Salary Band 4A	Information Security Officer (ISO)3A
Reports to:	Head of Finance and Administration (LFA) CISO / ISM-T (for technical subjects)
Duration	2 Year Contract
Duty Station	Hatfield, Pretoria

Background

The Deutsche Gesellschaft für Internationale Zusammenarbeit GmbH (GIZ) is a public-benefit federal enterprise working in more than 100 countries worldwide. We work on behalf of the German Government and support public and private sector clients in a wide variety of areas, including economic development and employment, energy and environment, and peace and security. GIZ works project based and has decentralized activities in South Africa, Lesotho and eSwatini. The Country Office (CO) is the governance and service structure of GIZ South Africa, Lesotho and Eswatini, together with the recently commissioned started WE4D (Promoting female employment for Africa's green transformation).

In order to protect all valuable information processed by GIZ worldwide, it is necessary to establish an information security management system (ISMS). GIZ aims to implement such a system based on two standards, ISO/IEC 27001, and the BSI Baseline. The head office is focusing on building the ISMS according to the German standard, while the country -and project offices are developing the ISMS according to ISO/IEC 27001. To successfully implement the ISMS in the country offices, it is necessary to have a person who takes care of the function as Information Security Officer (ISO).

There are various roles and functions to ensure information security at GIZ. Coordination at the corporate level is handled by the Chief information Security Officer (CISO) and his/her ISM-T team. However, for the local implementation and operation of information security, there is a need for a new function called the local ISO, which is filled by a full-time person. The local ISO works closely with other existing functions such as IT-Professionals (IT-Pro) Digitalization Partners (DIPA), Head of Units and Country Office Management level. It is important to note that Information Security Officers cannot be IT Professionals, Digitalization Partners, or Head of IT Units at the same time to avoid conflicts of interest.

The ISM-T and CISO provide technical leadership for the implementation of the global information security management system (ISMS) [1], while disciplinary leadership is provided by the management level of the country office. The Information Security Officer's role is to serve as the point of contact for the implementation and continuous management of the local ISMS. They are responsible for monitoring the security policies and controls and has expertise in information security risk assessment in the respective area.

[1] During the beginning of the implementation of the global information security management (ISMS) the LSS-ISMS team is responsible for provision of technical support and leadership.

A. TASKS AND RESPONSIBILITIES

Responsibilities

The Information Security Officer (ISO) is responsible for establishing, implementing, and maintaining an information security management system at GIZ South Africa, Lesotho and eSwatini, in collaboration with the ISM team at Headquarters of GIZ in Germany. Based on the already introduced SOPs and measures. The ISO is advising and supporting all units of the Pretoria County Office (CO) and the various projects of GIZ South Africa, Lesotho and eSwatini.

The ISO, 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. In this position the ISO must control the necessary measurements that are in place.

The ISO is a facilitator and advisor of the documented measures within the policies.

Tasks

Next to the above-mentioned responsibilities the ISO has the following tasks:

Development of an ISMS

- Implementing, coordinating, and continuously improving the GIZ South Africa, Lesotho and eSwatini security management system (ISMS) based on the ISMS country project plans.
- Creating, coordinating, and revising the security policies, SOPs and related sub-concepts adapted to the context of GIZ South Africa, Lesotho and eSwatini.

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 Security Risk Advisor (SRMO) and projects.
- Support in the implementation and coordination of security-relevant processes.
    - Establishment of a reporting process for security-relevant incidents and their investigation within the country office and with HQ/ISMT.
- Monitor the effectiveness of the information security program and make recommendations for improvements to the departments of the country office or commissioning manager.
- Support and maintain incident management
    - Support establishing an incident management process
    - Support in evaluating the incident and defining the next steps in the country office
    - Involve 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

- Develop an internal audit plan based on the audit program from HQ/ISMT
- Support and conduct internal audits for the implementation of applicable security control objectives.
- Prepare and support the continuous improvement through the certification and surveillance audit.
- Contact person for all internal and external non-conformities in audits.

Awareness and central contact person

- Provide guidance and support to employees on information security best practices.
- Initiation, 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).
- Close interaction and communication to Headquarter ISM-Operations and relevant stakeholders.
- The ISO should support in implementing and improving existing awareness measures and programs.
- Advisor/supporter for new and follow-up projects (InfoSec checklist)

Interfaces to other roles/departments

The ISO tasks have many interdependencies with the tasks of an IT-Pro, DIPA and the SMRO, so it is important to define the distinction of those roles in the context of information security.

