भारतीय राष्ट्रीय भुगतान निगम
NATIONAL PAYMENTS CORPORATION OF INDIA

PRE BID REPLIES FOR NPCI:RFP:2012-13/0024 dated 27.12.2012-RFP FOR ENGAGING AGENCY FOR ISO27001 Certification

Sr. No	Document Reference	Page No	Clause No	Description in RFP	Clarification Sought	NPCI Comment
1	Scope of Work	12	3.2	The engaged Service Provider shall conduct the awareness and On-Floor sessions for different audience of NPCI at all NPCI locations.	Please specify the sites of NPCI where ISO 27001 has to be implemented.	Locations: Mumbai - 3 Locations , Chennai - 2 Locations, Additional locations for CTS are Delhi & Hyderabad.
2	ISO 27001 Certification Framework	12	3.1	Prepare guidelines, procedures and other subordinate documents. The Selected Bidder would have to revise or formulate new required documentation such as IT Security policy, Standard & guidelines, Procedures, subordinate documents, Baseline security etc. The required documentation should also include the steps to be performed for ongoing ISO27001 compliance	Will there be an Internal ISMS NPCI team/forum?	Yes
3	ISO 27001 Certification Framework	12	3.1	Prepare guidelines, procedures and other subordinate documents. The Selected Bidder would have to revise or formulate new required documentation such as IT Security policy, Standard & guidelines, Procedures, subordinate documents, Baseline security etc. The required documentation should also include the steps to be performed for ongoing ISO27001 compliance	Will NPCI provide updated asset list (technology, people, paper, etc).	All assets at all locations to be covered. Details will be shared with L1 bidder.
4	ISO 27001 Certification Framework	12	3.1	Prepare guidelines, procedures and other subordinate documents. The Selected Bidder would have to revise or formulate new required documentation such as IT Security policy, Standard & guidelines, Procedures, subordinate documents, Baseline security etc. The required documentation should also include the steps to be performed for ongoing ISO27001 compliance	Will NPCI fill-up the Risk analysis sheet as per the template provided by the Bidder.	Yes
5	ISO 27001 Certification Framework	12	3.1	Engage External certification Audit. The Service provider would have to provide assistance for engaging external certification agency for certification audit and extend support during Certification audit.	Has the bidder to include the cost of external certification audit or the bidder has to just provision for assistance during the certification audit.	Yes, Bidder has to include the cost & provide details in Annexure C2 (Part-2)

PRE BID REPLIES FOR NPCI:RFP:2012-13/0024 dated 27.12.2012-RFP FOR ENGAGING AGENCY FOR ISO27001 Certification

Sr. No	Document Reference	Page No	Clause No	Description in RFP	Clarification Sought	NPCI Comment
6	ISO 27001 Certification Framework	12	3.1	The agreement with the bidder will be applicable for period of 3 years which includes the first ISO27001 certification process and subsequent surveillance audits.	The annual surveillance audits will verify the maintenance of ISMS. The ISMS has to be maintained for aspects specified in SOA relating to the IS Policy, IT Policy and the SOP's. Will ISMS be maintained by NPCI or the bidder has to provide maintenance services (maintain PDCA Cycle). If the bidder does not require to be part of the PDCA cycle, then please suggest if bidder service will be limited to pre-surveillance compliance audits, which will be an annual event only. Please specify the functioning of the NPCI ISMS forum for maintaining ISMS.	No change in RFP (re-certification at the end of 3rd year is not in scope)
7	Pre-requisite	14	4.1	The bidder must also possess the technical know-how and the financial wherewithal that would be required to successfully implement the replication solution and support services sought by NPCI for the entire period of the contract.	Please share the replication plan.	Details will be shared with L1 Bidder
8					Does NPCI planned phases of ISMS implementation to cover multiple locations or all locations are to be covered in One Phase? ----Input to ascertain resource deployment at each location	All locations to be covered in one phase
9					Do we need to carry out VAPT as part of ISMS scope?	Yes
10					Are internal audits to be conducted post certification – what is the Audit periodicity required	As per ISO 27001 requirement
11	ISO 27001 Standards Awareness	12	3.2	The Engaged service provider shall provide Mailers & Posters for raising awareness.	What are the no. of mailers and posters required? Please elaborate on the expectations from mailers and posters.	Posters- 100 Posters of at least 10 different types. Mailers- On weekly basis, for ONE year
12	ISO 27001 Standards Awareness	12	3.2	The Engaged service provider shall provide Mailers & Posters for raising awareness.	What are the total no. of employees to be covered for the ISMS awareness sessions at each location, and what would be the batch size	Details will be shared with L1 Bidder
13					If internal audits are to be conducted, is the DR site also to be included under the scope	Yes

