COMPLIANCE

ANTI-CORRUPTION

INTEGRITY

Annual GIZ Compliance Report

2022

Contents

1. Summary of key results

The consolidation and further development of the **Compliance Management System (CMS) as an overall system** (see Section 3) remains a key area of priority. Refining the **Internal Control System (ICS)** is also a key focus (see Section 4). Integrated reporting covers the Tax Compliance Management System (TCMS) and, since 2022, the Information Security Management System (ISMS).

In addition to compliance management, GIZ's CMS encompasses internal anti-corruption and integrity management. At GIZ, the **CMS is an important component of the broad-based ICS**. Both systems **take a risk-based approach** (see Section 2). The risk-oriented approach and differentiated response to risks in the systems have continued to be **effective**, with the result that **no significant process adjustments were necessary** in the 2022 reporting period. 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 CMS is subject to an ongoing monitoring and improvement process. To date, GIZ has used Auditing Standard 980 (principles of proper auditing for compliance management systems) of the Institute of Public Auditors in Germany (IDW) as the basis for its CMS in Germany, and it has implemented the seven basic elements set out in the standard. However, this IDW Auditing Standard is a German standard, and GIZ also has international commissioning parties and donors. As part of the implementation of its corporate strategy, GIZ has decided to audit its CMS in line with ISO 37301:2021 in 2023. In preparation for this audit, a digital filing structure was defined in accordance with ISO 37301 in the 2022 reporting year and populated with relevant information. The CMS applies across all GIZ locations and is managed from Eschborn in Germany.

To gain a comprehensive overview of specific compliance risks in the field structure, GIZ conducted an analysis of compliance risks in all country offices in 2022. The offices identified appropriate risk mitigation measures and have started to implement them. They have also implemented measures to promote their compliance culture. The process was initially completed by three selected country offices (focus countries) in close liaison with the Compliance and Integrity Unit. The good practices identified were then made available to all offices.

2. Evaluating and dealing with compliance and ICS risks

An effective compliance management system aims to prevent sanctions, financial loss and reputational damage. Nevertheless, there is no way to completely eliminate the possibility of breaches. Instead, the aim is to exercise **due diligence**, which is why GIZ has selected a **risk-based approach for the CMS**. At GIZ, the CMS and ICS are closely linked.

The **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. Roles and tasks are defined on the basis of the international standards of the **Three Lines Model**. The interaction between the three lines aims to avoid risks (**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** is operational management within the framework defined by GIZ's internal rules (P+R). In addition to process-integrated monitoring measures such as 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.

- In the **second line**, **overarching governance tasks** are performed, and **risk management** is supported and monitored. Key elements include the CMS, risk management, controlling, the ISMS and the ICS governance function.

- The **third line is the Auditing Unit**, which monitors the functioning and effectiveness of the ICS through routine risk-based audits, special audits and process audits. This enables the unit to identify possible weaknesses and scope for improvement.

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

As part of the risk-based approach, the ICS evaluates the effort and cost of carrying out controls in relation to the respective risk. Cost effectiveness and process efficiency issues are also taken into account. The core element of GIZ's CMS, which also takes a risk-based approach, is the analysis of key compliance risks. Based on this, the relevant areas of action and measures that make up the **compliance programme** are identified. The current compliance and integrity risks are reported regularly from across the entire company using the comprehensive risk identification system, for example, through regular risk assessments carried out by compliance officers. The Compliance and Integrity Unit is represented on the Audit Coordination Committee, the Risk Management Committee and the Risk Management Board and is informed in this context about any compliance measures that may be required and any structural control weaknesses.

3. GIZ's Compliance Management System (CMS)

Ensuring compliance is an increasingly important factor in the activities of German and international companies and institutions. GIZ is facing growing challenges with regard to the correct implementation of commissions due to ever-greater complexity, new commissioning parties and severe time pressure in 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**. The following sections of the report show which other significant milestones were reached in 2022 based on the seven core **CMS elements** outlined in IDW Auditing Standard 980.

