

PAKISTAN REVENUE AUTOMATION (PVT) LIMITED

TENDER DOCUMENT NO.P-12/2024

REQUEST FOR PROPOSAL (RFP) DOCUMENT

**PROCUREMENT
FOR THE
ISO 27001 CONSULTANCY SERVICES VERSION 2022 OR ABOVE**

December 2024



Online (e-bid) shall be submitted only at e-PAK Acquisition & Disposal System (EPADS), on or before 11:00 AM, 26th December 2024.

In case of any query, please contact Phone: (+92)51-9259353

Or visit

Admin & HR Department (Procurement Wing)

Pakistan Revenue Automation (Private) Limited,

Software Technology Park, 2nd Floor, Service Road (North), Sector I-9/3, Islamabad

Email: at procurement@pral.com.pk

Website: pral.com.pk



Table of Contents	Page
1) Invitation to Bid:	2
2) Instructions to Bidders:	2
3) Conditions for Eligibility:	4
4) SCOPE OF THE SERVICES/TERMS OF REFERENCE:	4
5. General or Special Conditions of Contract	13
6) Form of Contract	14
7) Delivery Timelines or Completion Date	14
8) Technical Evaluation Criteria	14
9) Financial Evaluation Criteria	15
10) Performance Security	15
11) Submission of Bids (Technical and Financial Proposal): -	15
12) Pre-Bid Meeting	15
b. Cover Letter for the Submission of Technical Proposal	16
Annex – A (Organization Information)	17
Annex – B (Eligibility Criteria Check List)	18
Annex – C (Relevant Experience)	19
Annex – D (Technical Evaluation Criteria) for ISO 27001 CONSULTANCY SERVICES.	20
Annex – E (Key Management Staff of the Company)	23
Annex-G (Penalty Clauses & Payment Terms)	25
Annex – H (Declaration)	26
Annex – I (Cover Letter)	27
Annex-J (Draft Agreement)	28
DATED _____ 2024	28
ANNEXURE J: DRAFT CONTRACT	29



1) Invitation to Bid:

Pakistan Revenue Automation (Private) Limited (acronym – PRAL). PRAL is a private limited Company registered under section 32 of the companies ordinance, 1984 (XLVII of 1984). PRAL is working with federal and provincial tax and revenue agencies to provide wide variety of tax and revenue collection automation solutions, since its incorporation in June, 1994. Online (e-bids/proposals) are invited from bidders for provision of ISO 27001 Consultancy Services..

All interested and eligible bidders are requested to go through the RFP document and provide relevant required information and supporting documents mentioned in this document.

2) Instructions to Bidders:

The selection of Consultancy company/firm will be based on **Least Cost Method** as provided in Regulation 3(C) of the Procurement of Consultancy Services Regulations, 2010 through **Single Stage Two Envelopes** bidding procedure. The Bidder is expected to examine all instruction forms, terms and specifications in the bidding documents. Failure to furnish all information required by the bidding documents and/or to submit a bid not substantially responsive to the bidding documents will be at the bidder's risk, which may result in rejection of bid. .

- 2.1 The PDF copy of the Technical and financial proposal/bid along with the bid security shall only be submitted online on EPADS no hardcopy shall be entertained.
- 2.2 In the first instance, the "Technical bid/Proposal" shall be opened for technical evaluation and the "Financial Proposal" shall remain unopened in the system.
- 2.3 PRAL shall evaluate the Technical Proposal in a manner prescribed in section-8 given in the document, without reference to the price and condition PRAL shall reject any proposal which does not conform to specified requirements.
- 2.4 During the technical evaluation, no amendments in Technical Proposal shall be permitted.
- 2.5 After evaluation of the technical proposals, PRAL shall open the financial proposals of the technically responsive bids online, and shall communicate the date, time & venue through system in advance, within the bid validity period.
- 2.6 The financial bids whose technical bids declared non-responsive, shall not be opened.
- 2.7 The Technical and Financial Proposal will be evaluated based on PRAL's evaluation criteria as provided in section-08 and 09 of this document.
- 2.8 This document has different sections carrying information of eligibility, technical evaluation criteria, Scope of work/Term of Reference, conditions of RFP and form of contract etc. to assist the potential bidders to develop their technical proposals.
- 2.9 A bidder who shall obtain 70 or more marks, along with a compulsion to obtain 10 marks in Serial # 4 of Annexure-D shall be considered as technically qualified for the assignments.
- 2.10 PRAL reserves the rights to request submission of additional information from the bidders to clarify/further understand aspects of technical proposal, if required. PRAL also reserves the right to verify any information provided by the bidder.



- 2.11 PRAL has the right to visit business premises to verify the information shared in RFP documents. Bidder presenting information intentionally incorrectly or fraudulently will be disqualified.
- 2.12 PRAL reserves the right to award or not to award the contract and bidders who fail to submit complete and attach all the relevant documents shall be disqualified. No bid shall be accepted in hardcopy.
- 2.13 Bidders to strictly ensure that their bid documents are submitted before the closing time and date of the tender, else the system will not accept the bids after the closing time.
- 2.14 Questions about the bidding document can be made only in writing through EPADS or Email: at procurement@pral.com.pk and must be asked on or before COB December 12, 2024.
- 2.15 Although adequate thought has been given in the drafting of this document, errors such as typos may occur for which PRAL will not be responsible.
- 2.16 Consultancy Firms/Companies cannot apply by forming a consortium (both local or International firms/Companies).
- 2.17 In case the bid opening day falls on a public holiday, the next working day shall be considered as the opening day for the same.
- 2.18 In case of any disruption/failure in submitting the bid on EPADS, PRAL shall not be held liable, since the EPADS is owned and operated by PPRA.
- 2.19 In case of any disruption observed on the day of bid opening due to any reason related to server/internet connectivity, the next working day shall be considered as the opening day for the same.
- 2.20 Consultancy firm shall have required skills, expertise and team by which it can solely and exclusively supply all services/deliverables as specified in the bidding document without assigning it to any other individual/firm and hence shall not propose any "Joint Venture" in its bid. A Consultancy firm offering services through joint venture with any other individual/firm shall be rejected.
- 2.21 The Procuring Agency, at its discretion, may extend "Deadline for Submission of Bids". In such case, all rights and obligations of the Procuring Agency and Bidders previously subject to the deadline shall thereafter be subject to the extended deadline.
- 2.22 The bidder should be a registered supplier on the e-Pak Acquisition & Disposal System (EPADS) to participate in the subject tender. To register electronically suppliers can visit <https://eprocure.gov.pk/#/supplier/registration>
- 2.23 The scanned copy of the Bid Security to be uploaded along with the online bid and the hardcopy of the bid security and original copy of the Affidavit shall only be submitted at PRAL office, Procurement Department, Software Technology Park, 2nd Floor, Service Road North, Sector I-9/3, on or before 11:00 AM 26th December 2024.
- 2.24 Alternate bidding proposals are not allowed, if a bidder submits more than one technical or financial proposal against the assignments, all proposals of that bidder shall be rejected.
- 2.25 Upon completion of financial evaluations in accordance with "Evaluation Criteria for Financial Proposals", Procuring Agency will select "Highest Ranked Bidder" for "Negotiation/Discussion" on technical issues including methodology, work plan, staffing, timelines and special conditions etc., as permitted under Clause (10) of PPRA Regulations-2010.



