Annex C

DRC

Terms of Reference (TOR)

For

Information and Cyber Security Consultancy

1. Who is the Danish Refugee Council?

Founded in 1956, the Danish Refugee Council (DRC) is a leading international NGO and one of the few with a specific expertise in forced displacement. Active in 40 countries with 9,000 employees and supported by 7,500 volunteers, DRC protects, advocates, and builds sustainable futures for refugees and other displacement affected people and communities. DRC works during displacement at all stages: In the acute crisis, in displacement, when settling and integrating in a new place, or upon return. DRC provides protection and life-saving humanitarian assistance; supports displaced persons in becoming self-reliant and included into hosting societies; and works with civil society and responsible authorities to promote protection of rights and peaceful coexistence.

Operating since 2004 in Lebanon, DRC has addressed the needs and rights of vulnerable populations, working initially with Palestinian refugees (since 2004), Iraqi refugees (2007-2010), Lebanese IDPs (during the 2006 conflict), migrant domestic workers (since 2009), responding to the Syrian refugee crisis (since 2011) and to Lebanese crisis (since 2019).

DRC Lebanon is currently delivering programming in protection, livelihoods, and community development interventions. This myriad programming seeks to address the immediate needs of displaced populations and concurrently support vulnerable host populations. DRC has four offices spread throughout Lebanon in, Beirut, the Beqaa and North (Tripoli and Akkar).

For further information about DRC, please refer to our website: https://drc.ngo/

2. Purpose of the consultancy

The Danish Refugee Council based in ***Lebanon*** seeks proposals from a consultant for reviewing, assessing, analysing the DRC's Lebanon information management system functions ALPHA and RIMS, focusing on the system's application security, network security, database security, server, cloud security and data from cyber threats, in order to understand the risks and how vulnerable the systems. Then, the consultant will suggest recommendations, practices, and tools and develop a cybersecurity strategy in order to minimize those risks and enhance the protection of DRC Lebanon

systems when it comes to cyber threats. Alpha and RIMS are both online systems hosted on the cloud. RIMS is being used by more than 110 organizations to manage and track internal and external referrals within and across humanitarian sectors. Also, the information and Cyber Security Consultant is responsible for answering audit questions, and advise on security improvements recommendation along with detailed written guidelines. Finally, he/she will support data protection focal points in drafting the data protection policy by reviewing the existing information security policies and adding them as annexes to the data protection policy.

3. Background

Some of the Danish Refugee Council's interventions are designed to improve protection and effectiveness of the humanitarian response in Lebanon by enhanced coordination through joint analysis, planning and response. DRC Lebanon manages and collects data using different methods in paper format or in digital forms such as excel online systems. DRC Lebanon has developed a beneficiary centric integrated system for three main sectors Protection, Economic Recovery, a Referral Information Management System "RIMS" that serves as humanitarian common platform to manage referrals between partners in Lebanon along with internal information management systems for MEAL and Safety departments. The Referral Information Management System "RIMS" has the capacity to generate two categories of valuable data that can be used to improve humanitarian response: 1) information on the effectiveness and timeliness of referral processes and 2) gaps in service provision across sectors. To that end, DRC analyses aggregated information from RIMS partners to produce analysis on relevant trends and gaps. DRC Lebanon has developed Memorandum of Understanding, draft Data protection policy for RIMS with embedded basic Data Sharing Agreement to regulate the relation between different RIMS users who are Local NGOs, International NGOs, and UN Agencies.

4. Objective of the consultancy

The purpose of this consultancy is to review DRC's information security and data SOPs, and then to assess on regular basis the information management systems that DRC developed including Alpha and RIMS. Additionally, advise on measures that should be taken to overcome identified security issues.

