# Corporate Governance und Compliance im Fokus

## Welche Auswirkungen hat die Änderung des Deutschen Corporate Governance Kodex auf Ihr Compliance Management System?

Der Deutsche Corporate Governance Kodex (DCGK) trat in seiner neuesten Fassung mit der Bekanntmachung durch das Bundesjustizministerium im Bundesanzeiger zum 27. Juli 2022 in Kraft. Kodex-Änderungen basieren in der Regel auf aktuellen Entwicklungen in der Corporate Governance und den damit verbundenen Themen, wie in diesem Fall insbesondere der Einrichtung eines (konzernweiten) Compliance Management Systems (CMS) sowie der Erhöhung der Transparenz und der Förderung der Nachhaltigkeit. Damit wird der Entwicklung der letzten Jahre, dass Compliance wesentlicher Bestandteil einer guten Corporate Governance eines Unternehmens ist, Rechnung getragen.

Ein Jahr nach Inkrafttreten des neuen Kodex, lässt sich feststellen, dass das Bewusstsein von Vorständen und Aufsichtsräten in Bezug auf Compliance in den letzten Jahren grundsätzlich enorm gestiegen ist, was auch durch die explizite Aufnahme in der neuen Fassung des DCGK bestätigt wird.

## Compliance ist wesentlicher Bestandteil einer guten Corporate Governance eines Unternehmens.

### Was fordert der neue DCGK von Ihrem CMS?

Bisher beinhaltete der DCGK lediglich die Empfehlung zur Einrichtung eines (konzernweiten) CMS. Laut den Grundsätzen 4 und 5 des DCGK (in der Fassung von 2022 ist der Vorstand verpflichtet, ein angemessenes und wirksames CMS als Bestandteil des internen Kontrollsystems bzw. Risikomanagementsystems (IKS/RMS) im Konzern einzuführen.

Diese Grundsätze spiegeln die geltende Rechtslage wider: Gemäß § 91 Abs. 3 AktG i.d.F. des FISG müssen börsennotierte Unternehmen ein angemessenes und wirksames IKS bzw. RMS einrichten. Das IKS umfasst auch die Grundsätze, Verfahren und Maßnahmen, die erforderlich sind, um die Einhaltung der maßgeblichen rechtlichen Vorschriften zu gewährleisten. Aus Sicht der Regierungskommission besteht daher auch eine Verpflichtung zur Einrichtung eines an die Risikolage des Unternehmens angepassten CMS.

Der Vorstand trägt gemäß Grundsatz 4 S. 2 die Verantwortung für die Überwachung der Angemessenheit und Wirksamkeit des CMS. Laut der Begründung zu A.5. des DCGK 2022 ist die CMS-Überwachung eine Kernfunktion der Internen Revision. Dies ermöglicht es dem Vorstand, in regelmäßigem Turnus die wesentlichen Merkmale des IKS bzw. RMS einschließlich des CMS nicht nur wie in der Praxis bislang üblich zu beschreiben, sondern auch dessen Angemessenheit und Wirksamkeit zu bewerten.

Zudem muss der Aufsichtsrat oder sein Prüfungsausschuss in der Lage sein, die Angemessenheit und Wirksamkeit des CMS im Rahmen seiner allgemeinen Überwachungspflicht zu beurteilen – unabhängig von der Stellungnahme im Lagebericht. Grundsatz 16 ergänzt dies, indem er vorschreibt, dass der Vorstand den Aufsichtsrat regelmäßig, zeitnah und umfassend über Compliance-Themen informieren muss.

