THE HASHEMITE KINGDOM OF JORDAN

TELECOMMUNICATIONS REGULATORY COMMISSION (TRC)

Tender No. /2021

Consultancy Services to support TRC obtaining "ISO27001:2013" Certification

خدمات استشارية لحصول الهيئة على اعتمادية (ISO27001:2013)

Deadline for submission of Bids is Hrs. of / /2021

Deadline for purchasing the Tender documents is Hrs. of / /2021

Request for Proposals (RFP)

Consultancy Services to support TRC obtaining "ISO27001:2013" Certification

خدمات استشارية لحصول الهيئة على اعتمادية (ISO27001:2013)

Introduction

The Telecommunications Regulatory Commission (hereinafter called **TRC**) is looking for a professional consulting entity ("the Firm") to provide it with professional services leading TRCs' Data Centers to be certified with ISO 27001:2013 standard for which this Request for Proposals (RFP) is issued.

TRC invites Auditing/specialized Firms/company to provide TRC with a Technical and Financial Proposal for the project: **ISO27001 TRC JORDAN.** More details about the required tasks are included within this document.

For all required technical aspects and clarifications during the mandatory site survey stage, the bidder can contact directly to the Head of Cyber security Section;
Mr. Narret Koff, Telephone: 06-550 11 20 Ext. (2330), e-mail narret.koff@trc.gov.jo, noting that contract conditions and financial proposals must not be discussed at this stage.

The RFP includes the following sections:
Section I: **Terms of Reference**
Section II: **Instructions to Service Providers / Consulting Firms**
Section III: **Technical Evaluation**
Section IV: **Financial Evaluation**
Section V: **Payment Conditions**
Section VI: **General Conditions**

All Proposals must be delivered by hand to **TRC** (Procurement and Purchases Section) at the following address and during office hours (8:30 AM to 3:30 PM) from Sunday to Thursday:

Bayader Wadi Al Seer District, Deir ghbar Area, Extension of Alshaheed Mohamad Al Zoghoul Street. Building No (13), Telephone: (962 6) 5501120 ext. (2750)

Section I: Terms of Reference

1. Executive Summary

The purpose of this Request for Proposal (RFP) is to request proposals from a qualified firm of ISO27001 information security services and audit of the **"TRC's Data Center and ASMS Server Room"** which are located in Amman, Jordan.

Further, the Firm shall provide onsite advisory and support to the **TRC** throughout the course of formal assessment to be conducted by a Certification Body. The scope of service is detailed in this document.

2. Organization information

The Telecommunications Regulatory Commission (TRC) was established by means of the Telecommunications Law No. 13 of 1995, and its amendments as an independent jurisdictional body tasked with regulating the telecommunications and information technology sectors.

In accordance with the Telecommunications Law No (13) of 1995 and its amendments, The Commission shall undertake according to **Article (6/i/3)** "Maintaining the civilian portion of the National Plan for Frequency Allocations and the National Register of Frequency Assignments, and publishing them to the public". In addition to that, The Commission shall undertake according to **Article (6/L)** "To grant Type Approvals and to regulate the import and usage of Telecommunications Terminal Equipment required for individual and private uses, or for use in specific zones, and to monitor such usage".
In this regard, **Article (59)** of Telecommunications Law directed TRC in the way that:

The Commission shall verify the
Licensees' compliance with the License conditions and the provisions of the Law, and may take any actions it deems appropriate for this purpose, including:

a) Conducting a physical on-site inspection of network locations and Telecommunications equipment.
b) Examining the Licensee's technical records and ensuring that sound and accurate systems are being used for issuing invoices.
c) Ensuring the standard of service provided to Beneficiaries and their complaint.
d) Reviewing the Licensee's records of maintenance and defects to ensure the efficiency of the service management.