2.26 In case of failure of negotiations with selected bidder, next ranked bidder will be invited for such negotiations / discussion

2.27 Process to select next ranked bidder for negotiations / discussion will continue till its "Success".

3) Conditions for Eligibility:

The bidders, fulfilling the following criteria, will be considered eligible for the bidding process.

3.1 Evidence of the bidding firm/company's registration/Incorporation is required (Copy of certificate of incorporation/company registration certificate is required)

3.2 Have National Tax Number (NTN) and GST/ PST (if applicable) in the name of Organization (Provide a copy of registration)

3.3 Should be active taxpayer on the date of submitting the bid. (Status report must be provided)

3.4 Affidavit on stamp paper, declaring that the Consultancy company/Firm is not blacklisted by any Telco/FMCG/autonomous body/government/semi government or any organization. (Affidavit on stamp paper original signed & stamped)

If bidder fails to provide above mentioned information using "Eligibility Criteria Checklist" (Annexure B), they shall be dis-qualified and declared ineligible from the bidding process and its technical evaluation will not be carried out.

4) SCOPE OF THE SERVICES/TERMS OF REFERENCE:

The following scope of work identifies the tasks and responsibilities that the qualifying Consultancy Company/Firm shall deliver upon, by working closely with the Operations and Software Development Departments of PRAL:

1. PURPOSE

The Federal Board of Revenue's (FBR) Data Center and AEOI offices are already ISO 27001 certified. PRAL intends to acquire consultancy services to facilitate the renewal of the certification. PRAL's HQ-based Software Development Department and other departments will implement ISMS protocols from scratch. The consultancy services are required for one year, until FBR's ISO 27001 certification renewal in 2025.

As the Data Center and AEOI offices are already certified, documentation is complete. However, the consultancy firm will reevaluate these documents to ensure 2025 certification.

2. DESCRIPTION AND SCOPE OF WORK

PRAL seeks the engagement of professional services firms with a strong track record in projects involving ISO 27001 certification. For that reason, online bids/proposals are invited from eligible, reputed firms, who are involved with ISO 27001 implementing and acquiring solutions. If during the course of the contract, the ISO version is updated Consultancy firm will be responsible for preparing PRAL to achieve the desired level of certification for FBR. Bidders are expected to follow a structured **Software Development Lifecycle (SDLC)** to align with the security and quality standards required for ISO 27001 certification. This SDLC framework must be adhered to at each stage i.e. Requirement



Gathering and Analysis, Design, Implementation / Coding, Testing, Deployment, Maintenance to ensure compliance with ISO 27001 requirements. Refer to appendix C for standardized SDLC and ISO documentation templates to be utilized for this purpose. Bidders should include specific plans detailing how they will address each phase, with emphasis on security controls, documentation and quality assurance processes.

Given the Data Center and AEOL offices' current certification, the necessary documentation is in place. The consultancy firm will now assess and update these documents as needed to ensure successful recertification in 2025.

3 Security and Privacy

PRAL reserves the right to validate the compliance with security of the proposed solution prior to authorizing payment. PRAL also reserves the right to reject the proposed solution or to require correction by the bidder should any part of the solution provided not be to PRAL's satisfaction. The bidder shall also assume all costs associated with any correction(s) required by PRAL. The bidder shall also abide by the security procedures in place by PRAL. The bidder/contractor must certify that any information obtained during the course of performing the tasks will not be disclosed to any external party.

4 MANDATORY TECHNICAL REQUIREMENTS

i. CONSULTATION

Consultation is the key aspect of seeking ISO certification and the main purpose for getting consultation services is the fast track process to the certification. The consultant is required to understand the business context and relevance of information security at start of ISO 27001 implementation analysis. The consultant will assist PRAL with detail risk assessment/gap analysis including information asset identification, IT security risk assessment including threats, impacts, vulnerabilities and probabilities resulting in identification of risks, and gaps.

The step that takes maximum time is the implementation and measurement journey through definition of ISO 27001 policy, procedure and documentation on one hand and the implementation of risk based gaps on the other. The consultant, who will also be the lead implementer, will assist with the required documentation for the successful completion of acquiring the ISO 27001 certification by FBR.

Annotation

Bidders are required to provide a schedule of specific activities and services to be supplied under the tender and grouped under the following categories:

- a) Training on ISO 27001 with documentation (soft and hard copy).
- b) ISO 27001 certification (Consultancy).
- c) *Review and enhancement of PRAL Information System security policies.*



d) *Implement an ISMS based on the requirements of ISO 27001:2022.*

Implementation Schedule

1. Bidders are required to fill the table below or use its format to respond.
2. Bidders MUST provide a substantive response for all features irrespective of any attached technical documents. Use of Yes, No, tick, compliant etc. will be considered non responsive.
3. Bidders MUST append official company stamp and/or authorized signature on all attached technical data sheets.

Implementation Schedule Table

Sr. #	Subsystem / Item	Activity Start Week (after award)	Duration in weeks
1.	Training on ISO 27001 with documentation (soft and hard copy).		
2.	ISO 27001 ISMS development.		
3.	Pre-implementation audit.		
4.	ISO 27001 Pre – Certification Assessment		
6	Review and enhancement of PRAL IS security policies		

Bidders should outline their project management approach, including frequency of status updates, key milestones and escalation procedures. A communication plan detailing regular check-ins and reporting frequency is required to ensure alignment with PRAL’s project team.

The selected Bidder shall be required to undertake to perform all such tasks, render requisite services and make available such resources as may be required for the successful completion of the entire assignment at no additional cost to PRAL.

The selected Bidder will be responsible for carrying out risk assessment of the identified business units of Data Centers, Software Development department at PRAL HQ, AEOI Offices and provide risk assessment framework and templates to PRAL as per the broad objectives as outlined below:

1. A comprehensive risk assessment of the operations.
2. Development of risk management framework which would ensure that the IT risks are managed by PRAL on an ongoing basis.
3. Develop risk assessment templates for the various Information System Assets for



units, which would enable PRAL to self-assess the risks at any point of time.

The selected Bidder will ensure knowledge transfer to PRAL at every stage of the project to enable PRAL to carry out the work as specified in this RFP in future after completion of this assignment.

PRAL may, at its full discretion, choose to avail the services for all services or part thereof. Such decision may be advised in course of the project.

5. PROJECT SCOPE

The primary focus of the scope is to obtain ISO 27001 Consultancy for FBR and PRAL selected offices mentioned in Appendix A. However, the detailed scope is detailed as under.

The project scope includes ISO 27001 Consultancy for above referred offices including Regular Risk assessment.

