DICO-Handreichung zu A.5 DCGK2022 – Angemessenheit & Wirksamkeit von Compliance-Management-Systemen

2. Auflage - Stand April 2023

DICO
Deutsches Institut für Compliance

A. Einleitung

Am 27. Juni 2022 ist der neue Deutsche Corporate Governance Kodex (DCGK) 2022 in Kraft getreten. Einen Schwerpunkt der Änderungen bilden die Anforderungen an die Compliance-Organisation in börsennotierten Unternehmen.

Die Einrichtung eines (konzernweiten) Compliance Management Systems (CMS) war bislang in A.2 Satz 1 DCGK lediglich als Empfehlung an den Vorstand ausgestaltet. Nunmehr ergibt sich aus den Grundsätzen 4 und 5 DCGK eine Pflicht des Vorstands, ein angemessenes und wirksames CMS (als Bestandteil des IKS/RMS) im Konzern einzurichten. Die Grundsätze sollen die geltende Rechtslage abbilden: § 91 Abs. 3 AktG i.d.F. des FISG schafft für börsennotierte Gesellschaften eine Pflicht zur Einrichtung eines angemessenen und wirksamen internen Kontrollsystems (IKS) und Risikomanagementsystems (RMS). Das IKS umfasst nach der Regierungsbegründung (BT-Drs. 19/26966, S. 115) auch die Grundsätze, Verfahren und Maßnahmen, die erforderlich sind, um die Einhaltung der maßgeblichen rechtlichen Vorschriften zu sichern. Damit besteht nach Ansicht der Regierungskommission – im Einklang mit den im Ergebnis übereinstimmenden Einschätzungen im aktienrechtlichen Schrifttum – auch eine Pflicht zur Einrichtung eines an der Risikolage des Unternehmens ausgerichteten CMS.

Die Angemessenheit und Wirksamkeit des CMS muss der Vorstand intern überwachen (Grundsatz 4 S. 2). Die Überwachung des CMS stellt eine der Kernaufgaben der Internen Revision dar (Begründung zu A.5. DCGK 2022). Die Erfüllung der Überwachungspflicht soll dem Vorstand ermöglichen, eine Stellungnahme im Sinne der neugefassten Empfehlung A.5 DCGK 2022 abzugeben. Danach soll der Vorstand zukünftig die wesentlichen Merkmale des IKS/RMS (und damit auch des CMS) im Lagebericht beschreiben und zur Angemessenheit und Wirksamkeit der Systeme Stellung nehmen. Die Stellungnahme wird sich regelmäßig darauf beziehen, worin die interne Überwachung und ggf. externe Prüfung der Systeme bestanden hätten (Begründung zu A.5. DCGK 2022). Unabhängig von der Stellungnahme im Lagebericht ist auch der Aufsichtsrat bzw. sein Prüfungsausschuss in die Lage zu versetzen, Angemessenheit und Wirksamkeit des CMS im Rahmen seiner allgemeinen Überwachungspflicht zu beurteilen (vgl. auch § 107 Abs. 3 S. 2 AktG). Flankiert werden diese Aspekte durch den Grundsatz 16, wonach der Vorstand den Aufsichtsrat regelmäßig, zeitnah und umfassend über Fragen der Compliance informiert.

Der Kodex richtet sich an börsennotierte Gesellschaften und Gesellschaften mit Kapitalmarktzugang i.S.d. § 161 Abs. 1 S. 2 AktG. Im Rahmen der jährlichen Entsprechungserklärung müssen Vorstand und Aufsichtsrat gem. § 161 AktG erklären, ob den Empfehlungen des DCGK entsprochen wurde und wird. Nicht kapitalmarktorientierten Gesellschaften können die Empfehlungen und Anregungen des Kodex zur Orientierung dienen.

