Reference No. QCI/PPID/0724/321

Request for Proposal
for
Engagement of an agency for Aadhar Compliance Audit e-KYC Application

Quality Council of India (QCI),
Institution of Engineers Building,
2nd Floor, 2, Bahadur Shah Zafar Marg,
New Delhi-110002
T: +91-11-23378056 / 57; F: +91-11-23378678
W: www.qcin.org E: info@qcin.org

Tender Notice

1. Quality Council of India invites proposals for **"Engagement of an agency for Aadhar Compliance Audit e-KYC Application".**

2. The content of this RFP enlists the requirements of the Quality Council of India. It includes the Bidding Terms which details out all that may be needed by the potential bidders to understand the financial terms and bidding process and explain the contractual terms that the Quality Council of India wish to specify at this stage.

3. After the submission of the Technical and Financial Proposals according to the instructions provided in the sections below, the bids will be evaluated through a two- stage process.

4. The Documents to be submitted:

Form A	Covering Letter with the Proposal in response to the RFP Notice
Form B	Relevant Project Experience
Form C	Details of the responding organization
Form D	Non-Blacklisting Undertaking
Certificate	Valid Empanelment Certificate from STQC or CERT-IN (IT Security Auditing)
-	Technical & Financial Bid

5. The Technical Bids and Financial Bids may be submitted at the following address on or before **July 23, 2024, 2 PM** via hand/post to:

   Deputy Director (Finance & Accounts), Quality Council of India,
   Institution of Engineers Building, 2nd Floor, Bahadur Shah Zafar Marg, New Delhi-110002

Tender Summary

S. No.	Particulars	Details
1	Project Scope	Engagement of an agency for Aadhar Compliance Audit e-KYC Application
2	Address	Deputy Director (Finance and Accounts) Quality Council of India 2nd Floor, Institution of Engineers, New Delhi-110002
3	Contract Period	Four (04) months
4	Method of Selection	Least Cost System (LCS)
5	Last Date of Submission of Proposal	July 23, 2024, 2 PM

I. INTRODUCTION: QUALITY COUNCIL OF INDIA (QCI)

The Quality Council of India (QCI) is an autonomous body set up jointly by Ministry of Commerce and Industry, Government of India and the Indian industry. The mandate of QCI is to lead nationwide quality movement in India by involving all stakeholders for emphasis on adherence to quality standards in all spheres of activities primarily for promoting and protecting interests of the nation and its citizens. To achieve this, QCI is playing a pivotal role in propagating, adoption and adherence to quality standards in all important spheres of activities including education, healthcare, environment protection, governance, social sectors, infrastructure sector and such other areas of organized activities that have significant bearing in improving the quality of life and well-being of the citizens of India.

II. BACKGROUND

The Sarpanch Samvaad project leverages Aadhaar authentication to streamline and secure interactions and communications within the community. To maintain the integrity and trust of our system, it is crucial that all processes related to Aadhaar authentication are fully compliant with UIDAI regulations. This includes implementing robust data privacy measures, secure authentication protocols, regular security audits, effective incident response mechanisms, and comprehensive employee training programs.

III. SCOPE OF WORK:

The scope of work is to conduct Aadhar Compliance Audit for e-KYC Application includes detailed procedures and controls that need to be implemented and monitored regularly to ensure compliance with UIDAI's requirements. It covers various aspects including, but not limited to:

- Data Privacy and Security
- Authentication and Authorization Protocols
- Regular Security Audits
- Incident Response Mechanisms
- Employee Training and Awareness

S. No.	Compliance Control	Yes/No/NA	Auditor Remarks
A1	Security Policy Framework		
1	Authentication Service Agency shall establish dual redundant, secured leased lines or MPLS connectivity with CIDR, in accordance with the procedure and security processes as may be specified by the Authority for this purpose.		
2	Encrypted PID blocks and license keys, that came as part of authentication must not be stored anywhere in its system.		
3	The ASA should ensure with respect to above, that Session key must not be stored anywhere except in memory and should not be reused across transactions. Only re-use of session key is allowed when its use as seed key when using synchronized session key scheme.		
4	It is mandatory that network between ASA and AUA be secure. It is strongly recommended to have leased lines or similar secure private lines between ASA and AUA. If a public network is used, a secure channel such as SSL/TLS should be used.		

5	How does ASA ensure strong governance and technical security control/ solution are implemented for restriction, governance and monitoring of internet access for operator as well as staff? Evidence- Network Diagram; Security Architecture Diagram; Information security Policy & Procedure document or policy document providing brief of internet access control are Training and awareness, Developing Acceptable use policy, URL/DNS filtering, Firewall, Network access control's, Proxy Server etc)		
6	Does ASA ensure operator employed for performing authentication functions and for maintaining necessary system and infrastructure, and process'(s) requisite qualification for undertaking such works.		
7	Does ASA have data classification and labeling policy in place? What is the data classification level applied to Aadhaar and correlated data? Please share data labeling and classification policy? Evidence required- Data Labeling / Data classification policy		
8	What are the detection, prevention and recovery controls installed on end user device, server and critical assets by ASA to protect against malware, how are these solution implemented, combined with appropriate user awareness. Evidence- Antivirus solution screenshot highlighting last update date and configuration setting.		
9	Does ASA have planned, established, implemented and maintained an audit program(s), including the frequency, methods, responsibilities, planning requirements and reporting. Does the audit program(s) take into consideration the importance of the processes concerned and the results of previous audits? Evidence- Please provides below- Detail of Internal audit, frequency, team responsible to perform and how identified risks are tracked; Please provide external audit certificate. Please provide detail of audit per regulatory requirement and audit certificate or report.		
10	Does ASA have documented, approved and published data privacy policy, in line with Authority requirement, and IT Act 2011. (Please share the data privacy policy based on which ASA and link to website.) Evidence- Data Privacy policy and link to policy on website.		

11	The ASA server host shall reside in a segregated network segment that is isolated from the rest of the network of the ASA organization. The ASA server host shall be dedicated for the Aadhaar Authentication purposes and shall not be used for any purpose other than those specified in the application for appointment as ASA. Evidence- Network architecture diagram, data flow diagram or supporting artifact		
12	It is mandatory that Authentication Service Agencies shall have their servers used for Aadhaar authentication request formation and routing to CIDR to be located within data centers located in India.		
13	ASA shall maintain logs of (a) identity of the requesting entity; (b) parameters of authentication request submitted; and (c) parameters received as authentication response: Is maintained at least for 2 years or applicable by law. ASA should comply with regulation 20 of Aadhaar act 2016 (Maintenance of logs by Authentication Service Agencies)		
14	Does ASA store Aadhaar number, UID token, Virtual ID (VID), PID information, ANCS Token device id ASA related data and any resident related PII data received as a part of authentication/ e-KYC response in their transaction logs.		
15	Does ASA comply with log retention period defined per The Aadhaar (Authentication and Offline Verification) Regulation, 2021? Is audit trail of authentication transactions maintained by the ASA for a period of 2 (two) years and Upon expiry of the period of two years, the audit trail archived for a period of five years, or regulations governing the ASA. Evidence- Logging and monitoring policy.		
16	ASA should only engage with the AUA approved by the Authority and keep the Authority informed of the list of requesting entities that it serves along with all relevant details of its agreements with the AUAs. In case of disengagement with an AUA / KUA, the ASA shall inform UIDAI within a period of 7 days from the date of disengagement.		
17	Does ASA perform basic compliance and completeness checks on the authentication data packet such as checking structural validity of the ASA packet and checking signature of the ASA to ensure no unwanted, malicious requests are sent through.		
18	ASA should ensure that its operations are audited by an information systems auditor certified by a recognized body on an annual basis, and provide a		

