Annual GIZ Compliance Report

2020

giz Deutsche Gesellschaft
für Internationale
Zusammenarbeit (GIZ) GmbH

Compliance and Integrity Unit
September 2021

Content:

1. Summary of key results

The consolidation and further development of the Compliance Management System (CMS) as an overall system remains a key area of priority. In the reporting period, the risk-based approach and differentiated response to risks continued to prove effective, such that no significant process adjustments were necessary. GIZ has a comprehensive risk management system via which compliance and integrity risks are regularly reported from across the entire company before being assessed and systematically dealt with. The relevant risks are addressed as part of the annual compliance programme. For this, GIZ can draw on a large number of established and proven principles and measures, which are refined in line with requirements.

The CMS is subject to a continuous improvement process, which is monitored by the Compliance and Integrity Unit on an ongoing basis. Needed adjustments are regularly documented in operational plans and their implementation is reviewed on the basis of monitoring plans. The Compliance and Integrity Unit reports the findings annually to the Management Board and every two years to the Supervisory Board to support these bodies in their monitoring function. As the CMS is also part of GIZ's comprehensive internal control system, the work of the Compliance and Integrity Unit is also subject to internal audits by the Auditing Unit.

2. GIZ's Compliance Management System (CMS): implementation status

Ensuring compliance is an increasingly important factor in the activities of German and international companies and institutions, a fact also reflected in the business environment and trends monitoring process. In particular, GIZ is facing growing challenges in terms of the correct implementation of commissions due to ever-greater complexity, new commissioning parties and working under severe time pressure in increasingly difficult locations.

The CMS is intended to help the GIZ workforce address these challenges in a professional manner, give them more certainty in their actions and avoid potential breaches of compliance rules at organisational level. In this spirit, GIZ works continuously to expand its CMS in a targeted manner based on the standard issued by the Institute of Public Auditors in Germany (IDW AuS 980) and the international management standard ISO 37301. This ensures that the CMS is comprehensively updated taking into account all relevant factors. GIZ's CMS also encompasses internal anti-corruption and integrity management.

The following sections of this report show which other significant milestones were reached in 2020 in the **seven core CMS elements**:

- **Compliance culture:** Orientation towards values is essential for GIZ's compliance management and therefore also the personal integrity of its workforce. A raft of preventive measures are thus geared towards a compliance culture that fosters the alignment of everyone's behaviour with the corporate values and compliance requirements. The culture of responsibility was reinforced further by introducing additional specific responsibilities for compliance issues.

- **Compliance objectives:** Compliance is mainstreamed in the Corporate Strategy as a governance element. Accordingly, the compliance objectives are based on GIZ's objectives. In 2020, a specific compliance objective on data availability was also included in the corporate objectives (also see Section 4.1. Case management system).

- **Compliance risks** (see Section 3)**:** GIZ's CMS takes a risk-based approach. Since 2020, compliance risks of particular relevance have been recorded in separate risk

maps. This practice provides company-wide risk management with a continuous overview of the specific compliance risk situation.

- **Compliance programme** (see Section 4)**:** The compliance programme covers the compliance principles as well as all the preventive, explanatory and reactive measures implemented by GIZ to ensure compliance and limit its exposure to compliance risks. Appropriate mechanisms are in place to ensure that breaches of the compliance rules can be detected and dealt with effectively.

- **Organisation of compliance management:** the focus here is on ensuring that compliance management is firmly embedded within the company. At GIZ, this is achieved by making sure that the CMS has the resources needed to perform its designated function: the roles and responsibilities of those units involved in operating the CMS as well as the associated procedural structures are in place and a well-functioning governance structure with specialist bodies (Compliance Commission and Compliance Committee) has been established.

  The Compliance and Integrity Unit has coordination and controlling functions within the company-wide CMS that include identifying the need for action and demanding the necessary measures. Through the establishment of the 'Compliance and Integrity Advisory Services, Case Management' section within the unit, case management has been further professionalised since October 2020 by pooling case processing in this specialised section and by introducing standardised procedures in case processing (e.g. whistleblower and accused protection, low-threshold access options).