Die Kodex-Änderungen bedeuten in Verbindung mit § 91 Abs. 3 AktG einen Wandel von der in der Praxis bislang üblichen deskriptiven zu einer stärker bewertenden Compliance-Berichterstattung. Das gilt jenseits der Frage, ob A.5 DCGK 2022 tatsächlich eine „Pflicht“ zur Veröffentlichung einer bewertenden Aussage über die Angemessenheit und Wirksamkeit der Systeme begründet. Denn zumindest unternehmensintern werden der Vorstand und Aufsichtsrat bzw. sein Prüfungsausschuss im Rahmen ihrer jeweiligen Überwachungsaufgaben sowohl von der Compliance Funktion, als auch von der Internen Revision Auskunft verlangen, ob die Governance Systeme (also das CMS, wie auch das IKS/RMS) im Einklang mit § 91 Abs. 3 AktG angemessen und wirksam sind.

Auch in der Berichterstattung nach außen stellt sich die Frage, wie eine Gesellschaft oder ein Unternehmen die neue Kodexempfehlung A.5 umsetzen soll. Der DCGK 2022 macht insofern selbst keine klaren Vorgaben, sondern verlangt nach Konkretisierung.

Wie in seiner Stellungnahme zum DCGK-Entwurf 2022 angekündigt, will DICO mit dieser Handreichung seinen Beitrag dazu leisten. Im Folgenden werden verschiedene Optionen dargestellt, wie die Stellungnahme zu A.5 DCGK 2022 im Lagebericht abgefasst werden kann und wie Unternehmen in inhaltlicher und prozessualer Hinsicht zu einer Aussage über die Angemessenheit und Wirksamkeit ihres CMS kommen können.

I. Inhalt der Stellungnahme nach A.5 DCGK 2022 im Lagebericht, inkl. Praxisentwicklungen)

1. Überblick und Praxisbeispiele zur Stellungnahme

A.5 DCGK 2022 enthält die Empfehlungen, im Lagebericht zum einen die wesentlichen Merkmale des gesamten IKS und RMS zu beschreiben und zum anderen zur Angemessenheit und Wirksamkeit dieser Systeme Stellung zu nehmen. Da diese Empfehlungen über den gesetzlich vorgesehenen Inhalt des Lageberichts hinausgeht (vgl. §§ 289 Abs. 4, 315 Abs. 4 HGB) handelt es sich dabei um sogenannte „Lageberichtsfremde Angaben". Diese sind von der inhaltlichen Prüfung des Lageberichts durch den Abschlussprüfer ausgenommen, wenn sie eindeutig von den inhaltlich zu prüfenden Lageberichtsangaben abgegrenzt und als nicht geprüft gekennzeichnet sind (vgl. Begr. DCGK zu A.5; §§ 289 ff., 317 Abs. 2 HGB). Die Angaben müssen als Lageberichtsangaben dennoch ein den tatsächlichen Verhältnissen entsprechendes Bild vermitteln (§ 298 Abs. 1 Satz 1 HGB), durch den Abschlussprüfer geprüft wird dies inhaltlich allerdings nicht.

In Bezug auf Compliance sind die wesentlichen Merkmale des CMS als Bestandteil des IKS/RMS zu beschreiben. Empfehlung A.5 Hs. 1 DCGK führt damit zunächst im Wesentlichen die bisherige Rechtslage fort, wonach der Vorstand gem. A.2 DCGK 2019 die Grundzüge des CMS offenlegen soll. Wie erwähnt geht A.5 DCGK 2022 indes weiter, indem zur Angemessenheit und Wirksamkeit von IKS und RMS (unter Einschluss des CMS) im Lagebericht Stellung genommen werden soll. Welchen Inhalt diese Stellungnahme haben muss, gibt der DCGK bis auf den Umstand als solchen hingegen nicht vor. Im Ausgangspunkt stehen den Unternehmen drei Gestaltungsvarianten zur Verfügung:

(1) Rein **deskriptive Lösung**: Beschreibung der Systeme einschließlich Beschreibung der Überwachungsmaßnahmen sowie damit verbundener Hinweis, dass die ergriffenen Maßnahmen darauf ausgerichtet sind, die Angemessenheit und Wirksamkeit der Systeme sicherzustellen.