PRE BID REPLIES FOR NPCI:RFP:2012-13/0024 dated 27.12.2012-RFP FOR ENGAGING AGENCY FOR ISO27001 Certification

Sr. No	Document Reference	Page No	Clause No	Description in RFP	Clarification Sought	NPCI Comment
14		14	4.2	Eligibility Criteria: 2) The bidder should have minimum annual turnover of Rs.5 Cr. per year in the last 3 financial years i.e. 2009-10, 2010-11 and 2011-12 (or Calendar year 2009, 2010, 2011 or the Bidder's financial years).	Can you reconsider the eligibility criteria of Rs.5 Cr. per year in the last 3 financial years	No change in RFP
15	ISO 27001 Certification Framework	12	3.1	The Selected Bidder would have to revise or formulate new required documentation such as IT Security policy, Standard & guidelines, Procedures, subordinate documents, Baseline security etc	Kindly clarify the documents available with NPCI which needs to be revised and the list of documents which needs to be formulated by the consultant	All documentation work will have to be done by the Bidder
16	ISO 27001 Certification Framework	12	3.1	The agreement with the bidder will be applicable for period of 3 years which includes the first ISO27001 certification process and subsequent surveillance audits	The surveillance audit is once in a year for 2 years and at the end of 3rd year it is the re-certification. Kindly confirm whether surveillance audit only is covered or even the re-certification at the end of 3rd year. Also clarify whether the period of contract will be for 2 years if surveillance audit only is to be covered	No change in RFP
17	ISO 27001 Certification Framework	12	3.1	The bidder has to mention the certification agency in the technical bid. This deliverable would be considered in the technical evaluation.	Kindly clarify the evaluation method for evaluating the certification agency	BSI or Bureau Veritas would be preferred.
18	Eligibility Criteria	14	4.2(2)	The bidder should provide satisfactory performance certificates from two customers where the bidder has provided consultancy for ISO 27001 certification during last 5 Years	As per the policy of few organisations, they do not provide the completion certificate. We request you to consider the copy of ISO 27001 Certificate be sufficient wherever such completion certificate cannot be provided.	No change in RFP
20	Eligibility Criteria	14	4.2(5)	The bidder should not be currently blacklisted by any bank / institution in India or abroad.	The bidder should not be currently blacklisted by any bank / institution in India or abroad for any corrupt or fraudulent practices.	No Change in terms of RFP
21	Extension of Purchase Order & Repeat order	26	8.9	The term of this Contract shall be for a period from the date of ISO 27001 certification and acceptance of the same by NPCI. NPCI reserves the right to extend the contract subsequently. NPCI has also right to place repeat order to the Bidder for any of the services mentioned in the Purchase Order.	The term of this Contract shall be for a period from the date of ISO 27001 certification and acceptance of the same by NPCI. Both parties may extend the contract subsequently, at the rates mutually agreed upon.	No Change in terms of RFP

PRE BID REPLIES FOR NPCI:RFP:2012-13/0024 dated 27.12.2012-RFP FOR ENGAGING AGENCY FOR ISO27001 Certification