  The organisation of compliance management that has now become established has also generally proven effective in the field structure. In a small number of countries (e.g. Afghanistan, Ethiopia), country directors/heads of finance and administration are supported by compliance officers at country level.

- **Compliance communication** (including compliance training and reporting): Analysing and communicating compliance-related information and experiences has a positive impact on the compliance culture, facilitates transparent reporting, gives staff greater certainty in their day-to-day work and enables compliance risks and incidents to be dealt with more easily (see Section 4.4 for information on the compliance training measures implemented).

- **Monitoring and improving compliance** (see Section 5)**:** Compliance management systems can only be effective if they are capable of 'learning'. The suitability and effectiveness of the CMS is thus assessed on an ongoing basis and experiences are evaluated in order to highlight necessary adjustments.

3. Evaluating and dealing with compliance risks

3.1. The risk-based CMS approach and key risk-related issues identified following the implementation of this approach

An effective compliance management system aims to prevent sanctions, financial loss and damage to GIZ's reputation. Nevertheless, there is no way to completely eliminate the possibility of breaches. Rather, the aim is to exercise due diligence. To identify the key fields of action and measures for this, the **analysis of the main compliance risks is the starting point** for the compliance programme.

At GIZ, the **CMS is part of the comprehensive internal control system (ICS)**. The aim of the ICS is to avoid risks (prevention), identify problematic issues at an early stage (detection) and respond appropriately to non-compliance and unavoidable risks (response). It is based on the 'three lines' model in accordance with international standards:

- The first line includes the application of the cross-check principle and the separation of functions, monitoring by line management and the mechanism of internal controls.
- In the second line, in-process monitoring of the first line and the further development of the system is ensured through tools such as compliance management, risk management and financial control.
- As the third line, the Auditing Unit monitors the correct functioning and effectiveness of the ICS and identifies possible weaknesses and potential for improvement as part of its routine audits in Germany and abroad and in the course of process audits.

With its ICS, GIZ also has a **comprehensive risk identification system** via which current compliance and integrity risks from across the entire company are regularly reported.

The most problematic areas at the level of the company as a whole are also identified annually by **analysing the compliance risks** and are assessed in the form of a **risk control matrix**. The current risk control matrix (December 2020) provides an overview of the current high, medium and low compliance risks. In it, each risk topic is evaluated according to loss potential and probability of occurrence. The matrix takes a 'net' perspective, i.e. the risk-mitigating measures that are already established are taken into account. In addition, it lists individual compliance issues without explicit issue responsibility and provides an overview of compliance issue responsibilities for which no risk analysis is yet available. The table describes the additional action required in each case. In order to keep compliance risks to a minimum, the **priority fields of action and need for action** are derived from the risk control matrix and gathered in an **operational plan**. These are dealt with as part of the **compliance programme** through specific measures that are agreed with the relevant (specialist) units and mainly implemented by these.

The analysis of compliance risks is a **continuous improvement process**. It aims to deal with all relevant compliance and integrity risks according to their priority and ensure continuous updates and adjustments based on changing requirements.

Moreover, GIZ is subject to a **large number of external audits** in which it has to regularly prove proper use of the funds entrusted to it.

3.2. Risk-based compliance management in the field structure

In 2020, the corporate unit supported the continuation of the extensive implementation of compliance management in the field structure, based on prevailing needs.
The list of criteria grid for allocating countries to compliance risk categories is reviewed annually and updated as necessary (most recently at the end of 2020 for the 2021 process). In 2020, three countries were placed in the very high compliance risk category (previous year also three) and 22 countries in the high compliance risk category (previous year 21). The number of countries in the medium and low compliance risk category was 22 (previous year 21). The compliance risks identified locally have been regularly incorporated into the risk management process (RM 2.0) and reported as part of risk assessment, meaning that they are continuously fed into the company-wide process for tackling risks.

The risk-based approach and differentiated response to risks have proven effective, with the result that no significant process adjustments have been necessary. It should be noted that the implementation of the respective requirements varies in quality from country to country.

