Open to Internal and External Candidates

Position Title: National IT Security Officer (Identity and Access Management)

Duty Station: Manila (Global) Administrative Centre (MAC)

Classification: National Officer/NO-B

Type of Appointment: Fixed term, one year with possibility of extension

Estimated Start Date: As soon as possible

Closing Date: 06 August 2019

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 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:

This position is based in Manila Administrative Centre (MAC), headed by the Director of MAC. The Information and Communications Technology (ICT) is one of the divisions with its operations delocalized to MAC.

Under the overall supervision of the Chief Global ICT Operations, and under the direct supervision of the IT Security officer, the successful candidate will serve as a subject matter expert on the Identity and Access Management (IAM) field. He or she will work closely with IOM’s business areas and control functions to develop, integrate, and apply technical IAM solutions that will manage identities and access to IOM’s resources.

Core Functions / Responsibilities:

- Provide leadership and focus for the Identity and Access Management (IAM) Architecture and standards.
- Design and implement new roles and authorizations when new or changes to applications are introduced or when business functions move from one department to another.
- Primary support for the Identity and Access Management (IAM) tools.
• Responsible for gathering IAM business requirements and driving standardization to support business activities while maintaining the security of the application and data systems.
• Responsible for implementing identity lifecycle management workflows to support full automation of user provisioning activities.
• Responsible for onboarding applications and data assets into IAM products.
• Responsible for standardizing and automating business processes into the IAM solution.
• Excellent customer skills when working with business to accomplish desired outcomes.
• Responsible for integrating information systems with HR onboarding and off-boarding processes.
• Perform such other duties as may be assigned.

Required Qualifications and Experience

Education
• Master’s degree in Computer Science, Computer Engineering or a related field from an accredited academic institution with two years of relevant professional experience; or
• University degree in the above fields with four years of relevant professional experience.
• Industry adopted security certification (e.g., CISSP).

Experience
• Minimum four years of experience in the following:
  o design, documentation, and implementation of packaged or custom IAM solutions, including but not limited to Oracle, IBM, CA, SailPoint, RSA/Aveksa, ForgeRock, Okta, Dell/Quest, PingIdentity;
  o deploying Identity an Access Management solutions, Identity Governance and Privileged Management in MS Active Directory environment;
  o technical architecture experience integrating identity management, access management, and access governance software into Windows, SAP, Exchange Online, File Servers, in-house developed applications and Cloud (Azure) systems;
• In-depth understanding of IAM best practices for integrating .Net, Java, SharePoint and other applications with standard identity provisioning processes;
• In-depth understanding of capabilities and limitations of a wide range of technologies, platforms, architecture, methodologies; well-versed in current and emerging information security technologies;
• Experience with Cloud Identity as a Service such as Microsoft Azure Active Directory, and Identity Federation protocols such as SAML2, WS-Federation, OAuth 2, OpenID Connect, etc.
• Knowledge of Information Security including security architecture, industry trends and direction, system and technology integration, and standards, procedures and policies, and emerging technologies.

Languages

Fluency in English is required. Working knowledge of French and/or Spanish an advantage.
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.

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.

**How to apply:**

In order for an application to be considered valid, IOM will only accept applications which should include a cover letter (not more than one page) and résumé highlighting the required education and experience or a duly completed IOM Personal History Form. To access the form, please visit [https://www.iom.int/sites/default/files/vacancy/MAC/iom-personal-history-form1.xlsx](https://www.iom.int/sites/default/files/vacancy/MAC/iom-personal-history-form1.xlsx)

Interested applicants may send their applications to [machrsupport@iom.int](mailto:machrsupport@iom.int) no later than **06 August 2019**. VN Number and Position Title *(VN 046/2019 – National IT Security Officer)* should be specified in the SUBJECT field.

Applications from qualified female candidates are especially encouraged.

Only short-listed candidates will be invited for an interview.

**Posting period:**

From 23.07.2019 to 06.08.2019