- **Compliance culture**: 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. The system of responsibilities for compliance issues also helps strengthen the culture (of responsibility).

- **Compliance objectives**: As a component of corporate governance, compliance is anchored in the corporate strategy. Accordingly, the compliance objectives are based on GIZ's corporate objectives.

- **Compliance risks**: GIZ's CMS takes a risk-based approach. Relevant compliance risks are recorded and the results are integrated in the risk control matrix prepared by the Compliance and Integrity Unit.

- **Compliance programme**: 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 exposure to compliance risks. This ensures that breaches of the compliance rules are first and foremost prevented, but otherwise are 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, 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, 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. The relevant specialist units (e.g. Human Relations Department, Finance Department, Procurement and Contracting Division) are responsible for ensuring that processes and tasks are designed in accordance with the rules, that they meet legal requirements and that they are aligned with the requirements of commissioning parties and GIZ itself. For topics of particular relevance, GIZ has delegated clear and binding compliance responsibilities, thus ensuring that no responsibility gaps arise in the company.

- **Compliance communication** (including compliance training and reporting): Preparing and communicating compliance-related information has a positive impact on the compliance culture, facilitates transparent reporting, gives staff greater certainty in their

day-to-day work and enables compliance issues to be dealt with more easily. The Compliance and Integrity Unit reports to the Management Board each year. As of the 2022 reporting year, the Management Board also reports to the Supervisory Board each year (previously every two years). This abridged version of the report is published on the intranet and internet.

- **Monitoring and improving compliance**: 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 lessons learned are evaluated in order to pinpoint any adjustments that are needed. Findings arising from case management also play an important role.

Compliance programme

The compliance programme consists of the preventive, explanatory and reactive measures implemented to ensure compliance, including measures to prevent corruption and promote integrity. The following regulations and measures have been established at GIZ:

- Comprehensive binding internal regulatory framework 'Processes and Rules (P+R)'
- Code of Ethics
- Code of Conduct
- Basic Compliance Rules
- Compulsory web-based training on compliance
- System of responsibilities for compliance issues
- Whistleblower system with various access channels
- External ombudsperson
- Autonomous compliance and integrity advisory services and case management
- Central case management and reporting ('whistleblower system')
- Obligation to report serious compliance violations for all management personnel
- Response Body
- Anti-corruption policy that reflects GIZ's policy of zero tolerance in all cases of corruption
- Prevention of corruption through staff and task rotation
- Risk-based compliance management in the field structure
- Professional procurement and award management processes in Germany and in the field structure

Within this framework, the Compliance and Integrity Unit has implemented the following **measures**:

Risk-based compliance management in the field structure
In the reporting year, three countries were placed in the very high compliance risk category (compared to four in 2021) and 29 countries were placed in the high compliance risk category (compared to 26 in 2021). The number of countries in the medium and low compliance risk category was 65 (2021: 66). Where relevant to the entire company, the compliance risks identified locally are addressed through the company-wide risk management process.

- In 2022, the country offices carried out an analysis of their compliance risks, identified appropriate risk-reduction measures and started to implement them ('country risk profiles'). They also carried out measures to improve their compliance culture. The Compliance and Integrity Unit provided support through the Compliance Training toolbox.
- The Compliance and Integrity Unit advised the country offices of three focus countries (Iraq, Nigeria, Viet Nam/Laos) – selected to reflect the relevant aspects of GIZ's field structure – on identifying and analysing compliance risks as well as on how to develop and implement risk mitigation measures. All country offices were subsequently informed of any need for action and the good practices identified during this process. In 2023, an independent agency will carry out an audit in these three countries to determine whether GIZ's CMS is being implemented properly.