(2) Doppelte **Negativerklärung**: Erklärung des Vorstandes, dass keine Umstände bekannt sind, dass IKS/RMS nicht angemessen und wirksam sind.

(3) **Positiverklärung**: (Positive) Erklärung des Vorstands, dass die Systeme angemessen und wirksam sind bzw., dass sie angemessen sind und keine Umstände bekannt sind, die gegen deren Wirksamkeit sprechen.

Variante (1) findet sich in der Praxis bspw. im Geschäftsbericht der Infineon AG (S. 66/67), der der Lufthansa AG (S. 91/92) sowie der Drägerwerk AG & Co. KGaA (S. 55), jeweils zum Geschäftsjahr 2022. Im Lagebericht der Drägerwerk AG & Co. KGaA wird wie folgt formuliert: „Als Stellungnahme zur Angemessenheit und Wirksamkeit des IKS und des RMS einschließlich des CMS wird auf die in der Darstellung der jeweiligen Systeme sowie im Folgenden zum IKS aufgeführten Maßnahmen zur Überprüfung und Verbesserung verwiesen, die vom Vorstand veranlasst worden sind. […]"

Variante (2) wird von der überwiegenden Anzahl der Unternehmen genutzt, wie etwa in den Geschäftsberichten der thyssenkrupp AG, der Siemens AG, der Siemens Energy AG, Siemens Healthineers AG (jeweils zum 30.09.2022). Auch Unternehmen mit kalendergleichem Geschäftsjahr greifen für das Jahr 2022 auf diese Variante zurück, bspw. die adidas AG, die BASF SE, die BMW AG, die Covestro AG (S. 177) und die Daimler Truck AG (S. 137). Die Stellungnahme lautet dann in etwa wie folgt: Dem Vorstand sind aus seiner Befassung mit den Systemen keine Umstände oder Hinweise bekannt geworden, die gegen deren Wirksamkeit oder Angemessenheit (in ihrer Gesamtheit) sprechen.

Variante (3) wird von der Deutschen Bank AG (S. 70 Geschäftsbericht 2022) sowie der Symrise AG verwendet. So heißt es auf S. 59 im Geschäftsbericht 2022 der Symrise AG: „Symrise verfügt über ein umfassendes System von Kontrollen, die regelmäßig vom Vorstand geprüft und weiterentwickelt werden. Der vom Aufsichtsrat delegierte Prüfungsausschuss der Symrise AG beschäftigt sich in einer jährlichen Schwerpunktsitzung mit den bei Symrise implementierten Kontrollsystemen, um deren Angemessenheit und Wirksamkeit sicherzustellen. Der Vorstand ist überzeugt, dass die implementierten Kontrollsysteme bei Symrise in Ihrer Gesamtheit angemessen und wirksam sind."

Schließlich steht den Unternehmen natürlich auch die Möglichkeit offen, die Empfehlung nicht zu befolgen und auf Basis einer Abweichungserklärung keine Stellungnahme abzugeben.

2. Rechtliche Erwägungen zu den Anforderungen von A.5 DCGK 2022

Nachfolgend sollen die einzelnen Varianten in Bezug auf die Anforderungen des DCGK näher beleuchtet werden: Erfüllt die beschreibende Lösung ohne bewertende Aussage die Voraussetzungen einer „Stellungnahme zur Angemessenheit und Wirksamkeit"? Reicht es aus, über die Angemessenheit und Wirksamkeit der Systeme lediglich eine negative Erklärung abzugeben?

Literatur und auch das IDW haben erste Analysen zur Empfehlung A.5 Hs. 2 DCGK veröffentlicht. Einigkeit besteht, dass es einer bewertenden Aussage zum CMS als Einzelsystem (also eine Aussage i.S.v. „das CMS ist wirksam") nach A.5 DCGK 2022 im Lagebericht nicht bedarf, da (nur) eine gesamthafte Stellungnahme zum IKS/RMS verlangt ist.

