Annual GIZ Compliance Report

2023

Deutsche Gesellschaft
für Internationale
Zusammenarbeit (GIZ) GmbH

Table of contents

1. Summary

Compliance is of fundamental importance for GIZ's work and its credibility. The Management Board informs the Supervisory Board annually in an **integrated report** on GIZ's **Compliance Management System (CMS)**, **Internal Control System (ICS)**, **Tax Compliance Management System (TCMS)** and **Information Security Management System (ISMS)**.

GIZ's CMS is designed to anchor legally compliant behaviour in the thoughts and actions of all employees and to strengthen a culture of compliance in the long term. The Code of Ethics sets out GIZ's ethical principles, describes the conduct the company expects of all employees and indicates options for reporting misconduct, how this misconduct is investigated and possible ways in which GIZ may respond appropriately.

GIZ focuses on identifying potential structural risks and avoiding non-compliant behaviour within the company. **The CMS and ICS are based on a risk-based approach**, which also proved its worth in the 2023 reporting year, with the result that **no significant process adjustments were required**.

As a basis for further developing the CMS, since 2023 GIZ has followed the new international standard DIN ISO 37301 Compliance Management Systems, which is founded on the principles of responsible leadership, appropriateness, integrity, transparency, accountability and sustainability. By conforming to ISO 37301, GIZ can demonstrate the effectiveness of its CMS on the basis of an internationally recognised standard.

Central responsibility for the ICS is a prerequisite for achieving the desired ICS maturity level ‘monitored’. An ICS of this maturity level enables GIZ to gain an overview of risky processes within the company, identify and thus prevent relevant control weaknesses at overall company level, systematically learn from mistakes and fraudulent activities and to adapt control measures accordingly. At GIZ, the ICS and CMS are closely linked and constitute a key pillar of the company’s risk management system.

2. Evaluating and dealing with compliance and ICS risks

An effective **CMS** aims to prevent sanctions, financial loss and reputational damage. Nevertheless, there is no way to completely eliminate the possibility of breaches. The aim is therefore to address relevant risks by exercising **due diligence**.

GIZ's **ICS** is based on the **Three Lines Model** in accordance with international standards. The interaction between the three lines aims to avoid risks and the violation of regulations (prevention), identify problematic issues at an early stage (detection) and respond appropriately to non-compliance and unavoidable risks (response).

- The **first line of risk management** encompasses operational management in the framework defined by GIZ's internal Processes and Rules (P+R). In addition to process-integrated monitoring measures, for example the cross-check principle and the separation of functions, this also includes process-independent monitoring measures such as risk reporting at least every six months and the internal control of projects and offices.
- The **second line** performs **overarching governance tasks** and supports and monitors **risk management**. Elements include the CMS, risk management, controlling, the Information Security Management System and the ICS governance function.
- The **third line is the Auditing Unit**, which monitors the appropriateness and effectiveness of the first and second lines through routine risk-based audits, special audits and process audits. This enables the unit to **identify** possible weaknesses as well as scope for improvement.

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

As part of the risk-based approach, the ICS evaluates the work involved in carrying out controls in relation to the respective risk. Cost effectiveness and process efficiency issues are also taken into account. The core element of the risk-based CMS is the analysis of key compliance risks. Current compliance and integrity risks are reported regularly from across the entire company using the comprehensive risk identification system, for example through the risk assessments carried out by compliance officers, in the Audit Coordination Committee.

In June 2023, the Management Board decided to combine the existing compliance and risk management committees into two new bodies, the Risk and Compliance Committee and the Risk and Compliance Sub-Committee, in order to make the **link with company-wide risk management** even more efficient.

3. GIZ’S Compliance Management System

Ensuring compliance is an increasingly important factor in the activities of German and international companies and institutions. GIZ is facing challenges with regard to the correct implementation of commissions due to ever-greater complexity, new commissioning parties and severe time pressure in increasingly difficult locations. The CMS is intended to help **employees address compliance requirements in a professional** manner, to provide **greater certainty for taking action** and to prevent potential **breaches of compliance rules at organisational level**. CMS **reporting** is based on the following **CMS elements:** compliance context, compliance risk analysis, compliance organisation, compliance processes, compliance in business processes, compliance monitoring and improvement. GIZ achieved the following milestones in the 2023 reporting year:

3.1. Compliance context

The CMS is part of GIZ’s corporate governance. Its scope of application essentially covers all core, support and management processes, and it applies to GIZ’s business activities worldwide. The Management Board ensures that the commitment to compliance is maintained in the company and that corporate objectives do not jeopardise compliance-compliant behaviour. As a sub-area of corporate governance, compliance is anchored in the corporate strategy, and the compliance targets are derived from the corporate objectives.