5. Scope of work and Methodology

The consultant will be required to:

- Develop, review and update -when necessary- information security polices for both Alpha and RIMS including security of personal data, and sharing data with partners;
- In close coordination with the Data Protection Consultant and/or other Data Protection focal points the consultant will support -when needed- with providing inputs to the data protection policy including information security annexes that might be attached to the DRC's national data protection policy.
- Assess, review, and provide technical solutions on the current server hosting plan, data storage and management of servers;
- Assess, review, and provide technical solutions on the functionalities and features of Alpha and RIMS related to data security driven from global systems such as CPIMS+ and GBVIMS+

- Tests security vulnerabilities using different accredited tools for Alpha and RIMS to expose system's shortcomings and flaws, and use the results to improve security and prepare for outside attacks on monthly basis. Additionally, recommends good practices to keep IM Systems secure, produces monthly security snapshots, and quarterly full security reports. The systems are developed using ASP.net published version hosted on UBUNTU servers on Azure cloud services using Apache2 and Tomcat web services.
- Develop an early warning system –where possible- to help DRC's IM and IT Teams in identifying/noting the potential attempts/risks/signs of cyber-attack attempts or data breach
- Communicate with the Information Management Consultant who is supporting in the development and maintenance of DRC's Lebanon Information Management Systems in case any security vulnerability is identified as a result of the source code and/or internal system libraries.
- Support IM and IT teams in answering cyber security and security audit questions.
- Provides DRC's Lebanon IM Team with basic tools to test security vulnerabilities at application, server and database levels and creates procedures in case a data breach is detected;
- Review and update data security checklist to gauge if essential practices are in place in programme(s), on how to process data and information in a secure manner;
- Reviews and updates business continuity, backup and recovery plans for online systems and databases;
- Review and update the long-term plan and solution to keep the IM System secure.
- Other duties as agreed with the Head of Program and/or Information Management Coordinator in line with objectives above and weekly work plans.

The Consultant will be required to prepare a detailed methodology and work plan indicating how The objectives of the project will be achieved, and the support required from DRC.

6. Deliverables

The Consultant will submit the following deliverables as mentioned below:

Phase	Expected deliverables	Indicative description tasks	Maximum expected timeframe
Phase 1 Technical testing	**Conducts monthly security testing and generate detailed security reports**	Tests security vulnerabilities using different accredited tools for Alpha and RIMS to expose system's shortcomings and flaws, and use the results to improve security and prepare for outside attacks on monthly basis. Additionally, recommends good practices to keep IM Systems secure, produces monthly security snapshots, and quarterly full security reports. The systems are developed using ASP.net published version hosted on UBUNTU servers on Azure cloud services using Apache2 and Tomcat web services.	**10 working days divided across the consultancy period**

Phase	Expected deliverables	Indicative description tasks	Maximum expected timeframe
Phase 2 Assessment, Review, and development of security tools/SoPs	**Revision of existing Information and data security policies and tools including current server hosting plan, data storage and management of online servers, business continuity, backup and recovery plans for online systems and databases** **Assessment and review of ALPHA and RIMS IM systems**	Develops, reviews and updates -when necessary- information security polices for both Alpha and RIMS including security of personal data, and sharing data with partners; Assesses, reviews, and provides technical solutions on the current server hosting plan, data storage and management of servers; Assesses, reviews, and provides technical solutions on the functionalities and features of Alpha and RIMS related to data security driven from global systems such as CPIMS+ and GBVIMS+ Reviews and updates business continuity, backup and recovery plans for online systems and databases; Reviews and updates long-term plan and solution to keep the IM System secure. Reviews and updates data security checklist to gauge if essential practices are in place in programme(s), on how to process data and information in a secure manner; Develops an early warning system –where possible- to help DRC's IM and IT Teams in identifying/noting the potential attempts/risks/signs of cyber-attack attempts or data breach	**26 working days**
Phase 3 General technical support	**General technical support to IM Team and Data Protection consultant**	In close coordination with the Data Protection Consultant and/or other Data Protection focal points the consultant will support -when needed- with providing inputs to the data protection policy including information security annexes that might be attached to the DRC's national data protection policy Supports IM and IT teams in answering cyber security and security audit questions. Provides DRC's Lebanon IM Team with basic tools to test security vulnerabilities at application, server and database levels and creates procedures in case a data breach is detected;	**5 working days**

The Consultant will provide the documentation **by email including all excel, PowerPoint, word, and PDF documents**

7. Duration, timeline, and payment

The total expected duration to complete the assignment will be **no more than 41 working days.**

The consultant shall be prepared to complete the assignment no later than ***30/September/2023***.