Risk Assessment and mitigation plan should be done as per ISO 27001 Standards. The consultant would also develop the risk assessment template with a scoring system which would be used by PRAL in future to assess risks at the in-scope centers.

Risk Management and Contingency Planning: Bidders are required to submit a risk management plan that identifies potential risks (e.g., resource constraints, security threats) and outlines mitigation strategies. This plan should also include a contingency plan for addressing critical risks and maintaining project timelines.

The project scope in addition to the listed office also includes the in-house developed applications(s) for AEOI project. A comprehensive study with regards to Gap Analysis, Risk Assessment, Vulnerability Assessment, Penetration Testing of all related software and hardware as following the ISMS policies and procedures.

The Testing phase must include quality assurance measures, such as code reviews, penetration testing and vulnerability assessments. Bidders are required to document test results and provide evidence of issue resolution prior to deployment.

Scoping:

A detailed scoping would be required to be carried out to define the areas which would be covered encompassing the business processes, policies and procedures, IT infrastructure, IT organization, IT implementation etc. The scope would need to be approved by PRAL before further work is undertaken.

Deliverable:

- Description of approach and methodology
- Detailed scope.
- Implementation plan

Gap Assessment:



During this phase the selected Bidder would review the in-scope elements against the best practices, PRAL's own Security Policy & Guidelines, ISO 27001 guidelines. This phase would include but not limited to the following:

- Review of IT governance and organization.
- Review of Risk Management framework
- Review of IT processes and business processes around IT processes.
- Review of Policies Standards & Guidelines, Procedures and other subordinate documents.
- Review of Change Management Process including security testing of applications/updates/patches before moving to production.
- Review based on the IS Auditors Comprehensive Audit reports of IT Infrastructure etc.

Asset Identification, Ownership & Classification:

The selected Bidder would be required to identify, classify and document the entire Information System assets of various types in a logical manner. The selected Bidder will define owners in consultation with PRAL and will perform the Asset valuation based on the confidentiality, integrity and availability value of the asset. The selected Bidder will classify them according to the criticality based on the business area and usage.

Threat Analysis:

The selected Bidder will perform the Threat and Vulnerability analysis and Compute the probability of occurrence of the threat based on a scientific method.

Risk Assessment:

The selected Bidder would use standard risk assessment methodology and assess the risk based on the inputs from the above three steps i.e. Gap assessment, Asset identification, valuation and classification and Threat analysis. The selected Bidder will also evaluate the third-party relationships and perform risk assessment of the same. Risk Assessment would have to be carried out for all Information System assets without any sampling. Ongoing Risk assessment would need to be carried out for any new implementation in the Data Center and in the Software Development department at PRAL during the period of assignment.

Baseline Security Review:

The selected Bidder would review the Baseline security of IT Assets as per the industry best practices and Consultant recommended guidelines and ensure that Baseline security is implemented. Selected Bidder should ensure that Baseline security documents are available. In case of any gap found, the same has to be formulated by the Consultant.

Deliverables for Gap Assessment:



- Gap assessment report based on ISO 27001 standards.
- Review/Audit reports under various heads such as IT organization, Technical Infrastructure with detailed implementable steps.
- Asset Inventory, ownership and Classification, Asset Register
- Risk Management Framework.
- Develop process for ongoing Risk Assessment before introduction of any application, IT device.
- Risk Assessment Report
- Baseline security review report

Gap/Risk Remediation

The Selected Bidder will identify the gap in the existing environment vis-à-vis the ISO 27001 requirements and suggest the remediation plan with the detailed steps to be performed to achieve ISO 27001 certification.

The Selected Bidder will have to share details with the stake holders and would spell out a detailed remediation plan meant for various levels such as organization, policies and procedures, devices to facilitate implementation. The remediation plan has to be granular and deficiency specific based on risk assessment and generic recommendations should be avoided.

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 ISO 27001 compliance and Regular risk assessment.

The selected Bidder has to coordinate with the PRAL system integrator, monitor the progress in risk remediation and provide handholding support till the risk is remediated. The support has to be in the form of emails, telephone, and onsite visits, additional technical inputs etc. as may be required by PRAL during the tenure of the contract. In case the solution suggested by the selected Bidder cannot be implemented, in such cases, selected Bidder will suggest the alternative solution to PRAL.

Deliverables for Gap/Risk Remediation:

- Business unit wise Risk Mitigation and Gap remediation plan
- Revised or new IT Security policy, Standard & Guideline, Procedures and subordinate documents etc.
- Baseline security hardening guideline documents

Certification



- The selected Bidder has to perform the pre-certification audit on completion of the Gap remediation to ensure compliance as per ISO 27001 standards.
- The coverage needs to be comprehensive during this exercise as per the ISO 27001 requirement. This may require coordination with FBR SOC team.
- Prepare all the documentation required and enable PRAL to apply for ISO 27001.
- Provide onsite consultancy support during ISO 27001 Certification audit.

Post Certification

- The selected Bidder has to perform the steps enumerated as above to ensure ongoing compliance. The selected Bidder will perform risk assessment and perform ongoing risk assessment of any changes in the IT infrastructure assets.

Deliverables

- As above
- Ongoing Risk assessment reports.

Requirement for Consultancy:

- The bidding company should be an ISO 27001 certified firm.
- Consultants must be a permanent employee of the bidding company. Employment evidence is required with the bid.
- The bidding company should have at least 5 years of experience in providing information security consultancy.
- The bidding company must have experience of providing ISO 27001 consultancy to a minimum of 3 organizations in the Pakistani Government Sector and a minimum of 10 organizations in Private Sector (both international and local).
- The bidding company having experience in providing data center security consultancy will be preferred.
- The bidding company should have at least 2 certified lead auditors for ISO 27001 and they should also be permanent employees of the company.
- Provision of yearly training for 3 years in the field of:
 - Lead Implementer for ISO 27001 – 3 Days (10 resources)
 - Internal Auditor for ISO 27001 – 3 Days (10 resources)
 - Internal Penetration Testing & Vulnerability Assessment – 3 Days (10 resources)
- The bidding company should have experienced and certified trainers in the above domains.
- Yearly conduction of Vulnerability Assessment & Penetration Testing of assets, where ISMS consultancy is provided, such as Data Center Network, Application, AEOI Offices, etc.
- The bidding company should have experience of conducting Penetration Testing in at least 3 Government Sector Organizations and 5 Private Sector Organizations.
- Sample report on VA/PT to be provided with the proposal.



- The bidding company must work around with the timeline and deadline of the project provided.

Scope or Work for Vulnerability Assessment & Penetration testing:

The bidder will be responsible to Conduct comprehensive penetration testing to identify vulnerabilities in PRAL's information security management system (ISMS), covering FBR Data centers and all software applications developed by PRAL including, AEOI Project (hardware and AEOI application on selected locations).

The bidder will be responsible for complete Data Center(s) Hardware, Software Development at PRAL HQ and the AEOI Project (hardware and AEOI application). IRIS and other applications (including allied applications/ services) and AEOI are Web applications being used only on the intranet on selected locations. Thus, penetration testing via its web module running on web browser on the secure FBR's internal LAN should be carried out.