IT-Pro:
The IT-Pro is the contact person for the IT-infrastructure, user environment, helpdesk, IT documentation, IT-procurement and responsible for the implementation and operation of the IT security measures. The ISO checks the effectiveness of the measures and supports him/her from an information security perspective. The IT-Pro must approach the ISO when IT-infrastructure changes are planned and must consult the ISO for InfoSec related topics.

DIPA:
DIPA is the contact person for the ISO regarding digital transformation, digital literacy and security, data protection, Information and documentation management, cloud applications, internal IT-processes and GDPR. The DIPA must consult the ISO for InfoSec related topics.

SRMO:
SRMO is the contact person for the ISO regarding the safety of the employees and the building sites. The SRMO is responsible for the physical security of the employees, buildings and during traveling must consult the ISO for InfoSec related topics.

ISMT-T/CISO:
ISM-T/CISO is responsible for developing the InfoSec policies and methodologies. Furthermore, the ISM-T/CISO provides technical leadership to the ISO. The ISO must inform the ISM-T/CISO about changes in the local ISMS and must report on the status of the ISMS and any related issues or risks on a regular basis.
Regarding the cooperation's with the different roles/departments, regular formats of communication must be in place. These can happen in the framework of regular official management rounds or informal meetings.

B. Required qualifications, competences, and experience.

Qualifications

- Masters/MSc degree in Information Security or Information Technology.

Professional Experience

- At least 5 years' professional experience in an international organization.
- 3 years' work experience in corporate risk management.
- Experience in vulnerability management.
- Experience in moderation, interviewing, mediation
- Knowledge and experience in ISO/IEC certification and audits.
- Knowledge and experience in information security with methodological competences in ISO/IEC 27001 and related standards

Other knowledge, additional competences

- Good working knowledge of ITC technologies (related software, phone, fax, email, the internet) and computer applications (e.g. MS Office).
- Basic knowledge of IT-Management systems
- Ability to multi-task and work under pressure.
- Very good communications skills, being able to handle objections and conflict objectively and efficiently.
- Very good analytical skills
- Persuade and manage people
- Very good knowledge of the English and German language.
- Diligent, open minded and innovative and very good team-player.
- Finely tuned organisational skills and ability to work on one's own initiative at the conceptional level.
- Confidential handling of data and information
- Result orientated performance, reliable and pro-active
- Broad diversity, inclusion, and intercultural skills
- Willingness to scale up skills as required by the tasks to be performed – corresponding measures are agreed with management

Soft skills

As communication skills are a key factor in successfully cooperating within the organization, the ISO must be able to handle objections and conflict objectively and effectively as well as persuade and manage people. Being able to communicate back and forth between country director and different departments while staying impartial is key for the ISO role.

The ISO must also possess excellent social skills such as being pro-active, having a commitment to life-long learning and staying up to date with security and threat-related trends by attending necessary further training. They should also display the ability to suffer due to unwillingness and dissatisfaction from employees due to additional work or comply to additional regulatory frameworks.

To fulfill his role and function to the full extent he must be able to network effectively with all levels of expertise, extending from projects to GIZ-HQ. That requires being pro-active in all social interactions, forming networks that support and the achievement of future projects.

To ensure effective collaboration with colleagues the ISO must adapt to changing frameworks, "think inside" organizational structures and processes and compile comprehensive reports.

Since the ISO plays a significant role in safeguarding assets and people, they must display independence, credibility, impartiality, and unconditional discretion as essential qualities in his character.

C. ADDITIONAL INFORMATION

Additional Information

- This position is based in the GIZ South Africa / Lesotho / eSwatini Country Office currently based in **Hatfield, Pretoria**
- At GIZ, you will be offered a global network and an atmosphere that is characterized by diversity, respect, and genuine equal opportunities. Gender equality promotion is a matter of course for us.
- GIZ is a signatory of the Diversity Charter. Recognition, appreciation, and inclusion of diversity in the company are important to us. All employees shall be valued - regardless of gender and gender identity, nationality, ethnic origin, religion or belief, disability, social background, age, or sexual orientation.
- GIZ would like to increase the proportion of employees with disability. Applications from persons with disabilities are most welcome.
- **The contract period for this position is twenty-four (24) months.**

D. APPLICATION PROCESS

Suitable candidates should apply by submitting:

- A motivation letter **(max. 1 page)** stating why they should be the preferred candidate, the value added they will bring to this role and their **desired salary range.**
- A **detailed CV.**
- Proof of eligibility to work in South Africa (copy of SA ID)

Applications should be submitted to: recruit-pretoria@giz.de , with the email subject line: **"Application for Information Security Officer"** for the attention of **Head of Human Resource**.

Closing date for applications**: 18 August 2023.**

Please note that only shortlisted candidates will be contacted!

Applications without a motivation letter will not be considered!