The objective of **reviewing CMS** – with focus on both the field structure and Germany – has been **successfully completed**:

- In 2023, Deloitte audited GIZ's CMS for compliance with the international standard ISO 37301. According to Deloitte’s assessment, the CMS principles, procedures and measures (regulations) implemented at GIZ during the audit period (July, August 2023) do not reveal any material weaknesses with regard to the requirements of ISO 37301. Implementation of all individual findings is feasible in the near future or is already underway.
- The audit of the four focus countries was completed successfully by EY. The findings confirmed that the company’s compliance management system in the field structure is overall fit for purpose and has been properly implemented. Compliance culture, compliance organisation and P+R received particularly positive assessments.

3.2. Compliance risk analysis

In the CMS, which takes a risk-based approach, the analysis of the key compliance risks is the starting point for identifying the areas of action and measures relevant for ensuring its effectiveness.

The Compliance and Integrity Unit conducted a comprehensive evaluation of the country risk profiles for GIZ’s countries of assignment for the 2023 reporting year. The risk-based approach and the categorisation of countries have proven effective and were confirmed. In absolute terms, risk countries and high-risk countries display more medium and high net risks. The evaluation's findings were presented and discussed in both the Risk and Compliance Committee and the Risk and Compliance Sub-Committee and at meetings of the heads of finance and administration in the reporting year.

3.3. Compliance organisation

Compliance management is mainstreamed within the company by making sure that compliance structures have the resources needed to perform their designated function. The compliance roles and responsibilities of the different job categories and bodies are set out in the Basic Compliance Rules.

Orientation towards values is essential for GIZ’s compliance management and the personal integrity of its workforce. Many **preventive measures** are therefore geared towards a **positive compliance culture** that encourages all employees to act in accordance with corporate values and to observe compliance requirements. Compliance is also always a leadership task, and managers have a special role to play in shaping the culture of compliance. Through their day-to-day actions as manager and the example they set, they encourage staff to adhere to rules and act with integrity.

The Procurement and Contracting Section and the Property Section in particular have a high number of compliance officers and are responsible for complex processes and areas of law with corresponding risk profiles. Together with the Compliance and Integrity Unit, the sections held several workshops with the management teams in the 2023 reporting year and drafted recommendations and measures to foster a positive culture of compliance.

3.4. Compliance processes

GIZ’s compliance policy and strategy establishes the framework for all compliance processes. In addition to the central, binding regulatory framework of Processes and Rules (P+R), compliance-specific regulations include:

- Code of Ethics
- Code of Conduct
- Basic Compliance Rules
- Compulsory web-based training on compliance (WBT)
- Whistleblower system with various access channels
- External ombudsperson
- Independent and autonomous central compliance and integrity advisors
- Access point for complaints related to sexual misconduct, discrimination and bullying
- Obligation to report serious compliance violations for all management personnel
- Anti-corruption policy
- Response Body
- Risk-based compliance management in the field structure
- Professional contract award management in Germany and in the field structure

3.4.1. Anti-corruption management

In line with a Shareholder resolution, GIZ is obliged to implement the German Government's guidelines on preventing corruption in the federal administration as appropriate. These include rules on the cross-check principle, transparency, the separation of functions, corruption prevention structures and case management, which are implemented with the help of the CMS and ICS. Work areas that are particularly susceptible to corruption must also be identified in this context, and assignments in these areas must be of limited duration.

As part of a company-wide process, the Compliance and Integrity Unit has surveyed all departments and units and prepared a list of all divisions and sections that are at risk of corruption. Based on this survey, the Management Board adopted the list in May 2023 and decided that assignments to these positions were not to exceed six years. Job or task rotation must be carried out after six years and documented. If there are important grounds for not undertaking job or task rotation after six years, the line manager must outline the reasons, initiate suitable and effective compensatory measures for preventing corruption and document these accordingly.

3.4.2. Case management – Processing compliance and integrity cases

Reporting on compliance and integrity cases covers all processes related to criminal law, to GIZ's core regulatory framework P+R and to the Code of Conduct, as well as general requests for advice and complaints.