4. Compliance programme

4.1. GIZ regulations and measures

The compliance programme includes those regulations and measures designed to prevent corruption and promote integrity that are already firmly established at GIZ. The Compliance and Integrity Unit also ensures the implementation of the current compliance-related measures and systematically enhances the compliance programme on an ongoing basis.

The following **regulations and measures** have been **established** at GIZ:

- Code of Ethics
- Code of Conduct
- Contractual obligation requiring all those working for GIZ to observe the Code of Conduct
- Compulsory training on compliance
- Whistleblower system
- Compliance and integrity advisory services
- External ombudsperson
- Transparency of procurement processes in Germany and in the field structure
- Prevention of corruption through staff rotation
- Additional measures to prevent corruption

The Compliance and Integrity Unit also implemented the following measures in the period covered by this report:

- **Compliance training:** The two **new, mandatory, web-based compliance training courses** for all staff, development workers and managers have been rolled out company-wide since November 2020 following the technical modifications to the new learning platform of the Academy for International Cooperation (AIZ) and are mainstreamed as mandatory formats in the new onboarding process.

- **Anti-corruption management:**
  - In 2020, the GIZ's Compliance and Integrity Unit published the **Anti-corruption Policy**, which manifests GIZ's zero-tolerance policy in cases of corruption.
  - In December 2020, the Compliance Committee decided to establish the **Response Body**, which will handle all corruption-related cases during the initial two-year pilot phase. This approach is intended to ensure uniform handling of disciplinary action under employment law against GIZ staff in response to all cases of corruption in Germany and abroad.
  - In 2020, the Corporate Unit prepared a company-wide **inventory of work areas particularly susceptible to corruption**, which is to be carried out in 2021.

- **Internal control systems (ICS):**
  - To refine the quality of the ICS and to strengthen its governance role and visibility at overall company level, the Management Board decided in July 2020 to create an **ICS governance function** as part of the Compliance and Integrity Unit from 2021.
  - Its primary task is to carry out a **systematic ICS inventory** for GIZ that allows an objective assessment of the current ICS and its positioning in the maturity model. Based on this, an **ICS description** is prepared in **accordance with Auditing Standard** 982 of the Institute of Public Auditors in Germany (IDW AuS 982).

- On this basis, any risks and need for action are to be identified and measures for implementation are to be formulated, which are necessary for the gradual **refinement of the ICS**.

- **Business partner checks** (BPCs) are integral to a functioning compliance management system. Adequate BPCs are necessary to protect GIZ from financial loss and reputational damage as well as criminal violations. GIZ's **system of business partner checks** was **refined** in a one-year project in 2020. The existing, essential business partner check processes were analysed and evaluated with regard to the fulfilment of due diligence along defined target requirements (legal requirements, economic and professional suitability of business partners). The project led to the following findings:

  - GIZ generally deals adequately with business partner checks, although a need for action remains in several points; these were communicated to the relevant units.
  - There is a lack of digitalised documentation of the results of business partner checks.

- **Case management system:**

  - In 2020, the Compliance and Integrity Unit obtained new resources to **set up a central case management system** in connection with the Management Board's objective of ensuring the availability of data on compliance violations.
  - In this context, cases of intentional misappropriation of funds are now recorded jointly by the Auditing Unit and the Compliance and Integrity Unit (also see the Auditing Unit's annual report to the Management Board). For these cases, both units have jointly developed a binding report form that is posted in the central Processes and Rules (P+R) and a work instruction on reporting the misuse of funds.

- **Duty to supply information**: Since October 2020, GIZ's P+R has included an **extended obligation to report suspicions of serious compliance infringements for all management personnel** (P+R Rule 554). The rule explicitly identifies the case categories agreed with BMZ for the new annual BMZ reporting on relevant compliance incidents. To obtain the figures:

  - for the first report to the shareholder, a supplementary **individual enquiry** was initiated for **all country directors** regarding the items not yet reported to Head Office at that time;
  - taking this as a basis, a simplified **monitoring process** was agreed with the departmental advisors for reported cases in the context of future country reports to avoid any additional individual enquiries of this kind. This will be implemented for the first time in the 2021 reporting year.

