Working in Fragile Environments: Fit for Purpose?

Corporate Strategy Evaluation of GIZ’s Security and Risk Management in Foreign Assignments
GIZ’s corporate strategy evaluation

Corporate strategy evaluations are designed to promote corporate development. They evaluate the implementation and application of GIZ’s company-wide policies and strategies and look at the effectiveness, efficiency and quality of service delivery at GIZ. Their main aim is to identify aspects that serve to develop and refine the company’s basic approaches, methods and instruments. The findings and recommendations of corporate strategy evaluations provide the foundation for evidence-based learning and decision-making throughout the company.

Corporate strategy evaluations are carried out by independent, external evaluation experts. For each evaluation, the Management Board nominates one member of the Board or the Executive Management as a ‘mentor’ of the evaluation. Furthermore, an internal reference group is set up which consists of all relevant stakeholders and is chaired by the appointed mentor.

In order to ensure a valuable outcome for the company, the reference group monitors the evaluation process, discusses the findings and recommendations, and proposes appropriate measures to the Management Board.
Contents

Topic 04
Security and Risks in Foreign Assignments

Design 06
Gap Analysis: Fit for Purpose?

Main Findings 08
Good System – Inconsistent Implementation

Management Response 12
Enhancing Security in Structures, Processes and Culture
1. Topic

Security and Risks in Foreign Assignments

The general conditions for GIZ’s worldwide engagement are changing. In the past, one of the preconditions for engaging in development programmes was that there might be a reasonable chance of establishing sustainable structures in a stable partner country. Nowadays, GIZ is operating more and more in fragile contexts. In addition, the traditional division of labour between humanitarian assistance and development cooperation, as practiced in Germany, is dissolving. As part of its legal duty of care, GIZ therefore has a special responsibility to take precautionary measures to ensure the safety and security of its staff in its operations abroad. Effective security and risk management is essential in protecting the lives and health of GIZ staff at the project locations, and enabling effective project work.

New kinds of operations – new risks

GIZ now serves and will continue to serve a wider range of clients and programmes associated with new operations, such as in 2015 the resumption of activities in Somalia – one of the world’s poorest and most fragile countries. New types of project, such as support for the security sector, including public prosecutors in Pakistan and the police in Yemen, will reduce the perceived neutrality that GIZ once had. In Iraq for example, the German Government will engage in the anti-terror coalition via humanitarian and development assistance. As a result, GIZ becomes more exposed to new risks.

Meanwhile, more than half of the partner countries of German development cooperation are acutely affected by violent conflict or face the threat of escalating violence. As a consequence, GIZ increasingly has to ensure the health, safety and well-being of its staff in foreign assignments not only because of the legal and moral duty of care but in order to effectively deliver its services in countries with a precarious security situation.

Aid Worker Security

According to the 2014 Aid Worker Security Report, the year 2013 set a new record for violence against civilian aid and development operations, with 251 separate attacks affecting 460 aid workers. Of the 460 victims, 155 aid and development workers were killed, 171 were seriously wounded, and 134 were kidnapped. Overall, this represents a 66% increase in the number of victims from 2012.

Managing security – a precondition for working in fragile environments

A Security and Risk Management System (SRMS) aims to ensure a coherent, manageable and systematic approach to security across an entire organisation. Security of an organisation’s staff and assets is a precondition for sustainable implementation of its assistance and development objectives as it enables access to beneficiaries. The policy framework for GIZ’s SRMS is based on a set of international and national legal obligations and standards, such as ISO 31000:2009, German Occupational Law, Common Law and Company Law and the German Federal Foreign Office General (Travel) Guidelines.

GIZ’s own definition and understanding of security and risk management corresponds to ISO 31000:2009 on Risk Management, since it is designed to ensure:

1. The safety and security of German development cooperation personnel (national and international staff, consultants, etc.)
2. The security and sustainability of the investments that have been supported by German development cooperation
3. The ability to achieve the objectives of development cooperation measures.

GIZ’s SRMS Architecture

| Security Management | Crisis Management | Business Continuity Management | Human Resources and Knowledge Management |

Framework for Action:
- Security and Crisis Management in the Field
- Policy on the Safety and Security of Staff
- Specifications of the Federal Ministry for Economic cooperation and Development (BMZ)
2. Design

Gap Analysis: Fit for Purpose?