The scope includes:

1. **Vulnerability Scanning** — Automated software scan on Servers, Storage, Network and Network Services, Security Devices to uncover any potential security flaws.
2. **Security Scanning** — Uncovering of security soft spots and providing actionable steps on reducing the risk. This test can be manual or automated.
3. **Penetration Testing** — Simulating an attack from a hacker Data Center Hardware (Servers, Storage, Network Devices, Security Devices, AEOI web application (i.e. Analysing a specific system to determine possible spots on that can be exploited by hackers).
4. **Risk Assessment** — Analysing security risks that have been noticed. The severity of the risk will be determined as either low, medium, or high.
5. **Security Auditing** — Internal audit of complete system and operating systems for possible security gaps and finding anything suspicious.
6. **Ethical Hacking** — Hacking on AEOI Web Application, Data Center devices, Servers
7. **Posture Assessment** — This is a combination of Ethical Hacking, Security Scanning, and Risk Assessment to determine the overall security positioning of a company.

Objectives:

The main objectives of this exercise are following:

- To ensure compliance and to have assurance that PRAL infrastructure is secured against internal and external threats or intrusions.



- Conduct comprehensive security testing and verification of Applications, Databases, and network layers to assess the effectiveness of deployed security measures.
- Evaluate and verify existing security controls, identifying areas for improvement and recommending enhancements.
- Identify and implement suitable safeguards to strengthen Data Center infrastructure protection, secure coding practices, and software development environments.
- Develop and enhance Information Security Management System (ISMS) policies, procedures, and processes.
- Conduct risk assessments and vulnerability identification to prioritize remediation efforts.
- Ensure confidentiality, integrity, and availability of sensitive data and systems.
- Foster a culture of information security awareness among employees and stakeholders.
- Achieve certification to ISO 27001 standard, demonstrating commitment to information security best practices.
- Continuously monitor and improve the ISMS to maintain certification and ensure ongoing security.

Deliverables:

The Consultant should collect and organize its findings at the completion of the assessment and produce at minimum the following deliverables:

1. Executive report that highlights the security issues. The executive report should include the steps that were performed during the assessment, discuss the significant findings of the assessment and their business impact, and Offer recommendations to reduce or eliminate exposures to the vulnerabilities. This should be done for both, Internal and External assessments.
2. A detailed technical analysis report that includes the methodologies used during the assessments, list the tools used, screen shots of any exploited Services and/or systems, a complete list of findings that are categorized by risk level and resource requirement ratings, and recommendations to resolve issues. Underlying causes of technical vulnerabilities should be examined in the context of specific findings. Consultant should rate each identified vulnerability based upon the risk it poses to PRAL and the resources required to correct or to minimize the issue. The Consultant should use proper rating criteria as per the best practices, Check List or standards.
3. The deliverables will also include a Security Controls Gap Analysis identifying gaps in existing security controls, recommendations for improvement, and alignment with ISO 27001 requirements. An Implementation Plan will provide guidance on implementing recommended security measures, technical specifications, and configuration requirements.



Project Requirements

- Consultants must describe approach and methodology for delivering the proposed solution. They should detail how many employees are to be dedicated to the support of the project being proposed, and their range of experience and skill, Roles and responsibilities and relevant certifications (e.g., CISSP, CISM)
 - Consultants must provide a sample, high-level implementation plan based on their experiences of a project with similar scope. This should be in the form of a summary plan and should contain only sufficient detail as would be required to assess the Consultant's competency. In project management, the plan should therefore summarize the following:
 - Project team composition and organization
 - Approach and Methodology
 - Outline project plan in a simple task-list
 - Project reporting standards
 - List of software to be used for penetration
 - Issue reporting and resolution processes
 - Communication requirements
 - Facilities required
 - Consultant is responsible to identify any information needed to conduct the vulnerability assessment and penetration testing.
 - Consultant, with the assistance of the PRAL technical team, will prepare an issue resolution and escalation procedure to assure the efficient and timely resolution of issues and incidents, and to communicate "high risk" findings promptly.
 - Propose the measures to fix the loopholes and vulnerabilities identified during the whole process; conduct the validation testing once the fixes are applied.
- 5) PRAL may opt vulnerability assessment and penetration testing for all the sites or may choose one or more sites of its choice as per operational requirements therefore the bidders are required to quote the cost of Vulnerability assessment and penetration testing separately for each site.

5. General or Special Conditions of Contract

The successful bidder shall agree to the following terms of references to provide services to PRAL:

- 5.1 Consultancy firm shall not disclose either during or subsequent to the expiry of assignment(s), any confidential information acquired.
- 5.2 Consultancy firm shall be responsible for all administrative, design costs related to delivering the reports.



- 5.3 Consultancy firm will carry out activities in consultation with PRAL's designated team and all reports and other communication will be addressed to the General Manager (Operations) or as otherwise agreed and communicated between the Consultancy firm and PRAL.
- 5.4 PRAL shall be entered into a formal contract with the successful bidder and reserves the right to terminate the contract if performance of Bidder is unsatisfactory.
- 5.5 All documents and information received by PRAL from bidders will be treated in strictest confidence. Documents submitted to PRAL will not be returned.
- 5.6 All expenses related to participation in this bidding document shall be borne by the bidder.
- 5.7 Bidders must comply with PRAL's confidentiality and security policies throughout the project. All data and information received during the assignment should be treated as confidential, with measures in place to prevent unauthorized access. Non-compliance may result in contract termination.

6) Form of Contract

- 6.1 The successful bidder will sign a Contract with PRAL as per Draft attached as **Annexure-J**. Any amendment to the contract shall be made with mutual consent of both parties. All costs associated with entering into the said contract shall be borne by the successful bidder.
- 6.2 The duration of the contract shall be 01 year; however, it can further be extended up to 2 years on the satisfactory performance of the bidder with the mutual consent of both parties on the same terms & conditions. PRAL may cancel the contract based on unsatisfactory performance by the bidder, by giving a one (01) month notice.
- 6.3 In case of any dispute regarding services the decision of the PRAL shall be final & binding.
- 6.4 The competent authority may reject all bids or proposals at any time prior to the acceptance of a bid or proposal. PRAL shall upon request communicate to any bidder, the grounds for its rejection of all bids or proposals but shall not be required to justify those grounds.
- 6.5 All taxes will be deducted in accordance with the applicable laws.
- 6.6 The bid shall remain valid for the period of 120 days from the date of bid opening.
- 6.7 In case the selected bidder fails to deliver the project as per the agreed timelines, bank guarantee of the bidder will be forfeited, and the contract may be terminated.

7) Delivery Timelines or Completion Date

Timelines of the delivery of services shall start once the contract is signed/ issuance of Purchase/Service Order and remain valid till the expiry of the contract.

8) Technical Evaluation Criteria

This document is governed by the procedure approved by PRAL management. The technical proposal of eligible organizations will be evaluated against the requirements specified in the **"Annexure-D for ISO 27001 CONSULTANCY SERVICES**.

