Request for

Expression of Interest (EoI)

FOR "AUTOMATED DATA PROCESSING (ADP) AUDIT OF PRAL"

Federal Board of Revenue invites eligible Private and Public Sector, IT Organizations or Professionals, who are well reputed for Undertaking System/IT Audits for Quality Assurance.

FBR now invites eligible Consulting Firms having **C**ertified **I**nformation **S**ystems **A**uditor **(CISA)** and **C**ertified **I**nformation **S**ecurity **M**anager **(CISM)** credentials from the **I**nformation **S**ystems **A**udit and **C**ontrol **A**ssociation **(ISACA)** and at least five years of relevant work experience with specialized skills in auditing information systems.

Interested Consulting Firms must submit Expressions of Interest (EOI) for the above assignment and provide information indicating that they are qualified to perform the services by submitting brochures or brief documentation depicting the description of similar assignments, qualifications, certifications, references along with details of consultancy of similar services provided to other clientele in similar conditions, availability of appropriate skills among staff, etc.

Each Expression of Interest (EOIs) must clearly mention the name of the Consulting Assignment on the envelope. If firms are submitting EOI in a Joint Venture, then the experience and capacity of both the firms will be evaluated.

This hiring process will be in accordance with the procedures set out in Procurement of Consultancy Services Regulations, 2010. Interested Consultants may obtain further information regarding Terms of Reference (ToRs)/ Scope of assignment posted from FBR's Website at www.fbr.gov.pk/tenders or email at adeela.bukhari@fbr.gov.pk or visit the office of Chief-IT, Room No 142, First Floor, FBR House, G-5, Constitution Avenue, Islamabad between 0900 hours to 1600 hours on any working day.

The Expression of Interest must be delivered to the address below not later than 1500 hrs on **14th December, 2018**; no EoIs will be accepted thereafter.

Syeda Adeela Bokhari

Chief (Information Technology)

Room No. 142, FBR House, G-5, Constitution Avenue, Islamabad

Tel: 051-9202999

TERMS OF REFERENCE
FOR CONSULTING FIRM FOR AUDIT OF FBR –PRAL IT SYSTEMS

Introduction and Background:

PRAL is a Private Limited Company 100% owned by FBR governed by SECP Public Sector Companies (Corporate Governance Rule) 2013 read with Companies Ordinance1984 and PRAL Rules-2014. FBR and PRAL have been working together since 1994. PRAL is rendering its services in all spheres of Information Technology to FBR. These services include development of new software's systems, maintenance of existing systems and applications, continuing operational support at various locations of FBR throughout the country.

Systems Audit of PRAL was conducted back in year 2013 and again World Bank conducted System Analysis of its various systems and applications including IRIS, WEBoC, STRIVe, and several reports on FBR/PRAL systems were generated in 2016.

Protecting the information from disclosure to unauthorized parties data confidentiality, integrity and its availability to FBR Operations is one of the many duties of PRAL and Data security is required to protect personal information's of taxpayers from being modified by any unauthorized parties.PRAL assists FBR in provision of technical assistance wherever ICT related issues are involved.

FBR has developed ICT systems for e-Filing of Income Tax Returns and Web-enabled One Customs (WeBOC) for electronic cargo clearance. The said initiatives were taken to enhance trade facilitation and Ease of Doing Business. However to continuously improve our systems we conduct regular system Audits. Therefore to ensure the reliability and efficiency of the systems in place this audit is proposed to conduct detailed **A**utomated **D**ata **P**rocessing **(ADP)** Audit ofPRAL.

Keeping in view the substantial role of PRAL audit is obligatory as accountability check to increase efficiency. Audit will be conducted in accordance with **Procurement of Consultancy Services Regulations, 2010**. FBR is already working on improving its data basis but this Audit will help FBR to follow the right path for achieving quality, reliability, accuracy, security and completeness of its data basis

Purpose and Scope of the Consultancy

Objective:

The objective of the intended assignment is to conduct a forensic audit of the ICT systems of FBR for quality assurance through testing by qualified professionals.