The overall aim of the corporate strategy evaluation was to further improve the policy, standards and instruments of GIZ’s SRMS. The evaluation findings and recommendations are intended to help achieve a balance between personal security and GIZ’s corporate and human capacities to effectively deliver services in fragile states and environments.

1. Examining scenarios - analysis of future potential risks
In order to check how flexible and adaptable GIZ’s SRMS is to changing circumstances, the evaluation first identified megatrends with far-reaching impact on business, economies, industries, societies and individuals, such as the ongoing fragmentation of nation states, the evolution of global terrorist networks, the potential for increased intrastate and interstate conflicts, climate change, natural disasters, pandemics and the growing demand for food, water and energy.

2. Evaluation criteria and questions
In stage 1, GIZ’s current SRMS was reviewed and assessed against the internationally accepted standards using a series of security and risk management indicators. Apart from the ISO 31000:2009 standards, this included the:

- EISF Security Audit Tool (European Interagency Security Forum, 2013) with the eight key sections:
  - Governance and Accountability
  - Security Framework
  - Security and Risk Management Culture
  - Operations and Programme Management
  - Security and Risk Management Implementation
  - Training, Learning and Development
  - Resourcing
  - Effectiveness Monitoring

In stage 2, the collected data and the analysis in stage 1 were analysed against the background of current and future risk environments using the OECD-DAC Guidance for Evaluating Humanitarian Assistance in Complex Emergencies:

- **Relevance**
  Is the current security management system relevant for the global humanitarian context, as well as for the core activities and programmes of the organisation? Will it remain relevant in the face of future risks?

- **Effectiveness**
  Does the system enable the development and implementation of effective security management? Do field staff comply with security management procedures?

- **Efficiency**
  Are adequate resources (human, physical, financial) made available and used efficiently?

- **Sustainability**
  Does the system facilitate a continuous, cyclical process of review and adaptation?

- **Coverage**
  Is the system appropriate to ensure adequate security management across the entire organisation?
- **Coherence**
  Is the security risk management approach aligned with the work and approach of other organisational approaches and with best practice across similar organisations working in the same risk environments?

3. **Data collection**
   The evaluation combined a desk study, semi-structured interviews with staff responsible for managing and maintaining the overall SRMS of GIZ, an online staff survey in 27 countries (response of 1,168 of 6,768 approached) and four country case studies (Kenya, Mali, Honduras, Pakistan). International benchmarking was intended to enable GIZ to build upon the best practices of other players in the field of international cooperation and humanitarian assistance. Therefore, additional interviews were conducted with HQ staff responsible for SRMS of United Nations, Department for International Development (DFID), Danish International Development Agency (DANIDA), Service Civil International (SCI), Save the Children).

---

### Online Staff Survey

**Have you been involved?**

*What kind of incident?*

*More than 68% of GIZ staff answered this question with ‘no’, some 28% answered ‘yes’.*

---

1. Organisation for Economic Co-operation and Development - Development Assistance Committee, 1999. The OECD-DAC principles included in this guidance document were originally established to evaluate development assistance programmes. Later the principles were complemented to encompass programmes covering crisis and conflict issues by adding the principles of ‘coverage’ and ‘coherence’. The principle of ‘impact’ was omitted, as it was deemed difficult to deduce whether specific security processes have directly resulted in the avoidance/reduction of security incidents and their severity.
3. Main Findings

Good System – Inconsistent Implementation

On paper, GIZ currently has a good and relevant SRMS. It complies with ISO 31000:2009 and compares well with the benchmarked organisations. In practice, however, it is not implemented consistently across countries and regions and not used by all staff. Security measures at the local, country and regional levels are developed in a fragmented and isolated way without central governance. As the evaluation showed, GIZ needs a company-wide security culture that is comprehensively communicated and accepted, and ensures consistency and the local application of a uniform system. The evaluation nevertheless showed that, where GIZ’s SRMS is effectively applied, many staff have expressed their satisfaction with the system. A majority of the staff involved in this evaluation feel safe both inside and outside of work.

