IMPLEMENTING THE PERSON-CENTERED APPROACH TO SECURITY RISK MANAGEMENT IN PAKISTAN

1.Context and kick-off

Given Pakistan's political, economic, and security crisis since 2022, the 2023 Country Planning focused on preparing the Country Office and projects to ensure business continuity in case of a further deterioration of the security situation. In this context, security processes and procedures implemented by the Risk Management Office (RMO) Pakistan came under scrutiny. Among the aspects highlighted by the Country Management was a necessity that RMO output integrate gender and diversity considerations into their measures. The rationale behind this request was to ensure that, in a crisis, security risk management policies are inclusive and consider the needs of all staff members.

2.Team formation and strategy - Stressing cooperation beyond RMO and GIZ Pakistan

The first step in our integration of gender and diversity in RMO policies and procedures was to form a workgroup that included not only RMO staff but also the Gender Advisors from the Country Office. Integrating staff beyond RMO in our workgroup gave us a unique vantage point and ensured that we did not get stuck in our "SRM and gender bubbles" but instead thought outside the box and created valuable synergies.

After forming our workgroup, we initiated a scoping phase to understand what other organisations in Pakistan and RMOs within GIZ are doing regarding inclusive security risk management and, at the same time, reflect on the gaps we may have in our policies and processes. It was helpful to exchange with risk management and gender advisors in Afghanistan, Iraq, Kenya, and India. Outside GIZ, we had a particularly fruitful discussion with IOM.

Another central point during our scoping phase was understanding how "gender and diversity considerations" are implemented in security risk management (SRM). That is how we came across the person-centred approach to security risk management. This approach recognises staff diversity as a central factor in SRM.

3.Person-centered approach to Security Risk Management

The premise of the person-centred approach to security risk management is that staff should not be perceived as a homogenous group. Instead, we must recognise that they have diverse profiles based on their personal identity characteristics. Personal identity characteristics include sex and gender identity but encompass much more than just that, for example, age, ethnicity, nationality, religion, sexual orientation, physical and mental health and ability, to name a few. These intersectional identity characteristics interact with a staff member's organisational role and the operational context to affect the risks they face. Security risk managers must consider staff diversity when assessing risk and recommending mitigation measures. This does not mean, however, that risk management should over-regulate or police certain groups over others; instead, we should broaden the scope of our recommendations so that they are inclusive and cater to staff with diverse profiles.

4.Workplan development

Based on the scoping phase, we identified priority areas for the revision of our processes and procedures:

- **Sensitisation of RMO staff to gender and diversity as central factors in security risk management:** Sensitising RMO staff is a central requirement to implement a person-centred approach in our processes and procedures.

- **Security briefing and welcome package:** The security briefing and welcome package represent the first information resources international staff and visitors receive about risks in Pakistan. Therefore, they must address risks while considering diverse staff profiles.

"RMO PAKISTAN CREATES SYNERGIES WITH CROSS COUNTRY OFFICES TO ACHIEVE A TRULY INCLUSIVE SECURITY RISK MANAGEMENT"

- **Travel management, site security assessment, incident reporting RMO SOPs:** We selected these SOPs as they deal with situations where staff may face different risks and have different sensibilities based on their personal identity characteristics.

- **Train RMO staff in psychological first aid and responding to sensitive incidents:** RMO is often the first point of contact for staff when reporting security incidents. Therefore, they must understand how to respond to sensitive incidents compassionately and appropriately.

- **Identify gender and anti-sexual harassment training requirements for the next guard tendering process in mid-2024:** In 2022, there was an incident of gender-based violence involving a guard and an international staff member of an international organisation in Islamabad. Therefore, it is central that the guard company we contract takes this issue seriously and fulfils specific training requirements.

For the implementation of our plan, we gave ourselves a timeframe of around one year until March 2023. We agreed to tackle the revision of each document by reviewing them individually and then discussing proposed changes during workgroup meetings, in which at least one CO Gender Advisor, one RMO staff member from the operational department, and one from the analysis side would participate.
Our work plan did not mention any specific staff profile that we would target to make our documents and policies more inclusive. As far as possible, we have amended these documents to apply to all staff profiles. However, in practice, a particular focus has crystallised on personal identities related to:

- Gender and gender identity
- Physical/mental health and ability
- Sexual orientation
- Nationality/contract type

These common personal characteristics may yet be overlooked in risk management policies.

SOPs MUST ACKNOWLEDGE STAFF DIVERSITY AS A CENTRAL FACTOR IN RISK MANAGEMENT

5. Implementation

a. Enhancing gender and diversity competence among RMO staff

To sensitise RMO staff to topics around gender and diversity, we organised a workshop on the person-centred approach in collaboration with the Gender Focal Person at the Corporate Security Unit. The workshop was structured in two main parts:
A **theoretical input** on the person-centred approach to security risk management and introduction into a risk assessment tool integrating personal identity characteristics (developed by the Corporate Security Unit).
A **practical exercise**, during which the participants were divided into three groups, and each group was presented with one security incident scenario. The scenarios reflected realistic security incidents in the Pakistani context, and the staff affected presented diverse profiles, including gender and gender identity, sexual orientation, medical conditions, disabilities, age, ethnicity, religion, and nationality. The participants then had to discuss how they would best respond to these incidents and what measures they would take to avoid similar incidents occurring in the future. This exercise was an opportunity to identify and reflect on how security and safety risks in Pakistan affect staff differently based on their profiles.