### Wie nachhaltig ist Ihre Unternehmensführung?

In der Fassung des Kodex von 2022 wird die Bedeutung von Nachhaltigkeit im Zusammenhang mit guter Unternehmensführung hervorgehoben. Sozial- und Umweltbelange, die zunehmend in den Fokus von Stakeholdern rücken, sollen demnach in börsennotierten Unternehmen stärker berücksichtigt werden. Identifikation und Bewertung der Chancen und Risiken in Bezug auf Sozial- und Umweltfaktoren werden dabei im Zuständigkeitsbereich des Vorstands verankert. Zukünftig sollte vom Vorstand ein besonderes Augenmerk daraufgelegt werden, dass nicht nur langfristige wirtschaftliche Ziele definiert, sondern auch soziale und ökologische Ziele festgesetzt werden, um durch das Unternehmen veranlasste menschenrechtliche und umweltbezogene Risiken zu reduzieren. Als Orientierungshilfe zur systematischen Steuerung der Chancen und Risiken dienen laut Kodex-Begründung die UN Sustainable Development Goals. Um die Zielerreichung sicherzustellen, sollen IKS und RMS bzw. CMS nachhaltigkeitsbezogene Elemente aufweisen, sofern dies durch gesetzliche Anforderungen nicht bereits erfolgt ist.

Für mehr Nachhaltigkeit muss mehr Verantwortung übernommen werden, sowohl auf individueller als auch auf unternehmerischer Ebene.

Warum die Kodex-Änderung mit dem Sustainability-Update notwendig war, liegt klar auf der Hand: Für mehr Nachhaltigkeit muss mehr Verantwortung übernommen werden, sowohl auf individueller als auch auf unternehmerischer Ebene. Durch die neuen Leitlinien des DCGK soll hierdurch auf unternehmerischer Seite ein wertvoller Beitrag zum verantwortungsbewussten Wirtschaften geleistet werden.

### Was ist nun konkret zu tun?

Der Kodex ist eine freiwillige Selbstverpflichtung börsennotierter Unternehmen und Unternehmen mit Kapitalmarktzugang im Sinne des § 161 Abs. 1 S. 2 AktG. Im DCGK besteht grundsätzlich der „Comply or Explain"-Grundsatz, der Unternehmen dazu verpflichtet, entweder die im Kodex festgelegten Empfehlungen zu befolgen oder ihre Abweichungen davon zu erklären. Darüber hinaus gilt der DCGK auch für Unternehmen aller Rechtsformen und Größen als Best-Practice-Empfehlung, welche als Orientierungshilfe genutzt wird, da dessen Empfehlungen zu späteren Zeitpunkten oftmals ihren Weg in rechtliche Vorgaben gefunden haben.

Das Identifizieren, Bewerten und Steuern von Risiken – auch in Bezug auf Compliance-, Sozial- und Umweltaspekte – ist eine essenzielle Aufgabe für jedes Unternehmen unabhängig von Rechtsform, Branche und Größe, um es regelkonform und nachhaltig zu führen und folglich Rechtsverstöße und Reputationsverluste damit zu verhindern.

Die neuesten Änderungen des DCGK und einschlägige Gesetzesänderungen (z.B. das Lieferkettensorgfaltspflichtengesetz (LkSG)) zeigen, dass diese Aufgabe auch zukünftig immer mehr an Bedeutung gewinnen wird – nicht nur in Form der Anpassung interner Unternehmensprozesse, sondern auch für die externe Berichterstattung. Der Grund hierfür ist das zunehmende Interesse externer Stakeholder und der Öffentlichkeit.

Das Identifizieren, Bewerten und Steuern von Risiken – auch in Bezug auf Compliance-, Sozial- und Umweltaspekte – ist eine essenzielle Aufgabe für jedes Unternehmen unabhängig von Rechtsform, Branche und Größe.