	certified audit report, to the Authority, confirming its compliance with the policies, processes, regulations etc.		
A2	Security and Management of the Aadhaar Authentication Infrastructure		
19	Does Authentication Service Agency, has identified top management who is responsible for compliance towards UIDAI requirement? Evidence Required- TPOC and MPOC- Name, email and detail Escalation matrix with name, contact, and email detail of top management responsible for compliance toward UIDAI.		
20	Standard Operating Procedure (SOP) shall be developed for all information systems and services related to UIDAI operations. The SOP shall include the necessary activities to be carried out for the operation and maintenance of the system or service and the actions to be taken in the event of a failure.		
21	ASA shall ensure all infrastructure and operations including systems, processes, devices, software and biometric infrastructure, security, and other related aspects, are in compliance with the standards and specifications as may specified by the Authority for this purpose. The ASA shall at the minimum ensure: a) ASA server shall be hosted behind a firewall. The firewall rules shall block incoming access requests to the server from all sources other than the respective ASA s / ASA s. b) All server/network devices clocks shall be set to an agreed standard using an NTP server or must be managed centrally and procedure shall be made to check for and correct any significant variation. c) Regular patches should be updated at both application and server level. d) An auto lock out mechanism for workstation, servers and/ or network device shall be implemented. e) All the assets (e.g., desktop, laptop, servers, databases etc.) used by ASA shall be used after their hardening has been done as per the ASA hardening baseline document (unless the hardening baseline is defined by UIDAI).		
22	The client applications i.e. software used by ASA for the purpose of authentication, shall conform to the standard APIs and specifications laid down by the Authority from time to time for this purpose.		
23	ASA shall perform Source Code review of the modules and applications used for establishing connectivity with CIDR and undergo audit by a certified auditor and audit plan include organization information security policy inclusive of vulnerability assessment as well as penetration test on ASA network, infrastructure and application.		

	1. Network and application security policy 2. Vulnerability scans report with frequency 3. Third party penetration test report for ASA application, network and infrastructure		
24	Does all the assets (e.g., desktop, laptop, servers, databases etc.) used by ASA and their sub-contractors for Aadhaar Authentication are used only after their hardening as per the ASA hardening baseline document. Evidence required- ASA Hardening checklist		
25	Are sufficient security measures implemented to detect and prevent data leakage? Please provide detail of data leakage prevention solution or the alternative control implemented.		
	Evidence- Security policy highlighting control DLP policy and its scope.		
	Screenshot from DLP solution or any other supporting artifact.		
	Network intrusion and prevention systems/solution, Patch Management, encryption and identification and authentication mechanism, example DMZ, IPS/ IDS, WAF/Firewall, IAM solution etc. ASA should ensure to comply with Regulation 5, of Aadhaar (Data Security) Regulations, 2016.		
26	Does ASA conduct BGV check on employees, contractor, part timer or its third party having access to Aadhaar data or application or infrastructure used to process same? Are employees required to sign a non-disclosure agreement or confidentiality agreement prior to granting access to data and infrastructure? Evidence required- 1. BGV Check template or Pre employment check policy document 2. Copy of NDA or Confidentiality agreement signed		
27	Does ASA maintain inventory of assets consisting of informational assets and hardware assets? Are these assets labeled, classified, and monitored/ reviewed periodically?		
	Does the asset register have well defined owners and custodians and reflect correct classification scheme for each and every asset? Are the asset registers updated and reviewed periodically?		
28	Does ASA have data and asset disposal policy in place? Can you please confirm no obsolete asset is used example Windows 2008, End of Life device		
29	Does the user ID credential and access rights of personnel handling Aadhaar related authentication, data revoked/ deactivated within 24 hours of exit of the personnel.		
30	Does ASA maintain movement log register for equipment send out for repair, and ensures equipment		

	are sanitized it does not contain any Aadhaar related data. . Does ASA take the necessary steps to ensure the sanitization of the remanence data?		
31	ASA shall implement controls to prevent and detect any loss, damage, theft or compromise of the assets containing any Aadhaar related data.		
32	Does end user device have encryption software installed to secure data? Please share name of the software.		
33	ASA servers should be placed in a secure cabinet in the ASA Data Centre. The facility should be manned by security guards during and after office hours.		
34	The Test and Production facilities / environments must be physically and logically separated. Evidence- secure software development policy (SSDLC)		
35	ASA should ensure the license keys are kept secure and access controlled.		
A3	Cryptography and Key Management		
36	The key(s) used for digitally signing of authentication request shall be stored in HSM only. The HSM used shall be FIPS 140-2 compliant.		
37	The authentication request shall be digitally signed by the requesting ASA and/or by the Authentication Service Agency (using FIPS 140-2 compliant HSM), as per the mutual agreement between them and forwarded to CIDR.		
38	In case of decryption of e-KYC response data received from UIDAI for e-KYC request, the ASA can decrypt the data at its end only subject to UIDAI approval.		
A4	Compliance Requirements		
39	ASA shall comply with all the provisions as defined in the UIDAI Information Security Policy for External Ecosystem ASA.		
40	The ASA shall comply with all applicable laws in respect of storage and maintenance of authentication transaction logs, including the Information Technology Act, 2000.		
41	ASA shall, at all times, comply with any contractual terms and all rules, regulations, policies, manuals, procedures, specifications, standards, and directions issued by the Authority.		
42	ASA should be in compliance with the Intellectual Property provisions as defined in the agreement with UIDAI.		
43	ASA should comply with the Aadhaar Act, 2016 and any subsequent amendment(s).		
44	ASA should comply with Aadhaar (Authentication and Offline Verification) Regulations, 2021.		
45	ASA should comply with Aadhaar (Data Security) Regulations, 2016.		

