Pre-bid queries received from agencies

Date: 21/12/2018

#	Clause No.	Page No.	Section (Name & No.)	Statement as per tender/RFP document	Suggestion/ Query by Bidder	Rationale for suggestion	GSTN remarks/ comments
1	M. Other generic requirements, point 14	109	Section 7.7.3 Minimum Technical requirement for GRC tool	Training on the OEM platform should be conducted by the OEM at least once a year during the span of the project	Training on OEM platform should be conducted by the OEM at least once in three years during the span of the project	Major updates in GRC tools are generally received on three year basis hence once the training has been imparted by OEM initially in the preparatory phase, the next training is required only after 3 years period. For minor updates since GSTN has required a certified GRC resource from GRC service provider as part of the RFP, training can be imparted by the certified GRC resource.	Training on OEM platform - Once in a year for GSTN stqff (Max. 5 resources') in alignment with Certfication schema.
2	M. Other generic requirements, point 16	109	Section 7.7.3 Minimum Technical requirement for GRC tool	OEM certification on the product deployment a. Initial design b. Health-check at each milestone c. Final certification before Go-live	Recommend following clause instead Best practices and OEM specifications / recommendations shall be implemented for the design of GRC tool deployment, health check at each milestone and UAT/ Pre prod testing.	OEM certification will increase the administrative burden and commercials. The RFP already requires an experienced and certified GRC specialist and hence the implementation will already meet a certain level of standard based on best practices, OEM recommendation and experience from other similar projects. Hence OEM certification on implementation is not required and would not add much value.	No Change
3	1.2 Key Details	3	1.2	The bid submission date has been extended and now the last date of bid submission is 02nd January, 2019 till 03:00 PM.	We request you to kindly extend the submission date till 07th January, 2019 to allow us sufficient time to respond to the bid.	KPMG has annual block leave where our offices would be closed from 22nd December up-to 02nd January. There are announced in advance and teams would not be available during this duration.	11th January, 2019 till 11:00 AM
4	8	73	7.1 Overall Objective	Service Provider will factor in 250 man days of effort towards (during the contract period) performing the additional activities within the scope of this RFP as per the discretion of GSTN. Service Provider shall ensure the availability of skilled resources as and when required by GSTN for performing the aforesaid activities. Any effort beyond 250 man days will be considered through the change request process.	Please suggest how this cost has to be shown as part of Annexure 21		Clause pertaining to 250 man days removed. Please refer Corrigendum-6
5	Clause H	210	Annexure 21	Annexure 21, Financial Bid Summary clause H - On Demand Resource Costing	As part of Annexure 21, clause H (On demand resource costing) is required to be provided. Please confirm on the following: a. This cost is required to be provided for 36 man-months or 250 man-days . b. Would this be included as part of the Commercial bid evaluation and would the purchase order include this value or this is for reference for future change requests (if any).		Please refer Corrigendum-6
6	Clause B	213	Annexure 21 Track 2, GRC tool	Annexure 21, B. b) Track 2 - GRC Tool, there is a column for Cost of Requisite hardware and Infrastructure.	As part of Annexure 21, B. b) Track 2 - GRC Tool, there is a column for Cost of Requisite hardware and Infrastructure. However, as per the addendum requisite hardware and Infrastructure would be provided by GSTN. Please suggest if we are required to provide a value for this now as this is no longer part of bidder scope.		Please refer Corrigendum-6
7	32	13		8.5.1 Key Qualification Profile 4 - Application Security / Solution Security expert Professional Qualification: - CISA/ CISM/ CISSP/ CRISC - ISO 27001 LA/ ISO 20000/ ITIL Expert/ ISO 22301	The description of Professional Experience is more aligned to CEH certification. Kindly suggest if CEH certification could be included in the list and requirement could be modified as below: - CISA/ CISM/ CISSP/ CRISC/ CEH/ ISO 27001 LA/ ISO 20000/ ITIL Expert/ ISO 22301		No Change