**Implementierung eines angemessenen und wirksamen CMS**
Wichtig ist die Implementierung eines sowohl angemessenen als auch wirksamen CMS. Hierfür müssen zunächst die Compliance-Risiken adäquat identifiziert und bewertet werden, um angemessene Maßnahmen implementieren zu können. Ein CMS ist angemessen, wenn die Maßnahmen grundsätzlich zur Reduzierung vorhandener Compliance-Risiken geeignet sind. Wirksam sind die Maßnahmen, wenn sie von den Mitarbeitern effektiv umgesetzt werden – sprich: das CMS entsprechend den Vorgaben auch tatsächlich gelebt wird. Eine risikoorientierte Implementierung des CMS ist dringend zu empfehlen, um neben der wirksamen auch eine effiziente und ressourcenschonende Umsetzung des CMS im Alltag zu gewährleisten. Für die Ausgestaltung des CMS gibt es eine Vielzahl von (inter)-nationalen Compliance-Standards, wie beispielsweise den IDW PS 980, ISO 37301 oder auch andere Regelwerke wie COSO, DoJ-Guidance etc., die als Orientierungshilfe dienen können. Sofern Sie bereits ein CMS eingerichtet haben, bietet es sich in einem ersten Schritt an, eine Gap-Analyse zur systematischen Identifizierung von Verbesserungsmöglichkeiten durchzuführen. Ziele dieser Analyse sind die Ableitung praktikabler und passgenauer Handlungsempfehlungen und die Entwicklung eines risikoorientierten und priorisierten Maßnahmenplans.

**Governance-Strukturen als effektive Unterstützung des Vorstands**
Unsere Erfahrungen zeigen, dass optimierte Governance-Strukturen den Vorstand bei seinen Aufgaben effizient unterstützen können, wie z.B. bei der Einrichtung eines konzernweit einheitlichen IKS, RMS bzw. CMS und dessen Überwachung durch die 2nd Line, der Durchführung unabhängiger Prüfungen durch die Interne Revision sowie der Sicherstellung der unternehmensweiten Umsetzung der Business Conduct Guidelines und der damit verbundenen Richtlinien und Maßnahmen. In diesem Zusammenhang sind insbesondere ein übergreifender GRC-Ansatz und ein integriertes /harmonisiertes Risikomanagement wesentliche Erfolgsfaktoren.[1]

**Adressatengerechte Berichtsstrukturen**
Weitere wichtige Aspekte sind die Implementierung von internen und externen Berichtsstrukturen, welche, um die neuen Sozial- und Umweltfaktoren zu erweitern sind, sowie das Aufsetzen von adressatengerechten Dashboards. Dadurch kann eine zielgenaue und effiziente Übersicht über die Risikosituation geschaffen werden, die zum einen eine transparente und faktenbasierte Zusammenarbeit mit dem lokalen Management schaffen soll und zum anderen für eine routinierte und effiziente Berichterstattung im Lagebericht und an den Prüfungsausschuss im Aufsichtsrat sorgt sowie den Vorstand dazu befähigt, schnell und agil auf neue Risikosituationen zu reagieren.

**Regelmäßige Überwachung der Angemessenheit und Wirksamkeit des CMS**
Durch Befragungen der 1st Line, der 2nd Line, unterschiedlicher Compliance-Funktionen oder der gesamten Belegschaft können der Reifegrad Ihres CMS in Bezug auf Sozial- und Umweltaspekte und auch darüber hinaus, die Compliance-Kultur und das Bewusstsein für Compliance beurteilt werden. Hierbei können auch Einschätzungen zu Compliance-Risikobereichen, zur Wirksamkeit von Schulungen oder des Tone from the Top sowie zur Funktionalität von spezifischen IT Compliance Tools (z.B. Third Party Due Diligence) erfolgen. Durch umfangreiche Erfahrungen und die Analyse von Daten – auch im Zusammenhang mit neurowissenschaftlichen Modellen – haben wir bereits eine solide Datengrundlage geschaffen. Darüber hinaus sind regelmäßige und effektive Analysen und Bewertungen vorhandener Kontrollmaßnahmen beispielsweise durch interne oder externe Compliance Audits ebenfalls wichtige Schritte bei der Sicherstellung der Angemessenheit und Wirksamkeit des CMS. Auch bei vorliegenden Vorfällen ist es wichtig, Ursachen- und Fehleranalysen durchzuführen und entsprechende Maßnahmen zu ergreifen, um das Risiko vergleichbarer Vorfälle oder die Wiederholungsgefahr zu reduzieren.