The System Audit is to ensure the quality of systems installed, to know that they are following the required data security and design protocols, have proper rules for data governance and data strategy in place and if not what should be in place.

It is meant to analyze that the systems in place are capable, for complete automation and integration of all FBR's business processes? The Audit Team is expected to analyze the PRAL's capability and HR management to carry out the day to functions; its technical governance model; software development protocols; IT-infrastructure available and security mechanisms for systems and operational functionality of systems etc.

The Systems Audit will identify the strengths and weaknesses of the systems so that appropriate corrective measures can be taken.

Scope of Services:

The scope of work includes forensic auditing aimed at assuring the quality of the ICT Systems to check any vulnerability against data breaches or system hacking and acquiring general perception about the integrity and security of FBR's ICT systems. This also includes identification of the degree of changes/ improvements occurred between the time period of any previous System audit and the intended one FBR therefore will provide the Consultants with the Organizational access to its ICT systems and related data that is required to conduct this activity the firm will focus on:

i) System Audit of FBR's ICT Systems in terms of existing functionalities
ii) Frame proper rules for data governance and data strategy
iii) Chart down recommendations for risks compliance mechanisms and controls
iv) Complete ii) Analysis of System Databases for seamless integration with each other.
v) Security Checks with the System data
vi) Analyze the PRAL's capability and HR management to carry out the day to functions, its technical governance model
vii) software development protocols
viii) identify the strengths and weaknesses of the systems
ix) Preparation of Final report

Relationship between FBR and PRAL

PRAL is a technical service Provider to FBR since 1994. PRAL does not have IT-Infrastructure of its own. It is utilizing FBR's data centers, servers, storage to provide services to other Revenue Authorities of provinces including AJK and GB. The Audit will also determine the capacity of FBR's Data Centers'.

The proposal for upgradation of Data Centers; to Active Active Cloud based Data Center for FBR is already under implementation.

The Teams will assess PRAL's capability to generate financial statements. Can PRAl Teams ensure adherence to applicable laws, policies and standards related to IT, and finally evaluate their performance viz a viz operations. The Teams will point out any leakages, excesses, or wastages. The teams are also required to analyze the system design; security, availability; risk compliance mechanisms and whether proper controls are in place or not.

The Audit teams will also analyze the contractual relationship of FBR and PRAL and spot the loopholes in Services viz a viz remuneration; agreed Minimum Standards of Deiivery and their Performance; are there any deductions; penalties for not doing what is required.

How SLA between the 2 parties can be improved to ensure responsibility at both ends.

PRAL's Technical Governance

The audit should also determine the following:

1. Whether PRAL follows international best practice in its technical governance.
2. Whether PRAL has prepared comprehensive Standard operating Procedures (SoPs) for operations, support, maintenance, training, etc.; whether such SoPs are formally signed off by FBR; whether such SOPs are periodically reviewed and updated.
3. Whether PRAL has prepared checklists or guides for database administration, specifying tasks to be performed on daily, weekly or monthly basis.
4. Whether PRAL has developed a database backup system, including a coverage model which specifies what, when and how of back up and provides for periodic verification of restorability and usability of backup.

Application Software

The audit should also determine the following:

