S.No	Page No	Clause No	Description in RFQ	Clarification Sought	Additional Remarks (if any)	NPCI Response
1	8	-	Last date and time for Bid Submission	We request you to extend the last date of bid submission to at least 24 April 2017; .	-	Last Date for Bid Submission is extended till 14th April 2017
2	8	6	Last date and time of submission is 10th April	Please consider request to postpone this date to 18th April	Alternative, please grant 5-7 days after response to pre-bid queries to get all the documents in place.	Last Date for Bid Submission is extended till 14th April 2017
3	10	3.1	Note: Site visit shall mean and include all such location as NPCI may require the successful bidder to visit and provide its reports/findings to NPCI, in the format as per prescribed by NPCI from time to time.	Specify exact number of sites of ASPs including DC,DR, other offices	-	Total number of Application Service providers are 15 wherein maximum ASPs are located in Mumbai, Pune and Chennai For each ASP mainly operation and Data Center areas will be covered such that 2 sites max per ASP (note few of them have both located at one place).
4	10	3.1	Note: Site visit shall mean and include all such location as NPCI may require the successful bidder to visit and provide its reports/findings to NPCI, in the format as per prescribed by NPCI from time to time.	Specify the cities to be visited for all ASPs	-	Total number of Application Service providers are 15 wherein maximum ASPs are located in Mumbai, Pune and Chennai For each ASP mainly operation and Data Center areas will be covered such that 2 sites max per ASP (note few of them have both located at one place).
5	10	3.1	Note: Site visit shall mean and include all such location as NPCI may require the successful bidder to visit and provide its reports/findings to NPCI, in the format as per prescribed by NPCI from time to time	We will not provide any “CERTIFICATE” on analysis done. We will assess and provide gaps and recommendations accordingly.	-	Reports to be shared in the format as per prescribed by NPCI from time to time for Gaps and recommendations identified. NPCI will not be issuing "Certificate of Compliance", nor the engaged vendor. Requirenment is to issue a "Report on Compliance", after a site review.
6	10	3.1	Site visit would be on compliance to PCI- DSS	PCI DSS compliance - Specify detailed scope of work for this activity since the 5 systems and 5 network devices mentioned may not be related to PCI DSS	Does the bidder need to conduct PCI DSS audit for the client?	Yes, primarily compliance to PCI-DSS will be checked for the systems handling Card PIN / PI (Confidential) Data.
7	10	3.1	Site visit would be on compliance to ISO 22301	ISO 22301 - Specify detailed scope of work for this activity since the 5 systems and 5 network devices mentioned may not be related to ISO 22301	Does the bidder need to conduct ISO 22301 audit for the client?	Yes, domain areas pertaining to ISO 22301 to be covered which is relevant to the ASPs setup and context.
8	10	3.1	Site visit would be on compliance to ISO 27001	ISO 27001 - Specify detailed scope of work for this activity since the 5 systems and 5 network devices mentioned may not be related to ISO 27001	Does the bidder need to conduct ISO 27001 audit for the client?	Yes, domain areas pertaining to ISO 27001 to be covered which is relevant to the ASPs setup and context.
9	11	4.1	The Vendor should be a profit (profit after tax) making company in the last financial year.	Request NPCI to change it to “the Vendor should have positive net worth in last financial year”	-	Term amended as - The Vendor having profit (profit after tax) in the last financial year will be preferred during evaluation.
10	11	4.1	Eligibility Criteria f) The Vendor should be a profit (profit after tax) making company in the last financial year.	Request NPCI to change it to “the Vendor should have positive net worth in last financial year”	-	Term amended as - The Vendor having profit (profit after tax) in the last financial year will be preferred during evaluation.