In the **2023 reporting period**, the Compliance and Integrity Unit handled a total of **828 cases** (2022: 678), reflecting a continued increase in 2023. Among other factors, the increase is due to a higher volume of business and greater awareness of integrity issues.

Cases not relevant for investigation

- A total of 301 requests for advice were received (2022: 252). In terms of content, these related primarily to the avoidance of conflicts of interest, questions relating to gifts and other advantages as well as questions on interpreting P+R rules.
- A further 33 cases were not relevant for investigation. These involved matters not related to compliance violations (e.g. general queries about the situation in the partner country, non-selection in GIZ recruiting).

Cases relevant for investigation

- 226 reports (2022: 208) of possible breaches and irregularities were submitted by internal and external sources via GIZ's reporting channels. Most of the reports related to conflicts of interest, fraud or corruption-relevant incidents involving GIZ staff or business partners and other infringements of GIZ's rules and procedures. GIZ's online whistleblower portal was used 103 times (2022: 105). The ombudsperson was contacted by 10 whistleblowers (2022: 4).
- In the 2023 reporting year, 268 reports of possible or proven (internal) breaches and irregularities were submitted to the Compliance and Integrity Unit (incidents, 2022: 167). These primarily involved fraud relating to expenses and invoicing committed by GIZ staff, the fraudulent misuse of funds on the part of recipients of funding, and the theft of property belonging to GIZ or project partners.

Of the 494 (2022: 375) reports (incidents) received in 2023 that were relevant for investigation, it was possible to close 328 cases. Evidence of compliance breaches was established in 129 cases (2022: 68). Appropriate steps were taken and/or remedial action initiated (e.g. disciplinary measures, terminating business relationships, tightening up control processes and raising awareness among internal and external personnel involved in those processes).

The **concept for low-threshold access to** GIZ's **whistleblower/stop-it grievance system** is being introduced as of the fourth quarter of 2023. The country offices have prepared analyses of the local situation and have selected the contract persons for system access. GIZ's whistleblower system (including low-threshold access) can also be used to report human rights violations. This covers the violation of human rights due diligence and of environmental due diligence obligations (Sections 2 (2) and 2 (3) respectively of the Federal Act on Corporate Due Diligence Obligations in Supply Chains (LkSG)).

3.4.3. Compliance communication and training

Preparing and communicating compliance-related information has a positive impact on the compliance culture, gives staff greater certainty in their day-to-day work and enables compliance issues to be dealt with more easily.

To help the Management Board and Supervisory Board monitor the CMS, the Compliance and Integrity Unit provides an update on the CMS to the Management Board and to the Supervisory Board each year.

With the main focus on the CMS, the ICS and anti-corruption measures, the unit provides input for

- GIZ's Integrated Company Report,
- GIZ’s German Sustainability Code (GSC) reporting,
- GIZ’s progress reports to the UN Global Compact,
- GIZ’s annual report to the Federal Ministry of the Interior for the German Government's Integrity Report,
- the implementation status of the recommendations of the OECD Working Group on Bribery in International Business Transactions.

All employees with a GIZ email address must complete the web-based compliance and integrity training within the first 100 days of their employment. This training must be repeated every three years at the latest; the first repeat cycle started in November 2023. Managers must also complete the web-based compliance module for managers in the same time frame.

The content of these mandatory, web-based compliance and integrity training courses is routinely reviewed and was updated in 2023.

An offline compliance and integrity training programme is available for temporary workers, which the Compliance and Integrity Unit recommends they complete. The responsible line manager decides whether the training is mandatory for the relevant temporary workers.

3.5. Compliance in business processes

GIZ is evolving into a consistently process-oriented organisation in which compliance is a key component. Compliance requirements are systematically analysed and integrated when (re)modelling processes.

GIZ has introduced a **tool** known as the **standardised list of legal provisions** to continuously identify compliance obligations, assess the impact of identified innovations and changes and take any relevant and necessary action. The tool is managed on a decentralised basis by the compliance officers for the legal area for which they are responsible. All officers compiled a standardised list of legal provisions for their subject area in 2023, and an annual update process has been defined.