8	35	14		8.5.1 Key Qualification Profile 6 - Infrastructure/ Network Security Expert Professional Qualification: - CISA/ CISM/ CISSP/ CRISC - ISO 27001 LA/ TOGAF/ SABSA	Kindly suggest if requirement could be modified as below: - CISA/ CISM/ CISSP/ CRISC/ CEH/ ISO 27001 LA - TOGAF/ SABSA		No Change
9	36	15		8.5.1 Key Qualification Profile 9 - SOC Expert Professional Qualification: - CISA/ CISM/ CISSP/ ISO 27001 LA - SIEM OEM certification is a must	Kindly suggest if requirement could be modified as below: - CISA/ CISM/ CISSP/ ISO 27001 LA - SIEM OEM certification/ trained professional is a must		No Change
10	8.5.1	145		Profile 4 Application/ solution security expert 5. Professional Experience: Experience: 1) At least 8+ years of experience in managing software and web application assessments.	Kindly suggest if a work experience could be revised to as below: 1) At least 6+ years of experience in managing software and web application assessments.		No Change
11	7.1	77	Overall Objective - Point 5	Create a strong compliance framework supporting IMS framework (ISMS, ITSMS, BCMS framework, GIGW, W3C), cyber security ramework, risk and privacy framework etc.	Are we looking for reports on data governance and privacy framework on GRC tool where the gap analysis and reporting on various framework will be available on GRC tool itself		The bidder will be working as an extended arm of GSTN GRC team for performing all activities under this RFP. This includes, review of existing artefacts/ amending / developing documentation in compliance with aplicable standards and regulations. Same shall be incorporated in the tool and appropriate dashboards shall be available to GSTN management.
12	7.7.1	98	Objective	The service provider should ensure 99.90% uptime of GRC tool and 0% data loss i.e. Recovery Point Objective (RPO) should be 0 (zero) and Recovery Time Objective (RTO) should be less than 4 hours. Service provider should also ensure appropriate backup and/or archival requirement for GRC tool.	Are we looking for DR set up in GRC tool implementation or only HA setup		Yes, GSTN will provide required infrastructure. The GRC tool should work on HA setup also and should be able to support multi tenancy.
14	3.9.2.1	36	Evaluation for Track 1 : Business / IT Controls Testing	Bidder's Experience: Bidder's credentials, strength and Case Studies Experience in projects related to Business and IT controls review, assessment and testing and at least one project in tax domain/banking/ financial institutions in last 5 years in India and Abroad a. 1 citation of Rs.30 Lakh & above: 20 marks b. 2 citations of Rs.30 Lakh & above: 40 marks c. 3 citations of Rs.30 Lakh & above: 60 marks d. 4 citations of Rs.30 Lakh & above: 80 marks **Maximum marks = 80**	Bidder's Experience: Bidder's credentials, strength and Case Studies Experience in projects related to Business and IT controls review, assessment and testing and at least one project in tax domain/banking/ financial institutions in last 5 years in India and Abroad **a. 1 citation of Rs.25 Lakh & above: 20 marks** **b. 2 citations of Rs.25 Lakh & above: 40 marks** **c. 3 citations of Rs.25 Lakh & above: 60 marks** **d. 4 citations of Rs.25 Lakh & above: 80 marks** **Maximum marks = 80**	Rationale for suggestion: Generally Business and IT Controls review Engagements are small values engagement.	No Change
15	3.9.2.3	38	Bidder Certifications	Relevant Quality & Security Certifications: 20 marks a. Valid ISO 27001/ISO 20000/ 9001: 10 marks b. SSAE -18 SOC1 / SOC2 Type-II: 10 Marks	Relevant Quality & Security Certifications: 20 marks **a. Valid ISO 27001/ISO 20000/ 9001: 20 marks**	Rationale for suggestion: Point no. a. includes both relevant quality and security certifications.	No Change
16	8.3 Profile 2	140	Business Control Design Expert	Professional qualification: • CPA/ CIA/ CA • CISA / IS027001LA At least one certification from each category is a must **Professional Experience:** Must have experience of designing financial and functional control for at least 2 projects for clients in BFSI/ indirect tax/PSU domain	Professional qualification: **• CPA/ CIA/ CA** At least one certification from each category is a must Professional Experience: Must have experience of designing financial and functional control for at least **1 project for clients in BFSI/ indirect tax/PSU domain**	Rationale for suggestion: For business controls design CPA/CIA/CA is required and not audit certification.	No Change

17	8.3 Profile 3	141	Business Control Tester	Professional qualification: • CPA/ CIA/ ISO 9001 LA • CISA / IS027001LA • CSM/ PMI-ACP/ ASM/ SQA/ ISTQB At least one certification from first 2 categories is a must and any one certification from 3rd category would be given preference Professional Experience: Must have experience of conducting Internal control review for at least 2 projects for clients in BFSI/ indirect tax/PSU domain	Professional qualification: • **CPA/ CIA/ ISO 9001 LA** • **CISA / ISO 27001 LA** At least one certification from first 2 categories is a must. Professional Experience: Must have experience of conducting Internal control review for at least **1 project** for clients in BFSI/ indirect tax/PSU domain	Rationale for suggestion: For business controls testing CPA/CIA/CA along with CISA / ISO 27001 LA certification is required and not CSM/ PMI-ACP/ ASM/ SQA/ ISTQB.	No Change
18	8.5.1 Profile 5	151	Database and OS Security Expert	Professional qualification: • CISA/ CISM/ CISSP/ CRISC • IS027001 LA Expertise on auditing large database systems such as Big Data.	Professional qualification: • **CISA/ CISSP / IS027001 LA** **Rationale for suggestion:** Database and OS Security experts have certification either as CISA / CISSP or ISO 27001 LA certified.		No Change
19	8.5.1 Profile 14	158	Security Architect	Professional qualification: • CISSP/TOGAF/ SABSA • CISA/CISM At least one certification from each category is a must	Professional qualification: • **TOGAF/ SABSA** • **CISA/CISM/CISSP** At least one certification from each category is a must	Rationale for suggestion: TOGAF/ SABSA are security architect certifications and CISA/CISM & CISSP are security related certifications	Accepted as below. Please refer Corrigendum -6: Professional qualification: • TOGAF/ SABSA • CISA/CISM/CISSP At least one certification from each category is a must
20	7.X Deliverables		Format and or Sample	Deliverable Sample or Report format	Proposed to share Deliverable report or format for section 7 to ensure that output is in line to the expectation. Or we need to factor extra time and efforts at the beginning to agree on the deliverble formats.		No Change, it will be decided mutually. Successful Bidder to propose the format.
21	7.X Scope and Activities		Track1, 2 and 3	19 Activities to be performed on 06 module of GST, 12 GSTN Applications ,12 components, 10 applciations within GSTN, 5 Data Centers, NOC, SOC, Parnters, 4 partners UT/State/CBEC etc	If all the deliverables has to be matched to each of the components then efforts and manpower deployment would be significant.		No change
22	1.2 Key Details	10	Last date and time for bid/proposal submission	02nd January, 2019 till 03:00 PM	**15th January, 2019 till 03:00 PM**	Rationale for suggestion: As we have year end holidays scheduled from 22nd December to 01st January therefore, require more time for submission of technical bid.	11th January, 2019 till 11:00 AM