46	ASA should comply with Aadhaar (Sharing of Information) Regulations, 2016.		
47	The ASA should comply with all the requirements of UIDAI circular K-11022/204/2017-UIDAI (Auth-I) dated 22 June 2017. (Implementation of HSM in Aadhaar authentication services).		
48	ASA should comply with Regulation number 19 (Roles, responsibilities and code of conduct of Authentication Service Agencies), Chapter-III, Aadhaar (Authentication and Offline Verification) Regulations, 2021.		
49	ASA should comply with Regulation number 20 (Maintenance of logs by Authentication Service Agencies), Chapter-III, Aadhaar (Authentication and Offline Verification) Regulations, 2021.		
50	ASA should comply with Regulation number 21 (Audit of requesting entities and Authentication Service Agencies), Chapter-III, Aadhaar (Authentication and Offline Verification) Regulations, 2021.		
51	ASA should comply with Regulation number 22 (Data Security), Chapter-III, Aadhaar (Authentication and Offline Verification) Regulations, 2021.		
52	ASA should comply with all relevant laws, rules and regulations in respect to storage and maintenance of logs, including, but not limited to, Aadhaar Act, 2016 and its Regulations and the Information Technology Act, 2000.		
53	ASA should comply with all the circulars, notices, mandates issued by UIDAI from time to time.		
54	Please provide detail on grievance handling mechanism set (by ASA), and detail on channel's they can be approached via. Please share supporting evidence or link		
55	The requesting ASA should comply with provisions of ASA Agreement with UIDAI at all times		
56	The ASA should comply with Regulation number 23, Chapter-III, Aadhaar (Authentication) Regulations, 2016.		
57	ASA shall ensure that its operations and systems are audited by an information systems auditor certified by a recognized body on an annual basis and on a need basis to ensure compliance with UIDAI standards and specifications. The audit report shall be shared with UIDAI upon request; If any non-compliance is found as a result of the audit, management shall: a) Determine the causes of the non-compliance; b) Evaluate the need for actions to avoid recurrence of the same; c) Determine and enforce the implementation of corrective and preventive action;		

	d) Review the corrective action taken The ASA should ensure to comply with Regulation Aadhaar (Data Security) Regulations, 2016. Evidence- Risk management policy document		
58	ASA should ensure message security and integrity between there servers, and AUA server. If ASA can digitally sign the request XML if it is a domain- specific aggregator and forms the request XML on behalf of the AUA.		
59	ASA should ensure private key used for digitally signing the authentication request and the license keys are kept secure and access controlled. The private key should meet below parameter specified by the authority and documented in SPI		
	Specification document (latest): - a) Digital signature certificate used/ procured should be of class II or class III certificate		
60	ASA should connect to the Network Time Protocol (NTP) Server of National Informatics Centre (NIC) or National Physical Laboratory (NPL) or with NTP servers traceable to these NTP servers, for synchronization of all their ICT systems clocks. ~~असा~~ having ICT infrastructure spanning multiple geographies may also use accurate and standard time source other than NPL and NIC, however it is to be ensured that their time source shall not deviate from NPL and NIC. Reference- CERT-In Directive No. 20(3)/2022-CERT-In dated April 28, 2022.		
	Evidence- Clock Sync evidence from CMD;		
61	Does Authentication Service Agency, has set of policies for information security defined, approved by management, published and communicated to employees on and relevant external parties on periodic basis? Evidence- Latest Information security policy/procedure document		
62	Do all employees of the Authentication Service Agency and are relevant, contractors receive information security awareness education and training and regular updates in ASA policies and procedures, as relevant to job function.		
	Is new hire required to undergo mandatory information security and awareness training? Does, the training provided include all relevant security and privacy guidelines laid by the Authority.		
	Evidence- 1. Information security awareness training record; 2. Information security awareness training content or PPT.		
63	Does ASA have user access right provisioning and deprovisioning process in place?		

	How does ASA manage and monitor individuals access information facilities (such as Authentication application, audit logs, authentication servers, application, source code, information security infrastructure etc.) processing Aadhaar related information. What is the frequency of periodic user access right review?		
	Evidence- Access control procedure and policy document.		
64	Are access rights and privileges to information processing facilities for Aadhaar related information revoked within 24 hours of exit of respective personnel? Post deactivation, user IDs deleted if not in use? Evidence- Email or IAM solution screenshot as supporting evidence		
65	The ASA servers should be placed in a secure cabinet in the ASA Data Centre. Evidence- Physical and environmental security policy		
66	ASA Data Center hosting Aadhaar related information shall be fully secured, and access controlled.		
	ASA Data Center shall be manned by security guards during and after office hours CCTV surveillance shall cover the ASA servers.		
	Access to the ASA Data Center shall be limited to authorize personnel only and appropriate logs for entry of personnel should be maintained.		
	Physical access to ASA Data Center and other restricted areas hosting critical Aadhaar related equipment/information shall be pre-approved and recorded along with the date, time and purpose of entry.		
	The movement of all incoming and outgoing assets related to Aadhaar in the ASA Data Center shall be documented.		
	Signs or notices legibly setting forth the designation of restricted areas and provisions of entry shall be posted at all entrances and at other points along the restricted areas		
67	Lockable cabinets or safes shall be provided in the ASA Data Center and information processing facilities having critical Aadhaar related information. Fire doors and fire extinguishing systems shall be deployed, labeled, monitored, and tested regularly		
	Evidence- Physical and environmental security policy		
68	Preventive maintenance activities like audit of fire extinguishers, CCTV shall be conducted quarterly. Evidence- Physical and environmental security policy		
69	ASA personnel shall not intentionally write, generate, compile copy or attempt to introduce any computer code designed to damage or otherwise hinder the		

	performance of, or access to, any Aadhaar information. Evidence- Secure software development policy document;		
70	The ASA server shall reside in a segregated network segment that is isolated from the rest of the network of the ASA organization. The ASA server shall be dedicated for the online Aadhaar Authentication service purposes and shall not be used for any other activities not related to Aadhaar. Evidence- Network architecture diagram; Network and application security policy		
71	ASA and other sub-contractors providing Aadhaar authentication service to AUA shall ensure AUA information is not displayed or disclosed to external agencies or unauthorized persons. Also, Aadhaar data mapped with any other departmental data such as on ration card/birth certificate/caste certificate or any other document/service shall not be published or displayed at any platform.		
72	ASA must have its Aadhaar related servers hosted in data centers within India.		
73	ASA should inform UIDAI without delay within 72 hours after having knowledge of misuse of any information related to the Aadhaar related information or system, compromise of Aadhaar related information. Evidence- Incident response policy and plan document; Incident notification timeline; Contact personnel and channel of information to UIDAI.		
74	ASA should document all changes to Aadhaar authentication applications, Infrastructure, processes and Information Processing facilities, and maintain Change log/ register. Evidence- Change management policy		
75	ASA shall not publish any personal identifiable data including Aadhaar in public domain/websites etc.		
76	ASA shall define a procedure for disposal of the information assets being used for authentication operations. Information systems/documents containing Aadhaar related information shall be disposed of securely Evidence- Data retention policy; Data destruction policy		
77	ASA should ensure incident management framework is implemented in accordance to Information security policy requirement/circular with inclusion of forensic investigation. ASA shall perform Root Cause Analysis (RCA) for major		