Anti-corruption management

- In December 2020, the **Response Body** was established with the task of handling corruption-related cases in a two-year pilot phase. Having proven effective, the use of this instrument will be mandatory in all serious compliance violations from 2023 onwards. The aim is to establish uniform handling under employment law (disciplinary action) against GIZ staff in response to serious compliance violations in Germany and abroad. In 2022, the Response Body handled 17 cases (2021: 7) in which (labour) law responses affecting 22 staff members (2021:13) were discussed.
- In 2021, the Compliance and Integrity Unit carried out a company-wide **inventory of work areas particularly susceptible to corruption** and identified the associated risks. Various measures were subsequently implemented in follow-on processes in 2022. For example, as part of the current corporate objective on compliance management in the field structure all country offices implemented additional measures to improve the compliance culture and prevent corruption. Furthermore, the Compliance and Integrity Unit and the Human Relations Department worked together to develop a method of flagging work areas particularly susceptible to corruption in the HR system. This is to serve as the basis for monitoring the rotation requirements resulting from the analysis.

Case management

- **Reporting human rights violations:** No cases of human rights violations were reported in 2022.
- In order to meet the requirements of the German Supply Chain Act (LKSG), the whistleblower system was expanded to include an option for reporting violations of environment-related obligations (**violations of environmental law**).
- To reduce inhibitions and barriers to reporting violations, the Compliance and Integrity Unit worked with six countries to develop a concept for **low-threshold access to GIZ's whistleblower/stop-it grievance system** in the field structure (with a special focus on the stop-it scenarios for sexual misconduct, discrimination and bullying).

Handling compliance and integrity cases in 2022

Reporting on compliance and integrity cases covers all processes related to criminal law, GIZ's core regulatory framework P+R and the Code of Conduct, general requests for advice and complaints. In the 2022 reporting period, the **Compliance and Integrity Unit handled a**

total of 678 cases (2021: 553). The increase can be partly attributed to the introduction in October 2020 of mandatory reporting by managers of serious compliance violations and to the transfer of responsibility for the grievance desk for all complaints under the German General Act on Equal Treatment (AGG) to the Compliance and Integrity Unit and the inclusion of these cases in the unit's statistics. It can also be assumed that the improved whistleblower system, the continuous optimisation of the ICS and greater awareness of compliance issues in the workforce led to a reduction in the number of unreported compliance cases. Nonetheless, we cannot rule out the possibility that, in addition to a reduction in unreported cases, there was an actual increase in cases in 2022. One reason for this could be our work in fragile contexts, which often requires remote management.

Cases not relevant for investigation

- Some 252 requests for advice were received (2021: 266). 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.

- In addition, there were 51 other cases that were not based on compliance violations (e.g. general complaints about the situation in the partner country, non-selection in the GIZ recruitment process).

Cases relevant for investigation

- A total of 208 reports (2021: 143) 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-related incidents and other infringements of GIZ's rules and procedures. GIZ's online whistleblower portal was used 155 times in 2022 (2021: 123). The ombudsperson was contacted by 4 whistleblowers (2021: 5).

- In the reporting year, 167 reports of possible or proven (internal) breaches and irregularities were submitted to the Compliance and Integrity Unit (2021: 109). These primarily involved fraud relating to expenses and invoicing committed by GIZ staff, fraudulent misuse of funds on the part of funding recipients and property theft.

Of the 375 reports received in 2022 that were relevant for investigation, it was possible to close 297 cases. Of these, evidence of **compliance breaches was established** in **68** cases. 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).

Additional compliance processes

- **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. The Finance Department's tax team is responsible for compliance issues in the TCMS. The TCMS currently covers various preventive measures such as guidelines and sector-specific requirements, training courses, a comprehensive knowledge management system and a list of legal provisions, as well as detective measures such as system-based validations, plausibility checks, and selection of random-sample transactions for manual review.

- **Information Security Management System (ISMS)**: GIZ's ISMS is currently being set up or further developed. It specifies which instruments and methods are used at management level to steer tasks and activities related to information security. The aim is

to achieve and maintain an adequate level of protection with respect to the confidentiality, integrity and availability of GIZ information. In 2023, the Information Governance Unit, which was established on 1 August 2022, will assume responsibility for compliance issues in the ISMS.