4.2. Handling of compliance and integrity cases in 2020

4.2.1. Overview of compliance cases in relation to GIZ's core regulatory framework 'Processes and Rules'[1]

---

[1] For the 2020 reporting year, it should be noted that this annual compliance report only lists the case numbers from the reporting channels for which the Compliance and Integrity Unit is responsible. The Auditing Unit's 2020 annual report, on the other hand, lists all cases of misappropriation of funds reported in GIZ (including those reported through the reporting channels of the Compliance and Integrity Unit). With the new reporting to the shareholder, the correspondingly adjusted category system for the presentation of compliance incidents will also be introduced in the annual compliance report starting in the 2021 reporting year.

During the period covered by this report, the Compliance and Integrity Unit handled a total of 103 cases (previous year: 71) in relation to GIZ's core regulatory framework 'Processes and Rules'. The year-on-year increase is likely to be related to the new mandatory reporting from management personnel. The cases break down as follows:

- A total of 30 **requests for advice** were received (previous year 35). In terms of content, these related primarily to the avoidance of conflicts of interest, questions relating to the detection and prevention of corruption and to GIZ's reputation.

- A total of 51 **reports** (previous year 36) on possible breaches and irregularities were submitted from internal and external sources via GIZ's reporting channels on compliance-related incidents. Most of the whistleblowing reports related to fraud or corruption incidents perpetrated by or involving GIZ staff or business partners and other violations of GIZ rules and procedures.

- Given that management personnel have been required to report serious compliance violations to the Compliance and Integrity Unit (previously to the Auditing Unit) since October 2020 in accordance with the extended obligation to report, the Compliance and Integrity Unit has introduced a new reporting category for this purpose. In the reporting year, management personnel filed 22 **reports** of possible or demonstrated breaches and irregularities. These related primarily to invoicing fraud or attempted corruption by GIZ staff as well as misuse of funds by business partners. The rule was implemented relatively well, given that 65 of the total of 72 compliance and integrity incidents reported by the country directors in the individual enquiries of the field structure were already known or had been reported to Head Office. However, there is still room for improvement in the speed of information. In some cases, information was only provided after the incident had been handled locally, which can hinder the Compliance and Integrity Unit's ability to perform its mandate.

Of the 73 reports received in 2020, it was possible to close 49 cases. Of these, **evidence of compliance breaches** was established in 11 cases. Appropriate consequences were administered and remedial action was taken, for example disciplinary measures, write-offs, terminating business relationships, tightening up control processes and raising awareness among internal and external personnel involved in those processes.

4.2.2. Overview of integrity cases handled in relation to GIZ's Code of Conduct

During the period covered by this report, the Compliance and Integrity Unit handled a total of 228 cases relating to the Code of Conduct.

The number of **requests for advice declined** from 244 in 2019 to 156 in 2020. The main areas in which staff members sought help from the integrity advisor were: 'Employing or awarding contracts to closely connected or related parties', 'Personal and financial connections' and 'Gifts and other advantages'. Overall, by preventing or at least limiting the scope for potential misconduct and compliance breaches and by increasing awareness of GIZ's corporate principles, this channel for submitting requests and receiving advice on integrity matters plays a crucial role in the wider effort to prevent corruption while strengthening GIZ's orientation towards values.

At 72, the number of new **misconduct reports likewise decreased** in 2020 compared with 2019 (113). For 17 out of a total of 72 closed reports, it was **possible to identify misconduct** by GIZ personnel. Out of all cases of **proven misconduct** by GIZ staff, the most frequently occurring categories were 'Contractual and legal compliance' (5) and 'Sexual misconduct' (4). **Appropriate corrective action** (e.g. stopping payments; modifying responsibilities; procedural changes; additional inspections and analyses) was taken in all cases of proven

misconduct in order to bring about a solution (e.g. rectify any incomplete documentation or arrange repayments). Disciplinary, civil and criminal action was also taken and various penalties were imposed (written warnings, termination of employment). The reports received in 2020 concerning **breaches of the principles underlying the Code of Conduct** again related primarily to contractual and legal compliance and cooperation in partnership.

