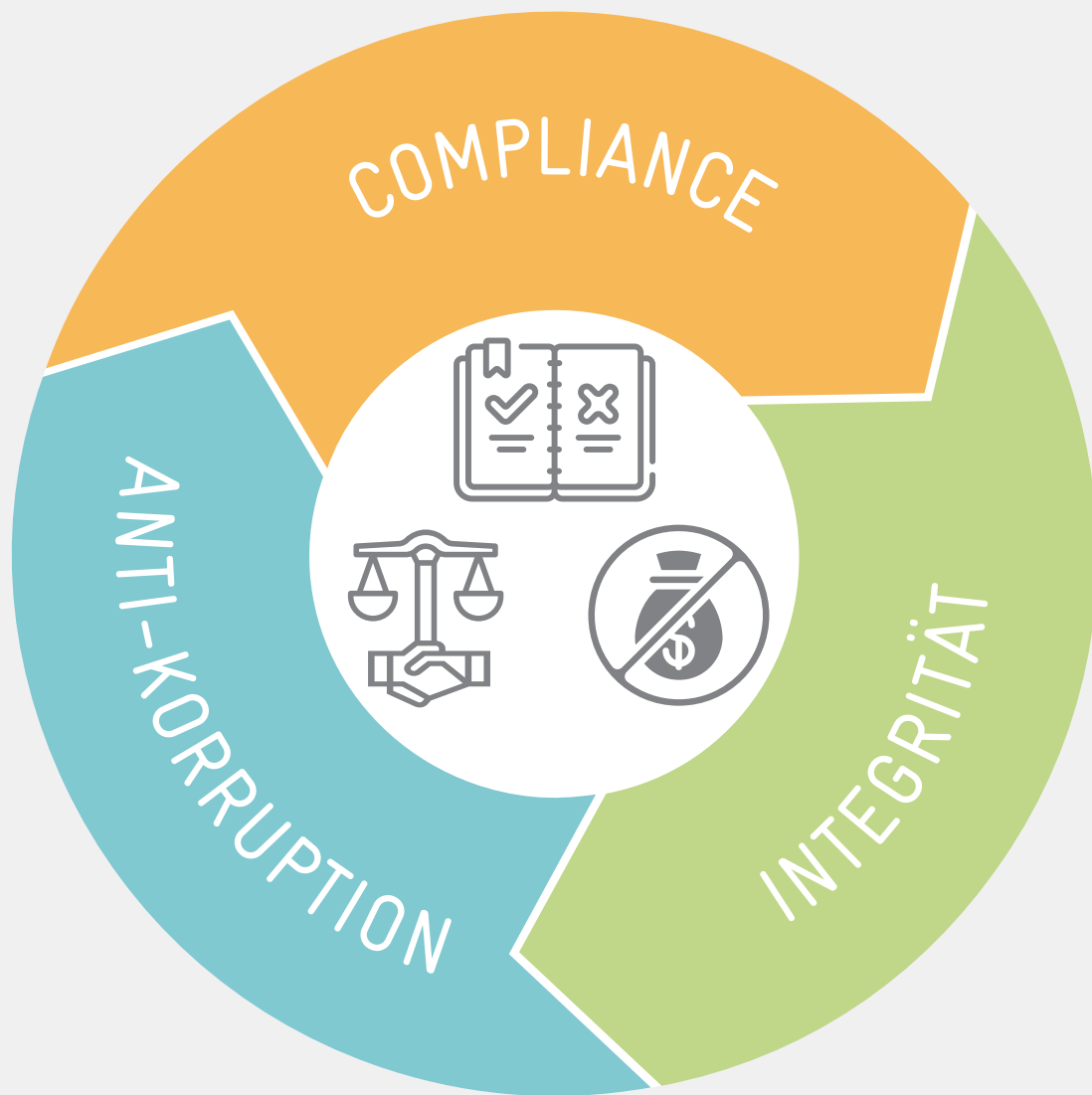




Compliance-Jahresbericht

2022

Inhalt

1. Zusammenfassung der wesentlichen Ergebnisse.....	2
2. Einschätzung und Bearbeitung der Compliance- und IKS-Risiken.....	3
3. Das Compliance Management System der GIZ.....	4
Compliance-Programm	5
Compliance-Überwachung und Verbesserung	9
4. Das Interne Kontrollsystem der GIZ	10
Überwachung, Berichterstattung und Verbesserung	12
5. Ausblick 2023: Aktuelle Handlungsbedarfe.....	14
Die Konsolidierung des CMS als Gesamtsystem	14
Die schrittweise Weiterentwicklung des IKS.....	14

1. Zusammenfassung der wesentlichen Ergebnisse

Die Konsolidierung und Weiterentwicklung des **Compliance Management Systems (CMS)** als Gesamtsystem (siehe Kapitel 3) ist weiterhin ein wesentlicher Schwerpunkt. Daneben ist die Weiterentwicklung des **Internen Kontrollsystems (IKS)** zentral (siehe Kapitel 4). Die integrierte Berichterstattung erfolgt zum Tax Compliance Management System (TCMS) und seit 2022 neu zum Informationssicherheitsmanagement System (ISMS).

Das CMS der GIZ umfasst neben dem Compliance Management das interne Antikorruptions- und Integritätsmanagement. In der GIZ ist das **CMS eine wichtige Säule des breit angelegten IKS**. Beide Systeme **basieren auf einem risikobasierten Ansatz** (siehe Kapitel 2). Der risikoorientierte Ansatz und die differenzierte Bearbeitung in den Systemen haben sich weiterhin **bewährt**, so dass im Berichtszeitraum 2022 **keine signifikanten Prozessanpassungen erforderlich** waren. Die GIZ verfügt über ein umfassendes System zum Risikomanagement. Compliance- und Integritätsrisiken werden hierüber regelmäßig aus dem gesamten Unternehmen gemeldet, anschließend bewertet und konsequent bearbeitet.