Zum Inhalt der Stellungnahme:
Der Wortlaut von A.5 Hs. 2 DCGK 2022 legt durch den Begriff „Stellungnahme" nahe, dass der Vorstand eine Bewertung zur Angemessenheit und Wirksamkeit der Systeme abgeben soll. Auch die Kodexsystematik geht in diese Richtung, da die Stellungnahme gem. A.5 Hs. 2 DCGK 2022 als eigenständige Empfehlung neben A.5 Hs. 1 DCGK mit der Empfehlung zur Beschreibung der wesentlichen Merkmale steht. Dem steht allerdings die Begründung zum Kodex gegenüber: „Die Stellungnahme zur Angemessenheit und Wirksamkeit dieser Systeme wird sich regelmäßig darauf beziehen, worin die interne Überwachung und ggf. externe Prüfung der Systeme bestanden haben."

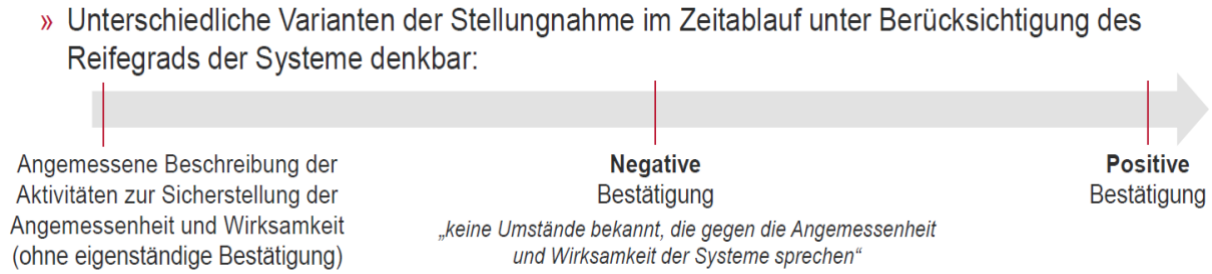
Weitere Anleitungen zum Gebrauch bzw. Vorgaben für eine bewertende Stellungnahme werden nicht gemacht. Auch nicht, ob der Kodex eine Positiv- oder Negativaussage erwartet. Im Ergebnis sind also Gestaltungsspielräume eröffnet.

Im Einzelnen:

- Variante (1), die sog. Beschreibungslösung, stützt sich vor allem auf die Begründung des DCGK, die jenseits der Beschreibung von Überwachungsmaßnahmen gerade keine weitergehenden Aussagen fordere (*Backhaus*, NZG 2023, S. 253 ff.; *Ghassemi-Tabar*, 2. Aufl. 2023, DCGK A.5 Rn. 15 ff.). Eine bewertende – zudem vom Abschlussprüfer nicht verpflichtend zu überprüfende –

Aussage sei zudem wenig aussagekräftig, wenn nicht zugleich überprüfbare Systeme und Verfahren zur Reifegradmessung existierten. Auch könne ein Dilemma des Vorstands vermieden werden, der sich bei einem Zwang zur Äußerung in Bezug auf Angemessenheit und Wirksamkeit ggf. selbst einer Organisationspflichtverletzung beschuldigen müsse, wenn Angemessenheit und/oder Wirksamkeit nicht bejaht werden könnten. Auf Basis einer fundierten Beschreibung der ergriffenen Maßnahmen zur Überwachung von Angemessenheit und Wirksamkeit der Systeme werde so in den Vordergrund gestellt, wie die Gesellschaft die nach § 91 Abs. 3 AktG bestehende Organisationsverpflichtung umsetzt. Dieses sei ein sinnvoller zusätzlicher Berichtsinhalt im Lagebericht. In diesem Sinne könne die Beschreibungslösung auch dauerhaft gewählt werden.

