to be performed from one location IIBF central office kurla
52	5. Indicative Requirement / Scope of Work:	The assessment/audit scope also includes a correction report, so that the identified security gaps can be plugged in as per advice and a final assessment/audit review should result in no-serious-security-lapses outstanding at the end of the exercise	Comment + Query	Please confirm, there is only one time re-test to assess if the gaps identified have been closed.	refer clause 13.d Terms & conditions
53	6. Documents to be submitted with the proposal:	Company Profile	Query	Please suggest what details are expected here. Please confirm if the Proposal is required in word or PPT.	preferably word/ppt/PDF
54	6. Documents to be submitted with the proposal:	Duly filled company information as per Annexure-VI.	Query	Please suggest what documentation is required to be submitted	please refer annexure - IV

55	6. Documents to be submitted with the proposal:	Duly filled company information as per Annexure-VI.	Query	Please suggest if CA certificate can be submitted for Turnover and net profit or positive net worth	vendor may submit the 2016-17 audited balance sheet on or before technical evaluation stage - II.
56	7. Terms and Conditions (d)	Selected vendor should assist IIBF / AMC vendor of IT system during implementation of findings(suggestions to improve) of Assessment/Audit.(Applicable for existing IT setup/infrastructure)	Comment + Query	The recommendations would be provided to the teams who would do the implementation. .... can provide guidance to the implementation team but would not be directly involved in the implementation. Please confirm	refer clause 13.d Terms & conditions
57	9. Payment	c) 25% on completion of implementation of findings (suggestions to strengthen & overcome weakness , applicable to existing IT setup / Infrastructure)	Query	The recommendations would be provided to the teams who would do the implementation. .... can provide guidance to the implementation team but would not be directly involved in the implementation. Please confirm	refer clause 13.d Terms & conditions
58	10. Expected Deliverables (c)	Technical support to the various IT Service Providers/vendors for implementing changes required to remove identified vulnerabilities. The support should include onsite training or handholding to the development team.	Query	Please confirm the expectation of the training and technical support.	Technical support to the various IT Service Providers/vendors for implementing changes required to remove identified vulnerabilities/control gap.
59	Annexure IX	I	Query	Please confirm what is expected of Section I , in Approach/ Activities and Methodology	As per ISO -31000
60		Contact person Name & contact Details with Phone No.	Query	Please suggest if contact details can be excluded as we are bound by client confidentiality clauses	no change in RFP clause
61	Terms and Condition	Note: Institute may consider group I and/ or group II for evaluation purpose.	Query	Request you to to please clarify if the evaluation of the vendor is based on both the Group 1 and 2 activity. And if one vendor is going to be chosen for both the group 1 and 2 activity	please ref. page 8 point 9.3 of RFP

62	Indicative Requirement / Scope of Work:	a) Penetration testing (IIBF CO-Setup)	Query	Please confirm the details of infrastructure on which penetration testing is to be performed 1. Count of infrastructure as per Annexure VII to be considered for PT 2. Please confirm list of devices and make and model as per annexure VII to be considered for PT 3. Accessibility 4. Number of Internal and External IP addresses. 5. Can all internal Ips be accessed from the same location. 6. Network Devices PT to be considered or not.	Audit to be performed from one location IIBF central office kurla, all hardware included. Detail of IP address etc. will be provided to shortlisted vendor
63	Indicative Requirement / Scope of Work:	b) Application Security	Query	1. Type of application security testing required (Black box , Greybox) 2. Please confirm if total number of applications can be considered as 10 Please confirm if JAVA and D2k applications are to be performed for application security. Please confirm the details of the application - No. of roles - No. of dynamic pages - Web based / thick client	1)As per OWASP top 10 , 2017 2)Yes please refer Annexure VII Existing Hardware/Software details
64	Indicative Requirement / Scope of Work:	c) Network Security Review	Query	- Please confirm if it is required to perform Architecture Review or any other activity is expected, if yes then how may locations(circles, remote sites, etc.) to be covered - Please confirm the number of devices to be considered - Please confirm if Firewall review is expected. If yes, please confirm the number of firewalls and number of rules per firewall	As per ISO -27001:2013 Audit to be performed from one location IIBF central office kurla, all hardware included. please refer Annexure VII Existing Hardware/Software details
65	Indicative Requirement / Scope of Work:	d) Overall Security Audits	Query	- Please confirm what is expected from Overall Security Audits	question not referring to floated RFP
66	Indicative Requirement / Scope of Work:	a) Source Code Reviews	Query	Please confirm the lines of codes and application count as per Annexure VII Application Details	please refer Annexure VII Existing Hardware/Software details

67	Indicative Requirement / Scope of Work:	b) BCP Audit	Query	1. Has the organization defined the BCM Policy, performed BIA & Risk Assessment, Business continuity plan including the functional recovery plans, emergency response and Crisis Management plan. 2. Is the organization certified against ISO 22301, 27001 3. No. of locations and department in scope of the existing BCM,and ISMS	question not referring to floated RFP
68	Indicative Requirement / Scope of Work:	c) WLAN Security	Query	1. Please confirm what activities are to be considered as a part of WLAN security - Penetration testing, configuration Review 2. Does the Team need to perform configuration review of the wireless routers. If yes can it be done on a sample basis	The clause 7 'Indicative Requirement / Scope of Work' , Group I, c - 'WLAN Security' stands deleted.
69	Indicative Requirement / Scope of Work:	d) Oracle middleware and Database	Query	Can Desktop review be conducted on sampling basis	no change in RFP clause
70	9.2 Technical Evaluation	Stage 2 - Presentation/Walkthrough/Demo/ POC/experience etc	Query	Please confirm what is the expectation of PoC	Please refer 9.2.1 Stage : 2 - Presentation/demo:

*