	incidents identified in it's as well as sub- contractors' (if any) ecosystem. It is recommended that ASA shall deploy as part of its systems, a Fraud Analytics module that is capable of analyzing authentication related transactions to identify fraud. Evidence- Incident response policy and plan document. Escalation matrix;		
78	ASA should implement exception-handling mechanisms and back-up mechanisms to ensure seamless provision of authentication delivery of services to the residents Evidence- Back- up policy;		
79	How does ASA ensure operational continuity and high availability of service? Please share business continuity and disaster recovery plan. 1. BCP and DR policy document 2. BCP Dr test detail 3. Crisis management detail		
80	End user device used for developing, process and handling Aadhaar data and application should timeout after session is idle for more than 30 minutes to 15 minutes based on criticality of application.		
81	ASA should ensure to integrate secure software development during application and software development lifecycle, to ensure security requirement is embedded throughout the development phase. Developer should be periodically provided training to ensure they are aware of SSDLC process. (Security testing (Dynamic and Static, architectural testing, code review. penetration test, User acceptance testing etc)		
82	ASA should utilize test data or non-production data for testing of application or software during testing phase.		
83	ASA should implement process and procedure to perform periodic information security risk assessment on its third-party having access to Aadhaar application and resident data. Evidence- Third party risk assessment policy, Name of fourth party and Fourth party name.		
84	How is segregation of duty achieved to conflict of duties and responsibilities to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets?		
85	What is the password construction policy used for creating of password? Does user require to change its password after first login? What is frequency of password?		

	Does the password policy meet's following requirement, if no please share brief comment- 1. Minimum password length of 8 characters 2. Contain at least one numeric, one uppercase letter, one lowercase letter and one special character 3. Password expiry after an interval; 4. Password age not less than 5; (Compliance as per Information security ASA policy shared by UIDAI) Evidence- Password construction policy		
86	Does ASA have implemented Single sign on to access UIDAI applications? What is the authentication mechanism utilized? (Example MFA etc) Evidence- Screenshot of SSO portal; Access and authentication policy or supporting artifact which provide overview on authentication process and mechanism		
87	Are password hardcoded in codes, login scripts, any executable program or files OR included in any automated log-on process, e.g. stored in a macro or function key?		

Note: In case of any interpretation issues between this checklist and Aadhaar Act or Regulations, the requesting entity should rely on the Aadhaar Act, its Regulations and other specifications issued by UIDAI.

- Number of e-KYC applications - 1
- Number of Roles - 1

Guidelines for the Auditor/Assessor:

- All below points need to be checked for the entire ecosystem of requesting entity including all applications, sub-contract agencies (where there are many sub-contractors reasonable sample agencies to be checked), SubAUAs (where there are many Sub-AUAs reasonable sample Sub-AUAs to be checked), physical and logical infrastructure of the requesting entity.
- The auditor/assessor is expected to mention details of the reason for compliance or noncompliance in the remarks section.
- The auditor/assessor is expected to provide reasonable evidence as part of the report to support the compliance status provided in the report.
- The auditor/assessor may add further points in this checklist to include details of the specifications/ requirements defined below. This is specifically for the points where the entire Regulation/ specification / notification / Circular / Policy etc. has been mentioned as a single check.

Reporting & Key Deliverable Requirement

Detailed report at the end of each audit providing observations, evidence and document details. Report should include but not limited to the below mentioned points:

- Audit report with status Repeat/ Exception or New
- Identify and highlight deficiencies in audit performed for the project
- Risk category – High, Medium, and Low
- Systems/Resource affected

- Risk implications of the issue highlighted.
- Wherever risk is highlighted auditor need to provide details recommendation for mitigation and help project to mitigate.
- Explicit reference to key policy, process and procedure documents of the project against identified risk/observation
- Recommendation for risk mitigation/ removal and identification of risk probability
- Suggestions for improvement – additional voluntary standards or regulations applicable
- Summary of audit findings including identification tests, tools used and results of tests performed
- Undertake source code review as per project requirement

IV. PRE-QUALIFICATION CRITERIA

S. No.	Basic Requirements	Specific Requirements	Documents Required
1	Registration	The Bidder(s) interested in participating in the Selection Process must be a duly registered legal entity in India, under any one of the following categories: • an Indian Company ("Company") registered under the Companies Act, 1956/ 2013 or any previous Companies' Act. • a Limited Liability Partnership ("LLP") registered under the LLP Act,2008. • a "Partnership Firm" registered under the Indian Partnership Act, 1932. With minimum five (05) years of existence at the time of submission of the bid and has rendered catering services during given period.	Registration documents of the Bidder as a company/firm or any legal entity along with: i. Incorporation Certificate of the company, or ii. Certified copy of registered Partnership Deed; copy of Statement filed in the Register of Firms disclosing names, addresses and relevant details of ALL partners of the Partnership Firm iii. MSME Certificate (if applicable) iv. Any other supporting document, as may be required
2	Turnover	Average Annual Turnover of the applicant during the last three (03) financial years, i.e. FY 2020-21, 2021-22, 2022-23, as per the last published audited financial statements), should be more than ₹ 40 lakhs from security work executed for the govt. organization.	i. CA Certificate certifying the turnover for FY 2020-21, 2021-22, 2022-23 with CA's Registration Number, FRN, UDIN, OR ii. Audited Financial Statements for FY 2020-21, 2021-22, 2022-23 (to support the claim)

3	Experience	The applicant should have completed assignments of Security Compliance Audit work as per following: a) Three (03) Similar Completed/ongoing works each one having Contract Value of ₹4 Lakhs, Or b) Two (02) Similar Completed/ongoing works each one having Contract Value of ₹6 Lakhs, Or c) One (01) Similar Completed works having Contract Value of ₹8 Lakhs within India in for Central or State Govt., Union Territory, PSU, CPSU, SPSU, Public Listed Companies	Copy of Work order/ Agreement/ Work Completion Certificates from the client
4	Certification	• ISO 27001 • ISO 9001 • ISO 17025 • STQC Certified or CERT-IN (IT Security Auditing)	Valid copy of certifications
5	Non-Blacklisting	The bidding entity must not be blacklisted / terminated / debarred by any state or central government or their agencies and should not have been found guilty of any criminal offence by any court of law, in the last three (3) years.	Submission as per format given in **Annexure-D**

V. Method of Selection

1. The bids shall be evaluated on Least Cost System (LCS).
2. The financial bids of only those bidders who qualify for the technical evaluation will be opened.
3. The contract shall be awarded to the bidder with lowest cost i.e., L1 bidder.

VI. Terms and Conditions:

1. **Contract Duration:** The contract will be assigned for a period of four (04) months, which may be extended further, subject to satisfactory performance of the service provider on the same terms & conditions and the requirements of QCI. The performance of the resources shall be reviewed on monthly basis and engagement of service provider shall be reviewed on quarterly basis.

2. **Authorization of Signatory:** The Bid may be signed either by the Principal Officer of the service providing firm or his duly Authorized Representative, in which case he/she shall submit a certificate of authority. All certificates and documents (including any clarifications sought and any subsequent correspondences) received hereby, shall, as far as possible, be furnished and signed by the Representative or the Principal Officer. The Principal Officer/ authorized representative of the firm shall sign the proposal and also initial all pages of the original Technical Proposal. The authorization shall be in the form of a written power of attorney accompanying the Proposal or in any other form demonstrating that the representative has been dully authorized to sign. The power or authorization, or any other document consisting of adequate proof of the ability of the signatory to bind the Bidder shall be annexed to the Bid.