11	11	4.1	b) The Vendor should be Qualified Security Assessor (QSA) Company that have been qualifies by the PCI Security Standards Council for validating an entity's adherence to PCI DSS.	Since, the engagement does not require the consultant to provide PCI DSS certification, we request you to drop this requirement.	-	No change in RFP terms
12	20	8.4	Penalty for default in delivery If the Bidder does not submit the final audit report as per the above delivery period, or such authorized extension of delivery period as may be permitted in writing by NPCI, NPCI shall impose a penalty @ 0.5% of the total value of the Purchase Order for each week's delay subject to a maximum of 5% of the total value of the Purchase Order, without prejudice to any other right or remedy available under the Purchase Order. In the case of delay in compliance with the order beyond 10 days of the stipulated time period, NPCI will have the right to cancel the order	We request amendment of this clause as below: 'Penalty for default in delivery If the Bidder does not submit the final audit report as per the above delivery period due to reasons solely attributable to the successful bidder, or such authorized extension of delivery period as may be permitted in writing by NPCI, NPCI shall impose a penalty @ 0.5% of the total value of the Purchase Order for each week's delay subject to a maximum of 2% of the total value of the Purchase Order, without prejudice to any other right or remedy available under the Purchase Order. In the case of delay in compliance with the order beyond 10 days of the stipulated time period, NPCI will have the right to cancel the order.	-	No change in RFP terms
13	20	8.5.3	8.5.3 The benefits realized by successful bidder due to lower rates of taxes, duties, charges and levies shall be passed on by the supplier to NPCI.	We understand that, since the rates quoted by us are exclusive of taxes, and that both parties will honour the prevalent tax regimes in the country, this clause will not be applicable. Kindly clarify.	-	No change in RFP terms
14	20	8.3	After the receipt of the Purchase Order vendor Engagement shall be for whole year as per schedule calendar.	Confirm that all the 15 ASP reviews will be conducted over a period of 1 year. Will there a provision to change the commercials if the bid extends beyond 1 year	-	Issued Purchase Order will be valid for the duration of 1 Year from the date of Issuance and the work will be completed within the given time frame.
15	20	8.6.1	Payment shall be after completion of audit as per each site and submission of final report certify by NPCI official, within 30 days from the date of receipt of correct invoice.	Clarification required that Unit price quoted will be paid after each ASP review along with all applicable taxes. Confirm the exact amount of time NPCI will take to certify the final report submitted by the bidder.	-	No change in RFP terms
16	21	8.9	Confidentiality The Bidder shall (whether or not he submits the tender) treat the details of the documents as secret and confidential. The Successful Bidder shall execute separate NDA on the lines of the draft provided in Annexure B hereof.	The Annexure B is not provided in the RFP. We request you to provide the same so that we can have this reviewed by our legal team. We also request you to let us provide the queries on the same, if any, after this document is provided to us.	-	NDA Will be Shared with successful bidder.

	21	8.11	The selected Bidder will be liable for all the deliverables. The Bidder's aggregate liability in connection with obligations undertaken under the purchase order, regardless of the form or nature of the action giving rise to such liability (whether in contract, tort or otherwise), shall be at actual and limited to the value of the contract/purchase order. The Bidder's liability in case of claims against NPCI resulting from willful and gross misconduct, or gross negligence, fraud of the Bidder, its employees, contractors and subcontractors, from infringement of patents, trademarks, and copyrights or other Intellectual Property Rights or breach of confidentiality obligations shall be unlimited.	Request that in para three the word unlimited may be replaced like in para 2 but you can put the limit to upto 2 times the value of the contract. We would therefore request to have an overall liability clause limiting the liabilities not exceeding 2 or 3 times the contract value.	-	Term amended as - The Bidder's liability in case of claims against NPCI resulting from willful and gross misconduct, or gross negligence, fraud of the Bidder, its employees, contractors and subcontractors, from infringement of patents, trademarks, and copyrights or other Intellectual Property Rights or breach of confidentiality obligations shall be 3 times the contract value.