Refer to Annex A.2 – Financial proposal for payment modality.

8. Proposed Composition of Team

- Head of Programmes
- Information Management Unit
- Information Management Coordinator
- Information Management Consultant
- Information and Cyber Security Consultant
- Programme Managers/Coordinators/Team Leaders
- Head of Programmes
- Country Director
- IT Officer
- RIMS Team
- Regional IT Specialist
- Regional MEAL Coordinator

9. Eligibility, Qualification, and experience required

Essential:

- 3-4 years of experience in Information Security.
- Advanced understanding of computers and software as well as programming and other technologies.
- Knowledge of CPIMS+ and GBVIMS+
- Experience in online hosting services on the cloud (Azure, Amazon...);
- Experience in performance tuning and index maintenance to meet/support needs of in-house development team.
- Knowledge of fault detection and resolution processes.
- Ability to communicate effectively with a variety of stakeholders including technical/non-technical audiences.
- Experience in humanitarian/development data management needs essential.
- Experience in developing policies/strategies or reports in advanced English
- Ability to work well under pressure, within complex and sensitive conflict environments.

Desirable:

- Experience in relational database management systems, preferably PostgreSQL.
- Experience in configuring Linux servers and web servers such as Apache2 and Tomcat.
- Knowledge of CPIMS+ and GBVIMS+ platforms.

Eligibility:

- The consultant has the authorization to work in Lebanon

Qualification:

- Bachelor degree (or equivalent experience) in computer science, information technology, computer engineering, or another relevant field.

Language requirements:

- Full proficiency in spoken and written English and Arabic.

10. Technical supervision

The selected consultant will work under the supervision of: **Information Management Coordinator**

11. Location and support

The consultant will be executing his/her tasks either at DRC office in Beirut or from home when the task does not require physical presence at DRC office.

The Consultant will provide her/his own computer and mobile telephone

12. Travel

There is no travels required for this consultancy

13. Submission process

Refer to the RFP BEY_22_08 Invitation Letter

14. Evaluation Criteria

Administrative

The documents listed below shall be submitted with the bid:

- Technical Bid Form or equivalent:
  - Provide at least two references
  - Provide Curriculum Vitae (CV) of key personnel offered to perform the consultancy services
  - Similar projects related to drafting/developing data protection policy, data protection impact assessment, information sharing protocols, and/or data asset matrix
- Financial Bid Form or equivalent
- Tender and Contract Award Acknowledgement Certificate

Technical

1-Lowest 10- Highest

Technical criteria #	Technical criteria	Points to be awarded	TOTAL weighting to be awarded
1	**Bidder qualifications**		**40%**
1.1	General capacity of the consultant	7	10%
1.2	Similar projects submitted that are related to drafting/developing information security policies, procedures, and SoPs	10	20%
1.3	Relevant degree, certifications, and or equivalent work experience in information and cyber security or a related field	7	10%
2	**Proposed services (documented by the technical proposal)**		**40%**

2.1	Content of the proposal suitable for the requirements	7	20%
2.2	Methodology of the research and meeting DRC timeline	10	20%
3	**Interview**		**20%**
3.1	Demonstrated technical capability to complete the consultancy services	10	20%

Financial

All bids that pass the Technical Evaluation will proceed to the Financial Evaluation. Bids that are deemed technically non-compliant will not be financially evaluated.

The service provider is required to submit a Financial Proposal in separate email **"Annex F Financial Proposal"**.

- The Financial Proposal must provide a detailed cost breakdown in USD including consultant's rate budget allowance, time and material, etc.
- Bidders must submit an overall firm-fixed price bid in USD.
- Invoicing and payment will be performed by bank transfer in USD.
- All costs will be fixed.

Only those shortlisted will be contacted for an interview with the panel to ensure their understanding of the consultancy services.