Das CMS unterliegt einem kontinuierlichen Überwachungs- und Verbesserungsprozess. Bisher hat die GIZ ihr CMS auf der Grundlage des Prüfstandards 980 (Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen) des Instituts der Wirtschaftsprüfer (IDW) in Deutschland aufgebaut und die dort festgeschriebenen, sieben Grundelemente umgesetzt. Dieser Prüfungsstandard des IDW ist ein deutscher Standard, die GIZ hat jedoch auch internationale (Auftrag-)Geber. Im Rahmen der Umsetzung der Unternehmensstrategie hat sich die GIZ entschieden, 2023 eine Prüfung ihres CMS entlang der DIN-ISO 37301:2021 vorzunehmen. Zur Vorbereitung dieser Prüfung wurde im Berichtsjahr 2022 eine digitale Ablagestruktur nach der Logik der ISO 37301 definiert und mit den relevanten Informationen befüllt. Das CMS ist standortübergreifend aufgebaut und wird dabei aus Eschborn, Deutschland, gesteuert.

Um einen umfassenden Überblick über spezifische Compliance-Risiken in der Außenstruktur zu erhalten, hat die GIZ in 2022 in allen Landesbüros eine Analyse der Compliance-Risiken durchgeführt. Die Büros haben entsprechende risikomindernde Maßnahmen identifiziert und mit ihrer Umsetzung begonnen. Darüber hinaus haben sie Maßnahmen zur Förderung ihrer Compliance-Kultur umgesetzt. Drei ausgewählte Landesbüros (Fokusländer) durchliefen den Prozess zu Beginn unter enger Begleitung der Stabsstelle. Dabei identifizierte good practices wurden allen Büros zur Verfügung gestellt.

2. Einschätzung und Bearbeitung der Compliance- und IKS-Risiken

Ein wirksames CMS soll Sanktionen, finanzielle Schäden und Reputationsschäden vermeiden. Gleichwohl ist es nie ganz auszuschließen, dass Verstöße vorkommen. Vielmehr geht es um die Anwendung einer **angemessenen Sorgfalt**, daher hat die GIZ einen **risikobasierten Ansatz für das CMS** gewählt. In der GIZ wirken das CMS und IKS eng zusammen.

Das **IKS** ist ein wesentlicher Bestandteil der Unternehmensführung und -abläufe und spielt eine **Schlüsselrolle bei Identifizierung, Bewertung, Management und Überwachung wesentlicher Risiken**, denen die GIZ ausgesetzt ist. Rollen und Aufgaben sind auf der Grundlage des internationalen Standards des **Drei-Linien-Modells** definiert. Das Zusammenspiel der drei Linien hat zum Ziel, Risiken zu vermeiden (**Prävention**), problematische Sachverhalte frühzeitig zu erkennen (**Detektion**) und auf Regelverstöße bzw. nicht vermeidbare Risiken angemessen zu reagieren (**Reaktion**):

- Die **erste Linie zur Steuerung von Risiken** bildet das operative Management in dem vom internen Regelwerk der GIZ (P+R) vorgegebenen Rahmen. Sie umfasst neben prozessintegrierten Überwachungsmaßnahmen wie dem 4-Augen-Prinzip und der Funktionstrennung auch prozessunabhängige Überwachungsmaßnahmen wie die mindestens halbjährliche Risikomeldung oder die Internen Kontrollen (IK) von Projekten und Büros.
- In der **zweiten Linie** werden **übergreifende Governance-Aufgaben** wahrgenommen und das **Management von Risiken** unterstützt und überwacht. Wesentliche Elemente sind u.a. das CMS, das Risikomanagement, das Controlling, das ISMS sowie die IKS-Governance-Funktion.
- Die **Stabsstelle Revision als dritte Linie** überwacht die Funktionsfähigkeit und Wirksamkeit des IKS durch risikoorientierte Routineprüfungen, etwaige Sonderprüfungen sowie Prozessprüfungen. Hierdurch identifiziert sie mögliche Schwachstellen und Verbesserungspotentiale.

Darüber hinaus unterliegt die GIZ einer **Vielzahl externer Prüfungen**, bei denen sie regelmäßig die ordnungsgemäße Verwendung der ihr anvertrauten Mittel nachzuweisen hat.

Im Rahmen des risikobasierten Ansatzes bewertet das IKS den Aufwand für eine Kontrolle im Verhältnis zum jeweiligen Risiko. Dabei finden auch Fragen der Wirtschaftlichkeit und der Prozesseffizienz Berücksichtigung. Kernelement des gleichsam risikobasierten CMS der GIZ ist die Analyse der zentralen Compliance-Risiken. Hieraus leiten sich die relevanten Handlungsfelder und Maßnahmen ab, das sogenannte **Compliance-Programm**. Über das umfassende System zur Risikoidentifikation werden regelmäßig aktuelle Compliance- und Integritätsrisiken aus dem gesamten Unternehmen gemeldet, z.B. aus regelmäßigen Risiko-Assessments durch Compliance-Themenverantwortliche (C-TV). Die Stabsstelle Compliance und Integrität ist zudem im Ausschuss für Prüfungscoordination, im Risikomanagement Ausschuss sowie im Risikomanagement Gremium vertreten und erhält darüber Hinweise über ggf. abzuleitende Compliance-Maßnahmen bzw. strukturelle Kontrollschwächen.

3. Das Compliance Management System der GIZ

Das Sichern von Compliance (kurz: Regeltreue) gewinnt in der deutschen und internationalen Unternehmens- und Institutionenlandschaft weiter an Bedeutung. In der GIZ sind dabei die steigenden Herausforderungen an eine korrekte Auftragsdurchführung hervorzuheben, die aus der wachsenden Komplexität, neuen Auftraggeberinnen und -gebern und hohem Zeitdruck an schwierigen Standorten erwachsen. Das CMS soll die Beschäftigten **beim professionellen Umgang mit Compliance-Anforderungen unterstützen**, die **Handlungssicherheit erhöhen** und etwaigem **Organisationsverschulden vorbeugen**. Der Bericht zeigt in den nachfolgenden Abschnitten auf, welche weiteren wesentlichen Meilensteine im Jahr 2022 nach Logik der **sieben zentralen CMS-Elementen** gemäß IDW PS 980 erreicht wurden.