3. Project Background

TRC intends to engage a Consulting FIRM/company for Implementation of Information Security Management Systems (ISMS) at **"TRC's Data Center and ASMS Server Room"** in DEIR GHBAR/AMMAN as per ISO 27001:2013 including IT Security Audits, and ISO 27001:2013 Certification through an Accredited Certification Body as per Terms and Conditions detailed in this Tender Document.

4. Requirements

The following are required under this project.

4.1 Consultancy Services

Proposed services should include, but are not limited to the following:

- Perform a gap analysis in order to assess and evaluate the controls to be implemented to achieve ISO 27001:2013 certification and accreditation.
- Review existing systems at **TRC** pertaining to security controls, policies, processes and any other established procedures on managing risk and improving information security to deliver results in accordance with the organization's overall policies and objectives.
- Apply the PDCA cycle for ISMS implementation, and shall include all Documentations, Reports, findings & Evidences.
- Review and validate the list of information assets of **TRC**, its ownership, classification of assets and prepare information asset registers.
- Review the risk assessment, identify risk, controls and remediation plans and propose changes if required.
- Review **TRC**'s Risk Assessment Methodology appropriateness to meet ISO27001 requirements for risk identification, mitigation and treatment and propose changes if required.
- Review the current Organizational Structure and advise/modify to create an environment where policies, procedures, plans, strategies and processes to manage and monitor regulatory, legal, risk, environmental and operational requirements are understood and inform the management of security risks following the GRC platform.
- Define all ISO 27001:2013 roles and responsibilities and mapping them to existing business departments or positions according to the approved Organizational Structure.
- Define and develop required information security policies and procedures for **TRC**.
- Define and create an evaluation method and metrics of the ISMS and the implemented controls. The plan should:
    - Describe the goal of measurement objective;
    - Define methods of collecting performance data;
    - Define the frequency and method of monitoring;
    - Define performance metrics, KPIs and dashboards for implemented security controls.
- Conduct ISO 27001:2013 awareness sessions to **TRC** staff.
- Propose any future recommendations to the TRC with any new security concerns.

4.2 Internal Audit Service

The formal assessment/ certification will be performed by an independent team that did not participate in the ISMS implementation. Activities during the onsite formal assessment should include, but are not limited to the following:

- Assess the ISMS and related activities, processes, procedures and documentations.
- Conduct an internal audit by an independent team that did not participate in the ISMS implementation.
- Assist the **TRC** team and provide consultancy on the Risk Treatment status, closure of Internal Audit findings, and other matters prior to the certification.
- Benchmark against the ISO 27001:2013 standard and identify any non-conformity.
- Provide assistance and support on remediating all non-conformities, including the revision of all necessary documentation.
- Any observations which may lead to noncompliance to ISO 27001:2013 should be advised to **TRC** team immediately and confirmatory testing should be completed after fixing of the observation. As many iterations of audit may be performed as required to get the required compliance to ISO 27001:2013.
- The Service Provider/ Firm shall include all required security awareness sessions for the involved personnel from **TRC through a recognized platform such as but not limited to LMS.**

4.3 Onsite Support during Formal Assessment

The Service Provider/ Firm shall be engaged with **TRC** for period of (1) year. It includes ISO 27001:2013 Certification through an Accredited Certification Body (which would be decided by the bidder in consultation with **TRC**) from the date of signing the purchase order, as per the scope of work mentioned in this document.

The Service Provider/ Firm shall provide onsite advisory and support throughout the course of formal assessment of the Certification Body. This should include, but are not limited to the following:

- Attend interviews and site-visits with the external assessors.
- Assist in the identification and collection of audit evidence.
- Follow-up on queries raised by the Certification Body.

Section II: Instructions to Service Providers / Consulting Firms

1. Introduction

1.1 Only eligible Service Providers / Consulting Firms may submit a Technical Proposal and Financial Proposal for the services required. The proposal shall be the basis for contract negotiations and ultimately for a signed contract with the selected Service Providers / Consultant Firm.

1.2 Service Providers / Consulting Firms should familiarize themselves with local conditions and take them into account in preparing the proposal.