Sr. No	Document Reference	Page No	Clause No	Description in RFP	Clarification Sought	NPCI Comment
22	Intellectual Property rights	27	8.11	All rights, title and interest of NPCI in and to the trade names, trademark, service marks, logos, products, copy rights and other intellectual property rights shall remain the exclusive property of NPCI and Bidder shall not be entitled to use the same without the express prior written consent of NPCI. Nothing in contract including any discoveries, improvements or inventions made upon with/by the use of the Bidder or its respectively employed resources pursuant to contract shall neither vest nor shall be construed so that to vest any proprietary rights to the Bidder. Notwithstanding, anything contained in Contract, this clause shall survive indefinitely, even after termination of this Purchase Order.	Each Party owns, and will continue to own all right, title and interest in and to any inventions however embodied, know how, works in any media, software, information, trade secrets, materials, property or proprietary interest that it owned prior to this Agreement, or that it created or acquired independently of its obligations pursuant to this Agreement (collectively, “Retained Rights”). All Retained Rights not expressly transferred or licensed herein are reserved to the respective owner. Notwithstanding, anything contained in Contract, this clause shall survive for one year ,after termination of this Purchase Order.	No Change in RFP

PRE BID REPLIES FOR NPCI:RFP:2012-13/0024 dated 27.12.2012-RFP FOR ENGAGING AGENCY FOR ISO27001 Certification

Sr. No	Document Reference	Page No	Clause No	Description in RFP	Clarification Sought	NPCI Comment
23	Indemnity	27	8.14	The Bidder shall indemnify, protect and save NPCI and hold NPCI harmless from and against all claims, losses, costs, damages, expenses, action suits and other proceedings, (including reasonable attorney fees), relating to or resulting directly or indirectly from a) an act of omission or commission of the Bidder, its employees, its agents, or employees of its sub-contractors in the performance of the services provided by this Agreement, b) breach of any of the terms of this Agreement or breach of any representation or warranty or false statement or false representation or inaccurate statement or assurance or covenant by the Bidder, c) bonafide use of the deliverables and or services provided by the Bidder, d) misappropriation of any third party trade secrets or infringement of any patent, trademarks, copyrights etc. or such other statutory infringements in respect of all components provided to fulfill the scope of this project, e) claims made by the employees, sub-contractor, sub-contractor's employees, who are deployed by the Bidder, under this Agreement, f) breach of confidentiality obligations of the Bidder, g) gross negligence or gross misconduct solely attributable to the Bidder or by any agency, contractor, subcontractor or any of their employees by the bidder for the purpose of any or all of the obligations under this Agreement.	**Request to amend as follows:** The Bidder shall indemnify, protect and save NPCI and hold NPCI harmless from and against all third party claims, losses, costs, damages, expenses, action suits and other proceedings, (including reasonable attorney fees), relating to or resulting directly or indirectly from a) ~~an act of omission or commission of the Bidder, its employees, its agents, or employees of its sub-contractors in the performance of the services provided by this Agreement,~~ b) ~~breach of any of the terms of this Agreement or breach of any representation or warranty or~~ false statement or false representation or inaccurate statement or assurance or covenant by the Bidder, c) ~~bonafide use of the deliverables and or services provided by the Bidder,~~ d) misappropriation of any third party trade secrets or infringement of any patent, trademarks, copyrights etc. or such other statutory infringements in respect of all components provided to fulfill the scope of this project, e) claims made by the employees, sub-contractor, sub-contractor's employees, who are deployed by the Bidder, under this Agreement, f) breach of confidentiality obligations of the Bidder, g) gross negligence or gross misconduct solely attributable to the Bidder or by any agency, contractor, subcontractor or any of their employees by the bidder for the purpose of any or all of the obligations under this Agreement.	No Change in RFP
24	Indemnity	28	8.14	The Bidder shall further indemnify NPCI against any loss or damage arising out of loss of data, claims of infringement of third-party copyright, patents, or other intellectual property, and third-party claims on NPCI for malfunctioning of the equipment or software or deliverables at all points of time, provided however, NPCI notifies the Bidder in writing immediately on being aware of such claim, and the Bidder has sole control of defense and all related settlement negotiations. Bidder shall be responsible for any loss of data, loss of life, etc, due to acts of Bidder's representatives, and not just arising out of gross negligence or misconduct, etc, as such liabilities pose significant risk.	**Request to amend as follows:** The Bidder shall further indemnify NPCI against any loss or damage arising out of loss of data, claims of infringement of third-party copyright, patents, or other intellectual property, and third-party claims on NPCI for malfunctioning of the equipment or software or deliverables at all points of time, provided however, NPCI notifies the Bidder in writing immediately on being aware of such claim, and the Bidder has sole control of defense and all related settlement negotiations. ~~Bidder shall be responsible for any loss of data, loss of life, etc, due to acts of Bidder's representatives, and not just arising out of gross negligence or misconduct, etc, as such liabilities pose significant risk.~~	No Change in RFP

