



TERMS OF REFERENCE (Individual Contractor Agreement)

Title: Risk Management Specialist (Information Security)

Project: All projects

Duty Station: Mexico City, Mexico

Section/Unit: LCR, MXPO

Contract/Level: ICS10 - IICA2

Duration: Ongoing

Supervisor: Risk Management Advisor (ICS11)

1. Background Information and organizational context

The United Nations Office for Project Services (UNOPS) is an operational arm of the United Nations, supporting the successful implementation of its partners' peacebuilding, humanitarian and development projects around the world. Mandated as a central resource of the United Nations, UNOPS provides sustainable project management, procurement and infrastructure services to a wide range of governments, donors and United Nations organisations.

UNOPS Mexico Country Office supports different collaboration initiatives by the Government of Mexico that are aimed at the fight against corruption and promoting transparency in public management, as well strengthening government actions in the areas of acquisitions, infrastructure and management of high impact projects in Mexico. The work requires strategic and operational perspectives, management of resources ensuring transparency, effectiveness and efficiency that promotes the development and continuous strengthening of internal management, in order to ensure high quality results, in accordance with the needs of the partner in Mexico. The objective of the most prominent project (PharmaMX) is to support the Government of Mexico in its effort to guarantee the right to health to the largest number of inhabitants through the planning and management of the consolidated purchase of medicines (period 2021-2024), as well as assistance in the profiling of the system and model of consolidated purchase of medicines for the health sector of the Government of Mexico

The Risk Management Unit is a new unit in the Mexico Country Office. It is managed independently from the PharmaMX project and is dedicated to controlling and managing key internal and external risks with organizational wide consequences, associated with the PharmaMX project. This involves an active collaboration with HQ function (such as Legal Group, Ethics & Compliance Office, Internal Audit and Investigations Group, Procurement

Group, UNOPS Enterprise Risk Management - ERM Unit, the Chief Information Security Officer, and Finance Group) and include aspects linked to:

- personnel/vendor due diligence;
- ensuring effective management and assurance of key risks associated with corruption, collusion, safeguarding, ethics, information security and supply chain;
- implementation of management actions;
- coordinating training and awareness efforts on the topics of all the relevant risks.

2. Functional responsibilities

Under the direct supervision of the Risk Management Advisor (Mexico Country Office) with support from the Chief Information Security Officer (HQ) and in collaboration with the ICT Specialist, the Risk Management Specialist- Information Security will focus on information risk management, info security compliance, training and awareness, incident management, implementation of appropriate governance & policies, privacy management, and threat intelligence & mitigation.

Summary of functions:

In relation to the PharmaMX project:

- I. Technology risk management
- II. Information security management
- III. Training and awareness raising
- IV. Reporting
- V. Knowledge Management

I. Technology risk management

- Performing risks assessments of information technology systems and information assets.
- Assessing system architecture and recommending to the Risk Management Advisor and the ICT Specialist in Support Services the design modifications necessary to meet organizational requirements for availability, integrity and confidentiality
- Generating system security requirements and specifications or analyzing, recommending configurations to the ICT Specialist, and assessing operational systems and networks, including OSes, web applications, or network devices.
- Ensuring that technology risks are identified and addressed as part of a project planning and implementation.

- In collaborating with the ICT Specialist performing tests and uncovering network vulnerabilities; devising action plans for their mitigations.
- Reviewing and advising on any business applications used within the projects, including advising on their deployment (to ensure segregation of duties between developers of the application and deployment).

II. Information security management

- Based on the findings of information security risk assessment and best practice, developing plans for information security enhancements, for endorsement by the Risk Management Advisor. Coordinating their implementations.
- Performing threat intelligence & mitigation
- Ensuring that sensitive data is appropriately classified and protected.
- Ensuring the appropriate key privacy and security obligations are included in the review of supplier contracts.
- In collaboration with the Senior Project Manager, develop plans to mitigate information security risk throughout the project delivery.
- Investigating Information/document security breaches and relevant incidents. Escalating as appropriate and recommending preventative actions for any further similar incidents.
- Contributing into the supply chain risk management and due diligence by providing a framework and criteria for third-party supplier privacy and information security reviews.