Fragmented, without central governance

The main findings of the evaluation show that in its present form, GIZ’s SRMS is theoretically able to respond to current risk scenarios but it has to be regularly updated, communicated and adapted to local circumstances to be fully effective. Currently, security measures at the local, country and regional levels are developed in a fragmented and isolated way without central governance. Whilst good processes exist within the Crisis Desk and the psychological support service COPE (COoperation with PErsonnel in Stress, Conflict and Crisis), new processes are being developed largely ad-hoc and not coordinated at the country level. The current patchwork approach – mostly based on the personal commitment of either the country director or the risk management advisor (RMA) – leads to inconsistencies, thereby jeopardising the investment made in systems, staffing and approaches. Also, it often reflects the professional background of the local RMA (e.g. military, UN) rather than any established GIZ security culture.

Security seen as separate add-on

From the benchmarking study it is apparent that staff safety and security enables the delivery of programming. Within GIZ, however, as all data confirm, security and risk management issues presently do not influence the design or implementation of GIZ programming. Security is seen as a separate add-on. Risk management advisors are rarely included in programme level discussions, though where they are, such as in Pakistan, their contribution adds value to the programming. Routine conflict analyses do not focus on the issues of staff safety and security. Security issues are isolated from business performance with no clear and transparent mechanisms for balancing the needs of both. This also includes the question of financing. With few exceptions, the costs of security are currently met at the country level through project funding instead of being incorporated into a budget.
Reactive instead of proactive
GIZ’s SRMS is largely seen as being reactive to crises rather than proactive in trying to mitigate risks. As the data shows, this is closely related to the fact that GIZ’s country risk rankings are mostly based on external sources such as the local or regional German embassies. One exception is Afghanistan. Here the SRMS is based on information derived from reviewing actual threats experienced by staff and an on-going assessment/analysis of potential threats. The evaluation shows broad agreement that for a more preventive approach, risk assessments should be more specific and based on real project experience, as each country and even each single region has its own set of risks and solutions. However, this entails building up capacity in the country office, in order to sufficiently gather and analyse information and draw the necessary conclusions.

Lack of clarity about roles and responsibilities
Concerning the question, ‘Who is responsible for your security?’, the online survey as well as the interviews and the case studies demonstrate a lack of clarity about roles and responsibilities. In high-risk countries, however, there is a greater understanding of security with only 3% of staff stating that they

---

**Online Staff Survey**

**Who is responsible for your security?**

- Country Director (59.3%)
- Safety and Security Officer (35.9%)
- Risk Manager (43.1%)
- Others (8%)
- Yourself (48.9%)
- I don’t know (7.2%)

*The correct answer would be: 100% ‘country director’, 100% ‘yourself’. RMAs and security officers only advise.*
did not know who was responsible for their security. Many interviewed staff members considered the country director to be responsible, supported by the RMA. Few, international and local staff alike, had read the security policy documents and therefore understood their own responsibilities under the policy.

Insufficient documentation
Seventy-nine per cent of staff are aware that documents or plans exist, only 46% are familiar with them and only half of those find them useful. Security documentation is seen as not transparent, not regularly updated and consisting of too many different elements. One criticism is that the quality of documentation depends on the attitude and skills of the RMA. With no obligation to implement the GIZ SRMS, there is no yardstick to measure whether the country system is compliant with the corporate SRMS.

Need for training
In order to enable GIZ’s staff to assume their own responsibility within the SRMS, introductory and training courses on safety and security are vital. However, the survey reveals inconsistent staff training. Almost half of the respondents had not received any training or introduction to security issues. There is local training, but it is neither mandatory nor done routinely or according to any specific standard. Project and programme managers in particular were therefore interested in training in order to be able to fulfil their responsibilities related to their own safety, to the safety of their colleagues, and to ensure the delivery of programme objectives. The evaluation also revealed a need to train the RMAs. Communicating in a way that will motivate staff to take notice of risk and security issues and if necessary to take action is a skill that many RMAs do not have and which most of the interviewees agreed should be developed to improve the overall SRMS.