3. **Performance Bank Guarantee:** QCI shall require the selected service provider to provide a Performance Bank Guarantee, within 30 days from the notification of award, for a value equivalent to 5% of the financial proposal value. The Performance Guarantee shall contain a claim period of three months from the last date as per the contract duration. The selected bidder shall be responsible for extending the validity date and claim period of the Performance Guarantee as and when it is due on account of non-completion of the submission of deliverables.

   The physical copy of Performance Guarantee should be submitted at QCI-HO within 30 days from the notification of award. In case the selected bidder fails to submit a Performance Guarantee within the time stipulated, the purchaser at its discretion may cancel the order placed on the selected bidder without giving any notice. Purchaser shall invoke the performance guarantee in case the selected bidder fails to discharge their contractual obligations during the period or purchaser incurs any loss due to bidder's negligence in carrying out the project implementation as per the agreed terms & conditions.

4. **Earnest Money Deposit (EMD)/ Bid Security:** Bidders shall submit, along with their Bids, Bid Security (EMD) of INR 20,000 as per the details mentioned below:
   a) By demand draft in favor of Quality Council of India, payable at New Delhi, or
   b) Deposit through RTGS/ NEFT as detail under**: -
      For payment of EMD through Bank transfer: -

Name of the Bank	Axis Bank LTD, 6/83, Padam Singh Road, Karol Bagh, New Delhi
Name of the Account	Quality Council of India
Saving Bank Account	223010100053020
IFSC Code	UTIB0000223

   Note:
   a) NO CHEQUES WILL BE ACCEPTED. The applicant whose EMD has been deposited by NEFT/RTGS, must enclose the transaction details/ evidence along with their technical bid, otherwise the bid will be rejected.
   b) Bid security in any other form will not be entertained.
   c) No interest will be payable to the Bidder on the amount of the EMD. Unsuccessful Bidder's EMD will be discharged/ returned as promptly as possible, but not later than 30 days of completion of the process
   d) In case bid is submitted without the bid security then QCI reserves the right to reject the bid without providing opportunity for any further correspondence to the bidder concerned. The EMD may be forfeited:
      - If a bidder withdraws its bid during the period of bid validity.
      - Bidder does not respond to requests for clarification of its Proposal.
      - Bidder fails to provide required information during the evaluation process or is found to be nonresponsive.
      - In case of a successful bidder, if the bidder fails to sign the contract in accordance with this RFP.

   *MSEs (Micro and Small) are exempted from paying Earnest Money Deposit. In this case participants are required to submit valid MSE registration certificates (Udyog Aadhaar) to avail exemption.

5. **EMD Refund:**

a) **For Unsuccessful Bidders**: The EMD of all unsuccessful bidders would be refunded without interest by QCI on finalization of the bid in all respects by the successful bidders within 45 days after finalization of tender.
b) **For Successful Bidders**: The EMD of successful bidders would be returned without interest upon submission of Performance Bank Guarantee by the successful bidders. The above-mentioned refund would be completed within 30 days of the issue of work order to the successful bidder.
c) In case bid is submitted without the bid EMD then QCI reserves the right to reject the bid without providing opportunity for any further correspondence to the bidder concerned.

6. **Payment Terms:**
   a) The payment shall be made as per the below given milestones:

S. No.	Milestones	Payment
1	Advance Payment on award of work	20%
2	On submission of 1st report	30%
3	On submission of 2nd report	30%
4	On final compliance submission	20%

   b) Milestones are defined as monthly resources cost.
   c) For each milestone to be marked as completed, the service provider should ensure that all the acceptance criteria are met and approved by QCI with signoffs.
   d) Payment shall be made on submission of invoices within 20 days of receipt of invoice complete in all respect.
   e) Incorrect Invoices, Under/Over Payment: In case an invoice is found to have been rendered incorrectly after payment, any underpayment or overpayment will be recoverable by or from the Service provider, as the case may be, and, without limiting recourse to other available means, may be offset against any amount subsequently due by QCI to the Service provider under this contract.

7. **Amendments to RFP:** At any time prior to the last date for receipt of applications, QCI may for any reason, whether at its own initiative or in response to a clarification requested by a prospective applicant, modify the RFP document by an amendment. In order to provide prospective applicants reasonable time to take the proposed amendments into account while preparing their proposals, QCI may at its discretion extend the last date for the receipt of proposals and/or make other changes in the requirements set out in the RFP. Any such amendment shall be communicated to the service providers.

8. **Conflict of Interest:**
   a) The bidder shall not have a conflict of interest that may affect the Selection Process, or the work envisaged under this RFP (the "Conflict of Interest"). Any Applicant found to have a Conflict of Interest shall be disqualified.
   b) QCI requires that the Service Provider provides professional, objective, and impartial advice and at all times hold the QCI's interest paramount, avoid conflicts with other assignments or its own interests, and act without any consideration for future work.
   c) The Service Provider shall not accept or engage in any assignment that would be in conflict with its prior or current obligations to other clients, or that may place it in a position of not being able to carry out the assignment in the best interests of the QCI.
   d) In the event that a Service Provider identifies a potential conflict of interest, they shall make a disclosure to QCI as soon as any potential conflict comes to their notice but in no case later than 7 (seven) days from the receipt of such proposals and any breach of this obligation of disclosure shall be construed as Conflict of Interest. QCI shall, upon being notified by the Service Provider

under this Clause, decide whether it wishes to terminate this service or otherwise, and convey its decision to the service provider within a period not exceeding 15 (fifteen) days.

9. **Ownership Rights:** Ownership of all new artifacts (data, reports, presentations and other publications) generated during the course of the assignment or otherwise with respect to the assignment, will rest with QCI and it will have the right to resell/ implement the same with any other organization.

10. **Fraud/Corruption**: QCI requires that the bidders participating in the selection process adhere to the highest ethical standards, both during the selection process and throughout the execution of the Contract. In pursuance of this policy, QCI defines, for the purpose of this paragraph, the terms set forth as applicable to both the parties:
    a) "corrupt practice" means the offering, giving, receiving, or soliciting, directly or indirectly, of anything of value (whether in cash or kind) to influence the action of a public official in the selection process or in Contract execution.
    b) "fraudulent practice" means a misrepresentation or omission of facts in order to influence a selection process or the execution of a Contract.
    c) "collusive practices" means a scheme or arrangement between two or more bidders with or without the knowledge of QCI, designed to establish prices at artificial, non-competitive levels.
    d) "coercive practices" means harming or threatening to harm, directly or indirectly, persons or their property to influence their participation in a procurement process or affect the execution of a Contract. QCI will reject a proposal for award if it comes to know that the bidder recommended for award has, directly or through an agent, engaged in corrupt, fraudulent, collusive or coercive practices in competing for the Contract in question; and
    e) QCI will terminate the Contract, if already awarded and will declare the bidder ineligible, either indefinitely or for a stipulated period of time, to be awarded a Contract, if at any time it determines that the bidder has, directly or through an agent, engaged in corrupt, fraudulent, collusive or coercive practices in competing for, or in executing, a Contract.