3.5.1. Tax Compliance Management System (TCMS)

The TCMS is a sub-area of the CMS that is currently being established and further developed. Its purpose is to ensure complete and timely fulfilment of tax obligations. Responsibility for compliance lies within the Finance Department’s tax team. The current tax compliance management system covers various preventive measures: guidelines, sector-specific instructions, training courses, a comprehensive knowledge management system, a list of legal provisions as well as detective measures that include system-based validations, plausibility checks, and selection of random-sample business transactions for manual review.

As part of the transition to the ERP software solution SAP S/4HANA (S4GIZ), extensive, system-based tax determination processes are also being prepared for rollout. Automating these processes will further improve compliance.

3.5.2. Information Security Management System (ISMS)

Responsibility for compliance within the framework of information security management was transferred to GIZ's Chief Information Security Officer (CISO) in 2023. As part of the development of an ISMS throughout GIZ, a separate process is being established to continuously identify relevant legal, contractual and internal requirements of interested parties with regard to the ISMS.

An initial review of the relevant legal framework for information security management was carried out in 2023.

3.6. Compliance monitoring and improvement

Monitoring appropriateness and effectiveness is a central element of an effective CMS. It allows us to identify vulnerabilities, develop suitable measures and, in turn, continuously improve the system. Good management tools are a key prerequisite in this context. Any necessary adjustments/improvements to the CMS are identified above all through the internal control system, the compliance risk control matrix and a review of company-wide reports. The Compliance and Integrity Unit produces a monitoring plan each year on this basis.

The plan outlines key measures for continuously improving and further developing the CMS and provides an overview of the content, nature and status of the measures implemented by the unit and its annually recurring (standard) activities. All measures planned for the 2023 reporting year were fully implemented, and adequate progress was made with the implementation of measures with multi-year planning horizons.

4. GIZ’s Internal Control System

GIZ’s Internal Control System (ICS) is an integral part of corporate governance and company workflows, and plays a key role in identifying, evaluating, managing and monitoring the material risks to which GIZ is exposed. GIZ's ICS is organised in accordance with the **requirements of Auditing Standard 982 of the Institute of Public Auditors in Germany (IDW)** ‘Principles of proper auditing of the internal control system for internal and external reporting’ (IDW PS 982). This requires **six elements** to be implemented and documented in an ICS description. With respect to the gradual refinement of the ICS (maturity level ‘monitored’), the following measures were implemented in these six elements in 2023.

4.1. Control environment, culture and organisation

The control environment sets the framework within which the rules and regulations are introduced and applied. This comprises all standards, processes and structures that form the basis for implementing internal controls. It is characterised by tone at the top and shaped by the basic attitudes, problem awareness and conduct of the employees.

4.2. Objectives

As a component of corporate governance, the ICS is anchored in the corporate strategy. Accordingly, the ICS objectives are derived from GIZ’s corporate objectives. For GIZ, these give rise to the following ICS objectives: correct and proper use of public funds, correct and efficient implementation of business processes, clear and reliable (internal and external) financial reporting, and compliance with pertinent laws, ordinances and regulations.

4.3. Risk assessment and scope

In order to achieve the ICS objectives, the focus is on commercial and administrative processes. GIZ adopts a risk-based approach in this context. The following processes (Head Office and field structure) were identified as posing a particular risk to the achievement of objectives and are therefore considered relevant to the ICS: procuring services, materials and equipment and construction work; awarding financing arrangements; managing remuneration and additional benefits; managing finances.

4.4. Processes and control activities

Control activities comprise steering and control measures that address the identified and assessed risks and thus aim to ensure that the ICS objectives are achieved. The ICS function regularly advises the specialist units and country offices on the design and implementation of controls in ICS-relevant processes. The following advisory processes merit specific mention for the 2023 reporting year:

- The Financial Services division was advised on preparing a risk-based audit concept for the financial processing of financing arrangements (grant agreements with German and non-German recipients), including a risk-based random audit. The aim was to increase the efficiency of the accounting process taking into account the risks and cost-effectiveness.
- The technical configuration of the internal controls in a software application is being closely monitored. The application will then fulfil ICS requirements for overarching audit evaluation requirements (qualitative and quantitative evaluations).

4.5. Information and communication

Communication about the ICS is carried out via the management structure, internal information and communication channels and training measures. The above-mentioned web-based training course (basic compliance module and compliance module for managers) also addresses ICS-relevant topics. The training catalogue of the Academy for International Cooperation (AIZ) also includes specific training courses that cover ICS-related commercial and administrative content. All employees completing the onboarding process are required to undertake basic training in commercial topics, while commercial staff are also required to take additional in-depth courses.