III. Training and awareness raising

- Developing and implementing training, communications and awareness raising for the project personnel and the wider local team, on how to address information security risks specific to the project. Collaborate with procurement on training vendors and other possible partners.
- Ensuring that all relevant personnel know and understand their information security obligations at each phase of the project life cycle
- Providing strategic advice and engaging with local management and critical third parties (e.g. vendors) to raise awareness on effective information security risk management.

IV. Reporting

- Providing periodic reports to the Risk Management Advisor and the Country Office Director on Information Security risk management.

- Providing periodic reports on Information Security risk management to the CISO, including ad hoc reporting on material risk events/investigations and handling of issues within the project.

V. Knowledge management

- Contributing to the regional network teamwork and collaboration as well as the corporate best practice toolkit, sharing innovative solutions and lessons learned;
- Ensuring full documentation of information security activity, to enhance knowledge-sharing/transfer within the team and beyond.
- Following and evaluating emerging technologies, staying up-to-date with trends and the information security management landscape.

Support in other duties as assigned.

3. Impact of Results

The effective and successful achievement of results by the incumbent directly affects UNOPS ability to deliver against its mandate and protects UNOPS reputation. The role is imperative to the effective management of information security risks for the project, impacting the visibility and image of the UNOPS as an effective service provider in project services and management and consequently strengthen its competitive position as a partner of choice in sustainable development and project services in Mexico.

4. Requirements

A. Education

- o An advanced university degree (Master's degree or PhD) preferably in Computer Science, Information Systems, Information Management, Risk Management or related field;
- o A first-level university degree (Bachelor's degree or equivalent) with a minimum of two (2) additional years of relevant work experience may be accepted in lieu of the advanced university degree;

B. Experience

- o A minimum of five (5) years (or more depending on academic credentials) of experience in the design, development, and deployment of secure ICT applications and infrastructure;
- o Strong experience developing and implementing information security policies, standards, and guidelines is required;
- o Strong experience in cross-functional collaboration in evaluating information security risks and implementing information security mitigating actions is required;

- o A strong grasp of privacy program implementation is an asset;
- o Solid experience in providing support for standardization and consistent integration of information security processes across existing and new (cloud) ICT environments is desirable;
- o Working knowledge of Google Suite is desirable.

C. Skills

- o Strong interpersonal and analytical skills;
- o Detail-oriented;
- o Excellent written and oral skills.

D. Languages

- o Full domain of Spanish is required.
- o An intermediate level of English is required.

E. Certifications

- o PRINCE2 Practitioner Certification is desirable.
- o Certifications in Information Security or IT Risk Management (such as CISSP, CISA, CRISC, CISM, etc.) are an advantage.

5. Competencies



Develops and implements sustainable business strategies, thinks long term and externally in order to positively shape the organization. Anticipates and perceives the impact and implications of future decisions and activities on other parts of the organization.



Treats all individuals with respect; responds sensitively to differences and encourages others to do the same. Upholds organizational and ethical norms. Maintains high standards of trustworthiness. Role model for diversity and inclusion.



Acts as a positive role model contributing to the team spirit. Collaborates and supports the development of others. Acts as positive leadership role model, motivates, directs and inspires others to succeed, utilising appropriate leadership styles



Demonstrates understanding of the impact of own role on all partners and always puts the end beneficiary first. Builds and maintains strong external relationships and is a competent partner for others (if relevant to the role).



Efficiently establishes an appropriate course of action for self and/or others to accomplish a goal. Actions lead to total task accomplishment through concern for quality in all areas. Sees opportunities and takes the initiative to act on them. Understands that responsible use of resources maximizes our impact on our beneficiaries.



Open to change and flexible in a fast paced environment. Effectively adapts own approach to suit changing circumstances or requirements. Reflects on experiences and modifies own behavior. Performance is consistent, even under pressure. Always pursues continuous improvements.



Evaluates data and courses of action to reach logical, pragmatic decisions. Takes an unbiased, rational approach with calculated risks. Applies innovation and creativity to problem-solving.



Expresses ideas or facts in a clear, concise and open manner. Communication indicates a consideration for the feelings and needs of others. Actively listens and proactively shares knowledge. Handles conflict effectively, by overcoming differences of opinion and finding common ground.

6. Signatures

Incumbent		
Name	Signature	Date
Supervisor		
Name	Signature	Date