Compliance training

According to the Code of Conduct and P+R, all workforce members must complete the **basic compliance module** and all managers must also complete the **compliance module for managers**. The web-based training (WBT) must be repeated every three years, and managers are responsible for ensuring that this is carried out. Both WBT courses are mandatory components of the onboarding programme for all new staff and must be completed within their first 100 days at work.

Due to changes to some requirements, updated versions of the courses were made available in August 2022. The basic compliance module now includes a section on the **Code of Ethics and Code of Conduct**, and the section on data protection and information security has been removed. Separate mandatory WBT courses must now be completed for both of these topics.

Country directors must ensure that all **national staff** who are unable to complete the web-based compliance and integrity training can take part in face-to-face training. This is laid down in P+R. For this purpose, the Compliance and Integrity Unit has published in its Compliance Training toolbox an **offline training version** with sections on the Code of Ethics and Code of Conduct, corruption prevention and conflicts of interest (both key components of the Code of Conduct), and equal treatment and anti-discrimination.

Compliance reporting

With the main focus on the CMS, ICS and GIZ's anti-corruption measures, the Compliance and Integrity Unit provides input for

- the print and online versions of GIZ's Integrated Company Report
- GIZ's German Sustainability Code (GSC) reporting,
- GIZ's progress reports on the UN Global Compact,
- GIZ's annual report to the Federal Ministry of the Interior for the German Government's Integrity Report, and on
- the implementation status of the recommendations of the OECD Working Group on Bribery on bribery outside Germany.

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

Monitoring and improving compliance

Monitoring adequacy and effectiveness is a central element of a functioning CMS. It enables us to identify vulnerabilities in the CMS, develop appropriate measures and so continuously improve the system. This calls for **good management tools**.

A number of sources are used to identify necessary adjustments, in particular the ICS system, the compliance risk control matrix, case management assessments, the Compliance and Integrity Unit's plan of operations and the review of reporting across the company. The

key measures for improving the CMS are set out in a monitoring plan (with the exception of ICS measures, which are subject to separate monitoring, see below). The plan is prepared annually and provides an overview of the content, nature and status of the unit's annual and recurring activities each year.

The monitoring plan was submitted to the Compliance Committee at its meeting in November 2022. The measures primarily cover the following four fields of activity: compliance risks, compliance programme, compliance communication and compliance monitoring. All measures planned for 2022 have been fully implemented, and adequate progress was made with the implementation of measures with multi-year planning horizons.

4. GIZ's internal control system

The legal necessity to establish an ICS derives from the Management Board's due diligence obligations and the Supervisory Board's monitoring duties. Situated below the Management Board level, GIZ's ICS is based on the Three Lines Model in accordance with international standards. The 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.

In July 2020, the Management Board decided to professionalise the ICS with a view to achieving the **maturity level 'monitored'**. This decision was based on a joint understanding that GIZ's size and legal status call for **overall company-wide responsibility and a coordination function** as well as a **structured, systematic representation of all key control processes for the ICS.** This is necessary in order to adequately develop this governance topic and meet growing external requirements with respect to documenting and monitoring control activities, including the statutory monitoring and verification obligations vis-à-vis the Supervisory Board. Every two years, the Management Board prepares a special report on the effectiveness of internal control systems, the risk management system and the internal audit system for the Supervisory Board's Audit Committee (last report: 16 May 2023).

The **advantage of achieving the maturity level 'monitored'** is that it enables us to gain an **overview of processes** within the company **that involve risk**, **to identify and thus prevent** relevant **control weaknesses** at the overall company level or to **systematically learn** from mistakes and fraudulent activities, and to **adapt control measures** accordingly. This means that processes can be continuously improved, including with regard to control issues, and that control weaknesses can be systematically rectified. This **improves both internal and external communication** and provides the **required basis for external verification of effectiveness**.

