Lebanese Red Cross
Terms of Reference for ICT Specialist Consultant

A. Summary

Purpose: to assist the Lebanese Red Cross in Building ICT Strategy.

Commissioners: Lebanese Red Cross

Duration: 12 months, extendable.

Timeframe: one year

Location: Lebanon

B. Background

The Lebanese Red Cross (LRC) is the largest local humanitarian organization in Lebanon and provides a variety of health and disaster response services, most important amongst which:

- Emergency medical services (140,000 patients per year)
- Blood transfusion services (45,000 units per year)
- Primary Health services (150,000 patients per year)
- Disaster Management Services including basic assistance, water and sanitation, etc..

The LRC is consistently the first responder to major incidents and disasters, such as the Beirut Port Explosion during which the LRC assessed more than 40,000 households and provided basic assistance in multiple forms including cash assistance, to more than 15,000 families.

One of the major limitations of LRC'' that was identified in the emergency and regular services of LRC, has been the absence of an over-archiving Beneficiary Information System.
With the assistance of UNHCR, which operates such a system (RAIS, or Refugee Assistance Information System), for refugees in Lebanon, the Lebanese Red Cross aims to develop a similar system to improve its own response as well as overall humanitarian response in Lebanon.

For this purpose, the LRC is currently recruiting a specialized consultant or company with specific expertise in Beneficiary Information Systems, to assist in this project.

C. Scope of work for the ICT Consultant

I- Introduction and objective

- In its quest to strengthen its information, digital, and cybersecurity strategy, the Lebanese Red Cross took a strategic decision to assess its information security risks, update its IT strategy, define a roadmap to implement an Information Security Management System (ISMS) and ultimately get ISO 27001 certified.

- The main objective is to improve the governance and management of the IT systems and to embed an information security culture within Red Cross by relying on standards and well-known best practices.

- In order to reach this goal ***while leading a flexible and practical implementation approach***, a three phases project will be carried out.
    1. Phase 1: Information Security Risk Assessment: Carry out an assessment of Red Cross Lebanon's current digital and cybersecurity practices, and produce a report that documents the current practices, strengths, weakness and risks identified.
    2. Phase 2: an IT governance strategy will be defined. The main objective is to generate business value from IT-enabled investments, achieve operational excellence through the reliable and efficient application of technology and maintain the IT-related risk at an acceptable level.
    3. Phase 3: Information Security Management System (ISMS) Implementation.

    While the above-mentioned phases can be conducted separately, phase 1 is a pre-requisite for phase 3.

    In this context, we are pleased to support RED CROSS and present our proposal to conduct the above-mentioned project.

II- Methodology and Standards

- The methodology utilized for the establishment of this Cybersecurity Consultancy is fully aligned with the international standards ISO 27032 / ISO 27001 / ISO 27005.
- We would follow project management best practices to manage this project.

III- ISO 27001 Risk Assessment

The methodology adapted while conducting the assessment is fully aligned with ISO 27005 standard. A normal audit process will be followed by covering the areas defined in ISO 27001:

1. Organization of information security
   - Internal Organization
   - Mobile devices and teleworking
2. Human Resources Security
   - Prior to employment
   - During employment
   - Termination and change of employment
3. Asset Management
   - Responsibility for Assets
   - Information classification
   - Media handling
4. Access Control
   - Business requirements of access control
   - User access management
   - User responsibilities
   - System and application access control
5. Cryptography
   - Cryptographic controls
6. Physical and Environmental Security
   - Secure Areas
   - Equipment
7. Operations security
   - Operational procedures and responsibilities
   - Protection from malware
   - Backup
   - Logging and monitoring
   - Control of operational software
   - Technical Vulnerability Management
   - Information systems audit controls
8. Communications security
   - Network security management
   - Information transfer
9. System acquisition, development, and maintenance
10. Supplier relationships
11. Information security incident management
12. Information security aspects of business continuity management
13. Compliance with legal and contractual requirements

Deliverables:

The outcome of the assessment is a report that highlights the Cybersecurity risks at different

dimensions: technical, organizational and human.