- **Compliance-Kultur:** Werteorientierung ist essenziell für das Compliance Management der GIZ sowie auch für die persönliche Integrität ihrer Beschäftigten. Viele präventive Maßnahmen zielen deshalb auf eine positive Compliance-Kultur, die eine Ausrichtung des Verhaltens aller an den Unternehmenswerten und den Compliance-Vorgaben fördert. Auch das System der Compliance-Themenverantwortungen trägt zur Stärkung der (Verantwortungs-)Kultur bei.
- **Compliance-Ziele:** Compliance ist als Teilbereich der Unternehmenssteuerung in der Unternehmensstrategie verankert. Entsprechend werden die Compliance-Ziele aus den Zielen des Unternehmens abgeleitet.
- **Compliance-Risiken:** Das CMS der GIZ basiert auf einem risikoorientierten Ansatz. Relevante Compliance-Risiken werden erfasst, die Ergebnisse fließen in die von der Stabsstelle Compliance und Integrität erstellte Risk-Control-Matrix ein.
- **Compliance-Programm:** Das Compliance-Programm umfasst neben den Compliance-Grundsätzen alle präventiven, aufklärenden und reaktiven Maßnahmen, die die GIZ zur Sicherstellung von Compliance und zur Begrenzung von Compliance-Risiken implementiert. So wird gewährleistet, dass Compliance-Verstöße primär verhindert, ansonsten wirksam aufgedeckt und bearbeitet werden können.
- **Compliance-Organisation:** Die Compliance-Organisation sorgt für eine Verankerung des Compliance Managements im Unternehmen. In der GIZ sind die Rollen und Verantwortlichkeiten der am CMS beteiligten Einheiten sowie die zugehörigen Ablauforganisationen festgelegt, eine funktionierende Governance-Struktur mit spezialisierten Gremien ist etabliert (Compliance-Ausschuss, Compliance-Committee). Der Stabsstelle Compliance und Integrität kommt im unternehmensweiten CMS eine Koordinierungs- und Steuerungsfunktion zu, die auch die Identifizierung von Handlungsbedarfen und die Einforderung notwendiger Maßnahmen beinhaltet. Die zuständigen Facheinheiten (z.B. Personalbereich, Finanzbereich, Abteilung Einkauf und Verträge) sind dafür verantwortlich, dass Prozesse und Vorgaben regelkonform ausgestaltet sind und der Rechtslage, den Auftraggeber- sowie den internen Anforderungen genügen. Für besonders relevante Themen hat die GIZ darüber hinaus eindeutige und verbindliche Compliance-Themenverantwortungen delegiert. Dadurch wird sichergestellt, dass im Unternehmen keine Verantwortungslücken entstehen.
- **Compliance-Kommunikation** (inkl. Compliance-Qualifizierung, -Berichterstattung): Die Aufbereitung und Vermittlung von Compliance-relevanten Informationen wirkt sich positiv auf die Compliance-Kultur aus, ermöglicht eine transparente Berichterstattung, erhöht die

Handlungssicherheit in der täglichen Arbeit und erleichtert den Umgang mit Compliance-Fragen. Die Stabsstelle berichtet jährlich an den Vorstand. Der Vorstand seinerseits berichtet ab dem Berichtsjahr 2022 ebenfalls jährlich an den Aufsichtsrat (bislang zweijährliche Berichterstattung). Diese gekürzte Berichtsversion wird im Intranet und Internet veröffentlicht.

- **Compliance-Überwachung und Verbesserung:** Ein wirksames CMS muss als lernendes System ausgestaltet werden. Deshalb werden die Angemessenheit und Wirksamkeit des CMS fortlaufend betrachtet und die Erfahrungen für notwendige Anpassungen ausgewertet. Eine wichtige Rolle spielen dabei auch die aus der Fallbearbeitung gewonnenen Erkenntnisse.

Compliance-Programm

Die präventiven, aufklärenden und reaktiven Maßnahmen zur Sicherstellung von Compliance, einschließlich Korruptionsprävention und Integritätsförderung, bilden das Compliance-Programm. Folgende grundlegende Regelungen und Maßnahmen sind in der GIZ etabliert:

- Umfassendes verbindliches internes Regelwerk "Prozesse und Regeln (P+R)"
- Ethik- und Verhaltenskodex
- Grundsätze integren Verhaltens (GiV)
- Compliance-Grundordnung
- Verpflichtende, web-basierte Compliance-Trainings
- System der Compliance-Themenverantwortungen
- Hinweisgebersystem mit verschiedenen Zugangskanälen
- Externe Ombudsperson
- Fachlich unabhängige Compliance- und Integritätsberatung und Fallbearbeitung
- Zentrales Fallmanagement und Meldewesen („Hinweisgebersystem“)
- Informationspflicht bei schwerwiegenden Compliance-Verstößen für alle Führungskräfte
- Reaktionsgremium
- Policy zur Korruptionsbekämpfung als Ausdruck der Null-Toleranz-Politik bei Korruptionsfällen
- Korruptionsprävention durch Personal- bzw. Aufgabenrotation
- Risikoorientiertes Compliance Management in der Außenstruktur
- Professionelles Vergabemanagement im Inland und in der Außenstruktur

Innerhalb dieses Rahmens hat die Stabsstelle Compliance und Integrität folgende **Maßnahmen** umgesetzt:

Risikoorientiertes Compliance Management in der Außenstruktur

Im Berichtsjahr waren 3 Länder im Bereich mit sehr hohem Compliance-Risiko (Vorjahr 4) und 29 Länder im Bereich mit hohem Compliance-Risiko (Vorjahr 26) verortet. Die Zahl der Länder mit mittlerem und geringem Compliance-Risiko lag zusammen bei 65 (Vorjahr 66). Die vor Ort identifizierten Compliance-Risiken werden, sofern sie für das Gesamtunternehmen Relevanz haben, im Rahmen des unternehmensweiten Risikomanagementprozesses bearbeitet.