Lack of clarity about the duty of care
The evaluation demonstrates that some 61% of staff members think that the security processes contribute to feeling safe at work. When asked how safe staff feel outside working hours, the quota of positive respondents falls to roughly 40%. Combined with this is a lack of clarity about the duty of care that GIZ has for its staff outside working hours. Especially in crisis areas, this duty of care is defined by several legal parameters. According to German Labour Law, for example, the employer is not allowed to interfere with the private life of employees. This ambiguity about the limitation of duty of care is also reflected in the widespread perception (survey, interviews and case studies) that the SRMS is only meant for international staff and has little or no relevance to national personnel.

Low regard for safety and security among staff
There are a significant number of staff members who do not know about SRMS and for whom the SRMS simply does not matter. In general, except for a select few countries such as Afghanistan, the evaluation showed that there is low regard for safety and security issues among staff – most likely owing to GIZ’s former stance as a neutral international actor. For some, security is even misinterpreted as a kind of internal policing. For instance, in Mali the need to get travel clearance is perceived as an attempt by
the RMA to exercise excessive control over project staff members and seen as an obstacle to carrying out project activities. To remedy this, GIZ in Pakistan for example has included the country’s Risk Management Office (RMO) in the annual planning process to strengthen its position.

On the other hand, the evaluation revealed that international staff are not always well informed about security risks, with some 42% saying that they only occasionally or never receive information about the risks in the country of destination. In addition, travel rules are not enforced, e.g. staff are only required to send an email informing about their work-related travel before going to the field. And if they don’t, there are no consequences.

Need for a clear corporate culture of security
In addition to the recommended update of structures and processes, the evaluation therefore above all highlighted the need to develop and communicate a clear corporate culture and conscious perception of security issues, roles and responsibilities and the extent of GIZ’s duty of care.

Summary of recommendations
Based on these findings, the evaluation made the following recommendations. In its Management Response, GIZ reflected upon the recommendations and even further developed them.

- Establish and communicate a clear definition of GIZ’s duty of care
- Agree on level of risk acceptable to GIZ
- Develop a security culture internally
- Establish and enforce accountability and responsibility for staff’s own safety and security
- Develop a global approach to security and risk management
- Build capacity at Head Office level to better implement and support a global, uniform GIZ SRMS
- Encourage and promote regional cooperation
- Continually review and update SRMS
- Recruit RMAs in line with new skills set
- Make training in safety and security compulsory for all staff
- Renegotiate appropriate funding level for safety and security with clients and commissioning parties
Management Response
Enhancing Security in Structures, Processes and Culture

Compared to other organisations, the international benchmarking indeed showed a gap between GIZ's current SRM practice and that of its peers. However, encouraged by the best practices shown in the benchmarking, the Management Board decided to work on structures and processes as well as a culture and awareness of security, in order to catch up and update GIZ's SRMS. First of all, it decided to establish a special corporate security unit that reports directly to the Chair of the GIZ Management Board.

First step: new corporate unit for security and risk management
With the establishment of a central Corporate Unit for Security and Risk Management, the Management Board is sending out a clear signal to strengthen GIZ's security architecture worldwide. The main task of the new unit will be to ensure the implementation of a uniform approach in all countries where GIZ is engaged. It has the policy-making power to instruct local RMAs, country directors and regional units how to build a consistent GIZ SRMS and how to monitor it. As a direct consequence of the findings of the corporate strategy evaluation, the Security Unit will also gather, analyse and assess local risks.

Three fields of action
The evaluation reference group and the Task Force on Delivery Capacity in Fragile States developed three fields in which action must be taken. All proposed measures followed the recommendations and were immediately accepted and decided by the Management Board:

1. to integrate SRM into GIZ's corporate strategy and core processes,
2. to strengthen and qualify professional SRM structures and quality standards (at Head Office and locally),
3. to communicate a global corporate-wide security and risk culture, raise the awareness of staff for security issues and train them accordingly.

1. Integrating SRM into corporate policy and core processes

Clear definition and communication of GIZ's duty of care
Corporate-wide strategic alignment of SRM calls for a shared understanding of the extent of GIZ's duty of care. As the evaluation showed, there is no uniform comprehension within GIZ, especially with regard to the limits and legal restrictions of the corporate duty of care for local staff in the partner countries.