1. Whether sufficient and relevant technical expertise is available for sustainable development of IT solutions.
2. Whether software development lifecycle is defined, documented, formally approved and actually applied for each software applications.
3. Whether complete and comprehensive documentation, including architecture, database structure, communication protocols, naming conventions, etc., are prepared for each software applications; and whether such documentation is continuously updated and synchronized with the actual software application.
4. Whether international best practices are followed for software development.
5. Whether functional specifications of each software application have been prepared by technical personnel alone or in consultation with business personnel.
6. Whether formal and appropriate revision / change control mechanism has been implemented; whether such mechanism evaluates all change requests to determine their appropriateness and priority; allows to keep track of each revision / change to the source code and to create development branches and versioning
7. Whether Quality Assurance policy has been defined, documented and known to all.
8. Whether Quality Assurance mechanisms to reduce incidence of bugs, ensure alignment between the specifications and client's needs, decrease coding complexity, etc. have been practically implemented;
9. Whether the systems apply adequate and appropriate data validations/checks to ensure quality (completeness, validity, accuracy and consistency) of data; whether the architecture, database model and storage procedures prevent of transactional systems prevent data:" duplication / redundancy. The auditor should review the data entry process of declarations, refund requests and other documents to verify that numbers are in the correct range, that negative numbers are not entered, that all numbers are correctly calculated, that the required fields 'cannot be left empty, etc. If it is possible to enter incomplete, invalid and inaccurate data, complete list be provided.
10. Whether the systems have redundant data sources; if yes, a comprehensive inventory of such data sources, their use and extent and severity of differences among the data sources be provided; whether amechanism has been devised and practically and effectively applied to maintain integrity in these redundant data sources.

11. Whether the software applications, IRIS, ITMS, STRIVe, CREST, and WEBoC, are end-to- end, integrated solutions in true sense; whether these have been developed according to functional specifications documents which outline end-to-end, integrated solutions; if not, what is the extent and gravity of deviation from functional specifications documents?
12. Whether entire business cycles of Inland Revenue and Customs have been automated; If not, what. is the extent and gravity of incompleteness (comprehensive list of leftover business processes be provided).
13. Whether any of the automated business processes is outdated, invalid, and illegal or does not correspond to the actual operations. The audit should include interviews with statistically: significant portion of operators and users to determine and document all such processes.
14. Whether a mechanism for managing changes/revisions in business processes authorization, propriety, timing and tracking) is in place;
15. Whether business integration, data. Integration and system integration have been effectively achieved. (Business Integration refers to integration of the business processes; Data Integration refers to separate systems using the same data sources; and Systems integration refers to a single integrated system performing all functions).
16. If not, whether at least data integration strategy has been prepared to identify which systems require what data Sources;, what types of protocols and mechanisms should be used to "access, that data; and which systems need read-only access to data and which systems require modification rights of data

IT-Infrastructure

The audit should also determine the following:

1. Whether adequate and appropriate infrastructure (servers, backup systems, standby servers, disk arrays and network storage system, routers, hubs and switches, firewalls, bandwidth control systems and network monitors andnetwork diagnostics equipment). is available to operate the systems, including all provisions necessary to cnsurc thc sustainability of the operation of these systems.
2. Whether the infrastructure is properly inventoried, containing all relevant details, such as technical specification, deployment date, warranty period and expected lifetime.
3. Whether the infrastructure is professionally managed i.e critical servers and key

network services have appreciate hardware redundancy/failure contingency plan which allow continuing operations even after critical hardware failures; fault prone components for critical servers (power supplies, processors, disk drivers, router, firewalls, etc) are timely identified and corrected ; servers and critical network component are housed in an controlled environment; servers and critical network components are physically in accessible by unauthorized personnel and administrative personnel, senior management, cleaning crews, general maintenance personnel, etc. do not have unrestricted access.

Data Warehousing & Data Mining

The audit should also determine the following:

1. Whether all databases are appropriately documented; whether the documentation is accurate, current, and actually used by developers; whether the documentation is available to data analysts; whether the documentation corresponds to actual physical data representation; whether the documentation includes clear instructions about the mechanisms to be used to populate or extract data from the data source.
2. Whether data warehouses are properly designed, have appropriate data models and are well documented.
3. Whether data warehouses provide the amount and quality of data required by data analysts.
4. Whether these data warehouses are sustainable and are periodically updated from transactional systems.
5. Whether data warehouses 're capable of producing reports / information required by different management levels; The audit should include interviews with statistically significant portion of operators and users to determine and document all cases where reports/ information are inaccurate, incomplete, late or are not produced at all.
6. Is there any mechanism for collating Big Data from other sources for detecting tax frauds?
7. Whether Data Science, Predictive analytics capabilities exists in PRAL if not how can they be developed, what tolls are required