- 8.1 **SDLC and Documentation Adherence:** Bidders should demonstrate a clear understanding of the SDLC phases, providing past project examples or documentation templates to illustrate compliance. Points will be awarded for completeness, quality of deliverables and alignment with ISO 27001 security requirements.
- 8.2 **Prior Experience with ISO 27001:** Bidders with direct experience in ISO 27001 projects, especially in government or large private sector contexts, will be given additional consideration. Documentation of previous projects, including client testimonials or case studies, will add value to the evaluation.



9) Financial Evaluation Criteria

The financial proposals of only eligible bidders with technically responsive (scoring minimum 70 marks), will be opened in the presence of all the bidders participated in the RFP. All bids shall be opened by the evaluation committee publicly online in the presence of the bidders or their representatives who may choose to be present, at the time and place announced prior to the bidding. Chairperson or member of the evaluation committee shall read aloud the total cost of the bid and shall record the minutes of the bid opening. All bidders shall sign an attendance sheet at the time of bid opening. The tender will be awarded based on least cost method.

Please provide information regarding Financials in **Annexure – F**”.

10). Performance Security

The successful bidder will be required to furnish a performance guarantee equivalent to 10% of the award value of contract issued by a scheduled bank operating in Pakistan acceptable to PRAL, within ten working days from the receipt of notice of successful bidder or the time as may be extended by PRAL. If the successful bidder fails to deposit performance guarantee within the time stated above, PRAL retains the right to cancel the notice for award of agreement and the bid security shall be forfeited. The performance guarantee /security will be returned after completion of contract period.

11). Submission of Bids (Technical and Financial Proposal): -

The complete bid containing the Technical and Financial proposals along with Bid Security shall only be submitted online in PDF format on EPADS, no hardcopy shall be entertained. Only the original copy of the bid security and Affidavit shall be submitted in hardcopy at the address given in the bidding document on or before 11:00 AM 26th December 2024. Technical proposals will be opened online on the same day i.e., 11:30 AM 26th December 2024 at PRAL Head Office Islamabad in the presence of bidder’s representatives who wish to attend it. The bidder who fails to submit the hardcopy of bid security on or before the closing date & time on the given address shall be disqualified from the bidding process. The Bid Security of the disqualified bidders will be returned after awarding the business to the successful bidder.

12). Pre-Bid Meeting

A pre-bid meeting will be held on 13th December, 2024 at 1500 hours at PRAL Office i.e. Software Technology Park, 2nd Floor, Service Road (North), Sector I-9/3, Islamabad for clarification of any queries from the potential bidders.

13). Bid Security

Bid Security amounting to Rs.150,000/- in the form of pay order or demand draft favouring Pakistan Revenue Automation (Private) Limited shall be submitted along with the financial proposal. The Bid Security should be valid for a period not less than 6 months.

- a. Any bid not secured by “Bid Security” shall be considered as rejected.



- b. If “Bid Security” is found less than Rs.150,000/- the bid shall be considered as rejected at any stage.

b. Cover Letter for the Submission of Technical Proposal

A cover letter as specified in **Annexure I** shall be submitted with the proposal.

Note: Please provide the required Information/Response to all Annexure mentioned in this document and mark them while submitting the bid.



Annexures

Annex – A (Organization Information)

Organization Information			
S #	Required Information	Response	
1	Legal name of the organization		
2	Year of Registration / Establishment of the Organization		
3	National Tax Number		
4	General / Punjab Sales Tax Number		
5	Date of inception of IS Audit Services		
6	Presence and location of offices in Pakistan		
7	Detail of Services provided by the company		
8	What is the legal status of your organization? Tick the relevant box (one box only). (Attach Copy/Copies of Registration Certificate/s)	Public Sector Organization	
		Section 42 Company	
		Public Ltd. Company	
		Private Ltd. Company	
		Private Partnership Firm	
		Other (Sole Proprietor are not allowed to participate)	
9	Name and designation of 'Head of Organization'		
	Mobile:		
	Phone/s:		
	Email:		
10	Name and designation of 'Contact Person':		
	Phone/s:		
	Mobile:		
	Email:		
8	Address of organization		



Annex – B (Eligibility Criteria Check List)

Eligibility Check List				
Sr. No.	Eligibility Criteria Details	Evidence/Proof Required	Attached Supporting Documents/Proof and mark Yes/No	
			Yes	No
1	Evidence of the bidding firm/company's registration/incorporation	Copy of certificate of incorporation/company registration	<input type="checkbox"/>	<input type="checkbox"/>
2	Provide National Tax Number (NTN) and GST/PST, (if applicable) in the name of Organization	Copy of registration	<input type="checkbox"/>	<input type="checkbox"/>
3	Should be active taxpayer on the date of submitting the bid.	Status report	<input type="checkbox"/>	<input type="checkbox"/>
4	Affidavit on stamp paper, declaring that company is not blacklisted by any Telco/FMCG/autonomous body/government/semi government or any organization.	Affidavit on stamp paper original signed & stamped	<input type="checkbox"/>	<input type="checkbox"/>



Annex – C (Relevant Experience)

Relevant Experience		
Sr. #	Required Information of the Clients	Response (Please provide exact information with Clients organization name, location/s and duration) Provide data in sequence given below
1	Details of the Clients to whom ISO 27001 Consultancy & Certification Services are provided.	Attached Purchase Orders/Service orders/ contracts
	Name of Clients Organization(s) along with the following details:	i.
	I. Industry Name	ii.
	II. Size of the Organization	iii.
	III. Addresses, email address, Phone #, website	
	IV. Contact person	
	V. Start and end dates of Services (For example – Jan 2009 to July 2024)	



Annex – D (Technical Evaluation Criteria) FOR ISO 27001 CONSULTANCY SERVICES.

No.	Description	Marks
1	<u>Relevant Experience</u>	40
	<p>i. Total experience of the bidder: Over 10 years: 8 Marks 8-10 years: 5 Marks 5-7 years: 3 Marks</p> <p>ii. Relevant experience of the bidder in last five (05) years. Over 5 assignments: 8 Marks 4-5 assignments: 5 Marks 1-3 assignments: 3 Marks</p> <p>Documentary Proof): Purchase/Service order/ copies of contract of last five years with contact details of clients should be furnished *Multiple projects with same client will be counted as one.</p> <p>Clientele of relevant services:</p> <p>i. Government Sector Over 7 clients: 8 Marks 6-7 clients: 5 Marks 3-5 clients: 3 Marks</p> <p>Documentary Proof of Government Sector): Purchase/Service order/ copies of contract of Government Sector with contact details of clients should be furnished *Multiple projects with same government sector will be counted as one.</p> <p>ii. Private Sector (Local & International) Over 20 clients: 8 Marks</p>	