- In 2022 haben die Landesbüros eine Analyse ihrer Compliance-Risiken durchgeführt, entsprechende risikomindernde Maßnahmen identifiziert und mit deren Umsetzung begonnen („Landesrisikoprofile“). Zudem haben sie Maßnahmen zur Erhöhung ihrer Compliance-Kultur durchgeführt. Die Stabsstelle hat sie dabei mittels der „Toolbox Compliance Trainings“ unterstützt.
- Die Landesbüros dreier Fokusländer (Irak, Nigeria, Vietnam/Laos), die exemplarisch die relevanten Aspekte der GIZ-Außenstruktur widerspiegeln, wurden zur Identifikation und Analyse von Compliance Risiken sowie Erarbeitung und Umsetzung risikomindernder Maßnahmen durch die Stabsstelle beraten. Identifizierte Handlungsbedarfe und good practices wurden anschließend sämtlichen Landesbüros zur Verfügung gestellt. Diese drei Länder werden in 2023 durch eine unabhängige Stelle daraufhin geprüft, ob sie das CMS der GIZ ordnungsgemäß umsetzen.

Antikorruptionsmanagement

- Im Dezember 2020 wurde das sog. **Reaktionsgremium** gegründet, das in einer zweijährigen Pilotierungsphase Fälle mit Korruptionsbezug bearbeitet hat. Dieses Instrument hat sich bewährt, sodass es ab 2023 bei allen schwerwiegenden Compliance-Verstößen verbindlich einzubeziehen ist. Ziel ist eine einheitliche Handhabung personalrechtlicher Maßnahmen gegen Beschäftigte der GIZ in Reaktion auf schwerwiegende Compliance-Verstöße im In- und Ausland. Das Reaktionsgremium hat im Jahr 2022 17 Fälle (2021: 7) bearbeitet, im Rahmen derer (arbeits-)rechtliche Reaktionen gegenüber insgesamt 22 Mitarbeiter*innen (2021: 13) erörtert wurden.
- Die Stabsstelle hat im Jahr 2021 eine unternehmensweite **Feststellung besonders korruptionsgefährdeter Arbeitsgebiete** durchgeführt, im Rahmen derer die besonders korruptionsgefährdeten Arbeitsgebiete und die damit verbundenen Risiken identifiziert wurden. In 2022 wurden verschiedene Maßnahmen in Folgeprozessen umgesetzt. So führten z.B. alle Landesbüros im Rahmen des aktuellen Unternehmensziels Compliance Management in der Außenstruktur zusätzliche Maßnahmen im Bereich der Compliance-Kultur durch, die auch der Korruptionsprävention dienten. Des Weiteren wurde zusammen mit dem Personalbereich an einer Methode zur Markierung der besonders korruptionsgefährdeten Arbeitsgebiete im HR-System gearbeitet. Diese soll als Grundlage für das Monitoring der aus der Analyse resultierenden Rotationserfordernisse dienen.

Fallmanagement

- **Hinweise auf Menschenrechtsverletzungen:** Für das Jahr 2022 sind keine Fälle im Bereich Menschenrechtsverletzungen zu berichten.
- Des Weiteren wurde das Hinweisgebersystem um eine Meldemöglichkeit für Verstöße gegen umweltbezogene Pflichten (**Verstöße gegen Umweltrecht**) erweitert, um die Anforderungen des Lieferkettensorgfaltspflichtengesetzes (LKSG) umzusetzen.
- Zum Abbau von Hindernissen und Hemmschwellen in der Hinweisabgabe hat die Stabsstelle Compliance und Integrität gemeinsam mit sechs Ländern ein Konzept für **niederschwellige Zugänge zum Hinweisgeber-/stop-it-Beschwerdesystem** der GIZ in der Außenstruktur erarbeitet (unter besonderer Beachtung der stop-it-Fallgestaltungen sexuelles Fehlverhalten, Diskriminierung und Mobbing).

Bearbeitung von Compliance und Integritätsfällen im Jahr 2022

Die Berichterstattung zu Compliance- und Integritätsfällen umfasst alle Vorgänge mit Bezug zum Strafrecht, zum zentralen Regelwerk P+R, zu GiV sowie allgemeine Beratungsanfragen oder Beschwerden. Im Berichtszeitraum 2022 hat die **Stabsstelle Compliance und Integrität** insgesamt **678 Vorgänge** (Vorjahr 553) **bearbeitet**. Die Steigerung der Vorgänge ist auch im Zusammenhang mit der seit Oktober 2020 eingeführten Meldepflicht von Führungskräften zu schwerwiegenden Compliance-Verstößen sowie der Übernahme der AGG-Beschwerdestelle (2021) durch die Stabsstelle Compliance und Integrität und der Aufnahme dieser Vorgänge in ihre Fallstatistik zu sehen. Zudem kann angenommen werden, dass ein verbessertes Hinweisgebersystem, die fortlaufende Optimierung des IKS sowie ein erhöhtes Compliance-Bewusstsein in der Belegschaft zu einer Verringerung der Dunkelziffer bei Compliance-Vorfällen führt. Gleichwohl ist nicht auszuschließen, dass neben einer Verringerung der Dunkelziffer auch ein tatsächlicher Aufwuchs an Vorgängen stattfindet. Grund hierfür könnte die Arbeit in fragilen Kontexten sein, die häufig mit Fernsteuerung einhergeht.

Nicht ermittlungsrelevante Vorgänge:

- Es gingen 252 Beratungsanfragen (Vorjahr 266) ein. Diese bezogen sich inhaltlich vor allem auf die Vermeidung von Interessenkollisionen, Fragen zu Geschenken und anderen Vorteilen sowie Fragen zu der Interpretation von P+R-Regeln.
- Hinzu kamen 51 weitere Vorgänge, denen kein Compliance-Verstoß zugrunde liegt (z.B. allg. Beschwerden über die Lage im Partnerland, Nichtberücksichtigung in der GIZ-Rekrutierung).