Security

The audit should also determine the following:

1. Whether a security model has been defined and documented; whether actual/perceived, internal/external threats to data/systems/infrastructure, have been accurately and comprehensively identified; whether a mechanism to protect data / systems / infrastructure against such threats has been efficiently and effectively implemented; and whether the said mechanism is regularly updated to match ever-changing threats.
2. Whether Operational risk assessments have been defined and documented; whether such risk assessments are periodically performed; and whether the results are fed back into the security model.
3. Whether a mechanism to deal with non- repudiation of transactions (where external or internal users cannot claim non-performance of a particular function) has been efficiently' and effectively implemented.
4. Whether a comprehensive patch arid upgrade control system for all servers, operating systems, databases and other critical third-party components has been implemented, except where management has specifically waived this requirement for backwards compatibility; if not a complete list, where patches and upgrades are not performed, be provided.
5. Whether viruses and Trojan horse controls are in place in servers, if not a complete list of servers which do not have viruses or Trojan horse controls be provided.
6. Whether adequate and effective security measures have been implemented to protect source code of all the software applications and databases from unauthorized access, modification, insertion; if not, whether it is possible to identify how, when and by whom such unauthorized access, modification, insertion was made; whether it is possible to add anonymous / camouflaged / untraceable malicious code, in the source code.. A complete list of all the software applications and databases which are vulnerable be provided.

Expected Deliverables

The audit should produce a detailed 'report of the findings for all the evaluations noted above in accordance with International Best Practices. All identified deficiencies must be supported

by evidence and examples and must be classified as minor, substantial or critical on the basis of relative importance. The payments are subject to acceptance of deliverables by Client.

Methodology & Activities

The Firm will develop methodology

- To develop methodology for penetration testing
- To develop auditing instruments
- To conduct a forensic audit of ICT System for quality assurance.

Period of Service

The Firm will complete the assignment in 4 months time

Expected Output:

i. **Inception ICT Audit Report PRAL**

Inception report for the study will be provided. This will include information on methodology, work plan and penetration testing methods

ii. **Interim ICT Audit Report PRAL**

Interim report for the study will be provided. These will include information on initial findings.

iii. **Draft Final ICT Audit Report PRAL**

Draft final report for the testing/audit will be provided.

iv. **Final ICT Audit Report PRAL**

Final report for the study will be provided at least two weeks prior to the end of the project.

Report will be reviewed and approved by the FBR research team and relevant technical wings of FBR to ensure that the assignment is complete in every respect and the best standards are met.

Consultant Firms shall clearly specify the timings of the submission of the report in their respective project schedules.

Qualifications of Firm

The interested consultants shall be a tax registered national management consultancy firm or an international management consultancy firm compliant with applicable regulations of Pakistan for this procurement and should have been incorporated for at least five, (5-7) years

for offering similar services and have completed five (5) similar projects of this scale and complexity and in comparable organizations. We expect that the ICT System audit will be managed by qualified and experienced senior professional. Team leader is required to hold at least MS degree in computer sciences and certifications in CISA, CISM accredited from ISACA with at least 05 years of professional forensic auditing experience in public sector and private sector institutions

Consultant should possess good knowledge of all concepts, principles and approaches required for assignment. The firm should provide details (documentary evidence e. g. contract award or reference letter from the clients stating scope of services and deliverables) of all such projects for the last 5 years or more during which they were completed. In case, of joint venture, the details of such projects will be provided separately as lead or associated consultant.

Should propose adequate approach, methodology & work plan for timely and effective completion of assignment. This particular parameter will be confirmed through a presentation to client.

Firm should have staff with adequate education, qualification and experience in area IT efficiency reviews. These staff member should possess IT relevant certifications or any other certifications but relevant to the scope of this procurement.