Auch das IDW hält die Beschreibungslösung nach Variante (1) für vertretbar, wie nachfolgend grafisch dargestellt (Grafik aus: *Sack*, Präsentation des IDW auf der DAI Konferenz „Corporate Governance & Gesellschaftsrecht“ am 14.03.2023, ferner auch *Naumann*, FAZ vom 23.01.2023, S.18 „Unternehmen besser führen“). Das IDW geht wohl davon aus, dass den Unternehmen mit steigendem Reifegrad der Systeme eine höhere Bandbreite an Stellungnahme möglich ist („Der Vorstand wird im Einzelfall die Aussage wählen, die dem Reifegrad und der Qualität der eingerichteten Systeme entspricht“ – *Naumann* a.a.O.):



- Für Variante (2) wird zunächst angeführt, dass der Kodex keine positiven Aussagen zur Angemessenheit und Wirksamkeit (im Sinne von Variante 3) verlangt bzw. kein Verbot einer Negativerklärung enthält. In Abgrenzung zu Variante (1) wird argumentiert, dass der Wortlaut wenig Interpretationsspielraum eröffne: Wäre eine Beschreibung ausreichend, wäre die Empfehlung A.5 Hs. 2 DCGK überflüssig. Ferner sei zur Herstellung der durch Empfehlung A.5 DCGK bezweckten Transparenz eine inhaltliche Bewertung erforderlich (*Kopp*, CCZ 2023, 125 ff.). Die reine Beschreibung sei für die Adressaten in Ermangelung einer eigenen Einschätzungsmöglichkeit wenig aussagekräftig und könnte von diesen daher ggf. kritisch aufgenommen werden. Die Zuspitzung, bei möglichen erkannten Schwächen dennoch zu einer Aussage angehalten zu sein, sei vom DCKG gewollt und könne nach § 161 AktG durch eine Nichtentsprechung mit A.5 DCGK sowie entsprechender Erläuterung („Soll-Vorschrift“) vermieden werden.

- Variante (3) enthält im Vergleich zu (1) und (2) explizitere Aussagen zur Angemessenheit und Wirksamkeit (entweder als doppelte Positiverklärung („angemessen und wirksam“ oder als Positiv-Negativ-Erklärung „angemessen und keine Zweifel an Wirksamkeit“). Eine derartige Stellungnahme mag insbesondere für Unternehmen in Betracht kommen, die für den jeweiligen Berichtszeitraum weitreichende bzw. umfassende interne und/oder externe Prüfungen und Bewertungen ihrer Governance-Systeme durchgeführt haben oder sich aus anderen Gründen in der Lage sehen, die Stellungnahme mit Positivaussagen zu unterlegen. Rechtliche Zweifel an der Zulässigkeit dieser Variante gibt es keine. Die doppelte Positivaussage bestätigt im Ergebnis, dass der Vorstand seiner Rechtspflicht aus § 91 Abs. 3 AktG nachgekommen ist. An sich also eine Selbstverständlichkeit. Allerdings hat eine solche Positivaussage und ihre (freiwillige)

Veröffentlichung im Lagebericht angesichts von Umfang und Komplexität der von § 91 Abs. 3 AktG erfassten Governance Systeme eine erhebliche Reichweite. Eine belastbare Aussage in diesem Sinne verlangt mithin eine ausreichend dokumentierte intern und/oder extern durchgeführte Bewertung der Systeme.

Bislang hat sich weder in Literatur noch Praxis eine dieser Ansichten durchgesetzt. Alle drei Varianten erscheinen in rechtlicher Hinsicht gut vertretbar. Aus der Art der gewählten Stellungnahme kann somit auch nicht auf die jeweiligen Gründe für die Wahl der Darstellungsform geschlossen werden.