PRE BID REPLIES FOR NPCI:RFP:2012-13/0024 dated 27.12.2012-RFP FOR ENGAGING AGENCY FOR ISO27001 Certification

Sr. No	Document Reference	Page No	Clause No	Description in RFP	Clarification Sought	NPCI Comment
25	Indemnity	28	8.14	The Bidder shall indemnify NPCI (including its employees, directors or representatives) from and against claims, losses, and liabilities arising from: a) Non-compliance of the Bidder with Laws / Governmental Requirements. b) Intellectual Property infringement or misappropriation. c) Negligence and misconduct of the Bidder, its employees, sub-contractor and agents. d) Breach of any terms of Agreement, Representation or Warranty. e) Act of omission or commission in performance of service. f) Loss of data.	**Request to amend as follows:** The Bidder shall indemnify NPCI (including its employees, directors or representatives) from and against claims, losses, and liabilities arising from: a) Non-compliance of the Bidder with Laws / Governmental Requirements. b) Breach of third party Intellectual Property infringement or misappropriation. c) Gross Negligence and wilful misconduct of the Bidder, its employees, sub-contractor and agents. d) ~~Breach of any terms of Agreement, Representation or Warranty.~~ ~~e) Act of omission or commission in performance of service.~~ f) Loss of data.	No Change in RFP
26	Indemnity	28	8.14	Indemnity would be limited to court awarded damages and shall exclude indirect, consequential and incidental damages. However indemnity would cover damages, loss or liabilities, compensation suffered by NPCI arising out of claims made by its customers and/or regulatory authorities.	Indemnity would be limited to court awarded damages and shall exclude indirect, consequential and incidental damages. However indemnity would cover damages, loss or liabilities, compensation suffered by NPCI arising out of claims made by its customers and/or regulatory authorities and which are caused by or attributable to the Bidder.	Added in Section 8.14: "and which are caused by or attributable to the Bidder".
27	Bidder's Liability	28	8.15	Indemnity would be limited to court awarded damages and shall exclude indirect, consequential and incidental damages. However indemnity would cover damages, loss or liabilities, compensation suffered by NPCI arising out of claims made by its customers and/or regulatory authorities.	Indemnity would be limited to court awarded damages and shall exclude indirect, consequential and incidental damages. However indemnity would cover damages, loss or liabilities, compensation suffered by NPCI arising out of claims made by its customers and/or regulatory authorities and which are caused by or attributable to the Bidder. In no circumstances will either Party be liable to the other in contract, tort, for breach of warranty, or otherwise, for any special, consequential, exemplary, or punitive damages, loss of revenue, business profits, interest or anticipated savings, loss of goodwill or reputation, loss of or damage to records or data, penalties or third party claims for loss or damage or other compensation arising from any act or omission of such party, or its Affiliates, officers, agents, and employees, even if it has been advised of the possibility of such losses or damages.	No Change in RFP

PRE BID REPLIES FOR NPCI:RFP:2012-13/0024 dated 27.12.2012-RFP FOR ENGAGING AGENCY FOR ISO27001 Certification