The aspect of cultural sensitivity

The topic of gender identity and sexual orientation remains a sensitive one in the Pakistani context. Therefore, it was crucial to approach it cautiously. At the beginning of the workshop, we clarified with participants that touching the security risks faced by staff with these characteristics was in no way a challenge to local cultural norms. Instead, it was a recognition on our part that staff with these characteristics exists, and we, as risk managers, must know how to best support them in dealing with the risks they face as part of our mandate.
Overall, the workshop was very well received, and participants were engaged. They appreciated the opportunity to reflect on staff diversity and how it affects risk management. Some participants wished the workshop lasted longer to allow more open-ended discussions.

"GIZ PAKISTAN RECOGNIZES THAT STAFF HAVE DIVERSE PROFILES THAT AFFECT THE SECURITY RISKS THEY FACE."

b. Amending RMO SOPs and relevant documents as per the work plan

Following the workshop, we initiated our work on amending RMO SOPs and other relevant documents from three central angles:

- Acknowledgement of staff diversity as a crucial factor in security risk management
- Provision of information to staff to make informed decisions about their security
- Adapt measures to facilitate staff members with diverse profiles

i. Acknowledge diversity as a crucial/essential factor in security risk management

Acknowledging an issue is often the first step towards making meaningful changes. Therefore, we included explicit references to staff diversity as a crucial factor in security risk management in all RMO SOPs and other revised documents. In this way, we put in black and white what we, as RMO staff, must consider when developing measures and giving recommendations, thereby contributing to changing practices in future.

At the same time, we also ensured that all our documents display inclusive language, including gender-neutral language. Employing gender-neutral language is not common in Pakistan; however, it is crucial to be inclusive and avoid wording that could be interpreted as biased or discriminatory.

ii. Provision of information to staff to make informed decisions about their security

As security risk management advisors, we must share information with staff members based on their personal profiles so that they can make informed decisions on their security and safety. Therefore, a crucial part of this project's implementation was ensuring that the revised documents included this information.

Concretely, this meant including:

- Crucial information on risks for specific groups, including the LGBTQI+ community, including resources they can consult
- Security-relevant information on cultural considerations, making sure we keep a broad perspective
- Security recommendations that cater to specific staff profiles
- Encourage staff to share any information on their personal profile that could be relevant to their safety and security voluntarily
- Information on what GIZ Pakistan already has in place to ensure the safety and security of staff with diverse profiles, including:
    - GIZ Pakistan's anti-sexual harassment policy
    - Policy on travel expenses as they relate to safety and security

iii. Adapt measures to facilitate staff members with diverse profiles

The most challenging aspect of this project was to make actual changes to our processes and procedures that would cater to staff with diverse profiles. Here, we focused mainly on two lines:

- Providing more training to specific staff profiles, such as drivers and security focal persons, who frequently deal with other staff members who may have specific safety and security needs – this includes, for instance, specified gender and disability awareness training
- Explore the flexibility within P+R to ensure that we can provide as much support to staff with specific needs as possible
- Ensure the provision of alternative security procedures and measures ensuring accessibility to all staff, including those with disabilities

6. Challenges

The main challenges that we have faced were two:

- **Time** – Reviewing SOPs as a group, finalise the documents, and get them approved from the Country Director is very time-consuming. Moreover, schedules are frequently busy! This has caused some delay in the implementation of our work plan, and while we expect to finalise all tasks by mid-2024, we would probably struggle to keep our original deadline of March.
- **Short-term outlook** – While we do believe that this initiative will have a long-term positive impact in ensuring the safety and security of all staff in GIZ Pakistan, it may not be noticeable in the short- and medium-term

IMPRESSIONS FROM THE WORKSHOP

"I appreciated the workshop's efforts to promote inclusivity and diversity. This [...] should continue to be emphasised in future workshops".

"Even if there may be religious sensitivities, we need to acknowledge that staff with [LGBTQI+] profiles exist and must be taken into consideration in our assessments".

"The workshop introduced a compelling concept: the person-centered approach. The discussion underscored the importance of embracing an inclusive lens in RMO operations".

"Addressing the security risks faced by LGBTQI+ staff is a recognition of ground realities."

TEAM!

Lidia Leoni, Sarwat Sughra, Nazia Kanwal, Brenda Mbaja Lubang'a, Manzoor Ali, Tahir Raza Rizvi, Zahid Zaman, Muhammad Sohail Khan

GALLERY