IOM
UN MIGRATION

Vacancy Notice – ES 2024/001

Open to Internal and External Candidates

Position Title	:	**Information Security Analyst**
Duty Station	:	**Valencia, Spain**
Classification	:	**General Service Staff, G6 – Full Time**
Type of Appointment	:	**Fixed term, one year with possibility of extension**
Estimated Start Date	:	**As soon as possible**
Closing Date	:	**March 17, 2024**

Established in 1951, IOM is a Related Organization of the United Nations, and as the leading UN agency in the field of migration, works closely with governmental, intergovernmental and non-governmental partners. IOM is dedicated to promoting humane and orderly migration for the benefit of all. It does so by providing services and advice to governments and migrants.

IOM is committed to a diverse and inclusive work environment. Internal and external candidates are eligible to apply to this vacancy. For the purpose of the vacancy, internal candidates are considered as first-tier candidates.

Context:

Under the direct supervision of Senior ICT Security Officer (SISO) and in close collaboration with relevant Information and Communications Technology (ICT) Units at Headquarters (HQ) and worldwide ICT Teams, the successful candidate will be responsible for supporting Information Security Programme, in the area of Information Security Risk Management including vendor risks, Data Security/Privacy governance, security compliance management.

Core Functions / Responsibilities:

1. Plan and implement Information Security Risk Management programme through the systematic and comprehensive mechanism. Review and update the Programme annually.
2. Run and continuously suggest improvements to the Information Security Risk Management globally and distribute a risk report monthly or as required including the dashboards.
3. Assist in global security compliance management. Track, measure and follow up regularly the global security compliance progress and generate a regular report at least monthly to SISO and other stakeholders.
4. Run and continuously suggest improvements to the Supply Chain/Third Party Information Security Risk Management. Create and distribute required reports monthly or as required including the dashboards.
5. Assist in SISO to approve or accept risks of Supply Chain/Third Party by clear and solid recommendations based on through analysis of Supply Chain/Third Party security risk posture.
6. Assist conducing annual risk assessment and compliance enforcement.
7. Assist in Information Security Project Management and integration of security into other Project Management
8. Perform such other duties as may be assigned.

Required Qualifications and Experience

Education

- University degree in the Information Security, Cybersecurity or equivalent with four years of relevant professional experience.
- Professional certification such as Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified Chief Information Security Officer (CCISO), Certified Secure Software Lifecycle Professional (CSSLP), Certified Secure Web Application Engineer (CASE), Certified Secure Web Application Engineer (CSWAE), Governance, Risk, and Compliance Professional (GRCP), Certified Ethical Hacker (CEH), or related will be a distinct advantage in addition to cloud computing certifications at associate/professional/specialty level from Azure and/or AWS.
- Information Technology Infrastructure Library (ITIL) and Prince2 Foundation are added advantages.

Experience

- Experience in FISMA, NIST, FIPS compliance, compliance implementation, management and auditing;
- Experience in project management of Information Security and Compliance;

- Experience in information security risk management
- Relevant security analysis and reporting work experience

Skills

- Strong analytical and interpersonal skills;
- Solid organization and document, project management;
- Strong ability to continue to learn and grow;
- Demonstrated skill in project management
- Demonstrated skill in creating security policies and procedures based on ISO27001:2013, NIST 800-53, FIPS and Computer Information System (CIS) controls;
- Strong analytical and problem-solving skills and proactive thinking skills; and,
- Strong English oral and written communications skills.

Languages

REQUIRED
For all applicants, fluency in English is required (oral and written).

DESIRABLE
Working knowledge of Spanish

Required Competencies

Values

- Inclusion and respect for diversity: respects and promotes individual and cultural differences; encourages diversity and inclusion wherever possible.
- Integrity and transparency: maintains high ethical standards and acts in a manner consistent with organizational principles/rules and standards of conduct.
- Professionalism: demonstrates ability to work in a composed, competent and committed manner and exercises careful judgment in meeting day-to-day challenges.
- Courage: Demonstrates willingness to take a stand on issues of importance. Empathy: Shows compassion for others, makes people feel safe, respected and fairly treated.

Core Competencies – Behavioural indicators – Level 2

- Teamwork: develops and promotes effective collaboration within and across units to achieve shared goals and optimize results.
- Delivering results: produces and delivers quality results in a service-oriented and timely manner; is action oriented and committed to achieving agreed outcomes.
- Managing and sharing knowledge: continuously seeks to learn, share knowledge and innovate.
- Accountability: takes ownership for achieving the Organization's priorities and assumes responsibility for own action and delegated work.
- Communication: encourages and contributes to clear and open communication; explains complex matters in an informative, inspiring and motivational way.

Other

Any offer made to the candidate in relation to this vacancy notice is subject to funding confirmation.

Appointment will be subject to certification that the candidate is medically fit for appointment and verification of residency, visa and authorizations by the concerned Government, where applicable.

Only candidates with Spanish nationality or with labour permit to work in Spain will be considered.

How to apply:

Interested candidates are invited to send their CV, PHF and cover letter via email to HRESAPPLY@iom.int, no later than March 17th, 2024, referring to this Vacancy Notice.

For further information, please refer to:
https://spain.iom.int/es/vacantes

Only shortlisted candidates will be contacted.

Posting period:

Until: March 17th, 2024