Ermittlungsrelevante Vorgänge:

- Insgesamt wurden 208 Hinweise (Vorjahr 143) auf mögliche Verstöße und Missstände von internen und externen Hinweisgebenden über die Eingangskanäle der GIZ gegeben. Die Mehrzahl der Hinweise bezog sich auf Vorfälle von Interessenkollisionen, betrugs- oder korruptionsrelevanten Sachverhalten und sonstige Verstöße gegen GIZ-Regeln und -Verfahren. Im Jahr 2022 wurde das Online-Hinweisgeberportal der GIZ 155-mal (Vorjahr 123) genutzt. Die Ombudsperson wurde von 4 Hinweisgebenden (Vorjahr 5) eingeschaltet.
- Im Berichtsjahr wurden 167 Sachverhalte (Vorjahr 109) auf mögliche oder nachgewiesene (interne) Verstöße und Missstände an die Stabsstelle gemeldet. Diese bezogen sich auf vor allem auf Spesen- und Abrechnungsbetrug durch GIZ-Personal oder missbräuchliche Mittelfehlverwendung bei Finanzierungsempfängern sowie Diebstähle von Eigentum.

Von den 375 eingegangenen, ermittlungsrelevanten Hinweisen und Meldungen aus dem Jahr 2022 konnten 297 Fälle abgeschlossen werden. Davon wurden in **68 Fällen Compliance-Verstöße nachgewiesen**. Es wurden angemessene Konsequenzen veranlasst bzw. entsprechende Korrekturmaßnahmen ergriffen (z.B. disziplinarische Maßnahmen, Beendigung von Geschäftsbeziehungen, Verschärfung von Kontrollprozessen, Sensibilisierung von internen und externen Prozessbeteiligten).

Weitere Compliance Prozesse

- **Tax Compliance Management System (TCMS):** Das TCMS ist ein im Auf- und Ausbau befindlicher Teilbereich des CMS, dessen Zweck die Sicherstellung der vollständigen und zeitgerechten Erfüllung steuerlicher Pflichten ist. Die Compliance- Themenverantwortung dafür ist im Steuerteam des Finanzbereichs angesiedelt. Das Tax Compliance Management setzt derzeit unterschiedliche präventive Maßnahmen um, wie

Handreichungen und fachliche Vorgaben, Schulungen, ein ausgeprägtes Wissensmanagement, das Führen eines Rechtskatasters sowie detektive Maßnahmen, wie systemgestützte Verprobungen, Plausibilitätskontrollen und stichprobenhafte Auswahl von Geschäftsvorfällen zur manuellen Überprüfung.

- **Informationssicherheitsmanagement System (ISMS):** Das ISMS in der GIZ befindet sich derzeit im Aufbau bzw. in der Weiterentwicklung. Es legt fest, mit welchen Instrumenten und Methoden die Leitungsebene die auf Informationssicherheit ausgerichteten Aufgaben und Aktivitäten lenkt. Ziel ist es, innerhalb der GIZ ein angemessenes Schutzniveau für Vertraulichkeit, Integrität und Verfügbarkeit der GIZ-Informationen zu erreichen bzw. aufrechtzuerhalten. Die zugehörige Compliance-Themenverantwortung wird im Laufe des Jahres 2023 in der am 1. August 2022 gegründeten Stabsstelle Information Governance angesiedelt.

Compliance-Qualifizierung

Alle Beschäftigten sind laut GiV und P+R zur Teilnahme am **Compliance-Basismodul** und alle Führungskräfte zusätzlich zur Teilnahme am **Compliance-Führungskräfte**modul verpflichtet. Die web-basierten Trainings (WBTs) unterliegen einem 3-jährigen Wiederholungsturnus, die Führungskräfte tragen die Verantwortung für die Sicherstellung der Durchführung. Beide WBTs sind verpflichtende Bestandteile des Einführungsprogramms für alle neuen Beschäftigten und müssen im Verlauf der ersten 100 Arbeitstage durchgeführt werden.

Seit August 2022 stehen aufgrund einiger veränderter Anforderungen inhaltlich aktualisierte Versionen zur Verfügung. Das Compliance-Basismodul wurde um das **Thema „Ethik- und Verhaltenskodex“ ergänzt** und die Kapitel zum Datenschutz und zur Informationssicherheit aus dem Compliance-Basismodul entfernt. Für beide Themen sind inzwischen eigenständige, verpflichtende webbasierte Trainings durchzuführen.

Für alle **Nationalen Mitarbeitenden**, die das Web-basierte Compliance- und Integritäts-Training nicht durchführen können, haben die Landesdirektionen laut P+R die Teilnahme an einer Präsenzveranstaltung sicherzustellen. Hierfür hat die Stabsstelle Compliance und Integrität in ihrer „Toolbox Compliance-Trainings“ eine **Offline-Trainings-Version** zu den Themen „Ethik- und Verhaltenskodex“, „Korruptionsprävention und Interessenkonflikte“ (beides Kerninhalte der GiV) sowie „Gleichbehandlung und Antidiskriminierung“ veröffentlicht.

Compliance-Berichterstattung

Die Stabsstelle liefert Beiträge mit dem Fokus auf das CMS, IKS sowie Antikorruptions-Maßnahmen der GIZ

- zur Print-Version des Integrierten Unternehmensberichts (IUB) der GIZ sowie zum IUB-Online,
- für die Berichterstattung der GIZ zum Deutschen Nachhaltigkeitskodex (DNK),
- für die Fortschritts-Berichterstattung der GIZ zum UN Global Compact,
- für den jährlichen Bericht der GIZ an das Bundesinnenministerium zum Integritätsbericht der Bundesregierung,
- zum Umsetzungsstand der Empfehlungen der OECD Working Group on Bribery zu Auslandsbestechung.

Sie nimmt regelmäßig an Austauschveranstaltungen insbesondere zu Antikorruption teil, etwa im Rahmen ihrer Mitgliedschaft bei Transparency International.

Compliance-Überwachung und Verbesserung

Die Überwachung der Angemessenheit und Wirksamkeit ist zentrales Element eines funktionierenden CMS. Sie ermöglicht es, Schwachstellen im CMS zu erkennen, Maßnahmen daraus abzuleiten und somit das **System kontinuierlich zu verbessern**. Hierfür sind **gute Steuerungsinstrumente** erforderlich.