Unter Berücksichtigung von Zielsetzung (Transparenz über Inhalt und Zustand der Governance Systeme) und Systematik von A.5 DCGK 2022 (Beschreibung [1. HS] plus Stellungnahme [2. HS]) sowie mit Blick auf die Kodexbegründung (Stellungnahme umfasst Darstellung der Überwachungs- und Prüfungsmaßnahmen) lässt sich aus unserer Sicht gleichwohl folgender Leitsatz aufstellen:

Je weniger die Angemessenheit und Wirksamkeit der Systeme in der Stellungnahme bewertet wird, desto ausführlicher und aussagekräftiger sollte die Beschreibung der Systeme und der vorgenommenen Prüfungs- und Überwachungsmaßnahmen ausfallen.

Für die konkrete Umsetzung sind schließlich in allen Varianten die noch folgenden Punkte zu beachten:

- Die Stellungnahme umfasst das gesamte IKS/RMS einschließlich CMS (Grundsatz 5, Empfehlung A.5).

- Zum CMS gehören die an der Risikolage des Unternehmens ausgerichteten Compliance Themen bzw. Maßnahmen, unabhängig davon, ob diese im Unternehmen in einem oder mehreren Management Systemen oder Programmen verortet bzw. wie diese im Einzelnen organisatorisch zugeordnet sind. Werden beispielsweise für die Risikolage des Unternehmens relevante Datenschutzrisiken außerhalb des CMS durch ein DMS oder Steuerrisiken durch ein TCMS gesteuert, sind diese vom CMS-Begriff des Kodex umfasst.

- Die Begriffe Compliance und CMS sind konzernweit zu verstehen. Dies ergibt sich aus der Verwendung des Begriffs „Unternehmen“ durch den Kodex in Grundsatz 5 (vgl. Präambel DCKG) und gilt ungeachtet der weithin diskutierten Frage, ob Compliance stets eine konzernweite Dimension hat.

- Etwaige Compliance-Vorfälle in der Berichtsperiode indizieren nicht zwingend die Unangemessenheit oder Unwirksamkeit des CMS (z.B. einfache Arbeitsfehler, Ausreißer, Exzesse – vgl. RegBegr FISG, BT-Drucks. 19/26966, 115). Anerkanntermaßen kann auch ein angemessenes und wirksames CMS nicht jeden Vorfall verhindern. Ferner richtet sich die Stellungnahme auf das gesamte IKS/RMS. Ob somit eine wesentliche Beeinträchtigung von Angemessenheit und Wirksamkeit in diesem Sinne vorliegt, ist anhand des Gesamtsystems und nicht anhand einzelner (im Gesamtsinne unwesentlicher) Teilaspekte zu beurteilen.

- Eine externe Prüfung oder Zertifizierung der Systeme ist für die Aussage zu Angemessenheit und Wirksamkeit keinesfalls erforderlich. Sie kann im Sinne einer Überwachungsmaßnahme aber dabei helfen, dem Vorstand eine angemessene Informationsgrundlage für seine Beurteilung zu geben.

Im Anschluss an diesen Überblick zu Inhalt und Systematik der Stellungnahme nach A.5 DCGK 2022 soll nun in dieser Handreichung anhand ausgewählter Praxisbeispiele illustriert werden, wie die zugrundeliegende Einschätzung bzw. Bewertung der Angemessenheit und Wirksamkeit des CMS erfolgen kann. Die dafür erforderliche Methodik und inhaltliche Kompetenz wird für Unternehmen und ihre Compliance Funktionen zunehmend elementar. Das gilt insbesondere für Unternehmen, die sich für Variante (2) (Negativerklärung) oder gar (3) (Positiverklärung) entscheiden. Denn die Veröffentlichung einer derartigen Stellungnahme im Lagebericht hat angesichts von Umfang und Komplexität der von § 91 Abs. 3 AktG erfassten Governance Systeme eine erhebliche Reichweite. Liegt keine ganz „frische“ umfassende externe Prüfung/Zertifizierung der Systeme vor, sind Unternehmen gut beraten, ihre intern durchgeführte Bewertung durch aussagekräftige und belastbare Dokumentation abzusichern.