11. **Termination of Contract:**
    a) **Termination for Default**
    QCI reserves the right to terminate / short close the contract, without prejudice to any other remedy for breach of contract, by giving 15 days' notice if the Service Provider fails to perform any obligation(s) under the contract and if the Service Provider, does not cure their failure within a period of 7 days (or such longer period as QCI may authorize in writing) after receipt of the default notice from QCI.

    b) **Termination for Insolvency**
    QCI may at any time terminate the contract by giving written notice without compensation to the Service Provider, if the Service Provider becomes bankrupt or otherwise insolvent, provided that such termination will not prejudice or affect any right of insolvent, provided that such termination will not prejudice or affect any right of action or remedy which has accrued or will accrue thereafter to QCI.

    c) **Termination for Convenience**
    QCI may by written notice sent to Service Provider, terminate the contract, in whole or part, at any time for its convenience, by giving 15 days' notice. However, the payment shall be released to the extent to which performance of work executed as determined by Service Provider till the date upon which such termination becomes effective.

    d) The Service Provider may terminate this contract, or any particular Services, by giving 15 days' written notice to QCI, if the Service Provider reasonably determines that the Service Provider can no longer provide the Services in accordance with applicable law or professional obligations.

12. The bidder should adhere to laws of land and rules, regulations and guidelines prescribed by various regulatory, statutory and Government authorities which are applicable to respective business, obligations and subject matters of the contract. QCI reserves the right to conduct an audit / on-going audit of the services provided by the bidder. QCI reserves the right to ascertain information from organizations to which the bidders have rendered their services for execution of similar projects.

13. **Intellectual Property Rights:** All the rights relating to the Trademarks and Copy Rights in respect of work generated by the selected service provider(s) on behalf of QCI and paid for by QCI shall vest with QCI. Provided that QCI would reimburse the Firm for any sums of money paid for the assignment / licensing of the copyright by way of fees, charges, or otherwise as provided by the guidelines, regulations, rules, or policies of any professional body or association, with prior approval from QCI. In order to perform the services, the service provider must obtain at its sole account, the necessary assignments, permits and authorizations from the title holder of the corresponding patents, models, trademarks, names or other protected rights and shall keep QCI harmless and indemnify QCI from and against claims, proceedings, damages, costs and expenses (including but not limited to legal costs) for and/ or on account of infringements of said patents, models, trademarks names or other protected rights.

    All documents, report, information, data etc. collected and prepared by the service provider in connection with the scope of work submitted to QCI will be property of QCI. The service provider shall not be entitled, either directly or indirectly, to make use of the documents and reports given by QCI for carrying out of any services with any third parties. The service provider shall not, without the prior written consent of QCI be entitled to publish studies or descriptive articles, with or without illustrations or data, in respect of or in connection with the performance of services. The pre-existing intellectual property of the service provider used in deliverables shall remain vested with the service provider.

14. **Language:** The Proposal should be filled by the bidders in English language only. If any supporting documents submitted are in any language other than English, translation of the same in English language is to be duly attested by the Bidders. For purposes of interpretation of the documents, the English translation shall govern. All correspondence and documents relating to the Proposal exchanged by the bidder and QCI shall also be written in the English language.

15. **Companies' Personnel:** The service provider shall employ and provide at its own cost such qualified and experienced audit personnel as are required to carry out the Services. Their salaries, claims, insurance, damages, compensation, travel etc. will be the liability of the service provider(s) and QCI will in no way be responsible for any such claims/ damages.

16. **Training:** The service provider shall organize user trainings upon completion of the development phase and shall facilitate a smooth handover and transition of the system by the user department.

17. **Ethics:** QCI expects all assessors, Service Provider to show highest ethical standards during the course of the assignment; if any complaints/information regarding any incident of bribery, corrupt payment, an unauthorized offer etc., is brought to the fore, the Service Provider shall take the necessary action (to the extent of expulsion/removal) as per its organization rules and laws applicable at that time; QCI is absolved of any liability/claim arising out of any such above situations; all personnel should have signed the code of conduct with the Service Provider and any conflict of interest shall be declared to QCI.

18. The contract will be awarded to the service provider whose proposal conforms to this RFP and is, in the opinion of QCI, the most advantageous and represents the best value to the assignment, price and other factors considered.

19. **Written Undertakings:** QCI may at any time require the Service Provider and its employees/advisors/professionals/ contractors, to whom confidential information may be disclosed in the course of execution of contract, to give a written undertaking in the form of a deed reasonably accepted to QCI and relating to the use and non-disclosure of the confidential information relating to QCI or any Government Department or relating to any Ministry and or such other information that QCI suggests to be confidential. Upon receiving a request aforesaid the Service Provider must promptly arrange for all such undertakings to be given to QCI.

20. **Security:** The Service Provider shall not disclose the details of this Contract with any third party at any point of time unless required by law. That the Service Provider and its employees/professionals/personnel are only authorized to access the information shared and or collected under this project and no third party shall have any access to any information either written or oral without the written consent of QCI.

    The Service Provider shall ensure that all the data collected and processed and information received under this project or during the execution of this project and or required to be shared with QCI, by the Service Provider under this Contract shall be in totally secure mode and that the Service Provider shall take all necessary steps to prohibit any unauthorized sharing/publishing of data in the public domain or with any other party or person who is not authorized by QCI to receive such information and or data. That the Service Provider shall ensure that all the data collected, and information received under this contract shall be used only for the purpose of execution of this contract and once the purpose of this contract is fulfilled then all the papers, drawings, notes, memoranda, manuals, specifications, designs, devices, documents, diskettes, CD's, DVD's. Tapes, Trade Secrets and any other material on any media containing or disclosing any confidential or proprietary technical or business information shared during the course of execution of this contract shall be returned to QCI.

21. **Maintenance of Confidentiality:**

    a) The bidder(s) must not divulge any confidential information and assure that reasonable steps are taken to provide for the safe custody of any and confidential information in its possession and to prevent unauthorized access thereto or use thereof. The shortlisted bidder(s) must not, without the prior written consent of QCI, disclose any confidential information of QCI or any government department or relating to any ministry or any other party. In giving written consent to the disclosure of confidential information, QCI may impose such conditions as it thinks fit, and the bidder must comply with these conditions. Confidentiality clause shall survive for a longer period of one year after the termination of contract or contract expiry period.

    b) No part of this document including the Annexure can be reproduced in any form or by any means, disclosed or distributed to any person without the prior consent of QCI, except to the extent required for submitting the bid. The information contained in this document is only disclosed for the purposes of enabling potential service providers to submit a proposal to QCI. This document should not therefore be used for any other purpose. These documents contain proprietary information furnished for evaluation purposes only; except with the written permission of the QCI, such information may not be published, disclosed, or used for any other purpose. The bidding firms acknowledge and agree that this document and all portions thereof, including, but not limited to, any copyright, trade secret and other intellectual property rights relating thereto, are and at all times shall remain the sole property of QCI. The title and full ownership rights in the information contained herein and all portions thereof are reserved to and at all times shall remain with QCI. service providers must agree to take utmost care in protecting the proprietary and confidential nature of the information contained herein.