Sr. No	Document Reference	Page No	Clause No	Description in RFP	Clarification Sought	NPCI Comment
28	Termination	30	8.2	For convenience: NPCI by written notice sent to Bidder may terminate the contract in whole or in part at any time for its convenience giving one months prior notice. The notice of termination shall specify that the termination is for convenience the extent to which Bidder's performance under the contract is terminated and the date upon which such termination become effective	For convenience: Both parties by written notice sent to each other may terminate the contract in whole or in part at any time for its convenience giving one months prior notice. The notice of termination shall specify that the termination is for convenience the extent to each others performance under the contract is terminated and the date upon which such termination become effective. If the contract is terminated for convenience client has to pay Wipro for the services rendered till the effective date	No Change in RFP
29	Declaration for Acceptance of RFP Terms and Conditions	38	Annexure E	I have carefully gone through the Terms & Conditions contained in the above referred RFP document. I declare that all the provisions of this RFP are acceptable to my company. I further certify that I am an authorized signatory of my company and am, therefore, competent to make this declaration.	**Request to amend as follows:** I have carefully gone through the Terms & Conditions contained in the above referred RFP document. I declare that all the provisions of this RFP are acceptable to my company, subject to the deviations provided herein. I further certify that I am an authorized signatory of my company and am, therefore, competent to make this declaration.	No Change in terms of RFP
30	Declaration Regarding Clean Track by Bidder	43	Annexure J	I have carefully gone through the Terms and Conditions contained in the above referred RFP. I hereby declare that my company/firm is not currently debarred/black listed by any Government / Semi Government organizations/ Institutions in India or abroad. I further certify that I am competent officer in my company/firm to make this declaration.	I have carefully gone through the Terms and Conditions contained in the above referred RFP. I hereby declare that my company/firm is not currently debarred/black listed by any Government / Semi Government organizations/ Institutions in India or abroad for any corrupt or fraudulent practices. I further certify that I am competent officer in my company/firm to make this declaration.	No Change in terms of RFP
31	Term	53	Article 12	This Agreement shall remain valid from the date last written below until the termination or expiry of this Agreement. The obligations of each Party hereunder will continue and be binding irrespective of whether the termination / expiry of the Agreement for a period of three years after the termination / expiry of this Agreement.	This Agreement shall remain valid from the date last written below until the termination or expiry of this Agreement. The obligations of each Party hereunder will continue and be binding irrespective of whether the termination / expiry of the Agreement for a period of **One** years after the termination / expiry of this Agreement.	No Change in RFP

PRE BID REPLIES FOR NPCI:RFP:2012-13/0024 dated 27.12.2012-RFP FOR ENGAGING AGENCY FOR ISO27001 Certification

Sr. No	Document Reference	Page No	Clause No	Description in RFP	Clarification Sought	NPCI Comment
32	Scope of Work	12	3.1	Identify and document the scope of ISO27001 certification	Request NPCI to clarify, if: a. Scope includes entrie NPCI operations or only IT operations/IT department b. Scope includes certification of HO & DCs or all NPCI locations including DCs c. Scope includes conducting VA & PT for existing NPCI IT infrastructure which is one of the requirement of ISMS or NPCI do such assessments on regular basis and reports from these assessments will be available to project team d. Bidder should account for cost of external certification and subsequent survillience audits as part of overall engagement cost	Scope of the project is all NPCI locations including all Data Centres
33	Scope of Work	12	3.1	Identify and document the scope of ISO27001 certification	Request NPCI to provide: a. List or number of functions/departments to be covered as part of engagement scope b. Details of in-scope IT infrastructre / IT environment c. Details of number of employees to be covered under awareness program or number of awareness workshops to be conducted by the bidder d. Expected / Target timelines for achieving ISO27001 certification	A) All departments/employees to be covered, all details/assets/infra would be shared with L1 Bidder. B) The milestones for achieving certification are mentioned in RFP (Section 8.5)
34	Scope of Work	12	3.1	ISO27001 Certification Framework	Request NPCI to throw light on current information security program, existing baseline information security policies & procedures, and their current state of implementation & maturity.	Details will be shared with L1 Bidder
35	Section 3 - Scope of Work	12	3.1	Identify and document the scope of ISO 27001 certification. Service Provider needs to identify functional areas and processes to be covered in the scope and document the scope as per ISO 27001 certification requirement.	1. How many locations have been considered within the scope of ISMS? Can we have an overview of these locations? 2. How many departments have been considered within the scope of ISMS? Can we have an overview of these departments? 3. How many people have been considered within the scope of ISMS? 4. How many third parties have been considered within the scope of certification? 5. How many servers, network devices and applications within the scope of certification? 6. What are the applicable regulations and legal requirements within scope?	Details will be shared with L1 Bidder