17	22	8.13	In case of order cancellation before acceptance of the product or service or both, any payment made by NPCI to the Bidder for the particular product and service would necessarily have to be returned to NPCI, at the option of NPCI, with interest @ 15% per annum from the date of each such payment. Further the Bidder would also be required to compensate NPCI for any direct loss incurred by NPCI due to the cancellation of the Purchase Order and any additional expenditure to be incurred by NPCI to appoint any other Bidder	Clarify the scenarios in which this clause will be executed by NPCI	-	Ref RFP Page 22, Section 8.13 i) & ii)
18	24	9.1) A) a)	IT Risk Assessment/ Vulnerabilities in Application OS/ Databases/ Network	If yes, How many total apps in scope?	-	Aprox Number of App's are 3 to 5, per ASP
				How many apps per ASP in scope?	-	Aprox Number of App's are 3 to 5, per ASP
				This includes only Vulnerability Scanning of system and network devices OR Configuration Review against the CIS Benchmark?	-	Yes scope of work include Vulnerability Scanning of systems and network devices with configuration reviews as per industries best practices.
				This includes only 5 OS, 5 DB and 5 network devices per ASP?	-	Rf Sec 9.2
19	24	9.1) A) b)	Review the functioning of each Application including system and Application interfaces	Is it Technical Testing requirement for interfaces to identify security issues?	-	Yes
				How many apps **per ASP** in scope?	-	Number of App's would be in between 3-5 per ASP's
				How many average count of interfaces per app?	-	5 Interfaces(approx) per app such as, web interface, secure RDP etc.

20	24	9.1) A) a)	IT Risk Assessment/ Vulnerabilities in Application OS/ Databases/ Network	Does this include web Application security Assessment also based on OWASP top 10?	-	Security Assessment would be on Industries best practices
21	24	9.1) A) b)	Review the functioning of each Application including system and Application interfaces	What is meant by "Review of functioning"?	-	Rf Sec 9 A b.
22	24	B	Adequacy of Documentations vis-à-vis the application OS/ Database/ Network in use.	Is the vendor expected to validate the completeness of existing SCDs against the current infrastructure	-	Yes on sampling basis
23	24	9.1	Site Visit shall mean and include all such location as NPCI may require the successful bidder to visit and provide its reports/findings to NPCI, in the format as per prescribed by NPCI from time to time.	We request you to clarify the number of site visits and their locations that form a part of the scope.	-	Total number of Application Service providers are 15 wherein maximum ASPs are located in Mumbai, Pune and Chennai For each ASP mainly operation and Data Center areas will be covered such that 2 sites max per ASP (note few of them have both located at one place).
24	24	9.1.C	Site visit would be on compliance to c. Business Continuity Management System ISO 22301 d. Information Security Management System ISO 27001	Kindly clarify if the locations are already ISO 22301 and ISO 27001 certified.	-	Its not necessary that ASP is ISO 22301 and ISO27001 certified.
25	24	9.1.C	h. Review of DR Site, inter alia, their capacity, readiness & security adequacy m. Physical security at Data Center and at operations area from were bank support is provided	Kindly provide us the locations of the Data Center and DR Site. We understand that the operations areas is at the same location as the Data Center. Kindly confirm.	-	Operations and Data-center area may or may not be the same as per ASP's infrastructe setup
26	24	9.1.C	k. Overview of services outsourced for technical support	Kindly provide us the number of vendors for which this activity is to be performed.	-	15 ASP's (as per current count, this may increase and contract may be extended for further ASPs with successful bidder)
27	24	9.1 A.a	IT Risk Assessment/ Vulnerabilities In Application OS/ Databases/ Network	Confirm that VA-PT of approximate 5 systems and 5 network devices forms the part of this activity and there is no other risk assessment to be carried out	-	Ref Section 9
28	24	9.1 C.e	General security controls on OS, applications, Database and Network	Confirm that configuration review, code review and application security testing will not be a part of this activity	-	RFP Scope have coverage on configuration review and application security testing. Note:Code review is not in scope. (However, if any such exercise and report is available then it has to be reviewed from quality and completeness perspective.)