Linking security and programming more closely
Risk assessments will be considered thoroughly and systematically in future project assignments. In future, country directors and risk management advisors in high- or medium-risk countries will be obliged to consult the new Corporate Unit concerning GIZ SRM standards and their implementation.

Appropriate funding for safety and security
To ensure that appropriate security provisions can be financially supported at the country, regional and
global level, GIZ will actively communicate the costs of an effective SRMS to its clients and commissioning parties. Based on professional, centralised risk analysis and assessment, appropriate funding will be integrated into all budget negotiations for projects in high- or medium-risk countries and regions.

Targeted recruiting of risk management advisors
GIZ will revise its job descriptions for RMAs. The specific skills range will be reviewed. Further skills that RMAs need, such as communication and persuasive power, will be included.

2. Strengthening professional SRM structures and quality standards
In order to be more proactive in the assessment of risks and to ensure compliance with SRM quality standards, structures at GIZ Head Office will be strengthened by the establishment of the Corporate Security Unit. This includes regular contact to German security authorities for a better exchange and analysis of information. As the evaluation showed, successful SRM calls for competent local security risk management advisors. In order to increase the consistency and effectiveness of SRM, GIZ will therefore form a pool of qualified RMAs.

3. Establishing a corporate-wide security and risk culture
Rules and processes do not exist in a vacuum. To make sure security is taken seriously, there has to be a paradigm shift. This will be achieved by an organisational push as well as the creation of an internal culture so that staff consider security as a needed, necessary and valuable aspect of organisational and operational success. GIZ will therefore launch a corporate-wide discourse as well as an awareness-raising campaign for staff and clients and commissioning parties about GIZ’s handling of risks. Accountability and responsibility for safety and security will also be reinforced by integrating SRM issues as appraisal criteria for senior staff in human resources policy and processes.

Compulsory training in safety and security for all staff
To make sure that international staff on foreign assignments in fragile contexts are qualified in security and risk management, training prior to the assignment is now compulsory, and is supplemented, if necessary, by additional training in the partner country. As shown in the evaluation, local staff often perceive SRM measures as applying primarily to international staff on foreign assignments. Therefore, local colleagues will be more explicitly integrated into security round tables and local training courses than in the past.

Annual objective 2016: consistent SRMS
Overall, the findings of the evaluation demonstrate that GIZ has a good security and risk management framework that can be developed and modified to suit local and future circumstances – but it simply needs to be implemented. A globally implemented approach to security and risk management will achieve consistency and accountability in all GIZ operations and be much more efficient and effective in ensuring staff safety and security. Translating the management response into action is therefore one of GIZ’s annual corporate objectives for 2016.
As a federal enterprise, GIZ supports the German Government in achieving its objectives in the field of international cooperation for sustainable development.

Copenhagen Group A/S and Safer Edge Ltd. were commissioned to carry out the corporate strategy evaluation GIZ’s Security and Risk Management in Foreign Assignments

Published by
Evaluation Unit
Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

Registered offices
Bonn und Eschborn
Friedrich-Ebert-Allee 36 + 40
53113 Bonn, Deutschland
T +49 228 44 80-16 40
F +49 228 44 80-26 44
E evaluierung@giz.de
I www.giz.de

Responsible for publication
Dr. Ricardo Gomez

Project management
Claudia Kornahrens

Concept and text
pfif – Pressefrauen in Frankfurt
Carmen Sorgler

Design
F R E U D E ! design, Rendel Freude

Photos
P 03 GIZ office GIZ / Markus Matzel, p. 05 Afghanistan GIZ / Britta Radike, p. 07 Addis Abeba GIZ / Thomas Imo/photothek.net, p. 08 Ramallah GIZ / Ursula Meissner, p. 10 South Sudan GIZ / Michael Tsegaye, p. 13 Tsunami Early Warning System GIZ / Ursula Meissner.
All pictures were made within the context of GIZ’s work.

Duplication
GIZ

Paper
Artic Volume 300g/m2 (cover) and 115g/m2 (inside page) FSC-certified

Editorial deadline
30.09.2016