1.3 **TRC** is not bound to accept any proposal and reserves the right to annul the selection process at any time prior to contract award, without thereby incurring any liability to the Service Providers / Consulting Firms.

1.4 The Service Providers/ Consulting Firms costs of preparing the proposal and of negotiating the contract, including visit/s to the **TRC**, are not reimbursable as a direct cost of the assignment.

1.5 Service Providers / Consulting Firms shall not be hired for any assignment that would be in conflict with their prior or current obligations to other procuring entities, or that may place them in a position of not being able to carry out the assignment in the best interest of the **TRC**.

1.6 **TRC** shall provide at no cost to the Service Provider / Consulting Firm the necessary inputs and facilities and assist the Firm in obtaining licenses and permits needed to carry out the services and make available relevant project data and report.

2. Preparation of the Proposal

- A Service Provider/ Consulting Firm Proposal shall have two (2) components in one envelop in two copies (Original and Copy):
    a. **Technical Proposal.**
    b. **Financial Proposal.**
- The Service Providers/ Consulting Firms are expected to examine in detail the documents constituting this Request for Proposal (RFP). Material deficiencies in providing the information requested may result in rejection of a proposal.

3. Technical Proposal

When preparing the Technical Proposal, Service Providers/ Consulting Firms must give particular attention to the following:

a. Bidder shall have an experience in ISMS implementation, and subsequently led (3) organizations/companies/government entities in Jordan to gain ISO 27001 Certification.

b. Bidder should have a minimum of four (4) resource personnel each with more than three (3) years' experience in ISO 27001:2013 implementation and internal auditing. The proposed team must also be valid certified in at least two (2) of the following certifications/professional qualifications.
    - ISO-27001 Lead Auditor (LA)/Lead Implementer (LI).
    - Certified Information Systems Auditor (CISA).
    - Certified Information Security Manager (CISM).
    - Certified Information Systems Security Professional (CISSP).
c. All Supporting Documents must be included.
d. The Technical Proposal shall provide the following information:

- A brief description of the Service Providers/ Consulting Firms organization and an outline of recent experience on assignments of a similar environment.
- A description of the approach, methodology and work plan for performing the assignment. This should normally consist of maximum of ten (10) pages including charts, diagrams, and comments and suggestions, if any, on Terms of Reference and counterpart staff and facilities. The work plan should be consistent with the work schedule.
- The list of proposed Professional Staff team by area of expertise, the position and tasks that would be assigned to each staff team members
- A description of previous ISO27001 engagements and contact details of the customers
- A time schedule showing the time proposed to undertake that the activities indicated in the work plan
- A detailed description of the proposed methodology and staffing for training if the RFP specifies training as specific component of the assignment.

4. Financial Proposal

a. The Financial proposal shall include all costs associated with the assignment. If appropriate, these costs should be broken down by activity/modules. All items and activities described in the Technical proposal must be priced separately; activities and items in the Technical Proposal but not priced shall be assumed to be included in the prices of other activities or items/modules.
b. Service Providers/ Consulting Firms shall express the price of their services in Jordanian Dinars (JD) and shall be inclusive for all fees and taxes.
c. The Financial Proposal shall be valid for **90 days**. During this period, the Service Provider/ Consulting Firm is expected to keep available the professional staff for the assignment.

5. Timeframe

The primary objective is to enable **TRC** to obtain ISO 27001:2013 certifications in 2021. Accordingly, the Firm would carry out a comprehensive study of the existing systems and procedures; documentation etc. in the set-up identified for certification and should harmonize them with ISO standards, culminating in the Certification. Accordingly, the entire project should be completed with **TRC** for period of (1) year from the date of signing the purchase order.