22. QCI reserves the right to accept or reject any bid, to annul the entire bid process or reject all bids at any time prior to award of contract, without thereby incurring any liability to the affected service provider(s) or any obligation to inform the affected service provider(s) the grounds for such decision. QCI also reserves the right to negotiate with the successful service provider, if necessary.

23. **Deployment of Technical Resources**: The Service Provider shall provide the technical and other staff during the execution of this project depending upon the requirement of work. The technical staff should be available at their own offices, QCI offices as and whenever required for discussions and to take instructions.

24. **Subcontracting:** There must be no further subcontracting without prior written consent of QCI; all manpower deployed by the Service provider shall be on-roll employees of the Service provider or must have a direct employment contract with the Service provider.

25. **Removal of Data:** The Service Provider must ensure that its employees/ professionals' subcontractors and/ personnel do not:
    a) remove any data or allow any data concerned with this contract to be removed from the places as notified/directed by QCI; or
    b) take any data or allow any data to be taken outside of India, without QCI's prior written consent.

26. **Access by QCI:**
    a) The QCI may, at all reasonable times and on giving reasonable notice to the Service Provider access the premises of the Service Provider to the extent relevant to the performance of this contract; require the provision by the Service Provider, its employees, personnel or professionals agents of records and information in a data format and storage medium accessible by the QCI by use of the Service Provider existing computer hardware and software; inspect and copy documentation, books and records, however stored, in the custody or under the control of the Service Provider, its employees, agents, professional or personnel; and require assistance in respect of any inquiry in to or concerning the Services or this Contract.
    b) For these purposes an inquiry includes any audit whether administrative or statutory review 'audit or inquiry (whether within or external to the Department), any request for information directed to the QCI by any authority or Government Department or any Ministry and any inquiry conducted by Parliament or any Parliamentary committee.
    c) The Service Provider must provide access to its computer hardware and software to the extent necessary for the Service Provider to exercise its rights under this clause, and provide QCI with any reasonable assistance requested by the Service Provider to use that hardware and software provided that any proprietary information including confidential information like profit margins, overheads and other such confidential information about its employees, sub-contractors, organization would not be made available.

27. During evaluation, QCI may, at its discretion, ask the respondents for clarifications on their proposals. The firms/agencies are required to respond within the time frame prescribed by QCI.

28. QCI may at its sole discretion and at any time during the evaluation of proposal, disqualify any respondent, if the firm:
    a) Submitted the proposal after the response deadline
    b) Made misleading or false representations in the forms, statements and attachments submitted in proof of the eligibility requirements
    c) Exhibited a record of poor performance such as abandoning works, not properly completing the contractual obligations, inordinately delaying completion or financial failures, etc. in any project in the preceding three years.

d) Submitted a proposal that is not accompanied by required documentation or is non-responsive, failed to provide clarifications related thereto, when sought
e) Submitted more than one proposal
f) Was declared ineligible by the Government of India/State/UT Government for corrupt and fraudulent practices.

29. **Knowledge transfer:** Subject to any qualification or provision to the contrary in the statement of work, the Service Provider must provide the following assistance to the QCI on termination or expiration of this Contract: transferring or providing access to the QCI to all information stored by whatever means held by the Service Provider or under the control of the Service Provider in connection with this Contract; and making Specified Personnel / employees and Service Provider Personnel available for discussions with the QCI as may be required. The time, length and subject of these discussions will be at the sole discretion of the QCI, provided that any matter discussed is not considered to reveal any 'commercial-in-confidence information of the Service Provider.

30. **Force Majeure**: Neither party shall be held responsible for non-fulfillment of their respective obligations due to the exigency of one or more of the force majeure events such as but not limited to Acts of God, war, flood, earthquakes, strike, lockouts, epidemics, pandemics, riots, civil commotion etc., provided on the occurrence and cessation of any such events. The affected party thereby shall give a notice in writing to the other party within one week of such occurrence or cessation. If the force majeure conditions continue beyond six months, the parties may then mutually decide about the future course of action.

Force Majeure shall not include:
a) any event which is caused by the negligence or intentional action of a Party or by or of such Party's agents or employees, nor
b) any event which a diligent Party could reasonably have been expected both to take into account at the time of the signing of the Contract and avoid or overcome with utmost persistent effort in the carrying out of its obligations hereunder.
c) Insufficiency of funds or manpower or inability to make any payment required for execution of services under this Contract.

31. **Indemnity:** Service Provider undertakes to indemnify QCI from and any losses that QCI may incur due to any deficiency in services rendered by Service Provider or any instance of corruption or improper payment.

32. **Taxes & Duties:** The service provider shall be liable to pay all direct and indirect taxes, duties, fees and other impositions levied under the laws of India.

33. **Rescinding of Work order:** The work order issued by QCI to Service Provider for the above scope can be withdrawn at any time by giving a notice period of 7 days if a Service Provider fails to perform/execute work as per the requirements specified in this document after two warnings (served in writing) or in case of non-compliance/breach of any of the terms and conditions of this order.

34. **Validity of Proposals:** The proposals shall remain valid for a period of 90 days from the last date of submission. In exceptional circumstances, QCI may solicit the bidder's consent to an extension of the period of validity. The request and the responses thereto shall be made in writing. A bidder consenting to such request shall not be required nor permitted to modify its Proposal.

35. QCI, by issuance of this RFP does not necessarily indicate or imply that the project will be commenced. The service provider will absolve QCI of all responsibilities if the project does not start

within a stipulated time frame. QCI reserves the right to withdraw this assignment any time without prior consultation or intimation to the service provider.

36. The service provider shall not make any alteration / changes in the bid after the closing time and date. Unsolicited correspondence from the service provider will not be considered.

37. The service provider shall be deemed to have complied with all clauses in this RFP. Evaluation shall be carried out on the available information in the bid and QCI is not liable to seek clarifications on the documents not submitted as part of the bid.

38. The firms / agencies submitting their proposals would be responsible for all of its expenses, costs and risks incurred towards preparation and submission of their proposals, attending any pre-proposal meeting and visiting the site or any other location in connection therewith. QCI shall, in no case, be responsible or liable for any such costs whatsoever, regardless of the outcome of the process.

39. **Disclaimer:** QCI shall not be responsible for any late receipt of applications for any reasons whatsoever. The applications received late will not be considered.