IV- Phase 2: Developing an IT strategy (Duration:)

This work aims to develop a sustainable IT governance strategy by translating high-level enterprise goals into manageable, specific, IT-related goals. The work is based on the COBIT Framework (leading framework for the governance and the management of enterprise IT).

Following is the list of activities that will be conducted.

- Activity 1: Assessing the dependency between the IT projects and non-IT projects, IT services, information systems and IT infrastructure as well as the IT related investments.
- Activity 2: Identifying the stakeholders' needs and the main Information Technology pain points and trigger events from a business perspective.
- Activity 3: Developing an IT Governance Strategy that aims for value creation leading to benefits realization and resources optimization.

Activity 1: Dependency Analysis

This activity aims to link distributed services and information systems to the IT infrastructure (local or outsourced). RED CROSS will be asked to provide a set of documents governing the information system: the current IT projects, asset classification and localization, the current networks architecture, the current providers' SLAs.

We will analyze the set of documents, develop the dependency model and assess the relevant IT local and outsourced investments.

Activity 2: IT Pain points and Trigger events

For a proper IT Governance Implementation, pain points and trigger events should be identified with the board. This activity will be led in brainstorming sessions to identify the stakeholders' needs and current faced IT problems.

Activity 3: IT Governance Strategy

The main objective of this activity is to develop a sustainable IT Governance Strategy. We will assess the desire to change and available options that aligns IT-related objectives with RED CROSS's business strategy. Moreover, we will identify the most important enterprise goals, prioritize IT-related goals and set a target for improvements. Quick wins and long-term solutions at both technical (services, infrastructure) and strategic levels will be identified as well.

Deliverables

The deliverable of this phase consists of the detailed IT Governance Strategy.

v- Phase III: ISMS Implementation

This phase consists in initiating the implementation of the Information Security Management System (ISMS). We will tackle the three dimensions: Technical, organizational and human.

1- At the technical level:

We will establish a roadmap for the implementation of the technical controls as recommended in the risk assessment phase (phase1).

2- At the organizational level:

We will review and update all the policies and procedures required by the ISO 27001 standard. Moreover, we will enforce the policies by leading internal awareness sessions.

3- At the human level:

We will initiate an information security awareness program to cover all the risks related to the personnel particularly, social engineering risks.

Moreover, we will tackle how to:

- Operate the ISMS: Maintain all the required records and perform corrective actions as needed.
- Monitor & measure the ISMS: Measure if the objectives and controls set for your ISMS are achieved.
- Initiate the internal audits by training the IT team to accomplish this task.

Deliverables

- Initiating the implementation of the technical security controls
- Reviewing and updating all the policies and procedures required by the ISO 27001 standard
- Initiating the ISMS monitoring processes.

D. Consultant profile

VI- Consultant fields of experience and certifications

The consultant should holds a Ph.D. in computer science, with experience in Information Technology Consultation, with extensive experience in IT Governance, IT security and risk management. Change management skills in large-scale projects requiring the commitment of managers at various levels of the organization.

Fields of expertise

IT Governance
IT Management
Information Security Management
Risk Management
Business Continuity Planning
Project Management
Portfolio Management
Team building Conflict Resolution
Training and development
Operational / Process Analysis
Clients' Needs Analysis
Budget Management
Global IT Services Legacy System Migration

Certifications

ISO 27001 Lead Auditor,
ISO 27005 Risk Manager,
ISO 27032 Lead Cyber Security Manager
COBIT 5 Implementer,
Certified Information Security Auditor (CISA),
Certified Information Security Manager (CISM)

E. Timeline

1. 13th of December 2021: ToRs published
2. 23th of December 2021: Deadline for submitting proposals
3. December 2021: selection of specialist and contract negotiations
4. January 2022: start of mission

F. Proposal Submission guidelines

Your proposals should include:

1. CVs and portfolios of the specialist(s)
2. Description of previous experience with Similar systems
3. At least 2 letters of recommendation
4. Proposed methodology and high level time-table for performing the requested scope of work
5. Confirmation of availability to start work in Lebanon
6. Detailed financial proposal with cost breakdown

Electronic copies of your proposal to be provided in a USB key to be enclosed in the sealed envelope upon bid submission.