The prerequisites for achieving the higher maturity level 'monitored' are a **clear and comprehensive description of the ICS**, a detailed description at the process level and **centralised responsibility** for monitoring and developing controls and producing corresponding aggregated reports. The Management Board therefore decided to assign overarching organisational responsibility for the ICS to the Compliance and Integrity Unit. GIZ's ICS was established in accordance with the requirements of Auditing Standard 982 issued by the Institute of Public Auditors in Germany (IDW Auditing Standard 982). This requires **six elements to be implemented** and documented in an ICS description. The description of GIZ's ICS was approved by the Management Board in May 2022. It covers the key decisions on the ICS's objectives and strategy, scope, ICS methodology, procedures and organisation.

With respect to the gradual refinement of the ICS (maturity level 'monitored'), the following **measures** were implemented in the **six elements in 2022**:

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 (ICs). It is characterised by tone from the top and shaped by employees' basic attitudes, problem awareness and conduct.

ICS objectives

As a component of corporate governance, the ICS is anchored in the corporate strategy. Accordingly, the ICS objectives are based on GIZ's corporate objectives. These give rise to the following ICS objectives for GIZ: 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.

Risk assessment and scope

In order to achieve the ICS objectives, GIZ takes a risk-based approach that focuses on commercial and administrative processes. The following processes (Head Office and field structure) were identified as being of 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.

In the reporting year, the risks associated with the **process of 'awarding financing arrangements'** from the perspective of compliance management and the ICS were **analysed and evaluated** by the Compliance and Integrity Unit and the Finance Department's Financial Services Division, which is responsible for this process. The division consequently received advice on revising the audit concept for the financial processing of financing arrangements and on introducing a risk-based methodology.

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. According to the ICS methodology developed in 2021, the above-mentioned ICS-related processes must be described and the relevant risks identified and evaluated. The **key controls** are defined accordingly. After weighing up the likelihood of occurrence, level of damage and effort/cost of the controls, the control requirements are defined for each process and documented in **risk control matrices**. Together, the risk control matrices document the control activities and the framework for monitoring the ICS. To ensure that the requirements of the ICS and the introduction of the ICS methodology documented in the ICS description are taken into account in the implementation of SAP S/4HANA (S4GIZ), the ICS function is involved in the S4GIZ workstream 'Procure to Pay' (procuring services, materials and equipment and construction work and awarding financing arrangements).

Information and communication

Communication on the ICS is carried out via the management structure, through internal information and communication channels (e.g. changes in P+R) and through training measures. The above-mentioned online basic compliance training module addresses ICS-related topics (including EU rules on state aid, preventing money laundering and terrorist financing, corruption prevention, financing, public price law and procurement law). GIZ's

training catalogue also includes courses on key ICS-related topics. 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.

The first joint **training course on the risk-based approach** was conducted by the ICS governance function, the Compliance and Integrity Unit and the Risk Management Section in 2022.

On 21 February 2022, the Compliance and Integrity Unit invited colleagues to take part in a company-wide **compliance dialogue on how to be agile in a regulatory environment** as part of a GIZ-internal series of compliance dialogue events. After an introduction by Managing Director Thorsten Schäfer-Gümbel, a panel discussion – followed at times by more than 500 colleagues – focused on how to be innovative, agile and creative while using the funds entrusted to GIZ responsibly, with integrity and in compliance with the rules.

Monitoring, reporting and improvement

Monitoring
GIZ's ICS is regularly monitored and improved through the supplementary elements and information provided by all three lines. The above-mentioned ICS description is a requirement for monitoring.