II. Ausgewählte Praxisbeispiele zur internen Bewertung des CMS

Wie kann nun die Compliance Funktion bzw. die börsennotierte Gesellschaft insgesamt zu einer internen Einschätzung über die Angemessenheit und Wirksamkeit der Systeme gelangen, die dann die Basis sowohl für die interne Berichterstattung an Vorstand und Aufsichtsrat/Prüfungsausschuss, als auch für die Stellungnahme nach A.5 DCGK im Lagebericht ist?

Die nachfolgenden Praxisbeispiele zeigen ohne Anspruch auf Vollständigkeit, wie Unternehmen und Compliance Funktionen sich der erforderlichen Beurteilung der Angemessenheit und Wirksamkeit des CMS nähern können und welche Ansätze und Methoden es gibt, sich dabei mit anderen Governance Systemen, wie insbesondere dem Internen Kontrollsystem (IKS) und dem Risikomanagementsystem zu verzahnen.

1. **DAX 40 Großkonzern 1**
2. **DAX 40 Großkonzern 2**
3. **Mittelgroßes DAX 40 Unternehmen**
4. **Casestudy“ zum Active Risk Assessment (ARA)**

B. Praxisbericht DAX-40 Großkonzern (Industriegeschäft) zur Angemessenheit und Wirksamkeit der Internen Kontroll- und Risikomanagementsystems (einschließlich Compliance)

I. Elemente des Internen Kontroll- und Risikomanagementsystems

Das Interne Kontroll- und Risikomanagementsystem des Unternehmens basiert auf einem fortlaufenden Prozess. Ziel ist es, Risiken für das Geschäft zu erkennen, nach Wichtigkeit einzustufen und ihnen effektiv und effizient zu begegnen. Dies umfasst die Festlegung von Kontrollzielen, die regelmäßige Überprüfung der Risiken und Kontrollziele und der Wirksamkeit wesentlicher der Risikominderung dienender Kontrollen.

Kein Internes Kontroll- und Risikomanagementsystem, auch nicht ein für wirksam befundenes, kann vollständige Sicherheit gewährleisten. Allen internen Kontrollsystemen sind Grenzen gesetzt; stets werden Unwägbarkeiten und Risiken verbleiben, die niemand mit Sicherheit vorhersagen kann.

Zu den Kernelementen, auf denen unser Internes Kontroll- und Risikomanagementsystem beruht, gehören unter anderem:

1. Risk and Control Framework (RCF)

Das Risk and Control Framework ist ein zentraler Bezugspunkt für alle weltweit gültigen Kontrollziele (control objectives), die von den Prozessverantwortlichen zur Absicherung gegen auf Konzernebene zentral identifizierte Risiken vorgegeben werden. Es bietet eine eindeutige und konsistente Auflistung von Kontrollzielen, die dem Management und den Mitarbeitern eine angemessene Kontrolle in ihrem Verantwortungsbereich ermöglicht. Die Kontrollziele sind auf der Grundlage des weltweit anerkannten COSO-Leitfadens "Enterprise Risk Management - Integrating with Strategy and Performance" (2017) in die vier Kategorien "Strategie", "Betrieb", "Finanzen" und "Compliance" gegliedert.

2. Interner Kontrollprozess (IC-Prozess)

Es besteht ein integrierter IC-Prozess, der die Kernelemente des COSO "Internal Control - Integrated Framework" (2013) berücksichtigt, um die Wirksamkeit der internen Kontrollen in Bezug auf strategische, operative, finanzielle und Compliance-Kontrollziele zu überprüfen. Die im Risk and Control Framework enthaltenen Kontrollziele bilden die Grundlage für die jährliche Beurteilung. Alle im Rahmen dieses Prozesses festgestellten internen Kontrollmängel werden bewertet und entsprechende Abhilfemaßnahmen werden vom Management eingeleitet. Dieser Prozess enthält unter anderem auch nachhaltigkeitsbezogene Kontrollziele, wie z.B. die korrekte Darstellung nachhaltigkeitsbezogener Finanzdaten im Sinne der EU-Taxonomie-Verordnung.