Indicative composition of team which may be proposed by consultants:

S.No	Position	Qualification & Experience	Number
1	Team Leader/IT Specialist	Master's Degree in Computer Science- IT, **C**ertified **I**nformation **S**ystems **A**uditor **(CISA)** and **C**ertified **I**nformation **S**ecurity **M**anager **(CISM)** credentials from the **I**nformation **S**ystems **A**udit and **C**ontrol **A**ssociation **(ISACA)** and 5-7 years of relevant work experience. Individuals/organizations with specialized skills in auditing information systems will be preferred.	One
2	IT Infrastructure Auditor	Master's Degree in Computer Science- IT, **C**ertified **I**nformation **S**ystems **A**uditor	One

		(CISA) and **C**ertified **I**nformation **S**ecurity **M**anager **(CISM)** credentials from the **I**nformation **S**ystems **A**udit and **C**ontrol **A**ssociation **(ISACA)** and 5-7 years of relevant work experience. Individuals/organizations with specialized skills in auditing information systems will be preferred.	
3	IT Coordinators	Master's Degree in Computer Science- IT, **C**ertified **I**nformation **S**ystems **A**uditor **(CISA)** and **C**ertified **I**nformation **S**ecurity **M**anager **(CISM)** credentials from the **I**nformation **S**ystems **A**udit and **C**ontrol **A**ssociation **(ISACA)** and 5 years of relevant work experience. Individuals/organizations with specialized skills in auditing information systems will be preferred.	Two

Relationship between FBR and Consultants:

The Consultants hired will work at FBR headquarters. The relationship between the Consultants and Management will be professional.FBR is not expecting any academic research paper but it expects that at the end of the assignment the consultants come up with precise objectives of the study, with concrete suggestions, recommendations, action plan with timeline as how those objectives can be achieved. All information and facts collected by the consultants will remain confidential and the work completed for which the agreed remuneration paid will be the copy right and intellectual property of FBR.

Selection Method:

A consultant will be selected in accordance with the Selection Based on Consultants Qualification method set out in **Procurement of Consultancy Services Regulations, 2010**.

Coordination

For all activities and clarifications under these ToRs the Consultant will coordinate with IT-Wing of FBR & PRAL.

Code of Conduct & Professional Ethics

i. **Services:**

- Performs his/her assigned duties with responsibly as per ToRs.
- Complete the tasks within given timeframe.
- The reports generated shall be based on facts and not on assumptions.
- Confidentiality of access to any data for analysis purpose shall be maintained.

ii. **National Interest:**

- Keep the interest of state, society and fellow citizens supreme in the discharge of duties and never compromise on the purpose of assigned tasks for any personal gains.
- Promote confidence in the integrity of the public service and the profession.
- Conduct business (on-site survey) in accordance with laws and regulations of the government.

iii. **Ethical and Professional Conduct**

- Maintain impartiality. Fairness and transparency at all levels.
- Give valid reasoning for recommendations.
- Communicate with clarity.
- Develop and maintain constructive professional relationships with FBR.
- Abstain from making malicious or false statements about any person or institution.
- Refuse gifts, favors or benefits of any.
- Report all incidents of outside influence immediately to the FBR Administration.

iv. **Leadership:**

- Act as a positive role model.
- Be open and accept differing views and perspectives.
- Discharge responsibilities conscientiously and prudently.
- Promote participatory decision-making.
- Respond appropriately to issues of inefficiency.

v. **Efficiency and Effectiveness**

- Value all the resources provided for conducting your assigned tasks, achieve high level outcomes.
- Be punctual and complete the assignments as per the decided schedule.
- Avoid using personal mobile phone during meetings, and discussions keep your cell phones on silent mode

vi. **Discrimination and Harassment**

- Ensure equality and freedom, and prevent discrimination on the basis of religion, sect, race, cast, social status, culture and region.
- Encourage women participation through a harassment-free and conducive work environment.

vii. **Political Affiliation**

- Avoid political discussions
- Do not issue statements in favor of or against a body or forum which identifies itself as a political entity.

viii. **Responsiveness**

- Exhibit commitment, zeal, enthusiasm, innovativeness, dignity and professionalism in discharge of assigned responsibilities.
- Take responsibility if any mistake/error (made intentionally or unintentionally)