PRE BID REPLIES FOR NPCI:RFP:2012-13/0024 dated 27.12.2012-RFP FOR ENGAGING AGENCY FOR ISO27001 Certification

Sr. No	Document Reference	Page No	Clause No	Description in RFP	Clarification Sought	NPCI Comment
36	Section 3 - Scope of Work	12	3.1	Prepare guidelines, procedures and other subordinate documents. The Selected Bidder would have to revise or formulate new required documentation such as IT Security policy, Standard & guidelines, Procedures, subordinate documents, Baseline security etc. The required documentation should also include the steps to be performed for ongoing ISO27001 compliance.	1. Does NPCI have existing information security policies, procedures and guidelines documented? 2. Does NPCI have a documented and implemented BCP? Has this been tested?	Yes
37	Section 3 - Scope of Work	12	3.1	Engage External certification Audit. The Service provider would have to provide assistance for engaging external certification agency for certification audit and extend support during Certification audit.	1. Is the service provider also supposed to provide the cost of external audit and surveillance audits in the proposal?	Yes
38	Section 3 - Scope of Work	12	3.1	The agreement with the bidder will be applicable for period of 3 years which includes the first ISO27001 certification process and subsequent surveillance audits.	1. What is the time-frame to get certified in terms of months as decided by NPCI? 2. How many surveillance audits does NPCI expect the vendor to conduct in 3 year contract? 3. Does NPCI also expect the vendor to allot time for document upgrade in the 3 year period along with surveillance audit?	Yes, As per ISO 27001 requirement and SOW.
39	Section 3 - Scope of Work	12	3.1	Conduct ISO 27001 Gap assessment. Service Provider shall conduct gap assessment against the ISO 27001 standard and provide the current status of ISMS to NPCI management. The identified service provider is required to provide assistance to NPCI internal team for closure of audit findings.	1. Does NPCI expect the vendor to carry out technical assessments such as vulnerability assessment and penetration testing? If yes then how many systems/IP addresses?	Yes, as per ISO 27001 standards
40	Section 3 - ISO 27001 Standards Awareness	12	3.2	ISO 27001 standard Awareness & Training Programs o The engaged Service Provider shall conduct the awareness and On-Floor sessions for different audience of NPCI at all NPCI locations.	1. Approximately how many batches of trainings should the vendor conduct? 2. How many locations should the trainings be conducted in? 3. How many people does NPCI require to be trained in all? 4. How many different audiences should we train? 5. Is the training one time or does it have to be repeated over 3 years? If yes, then how often? 6. For an automated solution, how many licenses would be required? (Considering 1 license per person for 1 year)	Details will be shared with L1 Bidder

PRE BID REPLIES FOR NPCI:RFP:2012-13/0024 dated 27.12.2012-RFP FOR ENGAGING AGENCY FOR ISO27001 Certification

Sr. No	Document Reference	Page No	Clause No	Description in RFP	Clarification Sought	NPCI Comment
41		14	4.2	Eligibility Criteria: 2) The bidder should have minimum annual turnover of Rs.5 Cr. per year in the last 3 financial years i.e. 2009-10, 2010-11 and 2011-12 (or Calendar year 2009, 2010, 2011 or the Bidder's financial years).	We understand that the objective of the turnover is that the company should be doing substantial business in Information Security. We would recommend that the turnover should be related to IS Audit / Information Security and it should be the minimum average annual turnover instead of the minimum annual turnover Thus, we propose the revised clause as under: The bidder should have minimum average annual turnover of Rs.5 Cr. per year in the last 3 financial years i.e. 2009-10, 2010-11 and 2011-12 (or Calendar year 2009, 2010, 2011 or the Bidder's financial years in the field of IS Audit / Information Security	No change in RFP