	<p>15-20 clients: 5 Marks</p> <p>10-14 clients: 3 Marks</p> <p>Documentary Proof of Private Sector (Local & International)</p> <p>Purchase/Service order/copies of contract of Private Sector (Local & International) with contact details of clients should be furnished *Multiple projects with same client will be counted as one.</p> <p>Experience in providing data center security consultancy and software development consultancy / ISO 27001 Audit: 8 marks</p> <p>Purchase/Service order/copies of contract with contact details of clients should be furnished</p>	
2	<p><u>Average Annual Turnover of Last Three (03) Years –</u></p> <p>Over Rs 20 Million. (Documentary proof required tax returns or financial audited reports from registered firm/company for the last three years)</p>	10
3	<p><u>Professional Staff</u></p>	40
	<p>Experience of the *Team Leader(s) – (Bidders to provide detailed CV of proposed team leader(s))</p> <p>a) Number of Certified Leads (permanent employees):</p> <p>Over 3 Leads : 8 Marks</p> <p>3 Leads : 5 Marks</p> <p>2 Leads : 3 Marks</p> <p>b) Total experience of Lead in relevant field- (Bidders to provide proof of experience)</p> <p>Over 15 years: 8 Marks</p> <p>11-15 years: 5 Marks</p> <p>5-10 years: 3 Marks</p>	



	<p>c) Experience of conducting assignments related to scope of services:- (Bidders to provide proof of experience)</p> <p>Over 20 assignment: 8 Marks</p> <p>16-20 assignments: 5 Marks</p> <p>10-15 assignments: 3 Marks</p> <p>Other Professional Staff:</p> <p>Technical Resources: (Bidder to provide detail of technical resources on company letterhead)</p> <p>Over 20 resources: 8 Marks</p> <p>16-20 resources: 5 Marks</p> <p>10-15 resources: 3 Marks</p> <p>Project Specific Certified Resources: Bidder to provide detail of Project Specific certified resources on company letterhead).</p> <p>Over 10 resources: 8 Marks</p> <p>08-10 resources: 5 Marks</p> <p>05-07 resources: 3 Marks</p> <p>*Note: Bidders can nominate one team leader for all heads of Scope of Services/Terms of Reference or they can nominate a different team leader for respective heads of Scope of Services/Terms of Reference based on experience/capabilities of their team leaders.</p>	
4	<p>100% Compliance to the scope of services / term of reference mentioned in the bidding document.</p> <p>(A written confirmation on company's letterhead is required that the bidder (company/firm) shall fully comply to the scope of services / term of reference mentioned in the bidding document)</p>	10
	Total Marks	100

Qualifying Marks for Technical Evaluation are **70**.

*Please mark/flag the supporting documents shared for technical qualification scoring.



Qualifying Marks for Technical Evaluation are **70**.

*Please mark/flag the supporting documents shared for technical qualification scoring.

*If the quoted item is below the required requirements/specification, the Bid shall stand non-Responsive

Annex – E (Key Management Staff of the Company)

Please attach CVs for your Key Management Staff

Key Management Staff of Company					
Sr #	Name of Management Staff	Designation	Qualification	Area of Expertise	Number of years in company



Annex – F (Financial Proposal)

Financial Proposal Format

Consultancy services, ISMS Training, Audit and Certificate Issuance		
<u>SR #</u>	<u>Description</u>	<u>Total 1 year Cost of all the sites (inclusive of all applicable taxes)</u>
<u>A</u>	Consultancy services, ISMS Training, Audit and Certificate Issuance as per scope of work mentioned in the tender document	PKR
	<u>Total Amount in Words for “A”</u>	
Vulnerability Assessment & Penetration Testing		
<u>SR #</u>	<u>Description</u>	<u>Total 1 Year site wise cost (inclusive of all applicable taxes)</u>
<u>B</u>	Vulnerability Assessment & Penetration Testing as per scope of work mentioned in the tender document	
<u>B.1</u>	PRAL HQs, KSL, STP, Sector I-9/3, Islamabad (All departments, Software Development, Operations Department, Services Department)	PKR
<u>B.2</u>	FBR Data Center Site-A, FBR House, Constitution Avenue Sector G-5, Islamabad	PKR
<u>B.3</u>	FBR Data Center Site-B, PRAL HQs, KSL, STP, Sector I-9/3, Islamabad	PKR
<u>B.4</u>	FBR Data Center Site-C, Custom House, West Wharf, Karachi.	PKR
<u>B.5</u>	AEOI Secure Room, AEOI Zone, ETC, Sector F-5/1, Islamabad	PKR
<u>B.6</u>	AEOI Center, FBR House, Constitution Avenue, Sector G-5, Islamabad	PKR
<u>B.7</u>	AEOI Secure Room, AEOI Zone, Lahore, 58-A/C-III, Gulberg III, Lahore	PKR
<u>B.8</u>	AEOI Secure Room, AEOI Zone, PNSC Building, Molvi Tamizuddin Road, Karachi	PKR
	<u>Total Amount in Words for “B”</u>	
<u>A+B</u>	<u>Total Cost A+B (inclusive of all applicable taxes)</u>	PKR

*Responsibility to include all and correct taxes is that of the bidders.

Note:

- 1- Bidders are required to quote rates for both A & B (Consultancy services, ISMS Training, Audit & Certificate Issuance and Vulnerability Assessment & Penetration Testing as per given financial format).
- 2- PRAL shall award contract for both the assignments to a single consultancy firm, based on overall total lowest evaluated bid for both A & B.

Authorized Signatory

Name _____

Designation _____



Signature _____

Stamp _____

Annex-G (Penalty Clauses & Payment Terms)

1. The successful consultancy firm is bound to make delivery of services within the delivery timelines mentioned in the contract. In case of failure then the procuring agency may cancel the contract and forfeit its performance security. The consultancy firm is bound to ensure services are in line with the scope of work and timelines mentioned in the contract, a grace period of 15 days is allowed for delays without penalties.
2. **Penalties for Non-Compliance:** Penalties for delays beyond the grace period: 2% maximum of total consultancy services charges / cost of Vulnerability Assessment & Penetration Testing of relevant site. **Notification and Cure Period:** PRAL will notify Consultant of non-compliance in writing. Consultant has 10 days to rectify issues before penalties apply.
3. Upon successful completion of deliverable against each assignment(s), the payment shall be made within 30 days after the submission of invoice. No advance payment shall be allowed against the assignments.
4. Any additional Cost/allied charges related to travelling, boarding, lodging etc. shall be borne by the bidder/Consultancy firm.
5. All the payment shall made in the PKR after the deduction of all applicable taxes



Annex – H (Declaration)

I, _____ hereby declare that:

- all the information provided in the technical proposal is correct in all manners and respects.
- and I am duly authorized by the Governing body/Board/Management to submit this proposal on behalf of "[Click here and type the name of organization]"

Name: -	
Designation: -	
Signatures: -	
Date and Place: -	



Annex – I (Cover Letter)

[Firm letterhead]

[Date]

To

Chief Executive Officer

[Address mentioned in Guidelines]

Re: Technical Proposal in respect of [Insert title of assignment]

Dear Sir,

We offer to provide the ISO 27001 consultancy services in accordance with your tender for Proposal dated [Insert Date of tender advertised]. We hereby submit our technical Proposal including the required documents.