QCI reserves the right

a) To reject any/all applications without assigning any reasons thereof.
b) To relax or waive any of the conditions stipulated in this document as deemed necessary in the best interest of the QCI without assigning any reasons thereof.
c) To include any other item in the Scope of work at any time after consultation with applicants or otherwise
d) To adopt method deemed fit to evaluate the proposals
e) To select multiple Service Provider for the project for allocation of work in different areas if it meets the essential criteria for qualification.

40. **Submission of Proposals:** The intending Service Provider is expected to prepare proposals covering the following aspects:

a) **Technical Bid**
   i. Signed and stamped Form-A, B, C, D attached as Annexure-A
   ii. Details of relevant previous experience
   iii. Supporting documents for the details required as per pre-qualification criteria
   iv. Any other details that the bidder may like to provide.

b) **Financial Bid:**

S. No.	Particulars	Cost*
1	One-time cost for conducting Aadhar Compliance Audit e-KYC Application	

**Exclusive of GST*

A detailed explanation of the pricing structure including all price components, unit costs, resource loading, estimates of overheads and any other assumptions made in arriving at the final all-inclusive price quote should be provided.

Please mention the following in preparing your bid:

i. Dated this [date / month / year]
ii. Authorized Signatory (in full and initials)
iii. Name and title of signatory
iv. Duly authorized to sign this proposal for and on behalf of [Name of service provider]

v. Name of the Firm
vi. Address of the Firm

41. **Submission Details**

a) The Financial and Technical Proposals should be submitted separately in the given format and signed by the Authorized Signatory. Financial bid, if submitted along with the technical bid is liable to be rejected.
b) All the pages of the proposal must be sequentially numbered and must contain the list of contents with page numbers. Any deficiency in the documentation may result in the rejection of the Bid.
c) All pages of the application shall be signed and stamped by the authorised signatory.
d) Please Note that Prices must not be indicated in the Technical Bid.

Interested parties may send the technical and financial bid in two separately sealed envelopes inside a larger sealed envelope super-scribing **"Engagement of an agency for Aadhar Compliance Audit e-KYC Application"** to Deputy Director (Finance & Accounts), Quality Council of India, Institution of Engineers Building, 2nd Floor, 2 - Bahadur Shah Zafar Marg, New Delhi - 110002, India latest by July 23, 2024, 2 PM.

A copy of only technical proposal, in the PDF format, shall be submitted to procurement@qcin.org on or before July 23, 2024, 2 PM.

Note: In case of any discrepancy in the submitted technical proposals (PDF version and Hard Copy), the documents submitted in the hard copy shall prevail.

For further queries, you may please contact the below mentioned:

For any queries, you may contact the below:

Procurement Team, QCI **Email id: procurement@qcin.org**

Annexures

Form A: Covering letter with the Proposal in response to RFP Notice

(To be submitted on the Letterhead of the responding firm)
To,
Deputy Director (Finance & Accounts),
Quality Council of India,
Institution of Engineers Building,
2nd Floor, 2, Bahadur Shah Zafar Marg, New Delhi-110002

Subject: Submission of proposal in response to the RFP for "-_____".

Dear Sir,

1. Having examined the RFP document, we, the undersigned, herewith submit our proposal in response to your RFP dated ____for "_____,in full conformity with the said RFP document.
2. We attach our technical response and our financial quotation in a separate sealed cover as required by the RFP both of which together constitutes our proposal, in full conformity with the said RFP.
3. We undertake, if our proposal is accepted, to adhere to assign a team dedicate to this project.
4. We have read the provisions of RFP and confirm that these are acceptable to us. We further declare that additional conditions, variations, deviations, if any, found in our proposal shall not be given effect to.
5. We undertake, if our proposal is accepted, to adhere to the scope of engagement or such modified plan as may subsequently be mutually agreed between us and QCI or its appointed representatives.
6. We agree to unconditionally accept all the terms and conditions set out in the RFP document and also agree to abide by this bid response for a maximum period of THREE MONTHS from the date fixed for bid opening and it shall remain binding upon us with full force and virtue, until within this period a formal contract is prepared and executed, this bids response, together with your written acceptance thereof in your notification of award, shall constitute a binding contract between us and QCI.
7. We affirm that the information contained in this proposal or any part thereof, including its exhibits, schedules, and other documents and instruments delivered or to be delivered to through this proposal is true, accurate, and complete.
8. This proposal includes all information necessary to ensure that the statements therein do not in whole or in part mislead the QCI as to any material fact. We agree that QCI is not bound to accept the lowest or any bid response you may receive. We also agree that you reserve the right in absolute sense to reject all or any of the products/ service specified in the bid response without assigning any reason whatsoever.

It is hereby confirmed that I/We are entitled to act on behalf of our corporation/company/ firm/organization and empowered to sign this document as well as such other documents, which may be required in this connection.

Dated this Day of 2024 (Signature) (In the capacity of)
Duly authorized to sign the Bid Response for and on behalf of: (Name and Address of Company) Seal/Stamp of Bidder
{Place}
{Date}

Form B: Relevant Project Experience

S. No.	Name of the Project/ Engagement	Client Name	Duration (Period)	Approximate value of the assignment

Form C: Details of the responding firm

S. No.	Particulars	Details to be furnished	
1.	**Details of responding Company**		
Name			
Address			
Mobile			Fax
E-mail	-		Website
2.	**Information about responding Company**		
Status of Company *(Public Ltd. / Pvt. Ltd etc.)*			
Details of Registration *(Ref e.g. ROC Ref #)*			Date Ref #
Details of Service Tax Registration			Date Ref #
3.	Current Year Turnover (Rs Crores) from _____ Services in India;		
4.	Company Profile (Operations in India)		
4.1	Average turnover from Indian Operations from _____services in last three years	(Turnover in Rs Crores)	
4.2	Full-time professional staff engaged in similar projects	(Number of Staff)	
4.3	Extent of operations in India (national spread) i.e. number of offices in India (client specific / project specific offices should not be considered)	(Number of Offices in different cities/towns and their address)	

Form D: Format for Non-Blacklisting Undertaking

(To be submitted on the Letterhead of the responding firm)

To,
Deputy Director (Finance & Accounts),
Quality Council of India,
Institution of Engineers Building,
2nd Floor, 2, Bahadur Shah Zafar Marg,
New Delhi-110002

Subject: Non-Blacklisting declaration in connection with RFP Ref. No. _____ dated____ for _____
Dear Sir,
This is to notify you that our Firm/Company/Organisation _____ intends to submit proposal in response to invitation for Tender Ref. No. _____ for <>. In accordance with the above, we declare that:

a. We are not involved in any major litigation that may have an impact of affecting or compromising the delivery of services as required under this agreement
b. We are not blacklisted by any Central/ State Government/ agency of Central/ State Government of India or any other country in the world/ Public Sector Undertaking/ any Regulatory Authorities in India or any other country in the world for any kind of fraudulent activities.

Dated this Day of (Year)
(Signature) (In the capacity of)
Duly authorized to sign the Proposal Response for and on behalf of:
(Name and Address of Company) Seal/Stamp of Bidder