Federal Board of Revenue
Pakistan Raises Revenue Project

TERMS OF REFERENCE

Selection of Chief Information Security Officer

Background and Objectives

Federal Board of Revenue is implementing the Pakistan Raises Revenue Project with the assistance of the World Bank. The objective of the project is to contribute to a sustainable increase in domestic revenue by broadening the tax base and facilitating compliance. PRRP comprises two components: Component-1 (US$ 320 Million): Result-based components and Component-2 (US$ 80 Million): Investment Project Financing.

The FBR (IT Wing) under the Program is looking to procure the services of the subject Consultant(s) as per below given key requirements/ deliverables.

Scope of Services

The consultant is required to complete (including but not limited to the) following tasks:

- Develop and improve FBR and Customs nation-wide information security governance, risk and compliance (GRC policy framework, process, procedures and deliverables by leading and managing the FBR IT GRC team-members and related key performance indicators within in the ISO 27001 framework.
- Exercise periodic risk and compliance checks within all domains of the FBR nation-wide information security governance, risk and compliance (GRC) program including:
    a. Information and cyber security threat and risk assessment
    b. Information and cyber security risk remediation, governance and tracking reports to IT Wing
    c. Define the assets in the scope of the information security program
    d. Access Control and Multi-Factor Authentication
    e. Network security
    f. Application security
    g. Infrastructure security
    h. Databases and data storage security
    i. IT disaster recovery planning
    j. Information security service provider management and compliance
    k. Information Security Testing and Tracking the Remediation of Findings
    l. Human resource security
    m. End-user security awareness program
    n. IT administrator security awareness program
    o. Operational security
    p. Physical and environmental security of paper media and buildings/facilities
    q. Confidentiality, integrity, availability, authenticity, and non-repudiation
- Develop and improve FBR cyber-SOC operations (SIEM, SOAR, EDR, WAF etc.) by leading and managing the FBR cyber-SOC team-members and related key performance indicators.
- Develop and improve the tools, service providers, team-members and processes of vulnerability scanning, penetration testing, source code testing, disaster recovery testing, anti-malware solutions, security event logs monitoring solutions and incident response solutions and service providers.
- Communicate the comprehensive information security risk posture to FBR IT Wing periodically.
- Participate in the technical evaluation of new products, projects and upgrades with the objective of improvement to the FBR information security posture and emerging threats.
- Compliance and governance of the information security program of FBR's external service providers e.g., PRAL.

Required Deliverables with Timelines:

Sr.	Deliverable	Timelines
1.	Inception Report	Within15 days from the date of joining
2.	Fully direct and lead the teams and tools for information security GRC, SOC, SIEM, SOAR, penetration testing, vulnerability management, source code testing and multi-factor authentication	From the date of joining
3.	Manage, track and report on the remedial efforts against the information security risks e.g., project deployments, configuration fine-tuning, incident response etc.	Monthly
4.	Conduct information security threat and risk assessments	Quarterly
5.	Conduct and report information security risk posture measurement	Quarterly
6.	Justify procurement requests for information security	As and when required, based on risk assessments or incidents
7.	Participate in evaluations and licenses being procured for information security improvement	As and when required
8.	Deliver information security awareness sessions to end-users and IT administrators	Quarterly

Qualifications and Experience

- University degree (at least 16 years of education) degree in information technology, or in a related field from a reputable University.
- Overall experience of at least 10 years having worked in Information Security in reputable organizations.
- Documented experience as Chief Information Security Officer for a minimum of three years.
- At least one international information security certification (CISSP, ISO 27001 or equivalent) is mandatory.
- Experience of having managed SOC, GRC, and Security Testing Teams.
- Experience of developing/ reviewing Business Continuity and Disaster Recovery Plans for reputable organizations.
- Must have sound knowledge of technology solutions used in Information Security, such as NGFW, WAF, EDR, Pen Testing, Source Code Testing, MFA, Email and Web Security Gateway, Vulnerability Management Tools, AVDF, VPN, SSL etc.
- Excellent logical, interpersonal, communication (both oral and written) and analytical skills.

Selection Process

An individual consultant will be selected in accordance with process stipulated in accordance with "World Bank: Procurement Regulations for Investment Project Financing Goods, Works, Non-Consulting and Consulting Services" (July 2016) revised November 2017 & August 2018.

EXPRESSION OF INTEREST FORM
(INDIVIDUAL CONSULTANTS)

1. **Position Applied for**: _____

2. **Name**: _____

3. **Current Residential Address:** _____

   Telephone/ Mobile No.: _____ **E-Mail Address:** _____

4. **Date of Birth**: _____ **Citizenship**: _____

5. **Education** [Bachelor and above only in reverse chronological order] [*Indicate college/ university and other specialized education giving names of institutions, degrees obtained, and dates of completion/ obtainment*] [most recent first]:

Degree	Major Subjects	Name of University	Division/ Grade	Passing Year

6. **Membership in Professional Associations**: _____

7. **Other Trainings/ Certifications** [*Indicate significant and relevant trainings/ certifications only since completion of requisite qualification(s)/ degree(s) as mentioned under "Education"*]:

Title	Institute	Year	Please indicate whether it is a Workshop/ Diploma/ Certification/ Training Cource or else	Local/ Foreign (If foreign, please write country name)
			Example; Workshop	

8. **Countries of Work Experience**: [*List countries where applicant has worked in the last ten years*]:

9. **Employment/ Consultancy Record** [*Starting with the present/ last position, list in reverse chronological order every employment held by applicant since graduation*]:

Dates of Employment		Employer/ Consulting Organization	Position Held	Supervisor Name & Designation	Employer Contact (Email/ Mobile/ Phone)
From	To				

10. **Specific Experience** [For each of key assignment that best demonstrates your suitability for this position, fill the below columns]:

	A) Assignment(s) Undertaken that Best Illustrates Applicant's Capability to Handle the Responsibilities/ Scope of Services as Required in/ by the TOR [*Among the assignments in which the applicant has been involved, indicate the following information for those assignments that best illustrate the applicant's capability to handle the tasks respecting the TOR vis-à-vis Employment/ Consultancy Record as listed under No. 9 above*]	**B) Detailed Tasks Assigned** [*List all tasks performed by applicant under this assignment; please also indicate the level of involvement and responsibility*]
	Name of assignment or project: _____ Client/ employer: _____ *(Government/ Semi Government/ Provincial Government Organization, Private Organization, International Organization, Local or International Donor Agency etc.)* Main project features: _____ Position(s) held: _____ From (Month/ Year): _____ to (Month/ Year): _____ Activities performed: _____ (Including nature and level of services performed/ delivered)	**Total Volume/ Value and Duration of the Project (where applicable):**

NOTE: Please be specific.

11. Certification:

	Yes	**No**
I, the undersigned, certify to the best of my knowledge and belief that this form correctly describes my qualifications and my experience	☐	☐

I understand that any willful misstatement described herein may lead to my disqualification or dismissal, if engaged.

(Please just write your full name with CNIC No) Date: _____

Signature of Applicant (Day/ Month/ Year)