We hereby declare that all the information and statements made in these proposals are true and accept that any misinterpretation contained therein may lead to our disqualification and forfeiting of our bid security. We undertake that we will initiate the delivery of services as per the client's request if our proposal is accepted. We understand that you are not bound to accept any or all proposals you receive.

Thank you.

Yours sincerely,



ANNEX-J (DRAFT AGREEMENT)

DATED _____ 2024

AGREEMENT FOR PROCUREMENT OF ISO 27001 CONSULTANCY SERVICES VERSION 2022 OR ABOVE

BETWEEN

Pakistan Revenue Automation Pvt Ltd

AND



ANNEXURE J: DRAFT CONTRACT

[To be on Rs. 100/- Stamp Paper]

The Contract for provision of professional ISO 27001 consultancy services (hereinafter referred to as “this Contract”) is made on this _____ day of _____, 1

By and Between

Pakistan Revenue Automation (Pvt) Limited, a company incorporated under the laws of Pakistan, having its registered office at 2nd Floor, Software Technology Park, Plot # 156, Service Road (North) Industrial Area, Sector I-9/3, Islamabad, which expression shall mean and include its successors-in-interest, executors and permitted assigns) of the one part;

And

M/s [●] having its office at [●] (hereinafter referred as “the Consultant”) of the other part;

Both PRAL and the Consultant may be collectively referred to hereinafter as “the Parties” and either of them individually as “Party”.

WHEREAS PRAL intends to engage the Consultant to perform the Scope of Services/Terms of Reference as defined in Clause 1.

AND WHEREAS the Consultant warrants and represents that the Consultant has necessary knowledge and relevant experience and capability to perform the Services in accordance with the terms of this Contract.

AND WHEREAS the Consultant has qualified through a competitive bidding processes conducted by PRAL and has agreed to perform and complete the required Services in accordance with the terms and conditions hereinafter set forth.

NOW THEREFORE, in consideration of the mutual covenants and contracts the Parties hereto, agree to the following terms and conditions:

1. Scope of Services/Terms of Reference

The Consultant shall perform its services as per the detailed Scope provided in Annexure-A hereof.

2. Payment Terms



2.1 The total price of the Contract is PKR XXXXX (Pakistan Rupees XXXXXX Only) (Contract Price) which is inclusive of all out of pocket expenses, applicable taxes & levies and is as per the break-up provided at Annexure A (Price Schedule) of this Contract.

2.3 No payment shall be made to the Consultant in advance as mobilization advance or on any other account.

2.4 Contract Price shall be payable, within thirty days, to the Consultant upon successful completion of each part of Scope of Services/Terms of Reference as per requirements and satisfaction of PRAL and receipt and acceptance of original error free invoices.

2.5 All payments shall be made online or through crossed cheque in Pak Rupees (PKR) in the favor of the Consultant.

2.6 Taxes will be deducted at source as per applicable laws at the time of payment.

2.7 The payment shall be made to the Consultant only when it is on the Active Taxpayers List (ATL) of FBR. If the Consultant is not in ATL at the time of processing of invoice, no payment shall be made until the Consultant appears in ATL of FBR.

3. Obligation of the Consultant

3.1 The Consultant undertakes and agrees that it shall perform the Services and carry out its obligations under this Contract with all due diligence, care, efficiency and economy and to the acceptable standards. The Consultant acknowledges and agrees that it shall, without incurring any additional cost to PRAL, be liable to re-perform and rework all or any part of the Services which are deficient in any manner. The Consultant shall always act, in respect of any matter relating to Services, as faithful advisor to PRAL and shall at all times support and safeguard PRAL legitimate interests in any dealings.

3.2 The Consultant agrees and undertakes that it shall upon completion of work related to its Services submit the same for PRAL approval. PRAL will give its approval within due time.



3.3 In case PRAL identifies any lack of compliance with the applicable laws or standards that could result in a legal claim against PRAL, and upon written request by PRAL, the Consultant undertakes and agrees to provide adequate proof of positive compliance with the concerned part of the applicable laws or standards at the earliest.

3.4 The Consultant undertakes and agrees with PRAL, its officers, employees, directors, consultants and advisors (the “PRAL Indemnified Persons”) that it shall keep the PRAL Indemnified Persons, both during and after the term of this Contract, fully and effectively indemnified and harmless against all losses, claims, damages, liabilities or expenses (including reasonable legal fees), suffered by the PRAL Indemnified Persons arising out of or in connection with this Contract or the Scope of Services/Terms of Reference to be provided by the Consultant, where such losses, claims, damages, liabilities or expenses is/are the result of the bad faith, gross negligence or willful misconduct of the Consultant, provided that the Consultant shall not be liable for indirect or consequential losses or damages; provided further the aggregate liability of the Consultant shall under no circumstances exceed twice the aggregate remuneration received by the Consultant from PRAL in terms of this Contract.

3.5 Delay in performance of Services beyond the lead time specified in this Contract may entail imposition of fine (liquidated damages) at the rate of 0.5% per day up and to a maximum of 10% of the total price of the Contract. This condition may be waived off by PRAL on its discretion or in case of force majeure which shall be proved by Consultant and supported by documentary evidence. Moreover, if the Consultant fails to complete the assignment within the time frame provided or if the liquidated damages amount reaches its maximum limit i.e. 10% of Contract price; PRAL, without prejudice to any other right of action / remedy it may have, reserves the right to terminate the Contract and forfeit performance guarantee(s).

4. Term & Termination

4.1 This Contract shall become effective upon signing by both the Parties and remain effective and valid for one (01) year. The Contract may be extended for another period of two (02) years on the same terms & conditions with mutual consent of the Parties.

4.2 Notwithstanding the foregoing, PRAL may without assigning any reason and at its sole and absolute discretion terminate this Contract at any time by serving on the Consultant fifteen days’ (15) prior written notice. Payment of the work completed by the Consultant, and accepted by PRAL, till serving such notice of termination shall be made to the Consultant.



5. Confidentiality

5.1 The Consultant agrees to hold in confidence for a period commencing with the signing date and ending five (5) years following the Term of this Contract, any information supplied to it by PRAL and designated in writing as confidential or which by its nature can reasonably be inferred to be confidential.

5.2 The Consultant further agrees to require its sub-consultants and employees to enter into appropriate nondisclosure contracts relative to such confidential information as may be communicated to them by the Consultant and / or the PRAL.

5.3 The provisions of clause 5 shall not apply to information within any one of the following categories:

- a. information which was in the public domain prior to a Party's receipt thereof or which subsequently becomes part of the public domain by publication or otherwise except by the receiving Party's wrongful act;
- b. information which the receiving Party can show was in the receiving Party's possession prior to its receipt thereof through no breach of any confidentiality obligation;
- c. information received by a Party from any other Person which did not have a confidentiality obligation with respect thereto; and
- d. other than as may be required by a Governmental Authority, and then only to the extent required, neither Party shall publish the terms and conditions of this Contract, unless the other Party provides its express prior written consent thereto.