Section III: Technical Evaluation

1. The bidder should possess the requisite experience, resources and capabilities in providing the services necessary to meet the requirements, as described in this RFP. The Bid must be complete in all respects and should cover the entire scope of work as stipulated in this document. Parties who do not meet the Eligibility Criteria will not be considered for further evaluation.
2. A proposal shall be rejected at this stage if it does not respond to important aspects of the TOR or if it fails to achieve the minimum technical qualifying score which is **70%.**
3. The technical proposals of Service Providers/ Consulting Firms shall be evaluated based on the following criteria:

	Technical Evaluation	Expected Response	Points
1	Proposal on Scope of Work (requirements) as specified in the RFP.	Proposal Document	30
2	Presentations on the skills and previous services provided on ISO 27001:2013 certifications.	Document/presentation detailing existent skills and previous services provided.	30
3	Experienced and skilled professionals having certifications (e.g. ISO 27001:2013 Lead Auditor, CISA, CISSP, CISM and CEH) to carry out ISO 27001:2013 certification implementation at **TRC**. Comparison of skilled resources will be done based on the number of resources with desired certifications.	Summary Document and copy of individual certificates	20
4	Customer references submitted by bidder	Document detailing customer references.	20
	Total		100

4. Technical Proposal shall not be considered for evaluation in any of the following cases:
   a. Late submission, *i.e.*, after the deadline set.
   b. Failure to submit any of the technical requirements and provisions provided under the Instruction to Service Provider/ Consulting Firm and Terms of Reference.
   c. Failure to Provide the Documentary evidence and/or the supporting files.

Section IV: Financial Evaluation

1. The Financial Proposal of Service Providers/ Consulting Firms who passed the qualifying score shall be opened; **the lowest Financial Proposal shall be awarded the contract.**
2. Price shall remain fixed during the contract period. There shall be no increase in price for any reason whatsoever. Therefore, no request for any escalation of the price shall be entertained.
3. The winning bidder shall conduct the following activities , deliver and implement the following actions and points:

Phase		Actions and Deliverables
Phase 1:	**Consultancy Services**	❖ **Section 1** ❖ Prepare **Reports** for the following points: • **Site Survey** and providing us with a detailed comprehensive **report** including the below points: • **Gap analysis** in order to assess and evaluate the controls to be implemented to achieve **ISO 27001:2013 certification and accreditation.** • Review existing systems at **TRC pertaining to security controls, policies, processes and any other established procedures** on managing risk and improving information security to deliver results in accordance with the organization's overall policies and objectives. • Apply the PDCA cycle for ISMS implementation, and shall include all **Documentations, Reports, findings & Evidences.** • Review and validate the list of information assets of **TRC**, its ownership, classification of assets and prepare information asset registers. • Review the risk assessment, identify risk, controls and remediation plans and propose changes if required. • Review **TRC**'s Risk Assessment Methodology appropriateness to meet ISO27001 requirements for

		risk identification, mitigation and treatment and propose changes if required. • Review the current Organizational Structure and advise/modify to create an environment where policies, procedures, plans, strategies and processes to manage and monitor regulatory, legal, risk, environmental and operational requirements are understood and inform the management of security risks following the GRC platform. • Define all ISO 27001:2013 roles and responsibilities and mapping them to existing business departments or positions according to the approved Organizational Structure. • Define and develop required information security policies and procedures for **TRC.** • Define and create an evaluation method and metrics of the ISMS and the implemented controls. The plan should: o describe **the goal of measurement objective;** o define methods of **collecting performance data;** o define **the frequency and method of monitoring;** o Define **performance metrics, KPIs and dashboards** for implemented security controls. • Conduct ISO 27001:2013 **awareness sessions** to **TRC** staff. • Propose any **future recommendations** to the TRC with any new security concerns.
	Internal Audit Service	❖ **Section 2** The formal assessment/ certification will be performed by an independent team that did not participate in the ISMS implementation. And shall submit report that covers the following points and status : • Assess the ISMS and related activities, processes, procedures and documentations. • Conduct an internal audit by an independent team that did not participate in the ISMS implementation. • Assist the **TRC** team and provide consultancy on the Risk Treatment status, closure of Internal Audit findings, and other matters prior to the certification. • Benchmark against the ISO 27001:2013 standard and identify any non-conformity. • Provide assistance and support on remediating all non-conformities, including the revision of all necessary documentation.

