INFORMATION SECURITY OFFICER

Main Role:
The incumbent as the focal point, must establish, implement, maintain, and continually improve the information security management system. The areas of action remain in the following domains: organizational, physical, people, technological. He/She must control the necessary measurements that are in place. He/She acts as the facilitator and advisor of the documented measures within the policies.

Reporting Relationship:
The Information Security Officer reports directly to the Head of Finance and Administration and holds office in GIZ Office Manila, Makati City.

In carrying out his/her role, the Information Security Officer, performs the following major functions/duties:

Major Functions/Duties:

Development of an Information Security Management System (ISMS)

- Implementing, coordinating, and continuously improving local information security management system (ISMS) based on the ISMS country project plans.
- Coordinating, creating and revising the security policies and related sub-concepts based on the context of the country or country region.

Implementation of measures

- Planning and coordinating the implementation of information security measures in close alignment with management level and key stakeholders such as e.g., HQ-ISMT, IT Department, central Data Protection Team, and Digitalization Partner local SRMO and projects.
- Supporting the implementation and coordination of security-relevant processes.
    - Establishing of a reporting process for security-relevant incidents and their investigation within the country office and with HQ/ISMT.
- Monitoring the effectiveness of the information security program and make recommendations for improvements to the departments of the country office or commissioning manager.
- Supporting and maintaining incident management
    - Supporting in establishing an incident management process
    - Supporting in evaluating the incident and defining the next steps in the country office
    - Involving all needed parties and communicate the incident to the CISO/ISM-T
    - Securing evidence after security incident

Advising and reporting to management

- Reporting on the local information security management system (ISMS) performance to local management level and HQ/CISO.
- Reporting of security risks and issues to local management and HQ/CISO.
- Advising the local management and HQ/CISO how audit findings should be implemented

Internal audits and support on external audits

- Developing an internal audit plan based on the audit program from HQ/ISMT
- Supporting and conducting internal audits for the implementation of applicable security control objectives.
- Preparing and supporting the continuous improvement through the certification and surveillance audit.
- Serving as the contact person for all internal and external non-conformities in audits.

Awareness and central contact person

- Providing guidance and support to employees on information security best practices.
- Initiating alignment with IT Prof (IT Professional) and Digitalization Partner (DiPa), and implementation of awareness-raising measures for information security in consultation with various stakeholders (such as IT professionals and local digitization partners).
- Closing interaction and communication to Headquarter ISM-Operations and relevant stakeholders.
- Supporting in the implementation and improvement of existing awareness measures and programs.
- Advising for new and follow-up projects (InfoSec checklist)

General Corporate Task – Performs work of other administrative staff and/or other tasks relevant to the job or organization unit when the need arises and participates in working groups and other corporate entrepreneurial or strategy-linked endeavors.

Competency Requirements:

- Knowledge and experience in information security
- Basic knowledge of actual Microsoft Software and Services ecosystem
- Methodological competence in: ISO/IEC 27001, risk management, vulnerability management, audit
- Has overview of tasks and objectives of the institution and can evaluate and classify them with respect to information security (an understanding of GIZ businesses and operations is an advantage)
- Ability to "think inside" organizational structures and processes
- Ability to work independently
- Ability to adapt, communicate and implement key requirements

Professional Qualifications:

- University degree or formal professional diploma in relevant field: computer science, management information system, or any technology related equivalent
- At least three years' experience as an ISO officer in a business-related field