Notwendige Anpassungen werden insbesondere aus dem IKS, der Compliance-Risk-Control-Matrix, den Auswertungen des Fallmanagements, dem Operationsplan der Stabsstelle Compliance und Integrität sowie der Sichtung der unternehmensweiten Berichterstattung abgeleitet. Ein Überwachungsplan enthält die wesentlichen Maßnahmen zur Verbesserung des CMS (mit Ausnahme der IKS-Maßnahmen, für die es eine eigene Überwachung gibt, siehe unten). Er wird jährlich erstellt und gibt einen Überblick über Inhalt, Art und Stand der jährlichen sowie der in jedem Jahr regelmäßig wiederkehrenden Maßnahmen der Stabsstelle.

Der Überwachungsplan wurde dem Compliance Committee in der November-Sitzung 2022 vorgelegt. Die Maßnahmen erstrecken sich im Wesentlichen auf die vier Handlungsfelder Compliance-Risiken, -Programm, -Kommunikation und -Überwachung. Alle für das Jahr 2022 geplanten Maßnahmen wurden vollständig und mehrjährig geplante Maßnahmen zeitlich adäquat umgesetzt.

4. Das Interne Kontrollsystem der GIZ

Die rechtliche Notwendigkeit zur Etablierung eines IKS ergibt sich aus den Sorgfaltspflichten der Unternehmensleitung und den Überwachungsaufgaben des Aufsichtsrats. Das IKS der GIZ ist unterhalb der Ebene des Vorstands gemäß internationalen Standards auf dem „Modell der drei Linien“ aufgebaut. Es ist ein **wesentlicher Bestandteil der Unternehmensführung und -abläufe** und spielt eine **Schlüsselrolle bei Identifizierung, Bewertung, Management und Überwachung wesentlicher Risiken**, denen die GIZ ausgesetzt ist.

Im Juli 2020 hatte der Vorstand beschlossen, das IKS zu professionalisieren und den **Reifegrad „überwacht“ anzustreben**. Ausgangspunkt der Entscheidung war ein gemeinsames Verständnis, dass die Größe und Verfasstheit der GIZ eine **unternehmensweite Gesamtverantwortung und Koordinierungsfunktion** sowie eine **strukturierte, systematische Darstellung aller für das IKS wichtigen Kontrollprozesse** erfordert, um dieses Governance-Thema angemessen weiterzuentwickeln und steigenden externen Anforderungen im Hinblick auf die Dokumentation und Überprüfung der Kontrollaktivitäten, einschließlich der gesetzlichen Überwachungs- und Nachweispflicht gegenüber dem Aufsichtsrat, gerecht zu werden. Ein gesonderter Bericht des Vorstands zur Wirksamkeit von internen Kontrollsystemen, Risikomanagement und internem Revisionssystem erfolgt zweijährlich an den Prüfungsausschuss des Aufsichtsrats (letzte Berichterstattung am 16. Mai 2023).

Der **Mehrwert des Reifegrads „überwacht“** besteht darin, einen **Überblick über risikobehaftete Prozesse** im Unternehmen zu haben, auf Gesamtunternehmensebene relevante **Kontrollschwächen präventiv zu erkennen** bzw. aus Fehlern und dolosen Handlungen **systematisch zu lernen** und **Kontrollmaßnahmen anzupassen**. Dies ermöglicht, dass Prozesse auch unter Kontrollaspekten kontinuierlich verbessert und Kontrollschwächen systematisch behoben werden können. Dadurch wird die **Sprechfähigkeit nach Innen und Außen erhöht** sowie die **notwendige Grundlage für eine externe Überprüfung der Wirksamkeit** geschaffen.

Voraussetzung für die Erlangung des höheren Reifegrads „überwacht“ ist eine **aussagekräftige Beschreibung des IKS**, eine detaillierte Beschreibung auf Prozessebene und eine **zentrale Themenverantwortung**, die Kontrollen überwacht, weiterentwickelt und darüber aggregiert berichtet. Entsprechend wurde auf Beschluss des Vorstands eine übergeordnete Themenverantwortung für das IKS organisatorisch in der Stabsstelle Compliance und Integrität verankert. Das IKS der GIZ ist nach den Anforderungen des Prüfungsstandards 982 des Deutschen Instituts der Wirtschaftsprüfer (IDW PS 982) aufgebaut. Danach müssen **sechs Elemente implementiert** und in einer IKS-Beschreibung dokumentiert sein. Die Beschreibung des IKS der GIZ hat der Vorstand im Mai 2022 beschlossen. Damit wurden wesentliche Entscheidungen zu Zielen und Strategie des IKS, zur Reichweite, zur IKS-Methodik und zum Ablauf und der Organisation getroffen.

Zur schrittweisen Weiterentwicklung des IKS (Reifegrad „überwacht“) wurden **2022** darüber hinaus folgende **Maßnahmen in den sechs Elementen** umgesetzt:

Kontrollumfeld, Kultur und Organisation

Das Kontrollumfeld stellt den Rahmen dar, innerhalb dessen die Regelungen eingeführt und angewendet werden. Dies umfasst die Gesamtheit der Standards, Prozesse und Strukturen als Grundlage für die Durchführung der Internen Kontrollen (IK). Es ist geprägt durch den Tone from the Top sowie die Grundeinstellungen, das Problembewusstsein und das Verhalten der Mitarbeiter*innen.

IKS-Ziele

Das IKS ist als Teilbereich der Unternehmenssteuerung in der Unternehmensstrategie verankert. Entsprechend werden die IKS-Ziele aus den Zielen des Unternehmens abgeleitet. Daraus ergeben sich für die GIZ folgende Ziele des IKS: Ordnungsgemäße Verwendung öffentlicher Mittel, ordnungsgemäße und effiziente Durchführung von Geschäftsprozessen, aussagefähige und zuverlässige (interne und externe) Finanzberichterstattung sowie die Einhaltung von relevanten Gesetzen, Verordnungen und Regularien.