- ICS-related issues and risks in commercial and administrative processes in the field structure were discussed in workshops at the 2023 regional conferences of the heads of finance and administration.
- The Financial Management Advisory Services Division was supported in setting up the internal control auditor network to ensure uniform quality standards and in designing and conducting internal control training courses.

4.6. Monitoring, reporting and improvement

GIZ's ICS is regularly monitored and improved through the supplementary elements and information provided by all three lines (in the Three Lines Model).

The **internal control** of projects and offices is the **key monitoring tool of the ICS**. It is used to systematically and routinely review and assess the effectiveness of controls in commercial and administrative processes in the implementation structure. Deviations from GIZ's internal rules and regulations are documented and appropriate measures are formulated. The implementation of such measures must be reported on.

Internal controls of GIZ country offices are carried out once a year in countries classified by the Compliance and Integrity Unit as having high or very high-risk potential, and every two years in all other countries. Projects outside Germany are subject to an internal control once a year, projects based in Germany every two years.

Internal control statistics on implementing internal controls of projects (in the field structure and in Germany) are prepared annually in the first quarter by the ICS governance function, and are reported to the Management Board and communicated to the auditor of the annual statement of accounts. For the 2023 reporting year, the **overall results** of the departmental and country-specific evaluations are as follows (2023 internal control statistics, as at 31 December 2023):

- Abroad, the overall result of 87% for 2023 is down on the previous year (89% in 2022). At EUR 1,056 million, the total turnover of the projects to be audited in 2023 is still only slightly lower than in the previous year (EUR 1,058 million). If we take into account the projects that did not have internal controls but did conduct an internal audit, the percentage of total turnover audited is slightly higher at 88%.
- The number of projects to be audited in Germany continued to fall in 2023 (to 344 compared to 545 in 2022). This is due in part to the changeover to a two-year audit cycle. The number of audited projects (168) was also lower than in 2022, resulting in a drop from 57% to 49% in 2023.

Other ICS monitoring measures include regular audits by the Auditing Unit and a range of external audits. In order to take account of findings from audits and compliance cases when identifying risks and deriving recommendations for action for the ICS, the ICS function is a member of the Audit Coordination Committee and engages in structured dialogue with the Auditing Unit and the Case Management Section within the Compliance and Integrity Unit.

5. Outlook for 2024

The CMS and **ICS** are designed as **learning systems** and are being continuously developed. The following measures are planned for 2024:

- The Compliance and Integrity Unit will be renamed the Governance, Risk, Compliance (GRC) Unit in May 2024. The reason for this change is the Management Board’s decision to merge the processes, instruments, methods and systems of risk management, compliance management and internal control.
- The compliance officer system will be continuously monitored. With regard to the overall system at GIZ, optimisation measures, such as a stronger focus on top risks and on potential consolidation options in the area of business partner checks, are to be examined.
- The entry into force of the German Federal Act on Corporate Due Diligence Obligations in Supply Chains (LkSG) necessitates action in the field of human rights compliance. In 2024, the implementation and monitoring functions are to be separated in the Quality and Sustainability Section.
- The concept for low-threshold access to GIZ's whistleblower/stop-it grievance system is to be established in all countries in the field structure by April 2024. Together with the Academy for International Cooperation (AIZ), the GRC Unit will develop a training programme for low-threshold contact persons who will be available centrally from May 2024.
- The GRC Unit recommends that all countries, in particular those with a high and very high compliance risk rating, implement measures to foster a culture of compliance. For countries with a very high compliance risk, in 2024 the unit will offer to run virtual training on fostering such a culture with all managers from the projects and the country office.
- The ICS function will continue to provide case-by-case advice on designing ICS key controls as part of the S4GIZ rollout.

Impressum

Deutsche Gesellschaft für
Internationale Zusammenarbeit (GIZ) GmbH

Sitz der Gesellschaft
Bonn und Eschborn

Friedrich-Ebert-Allee 36 + 40
53113 Bonn, Deutschland
T +49 228 44 60-0
F +49 228 44 60-17 66

Dag-Hammarskjöld-Weg 1 - 5
65760 Eschborn, Deutschland
T +49 61 96 79-0
F +49 61 96 79-11 15

E info@giz.de
I www.giz.de

Titelgrafik:
Olivia Ockenfels, odecologne