29	24	9.1 C.f	Information classification and reasonable security controls for protection of sensitive confidential information from business and It act perspective.	Confirm that review of any form of DLP tool or data classification policy review or data classification exercise is not a part of this activity.	We will review existence of technology in place to avoid data leakage	Ref RFP Page 24 clause 9.1 C)a,c,f
30	24	9.1 A.b	Review the functioning of each application including system and application interfaces	Confirm the number of application and interfaces at each ASP	-	Application will be between 3 to 5 and interfaces will be approx 5 per ASP

31	31		Format given for Power of Attorney	Confirm that minutes of meeting document of the organization which lists names of signing authorities of the firm along with a covering letter will be accepted. We will not be able to provide letter in the format given.	-	No Change in RFP
32	32	Annexure A7 2	The Vendor should be Qualified Security Assessor (QSA) Company that have been qualifies by the PCI Security Standards Council for validating an entity's adherence to PCI DSS.	As a proof, confirm if snapshot from the PCI DSS website will be accepted. We will not be able to provide any other proof.	-	YES, please print marking your name in the list.
33	32	Annexure A7 3	The vendor should be an information security consulting firm and vendor should be empaneled by cert - in as information security auditing organization.	Please confirm what evidence is required for this clause. Only a PDF with complete list of vendors is available on the respective website.	-	YES, please print marking your name in the list.
34	32	Annexure A7 4	The vendor should have conducted VAPT of at least 2 banking or financial institutions (please attach documentary evidence like work order, evidencing for having completed the VAPT assignment.	Please confirm if work orders will be accepted. We may not be able to provide completion letters from clients since there are different contractual agreements with clients.	-	Yes, masked work orders and work completion records, documents will suffice.
35	32	Annexure A7 5	The vendor should have minimum three years' experience in conducting vulnerability assessment and penetration testing for organizations having large network size & complexity / servers / applications.	Confirm what evidence is required for the same.	Can we provide the confirmation on letter head?	Ref pg 34 Annexure T2
36	33	Annexure T1 2	Skilled resource and tool for compliance check of PCI DSS Standard	If yes, please provide details of the assessments	-	
				If yes, please provide the scope of the each assessment	-	No change in RFP terms
37	33	Annexure T1 2	Skilled resource and tool for compliance check of PCI DSS Standard	Other than VAPT of Application OS/DB/ network are there any additional technical assessments as per PCI DSS (like ASV, SCR, Wireless PT, Firewall rule base) are also required to be executes by vendors?	-	No change in RFP terms
38	36	Annexure C2	* Travel & lodging expenses outside Mumbai location will be considered for reimbursement based on actuals. The limit for such expenses will be as per the NPCI defined standard and Policies.	Kindly provide us the limit for such expenses. This will be important at arriving at the commercials for this proposal.	-	No change in RFP terms

39	36	Annexure C2 Note	Travel & lodging expenses outside Mumbai location will be considered for reimbursement based on actuals. The limit for such expenses will be as per the NPCI defined standard and Policies.	Confirm that the bidder has to make arrangements for all travel and the amount will be adjusted against original invoices. Clarify the exact amount for Travel and lodging/boarding/others per day separately.	-	No change in RFP terms
40	-	-	-	a. We can tie-up with CERT-In empaneled provider and submit a consortium bid for Pentesting part. Here , a question will be if consortium bids are permitted	-	No
41	-	-	-	is it possible to quote for other parts of RFP other than Pentesting	-	No
42	-	-	-	I would need location of Sites where the visit is needed.	-	ASP's are majorly located in Mumbai, Pune and Chennai.
43	-	-	-	We have reviewed the proposal and it is not clear whether a joint bid can be made inorder to meet all the requirements. Please advice us on this.	-	No
44	-	-	-	Clarify if Sub-contracting is allowed for any of the activities mentioned in SoW?	-	No