6. Conflict of Interest

PRAL policy requires that Consultant provide professional, objective, and impartial advice and at all times hold the interest of PRAL paramount, strictly avoid conflicts with other assignments or their own corporate interests and act without any consideration for future work. Consultant has an obligation to disclose any situation of actual or potential conflict that impacts their capacity to serve in the best interest of PRAL. Failure to disclose said situations may lead to the termination of this Contract.

7. FORCE MAJEURE

7.1 For the purposes of this Contract, "Force Majeure" means an event or circumstance which is beyond the reasonable control of a Party, and which makes a Party's performance of its obligations under this Contract impossible, and includes, but is not limited to, war, riots, civil disorder, security risks, earthquake, fire, explosion, storm, flood or other adverse weather conditions, strikes, lockouts, other industrial action or any sanction or restriction imposed by any governmental



authority or body within or outside Pakistan which has a material adverse effect on the ability of the Consultant to carry out the Works/Services. Force Majeure shall not include:

- (i) any action or failure to take action by a Party;
- (ii) any event which is caused by the negligence or willful act or omission of a Party or that Party's Sub-Contractors or personnel or agents or employees; and
- (iii) any event which a diligent Party could reasonably have been expected both: (a) to have taken into account at the time of the Effective Date of this Contract; and (b) to have avoided or overcome in the course of carrying out its obligations under this Contract.

7.2 A Party seeking relief under this Clause shall notify the other Party forthwith of a circumstances or event of Force Majeure and shall furnish such relevant information as is available relating to such event.

8. Integrity Pact

8.1 The Consultant hereby declares that it has not obtained or induced the procurement of any contract, right, interest, privilege or other obligation or benefit from Government of Pakistan (GoP) or the PRAL or any administrative subdivision or agency thereof or any other entity owned or controlled by GoP through any corrupt business practice.

8.2 Without limiting the generality of the foregoing, the Consultant represents and warrants that it has fully declared the brokerage, commission, fees etc. paid or payable to anyone and not given or agreed to give and shall not give or agree to give to anyone within or outside Pakistan either directly or indirectly through any natural or juridical person, including its affiliate, agent, associate, broker, contractor, director, promoter, shareholder, sponsor or subsidiary, any commission, gratification, bribe, finder's fee or kickback, whether described as consultation fee or otherwise, with the object of obtaining or inducing the procurement of a contract, right, interest, privilege or other obligation or benefit in whatsoever form from GoP, except that which has been expressly declared pursuant hereto.

8.3 The Consultant certifies that it has made and will make full disclosure of all agreements and arrangements with all persons in respect of or related to transaction with the PRAL and has not taken any action or will not take any action to circumvent the above declaration, representation or warranty.

8.4 The Consultant accepts full responsibility and strict liability for making any false declaration, not making full disclosure, misrepresenting facts or taking any action likely to defeat the purpose of this declaration, representation and warranty. It agrees that any contract, right, interest, privilege or other obligation or benefit obtained or procured as aforesaid shall, without prejudice to any other rights and remedies available to the PRAL under any law, contract or other instrument, be voidable at the option of the PRAL.



8.5 Notwithstanding any rights and remedies exercised by the PRAL in this regard, the Consultant agrees to indemnify the PRAL for any loss or damage incurred by it on account of its corrupt business practices and further pay compensation to the PRAL in an amount equivalent to ten times the sum of any commission, gratification, bribe, finder's fee or kickback given by the Consultant as aforesaid for the purpose of obtaining or inducing the procurement of any contract, right, interest, privilege or other obligation or benefit in whatsoever form from the PRAL.

9. Miscellaneous

9.1 Any dispute or difference between the Parties as to matters arising from, related or pursuant to this Contract which cannot be settled amicably within thirty (30) calendar days after receipt by one Party of the other Party's request for such amicable settlement, may be referred to arbitration for settlement under the Arbitration Act, 1940 and the rules made thereunder by sole arbitrator to be appointed by the Parties. The arbitration shall take place in Islamabad. The proceedings shall be held in the English language. The resulting award shall be final and binding on the Parties and shall be in lieu of any other remedy.

9.2 This Contract may be amended by a mutual contract / consent between the parties. All such amendments shall be in writing signed by the duly authorized representatives of the Parties.

9.3 Any notice or request required or permitted to be given or made under this Contract shall be in English language. Such notice or request shall be deemed to be duly given or made when it shall have been delivered by hand or through electronic mail, registered mail or courier on the following address:

PRAL	Consultant
[Name of Representative]	[Name of Representative]
[Designation]	[Designation]
Land-line number:	Land-line number:
e-mail address:	e-mail address:
Address:	Address:

9.4 The Contract shall be governed by and interpreted in accordance with the laws of Pakistan as amended from time to time.

IN WITNESS whereof the Parties hereto have caused this Contract to be executed in accordance with the laws of Pakistan as of the day, month and year first indicated above.



For and on behalf of

PRAL

[Name of authorized signatory]

[Designation]

For and on behalf of

Consultant

[Name of authorized signatory]

[Designation]

Witness 1:

Witness 2:



APPENDIX A

Scope of Work

1. FBR Data Center Site A, FBR House, Constitution Avenue, Sector G-5, Islamabad
2. FBR Data Center Site B, PRAL HQ, KSL Software Technology Park, I-9/3, Islamabad
3. FBR Data Center Site C, Custom House, West Wharf, Karachi
4. PRAL HQ (All Departments), KSL Software Technology Park, I-9/3, Islamabad
 - 4.1. Software Development Department
 - 4.2. Operations Department
 - 4.3. Services Department
5. AEOI Center, FBR House, Constitution Avenue, Sector G-5, Islamabad
6. AEOI Secure Room, AEOI zone Islamabad, Evacuee Trust Complex, Sector F-5/1, Islamabad
7. AEOI Secure Room, AEOI Zone Lahore, 58-A / C-III, Gulberg III, Lahore
8. AEOI Secure Room, AEOI Zone Karachi, PNSC Building, Molvi Tamizuddin Khan Road, Karachi

APPENDIX B

Financial Format, Payment Terms & Delivery

APPENDIX C

SDLC and ISO Documentation Templates

This appendix provides standardized templates for SDLC documentation. Bidders should utilize these templates to ensure uniformity and compliance with PRAL's documentation requirements. The following templates are included:

1. Risk Assessment Template: A template to identify, assess, and document risks associated with each phase of the SDLC. Includes sections for risk description, likelihood, impact, and mitigation strategies.
2. Security Compliance Checklist: This checklist ensures compliance with ISO 27001 and internal security policies across SDLC phases. Sections include policy adherence, data protection measures and access control validations.
3. Testing and Quality Assurance Report Template: Provides a structured format for documenting test cases, outcomes, identified issues and corrective actions during the testing phase. Supports traceability and accountability in QA efforts.



4. Deployment and Maintenance Logs: Used to document deployment details, including configuration changes, system setup and ongoing maintenance activities. Supports consistent post-deployment security and functionality.