**Identifizierung relevanter Themenfelder und Regularien**
Bei der Beurteilung der An-gemessenheit eines CMS spielt immer auch der Geltungsbereich eine wichtige Rolle. Erstreckt sich das unternehmensweite CMS auf alle für Ihr Unternehmen relevante Themengebiete und Regularien? Dies lässt sich im Rahmen einer strukturierten Relevanzanalyse untersuchen, wobei grundsätzlich alle für das Unternehmen anwendbaren Themengebiete die Basis für die Betrachtung bieten. Mithilfe eines Filteransatzes unter Berücksichtigung von z.B. Geschäftsmodell, Kundenstruktur, Produktportfolio etc. erfolgt eine systematische und für Dritte nachvollziehbare Identifizierung der relevanten Themengebiete.

**Compliance-Risikoanalyse**[2]
Mit dem Ziel, alle wesentlichen Compliance-Risiken zu identifizieren, zu bewerten, zu steuern und zu reduzieren, sollte eine systematische Compliance-Risikoanalyse durchgeführt werden. Diese bildet das Fundament eines angemessenen und wirksamen CMS. Da die Compliance-Risikoanalyse in einem regelmäßigen Turnus und zusätzlich in erhöhten Risikosituationen ad hoc durchzuführen ist, ist eine ressourcenschonende Konzeptionierung dieses Prozesses essenziell für eine routinierte Berichterstattung und zur Gewährleistung einer guten Unternehmensführung. Eine Herausforderung, die Unternehmen in der Zukunft meistern müssen und daher in der Gegenwart nicht außer Acht gelassen werden sollte, ist die Implementierung eines effizienten Risikomanagements durch die Echtzeit-Beurteilung der Angemessenheit und Wirksamkeit des CMS. Hierfür kann ein datengesteuertes proaktives Risikomanagement eine Lösung sein.

[1] GRC-Ansatz: Ein integrierter Ansatz, der Governance (Unternehmensführung), Risk Management (Risikomanagement) und Compliance (Einhaltung von Gesetzen und Vorschriften) miteinander verbindet, um eine ganzheitliche Steuerung von Unternehmen zu ermöglichen und Synergien zwischen diesen Bereichen zu schaffen.

[2] https://www2.deloitte.com/content/dam/Deloitte/de/Documents/risk/Compliance-Risikoanalyse_2.0.pdf, abgerufen am 30.06.2023.