Risikobeurteilung und Reichweite (Scope)

Zur Erreichung der IKS-Ziele liegt der Fokus auf den kaufmännischen und administrativen Prozessen. Dabei verfolgt die GIZ einen risikobasierten Ansatz. Folgende Prozesse (Zentrale und Außenstruktur) wurden für die Zielerreichung als besonders risikobehaftet identifiziert und gelten entsprechend als IKS-relevant: Beschaffung von Dienstleistungen, Sachgütern und Baumaßnahmen, Vergabe von Finanzierungen, Vergütung und Zusatzleistungen managen, Finanzen managen.

Im Berichtsjahr wurden die Risiken im **Prozess „Finanzierungen vergeben“** aus der Perspektive des Compliance Managements und des IKS durch die Stabsstelle Compliance und Integrität gemeinsam mit der fachlich zuständigen Abteilung Service Finanzen im Finanzbereich **analysiert und bewertet**. In der Folge wurde die Abteilung bei Überarbeitung des Prüfkonzpts für die finanzielle Abwicklung von Finanzierungen sowie Einführung einer risikobasierten Methodik beraten.

Prozesse und Kontrollaktivitäten

Die Kontrollaktivitäten beinhalten Steuerungs- und Kontrollmaßnahmen, die den identifizierten und bewerteten Risiken begegnen und somit sicherstellen sollen, dass die IKS-Ziele erreicht werden. Nach der 2021 entwickelten IKS-Methodik sollen die oben genannten IKS-relevanten Prozesse beschrieben und die relevanten Risiken identifiziert und bewertet werden. Entsprechend werden die **Schlüsselkontrollen** definiert. Nach Abwägung von Eintrittswahrscheinlichkeit, Schadenshöhe und Aufwand der Kontrolle werden die Kontrollanforderungen für jeden Prozess definiert und in **Risikokontrollmatrizen (RKM)** dokumentiert. Alle RKM zusammen bilden die Dokumentation der Kontrollaktivitäten sowie den Rahmen für die Überwachung des IKS. Um sicherzustellen, dass die Anforderungen des IKS sowie die Einführung der in der IKS-Beschreibung dokumentierten IKS-Methodik bei der Implementierung von SAP S/4HANA (S4GIZ) berücksichtigt werden, bringt sich die IKS-Funktion in den S4GIZ-Workstream „Procure to Pay“ (Beschaffung von Dienstleistungen, Sachgütern und Baumaßnahmen sowie Vergabe von Finanzierungen) ein.

Information und Kommunikation

Die Kommunikation zum IKS erfolgt über die Führungskaskade, interne Informations- und Kommunikationsformate (z.B. Änderungen im Regelwerk P+R) sowie Qualifizierungs- und

Schulungsmaßnahmen. Das o.g. WBT Compliance-Basismodul behandelt IKS-relevante Themen (u.a. EU-Beihilferecht, Geldwäsche- und Terrorismusfinanzierungsprävention, Korruptionsprävention, Finanzierungen, Preisrecht und Vergaberecht). Auch der Fortbildungskatalog der GIZ beinhaltet Trainings zu den wesentlichen IKS-relevanten Themen. Im Onboarding-Prozess sind Basis-Fortbildungen zu kaufmännischen Themen für alle Beschäftigten sowie Vertiefungskurse für kaufmännisches Personal obligatorisch.

In 2022 wurde erstmals eine gemeinsame **Schulung zum risikobasierten Ansatz** von der IKS-Governance-Funktion, der Stabsstelle Compliance und Integrität und der Gruppe Risikomanagement durchgeführt.

Am 21.02.2022 hat die Stabsstelle Compliance und Integrität im Rahmen der GIZ internen Veranstaltungsreihe „Compliance-Dialog“ zum unternehmensweiten **Compliance-Dialog „Agil in einem regulatorischen Umfeld“** eingeladen. Nach Einleitung durch Herrn Schäfer-Gümbel, Vorstand, stand in einer zeitweise von über 500 Interessierten verfolgten Panel-Diskussion die Frage im Mittelpunkt, wie es gelingen kann, innovativ, agil und kreativ zu sein und zugleich die anvertrauten Mittel regelgerecht, integer und verantwortungsbewusst umzusetzen.

Überwachung, Berichterstattung und Verbesserung

Überwachung:

Das IKS der GIZ wird regelmäßig überwacht und durch ergänzende Elemente und Informationen, die aus allen drei Linien hervorgebracht werden, verbessert. Voraussetzung für die Überwachung ist die o.g. IKS-Beschreibung.

Berichterstattung:

- Die IKS-Funktion berichtet jährlich im **"Integrierten Compliance- und IKS-Jahresbericht"** an den Vorstand, der seinerseits dazu an den Aufsichtsrat berichtet.
- Einmal jährlich erstellt die IKS-Funktion eine **Gesamtauswertung aller durchgeführten IK von Projekten** in Innen- und Außenstruktur (IK-Abdeckung). Die Berichterstattung zur **IK-Statistik** war bis 2021 Aufgabe der Stabsstelle Revision, sie erfolgt im ersten Quartal. Interne Kontrollen zielen darauf ab, Abweichungen vom internen Regelwerk der GIZ, doloses Handeln und Abrechnungsrisiken frühzeitig zu erkennen, um Maßnahmen zur Gegensteuerung zu ergreifen. Sie stellen eine wesentliche **Unterstützung für das Management** bei dessen Kontrollaufgaben dar. Defizite in der kaufmännischen Performance können frühzeitig erkannt, Abrechnungsrisiken minimiert und Betrugsfälle aufgedeckt werden.
- Durch die im Jahr 2022 teilweise noch vorliegenden COVID-19 bedingten Einschränkungen in einigen Partnerländern kam es auch bei der IK-Durchführung zu Verzögerungen und Ausfällen von geplanten Prüfungen. Im **Ausland** lag die IK-Abdeckung jedoch wieder auf einem höheren Niveau (91%) als im Vorjahr (86 %).
- Die Anzahl der zu prüfenden Projekte in **Deutschland** hat sich gegenüber den Vorjahren auf 545 verringert (gegenüber 633 in 2021). Dies ist z.T. auf die entsprechende Umstellung auf einen zweijährigen Prüfturnus zurückzuführen. Allerdings ist die Anzahl der geprüften Projekte mit 312 deutlich höher als die Anzahl der geprüften Projekte in den Vorjahren. Entsprechend konnte die Quote gegenüber 2021 von 41% auf 57% gesteigert werden.