		• Any observations which may lead to noncompliance to ISO 27001:2013 should be advised to **TRC** team immediately and confirmatory testing should be completed after fixing of the observation. As many iterations of audit may be performed as required to get the required compliance to ISO 27001:2013. • The Service Provider/ Firm shall include all required security awareness sessions for the involved personnel from **TRC through a recognized platform such as but not limited to LMS.**
	Onsite Support during Formal Assessment	❖ **Section 3** The Service Provider/ Firm shall be engaged with **TRC** for period of **(1) one year.** It includes **1st time ISO 27001:2013 Certification through an Accredited Certification Body (which would be decided by the bidder in consultation with TRC) within the first (1) year from the date of signing the purchase order,** This should include, but are not limited to the following: Provide onsite advisory and support throughout the course of formal assessment of the Certification Body. This should include, but are not limited to the following: • Attend interviews and site-visits with the external assessors. • Assist in the identification and collection of audit evidence. • Follow-up on queries raised by the Certification Body.
	Additional Action Points	❖ **Section 4** The Firm shall deliver and implement the following points: 1. Internal Audit Report 2. Corrective and Preventive Actions Report 3. Internal Audit Plan 4. Internal Audit Presentation 5. Corrective actions log sheet 6. Improvement Actions log sheet 7. External Audit Report 8. ISMS Certification 9. Future Recommendations Report 10. Project Closing Presentation
	Conduct Training	❖ **Section 5** Training course for (12 Trainees) from TRC that covers the following Topics: • ISO 27001 Lead Implementer training for (12 Trainees). • ISO 27001 Lead Auditor training for (12 Trainees).

Section V: Payment Conditions

1. The contractor shall provide the Price for the Consultancy services during the phase (1) for the period of (1) one year.
2. The Payment for this service will be fully paid (100%) after signing the purchase order with TRC and before starting the implementation of Project; on the other hand, the bidder shall provide a Bank Guarantee with same amount paid by TRC, this Bank Guarantee will be given back at the end of the project.
3. The prices shall be in Jordan Dinars (JD) and inclusive of all taxes, according to the deliverables mentioned in the table above in section (**Section IV: Financial Evaluation**).
4. No hidden cost is acceptable.
5. 7. Offer validity shall not less than three months from submitting date.
6. The contractor shall provide the pricing for the following phases as optional:
   - **Phase 2: Support & Follow up during the Second year; in this phase** the firm shall deliver continual enhancement and Support during 2nd year for completion of Surveillance Audit-1 and submission of audit report by certification body.
   - **Phase 3: Support & Follow up during the Third year; in this phase** the firm shall deliver continual enhancement and Support during 3nd year for completion of Surveillance Audit-2 and submission of audit report by certification body.

Section VI: General Conditions

1. **The Bidder shall provide Compliance Sheet for all the requirements specified in this Document.**

2. **Negotiations**

The aim of the negotiations is to reach agreement on all points and sign a contract. Further, TRC has the right to negotiate fully or partially the Awarded Bidder technical and financial proposal.

3. **Award of Contract**

   a. The contract shall be awarded, through a notice of award, following negotiations and subsequent post-qualification to the Service Provider/ Consulting Firm with the Highest Rated Responsive Proposal.
      i. The Service Provider/ Consulting Firm is expected to commence the assignment, Phase (1): **within the (1st) year starting from the date of signing the purchase order.**

b. Amman Court has the jurisdiction to resolve any disagreement or dispute arising between parties under or in connection with the winning Contract.

c. TRC may, by written notice of default sent to the Contractor, terminate the Contract in whole or in part if:

   i. The Contractor fails to deliver any or all of the Services within the time period(s) specified in the Contract, or any extension granted by TRC;

   ii. The Contractor fails to perform any other obligation(s) under the Contract.