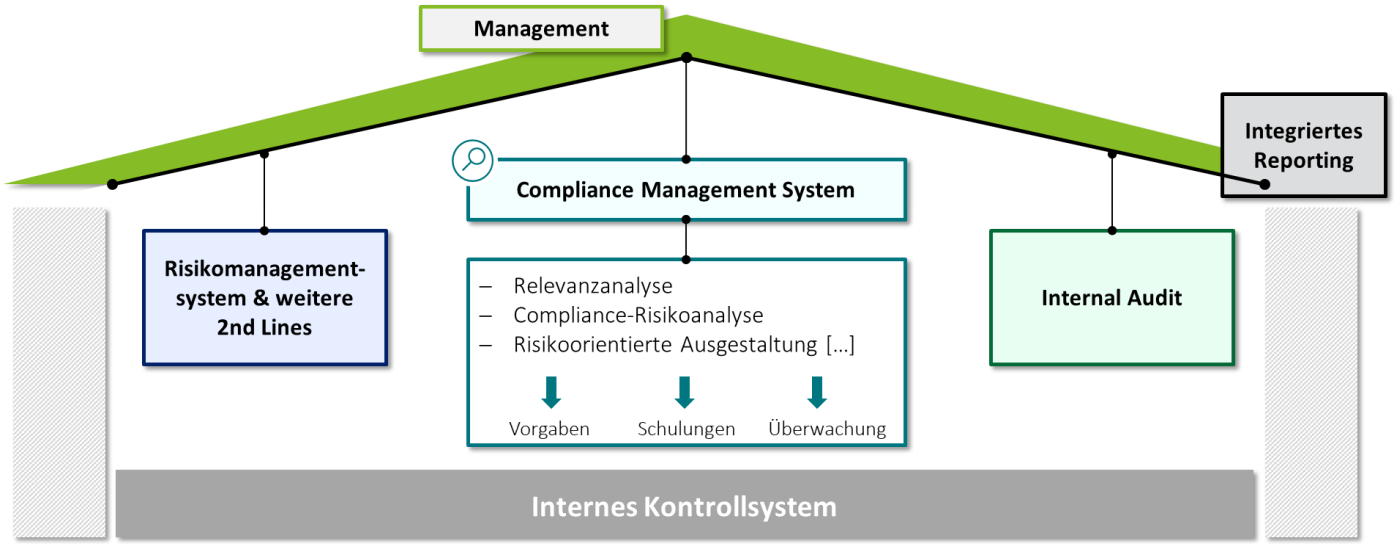


Abbildung: Einbettung der Compliance im „House of Governance“

## Welchen Mehrwert bietet Deloitte?

- Wir sind Compliance-Experten mit langjähriger Berufserfahrung in der Analyse[3], der fachlichen und technischen Konzeption, dem Aufbau bzw. der Optimierung sowie der Prüfung und Bescheinigung von Compliance Management Systemen[4] in Bezug zu sämtlichen Kern-Compliance-Themenfeldern einschließlich der Compliance in der Lieferkette (LkSG[5]).
- Wir sind zudem im regelmäßigen Austausch mit Aufsichtsbehörden, Prüfern und wichtigen Compliance-Institutionen und daher mit sämtlichen relevanten Compliance-Anforderungen bestens vertraut.
- Wir bieten ein hohes Maß an Umsetzungskompetenz und -erfahrung – unser Team legt großen Wert auf die praktische Umsetzbarkeit von erarbeiteten Konzepten und Strategien. Die risikoorientierte Ausgestaltung sowie die Angemessenheit stehen hierbei stets im Fokus.
- Wir bringen umfassendes Branchen-, Benchmark- und Best-Practice-Know-how mit – die Erfahrung in vergleichbaren Unternehmen ermöglicht uns eine effektive und effiziente Arbeitsweise.
- Wir arbeiten nicht nur für Sie, sondern mit Ihnen gemeinsam und gewährleisten dadurch einen reibungslosen und wirksamen Wissensaustausch.
- Kombiniert mit unserem Best-Practice- sowie Benchmark-Know-how bieten wir Ihnen Handlungssicherheit bei der Umsetzung neuer regulatorischer Anforderungen und fungieren als Ihr strategischer Partner in sämtlichen Compliance-Belangen.

[3] https://www2.deloitte.com/content/dam/Deloitte/de/Documents/risk/Deloitte-Broschuere-Compliance-Due-Dilligence.pdf, abgerufen am 30.06.2023.

[4] https://www2.deloitte.com/de/de/pages/risk/articles/compliance-management-system.html, abgerufen am 30.06.2023.

[5] https://www2.deloitte.com/de/de/pages/risk/articles/compliance-in-der-lieferkette.html, abgerufen am 30.06.2023.

# Ihre Ansprechpartnerinnen

**Susanne Schenk**
**Partner**
**Risk Advisory**
Tel: +49 40 32080 4265
sschenk@deloitte.de

**Saskia Korte**
**Manager – Wirtschaftsprüferin**
**Risk Advisory**
Tel: +49 40 32080 4638
skorte@deloitte.de

Deloitte.



Stand 07/2023