Reporting
- The ICS function prepares an **'Integrated Annual Compliance and ICS Report'** and submits this to the Management Board, which in turn reports on this topic to the Supervisory Board.
- Once a year, the ICS function carries out an **overall evaluation of all ICs conducted on projects** in Germany and in the field structure (IC coverage). Up to 2021, the Auditing Unit was responsible for **IC statistics** reporting, which is carried out in the first quarter. Internal controls aim to detect any deviations from GIZ's internal rules and regulations and to identify any fraudulent action and financial settlement risks at an early stage with a view to taking countermeasures. They provide significant **support to management** in performing its control tasks. Deficits in commercial performance can be identified early, financial settlement risks minimised and cases of fraud detected.
- The COVID-19-related restrictions still in place in some partner countries in 2022 led to delays and cancellations of planned audits in connection with the implementation of ICs. Nevertheless, IC coverage in **partner countries** was still higher (91%) than in 2021 (86%).
- The number of projects to be audited in **Germany** fell to 545 compared to previous years (2021: 633). This is partly due to the switch to a two-year audit cycle. However, the number of audited projects (312) was much higher than in previous years, increasing from 41% in 2021 to 57% in 2022.

Improvement (further development)
- In order to take account of findings from external audits, internal audits and compliance cases when identifying risks and assessing the need for action, the ICS function is a member of the internal Audit Coordination Committee. In 2022, there were **no indications of structural control weaknesses** in this connection.

- The **requirements for implementing ICs** on projects and offices were extensively **revised** in early 2022: 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. The office internal control is carried out at all office locations in the country. Projects outside Germany are subject to an internal control once a year, projects based in Germany every two years.
- In 2022, the **IC check lists** were **revised** with the aim of increasing risk orientation while ensuring that audit density remains high. This resulted in a reduction in the number of audit steps. The check lists now contain the key controls that must be performed as a standard part of each IC. A large number of audit steps were classified as advanced audit steps; these now have to be checked at regular intervals, but no longer as standard in each IC. This concept will come into effect with the introduction of the audit module in the MIRAI risk management software.

5. Outlook for 2023: Current need for action

Consolidation of the CMS as an overall system

The consolidation of the CMS as an overall system remains a key area of priority. This will be achieved primarily through the following planned measures as part of the **implementation of the corporate objective on compliance management** (multi-year objective for 2022 and 2023):

- **Audit of GIZ's CMS in line with ISO 37301:2021**: In order to prepare for the planned external audit of the CMS pursuant to ISO 37301 – compliance management – the Compliance and Integrity Unit has prepared digital documentation in accordance with ISO 37301 requirements. As part of the audit, a proposal will also be prepared in 2023 on how compliance reporting can be adapted from the current IDW structure to the ISO structure.

- **Compliance auditing in the field structure**: All available country risk profiles are to be evaluated with regard to structural risks and need for action. This will serve as the basis for assessing whether and how compliance management can be further developed in the field structure. The three country offices of the focus countries are to be audited by a specialised external body by the end of 2023 to determine whether the requirements of the company's compliance management system have been properly translated into practice.

- It is anticipated that GIZ's concept for **low-threshold access to its whistleblower system/grievance system in the field structure** will be introduced throughout the company as a binding document in the third quarter of 2023.

Further measures include

- Pressing ahead with plans to **expand effective protection for whistleblowers** in Germany and the field structure.

- **Developing the procedural principles and guidelines for investigations (establishing the facts)** in order to further professionalise case management and, in particular, decentralised investigative measures. These are to be introduced or in use throughout the company in the second half of 2023.

Gradual refinement of the ICS

The following measures are to be implemented for the gradual refinement of the ICS:

- Formulate the **ICS requirements for S4GIZ** (key controls and ICS methodology) and input in corresponding processes

- **Introduce the ICS methodology in the field structure**: Support the responsible units in preparing process descriptions and risk control matrices for ICS-related processes in the field structure

- **Identify risks and then determine required action** for the ICS (e.g. consider findings from external audits, internal audits, compliance cases, ICs)

- Provide continued close support for the development of the MIRAI risk management software to ensure that ICS requirements with regard to (qualitative and quantitative) **overarching audit evaluation needs** are taken into account