4. Confidentiality

a. Information relating to the evaluation of proposals and recommendations concerning awards shall not be disclosed to the Service Provider/ Consulting Firm who submitted Proposals or to other persons not officially concerned with the process. The undue use by any Service Provider/ Consulting Firm of confidential information related to the process may result in the rejection of its Proposal and may be subject to the provisions of **TRC**'s anti-fraud and corruption policy.

b. Further, the intended Bidders (who bought a copy of a tender) shall sign a Non-Disclosure Agreement (**NDA**), to be allowed to ask about the scope and to have additional details.

5. Conflict of Interest

All bidders found to have conflicting interests shall be disqualified.

6. Clarifications and Amendments to RFP Documents

a. At any time before the submission of the proposals, **TRC** may, for any reason, whether at its own initiative or in response to a clarification amend the RFP.

b. Service Providers/ Consulting Firms may request for clarification(s) on any part of the RFP. The request must be sent in writing or by standard electronic means and submitted to **TRC** at the address and time frame indicated in the invitation. **TRC** will respond in writing or by standard electronic means.

7. Intellectual Property

All intellectual property and other proprietary rights including, but not limited to, patents, copyrights, trademarks, and ownership of data resulting from the performance of the Services shall be vested in **TRC**, including, without any limitation, the rights to use, reproduce, adapt, publish and distribute any item or part thereof.

الشروط الخاصة بإعادة طرح دعوة العطاء رقم (٢٠٢١/١١)

تعتبر هذه الشروط مكملة لتعليمات الدخول في العطاء والشروط العامة للتعاقد وتكون لها في التطبيق قوة العقد لشراء اللوازم والخدمات وتكون ملزمة للمناقصين وللجنة حق استبعاد أي عرض غير ملتزم بكل أو بأحد هذه الشروط: -

١. يرفق بالعروض تامين للدخول في العطاء على شكل كفالة بنكية أو شيك مصدق صادرة / صادر عن بنك محلي بنسبة لا تقل عن (٣%) من قيمة العرض الإجمالية وحسب النموذج المرفق وسوف لن ينظر في أي عرض غير معزز بالتامين المطلوب ٠

٢. يعتبر صدور قرار الإحالة المبدئي وإشعار المناقص به ملزماً له إذا كان عرض المتعهد ساري المفعول على أن يصدر قرار الإحالة النهائي خلال فترة سريان العرض والكفالة.

٣. تقدم العروض على نسختين متطابقتين أصل وصورة٠

٤. يجب ذكر الاسم بشكل واضح ورقم صندوق البريد ورقم الفاكس والهاتف وتحديد المنطقة والرمز البريدي٠

٥. يجب أن تكون المواصفات الواردة في عرض المناقص واضحة ومبوبة بشكل جيد بحيث تكون الوحدة والكمية والسعر الإفرادي والإجمالي وفترة التسليم وبلد المنشأ واسم الشركة الصانعة مبينة إزاء كل مادة٠

٦. يعتبر تقديم العرض من قبل المناقص تأكيداً منه بأنه أجرى التزاماً مع الشركة المصنعة بكامل اللوازم المعروضة وضمن مواصفات وشروط دعوة العطاء (العرض المقدم من قبله)٠

٧. تقدم الأسعار بالدينار الأردني متضمنة التوريد في الموقع الذي تحدده الهيئة، وبحيث تكون الأسعار شاملة الرسوم الجمركية والضريبة العامة على المبيعات والرسوم والضرائب الأخرى وأية عوائد حكومية أو غير حكومية٠

٨. يلتزم المتعهد بتقديم كفالة حُسن تنفيذ بنسبة (١٠%) من قيمة اللوازم المحالة عليه وحسب النموذج المرفق

٩. على المناقص اعتماد دعوة العطاء ومرفقاتها لتعبئة عرضه عليها٠