In 2020, the **ombudsperson** was contacted in 10 cases (previous year: 19). These reports mainly related to the incorrect settlement of project funds and manipulation in contract award processes.

4.3. Compliance training

All groups that make up GIZ's overall workforce take part in the monthly **onboarding event** for new staff members, development workers and CIM integrated experts, and receive initial **basic information on compliance, integrity and anti-corruption** at GIZ.

From August 2015 to November 2020, participation in the approximately 45-minute **web-based training (WBT) course on ethical conduct** was mandatory for GIZ staff. Since November 2020, two new WBTs have been rolled out worldwide that are based on the compliance risk analysis and whose content is aligned with current compliance requirements. According to the Code of Conduct and P+R Rule 552, all members of the workforce are required to participate in the **new compliance basic module** (which takes about four hours to complete) and all management personnel are additionally required to participate in the **new compliance module for managers** (which takes about one hour to complete). The contents of the former WBT on the Code of Conduct have been integrated into the compliance basic module. The two new WBTs must also be repeated every three years. Managers are responsible for ensuring that the training is carried out. To this end, they have access to a monitoring function on the AIZ learning platform (learning-giz) that they can view at any time and that provides information on the current participation status of the staff for whom they have disciplinary responsibility.

Both WBTs are **mandatory components of the onboarding programme for all new staff** and must be completed by them within their first 100 days at work.

The **responsibility of managers to lead and set an example in the areas of compliance and integrity** is also one element of the **self-learning module 'Digital HR module for managers'**.

In the context of the **compliance management** process **in the field structure**

- the Compliance and Integrity Unit carried out **consultations** for several countries with high and very high compliance risks;
- the heads of finance and administration bear a special responsibility, which is why the Compliance and Integrity Unit offered them two **compliance practice workshops** tailored to their needs at the 2020 heads of finance and administration conference.
- the unit compiled a **toolbox** (which is available on IDA) in response to the need for more practical assistance expressed at the heads of finance and administration conference.

4.4. Other Compliance and Integrity Unit activities in 2020

The unit regularly participates in dialogue events, in particular on anti-corruption, for example in connection with its membership of Transparency International.

In the reporting year 2020, which was dominated by the COVID-19 pandemic, no further external activities took place.

5. Monitoring and improving compliance

Monitoring the adequacy and effectiveness is a central element of a functioning CMS. It enables the identification of vulnerabilities in the CMS, the derivation of measures and, in turn, the **system's continuous improvement**. This requires **good management tools**.

The appropriateness and effectiveness of the elements of the CMS are reviewed on an ongoing basis. Moreover, **necessary adjustments to the CMS** are derived from a number of sources, in particular the internal control system, the compliance risk control matrix, the Compliance and Integrity Unit's operational plan and appraisal of reporting across the company.

The Compliance and Integrity Unit produces a **monitoring plan** each year on this basis. In 2020, it refined the plan based on the recommendations of the Auditing Unit regarding the effectiveness of the CMS. The updated monitoring plan provides an overview of the content, nature and status of the unit's annual and recurring activities each year. These measures also include the regular updating and optimisation of the compliance risk control matrix, thereby integrating it directly. In addition to the monitoring measures, a description is provided of the CMS' primary fields of activity as well as their impact (if possible) and orientation. The measures planned there are **implemented in the current compliance programme** and the results are regularly monitored by the Compliance and Integrity Unit and **documented in the CMS handbook**. In future, the monitoring plan will be regularly **submitted to the Compliance Committee** at the end of the year for consideration and, if necessary, further guidance. In this way, the body's steering and guidance function will be strengthened.

In order to support the Management Board and Supervisory Board in their task of monitoring the CMS, the **Compliance and Integrity Unit provides an update on the CMS** to the Management Board each year and to the Supervisory Board every two years. An abridged version of the Management Board report is also published on IDA. It omits in particular the risks from the risk control matrix, as this is confidential information.