Verbesserung (Weiterentwicklung):

- Um Erkenntnisse aus externen Prüfungen, Revisionsprüfungen und Compliance-Fällen bei der Identifikation von Risiken und Ableitung von Handlungsbedarfen berücksichtigen zu können, ist die IKS-Funktion Mitglied im internen Ausschuss für Prüfungscoordination. In 2022 haben sich hier **keine Hinweise auf strukturelle Kontrollschwächen** ergeben.
- Die **Vorgaben zur Durchführung der IK** von Projekten und Büros wurden im Frühjahr 2022 grundlegend **überarbeitet**: Büros in Ländern, die nach Einschätzung der Stabsstelle Compliance und Integrität ein hohes bzw. sehr hohes Risikopotential aufweisen, werden jährlich durch eine IK geprüft, alle anderen alle zwei Jahre. Die Büro-IK wird an allen Bürostandorten des Landes durchgeführt. Projekte im Ausland werden jährlich durch die IK geprüft, Projekte in Deutschland alle zwei Jahre.
- In 2022 wurden die **IK-Checklisten** im Hinblick auf eine stärkere Risikoorientierung bei gleichzeitiger Sicherstellung einer weiterhin hohen Prüfdichte **überarbeitet**. Dabei wurde die Anzahl der Prüfpunkte reduziert. Die Checklisten umfassen nunmehr Schlüsselkontrollen, die standardmäßig im Rahmen jeder IK abgeprüft werden müssen. Eine große Anzahl von Prüfpunkten wurde als sogenannte Vertiefungsprüfungen klassifiziert, die nunmehr in regelmäßigen Abständen ebenfalls überprüft werden sollen, aber nicht mehr standardmäßig in jeder IK. Dieses Konzept wird wirksam mit Inbetriebnahme des Audit-Moduls in der Risikomanagement-Software „MIRAI“.

5. Ausblick 2023: Aktuelle Handlungsbedarfe

Die Konsolidierung des CMS als Gesamtsystem

Die Konsolidierung des CMS als Gesamtsystem ist weiterhin ein wesentlicher Schwerpunkt. Dazu dienen insbesondere nachfolgende, geplante Maßnahmen im Rahmen der **Umsetzung des Unternehmensziels „Compliance Management“** (Mehrjahresziel 2022 und 2023):

- **Prüfung des CMS der GIZ entlang der DIN-ISO37301:2021:** Für die Vorbereitung der geplanten externen Prüfung des CMS entlang der ISO 37301 Compliance-Management hat die Stabsstelle Compliance und Integrität eine digitale Dokumentation nach den Anforderungen der ISO 37301 erstellt. Im Rahmen der Prüfung soll in 2023 auch ein Vorschlag erarbeitet werden, wie die Compliance-Berichterstattung von der bisherigen IDW-Struktur auf die ISO-Struktur umgestellt werden kann.
- **Compliance-Prüfung in der Außenstruktur:** Sämtliche vorliegende Landesrisikoprofile werden auf strukturelle Risiken und etwaige Handlungsbedarfe hin ausgewertet. Auf dieser Grundlage wird geprüft, ob und wie das Compliance-Management in der Außenstruktur weiterzuentwickeln ist. Die drei Landesbüros der Fokusländer werden bis Ende 2023 durch eine externe sachkundige Stelle dahingehend geprüft, ob die aus dem Compliance Management System des Unternehmens resultierenden Anforderungen ordnungsgemäß umgesetzt werden.
- Das Konzept der GIZ für **niederschwellige Zugänge zum Hinweisgeber- und Beschwerdesystem in der Außenstruktur** wird im 3. Quartal 2023 als verbindliches Dokument voraussichtlich unternehmensweit eingeführt.

Weitere Maßnahmen sind u.a.:

- Der **Ausbau eines effektiven Schutzes von Hinweisgebenden** wird für die Innen- und Außenstruktur vorangetrieben.
- Um die Fallbearbeitung, insbesondere die dezentrale Sachverhaltsaufklärung, weiter zu professionalisieren, werden **Verfahrensgrundsätze sowie Leitlinien für die Sachverhaltsaufklärung** entwickelt. Diese sollen in der zweiten Jahreshälfte 2023 unternehmensweit angewendet bzw. eingeführt werden.

Die schrittweise Weiterentwicklung des IKS

Zur schrittweisen Weiterentwicklung des IKS stehen nachfolgende Maßnahmen an:

- Formulierung der **Anforderungen des IKS für S4GIZ** (Schlüsselkontrollen und IKS-Methodik) und Input in entsprechende Prozesse
- **Einführung der IKS-Methodik in der Außenstruktur:** Unterstützung der fachlich verantwortlichen Einheiten bei der Erstellung von Prozessbeschreibungen und Risikokontrollmatrizen für IKS-relevante Prozesse in der Außenstruktur
- **Identifikation von Risiken und Ableitung von Handlungsbedarfen** für das IKS (z.B. Berücksichtigung von Erkenntnissen aus externen Prüfungen, Revisionsprüfungen, Compliance-Fällen, IK)
- Weiterhin enge Begleitung der Entwicklung der Risikomanagement-Software „MIRAI“, um sicherzustellen, dass die Anforderungen des IKS an **prüfungsartübergreifende Auswertungsbedarfe** (qualitativ und quantitativ) berücksichtigt werden



Impressum

Deutsche Gesellschaft für
Internationale Zusammenarbeit (GIZ) GmbH

Sitz der Gesellschaft
Bonn und Eschborn

Friedrich-Ebert-Allee 36 + 40	Dag-Hammarskjöld-Weg 1 - 5
53113 Bonn, Deutschland	65760 Eschborn, Deutschland
T +49 228 44 60-0	T +49 61 96 79-0
F +49 228 44 60-17 66	F +49 61 96 79-11 15

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

Titelgrafik:
Olivia Ockenfels, odecologne