3. Interner Zertifizierungsprozess:

Es ist ein vierteljährlicher Zertifizierungsprozess eingerichtet, der das Management aller Gesellschaften und ausgewählter Einheiten verpflichtet, insbesondere die Richtigkeit, Vollständigkeit und Regelkonformität der Finanzberichterstattung für ihren jeweiligen Verantwortungsbereich intern zu bestätigen. Dieser Prozess bildet die Grundlage für den Bilanzeid des Vorstands der Obergesellschaft und für die Vollständigkeitserklärung des Vorstandsvorsitzenden, des Finanzvorstands und des Leiters Rechnungswesen und Controlling gegenüber dem externen Wirtschaftsprüfer.

4. Enterprise Risk Management (ERM):

Neben der Durchführung operativer Risikomanagement-Aktivitäten im gesamten Unternehmen bietet unser ERM-System eine standardisierte Methodik für die Identifizierung unternehmensweiten wesentlichen Risiken sowie für die Erfassung von Informationen über deren Auswirkungen und Eintrittswahrscheinlichkeiten. Darüber hinaus gibt es klare Verantwortlichkeiten und Verfahren für das Management dieser Risiken. Die Identifizierung und das Management von Risiken sind in die tägliche Steuerung unseres Geschäfts eingebettet. Unser ERM-System basiert auf dem weltweit anerkannten COSO-Standard "Enterprise Risk Management - Integrating with Strategy and Performance" (2017) und ist an die Anforderungen des Unternehmens angepasst, indem es die Ziele der Organisation in die fünf Kategorien Strategie, Betrieb, Finanzen, Compliance und Klima strukturiert. Zusätzlich entspricht es der ISO-Norm 31000.

II. Zuständigkeiten

Der Vorstand wird bei seinen Aufgaben im Rahmen des Internes Kontroll- und Risikomanagementsystems u.a. durch die folgenden Abteilungen und Ausschüsse mit definierten Zuständigkeiten unterstützt:

Risk and Internal Control unterstützt den Vorstand in seiner Verantwortung, ein integriertes Internes Kontroll- und Risikomanagementsystem einzurichten und dessen Wirksamkeit zu überwachen.

Assurance / Audit leistet unabhängige Prüfungen von spezifisch ausgewählten Revisionsbereichen im Rahmen eines Prüfungsplans, der auf identifizierten Risikofeldern des Unternehmens und ihrer verbundenen Unternehmen basiert.

Legal and Compliance stellt u. a. die konsequente Umsetzung der Business Conduct Guidelines des Unternehmens und der damit verbundenen Richtlinien und Kontrollen zur Korruptionsbekämpfung, zum Kartellrecht, zum Datenschutz, zur Geldwäschebekämpfung und zur Exportkontrolle sicher. Als Teil des Compliance-Systems wurden im Risk and Control Framework Compliance-bezogene Kontrollziele festgelegt, die die Organisation bei der Berichterstattung und dem Management entsprechender Risiken sowie bei der Überwachung der Wirksamkeit der Internen Kontrolle in diesem Bereich unterstützen.

Das **Ad-hoc-Komitee**, zusammengesetzt aus den Leitungen unterschiedlicher Funktionen wie Legal & Compliance, Investor Relations, Communicaton, prüft, ob Informationen / Tatsachen den Aktienkurs des Unternehmens unter Umständen erheblich beeinflussen könnten und daher per Ad-hoc-Meldung bekannt gegeben werden müssen und solche veröffentlichungspflichtigen Informationen/Tatsachen zur Freigabe vorbereitet.

Alle Leiter der berichtspflichtigen Geschäftseinheiten, ausgewählte Zentralfunktionen und Leiter (oder gleichwertige Positionen) von Einheiten, die an die vorgenannten berichten, sind dafür verantwortlich, die Kontrollziele einschließlich aller relevanten Leitlinien einzuhalten und ein effektives Internes Kontroll- und Risikomanagementsystem in ihrem Verantwortungsbereich einzurichten und aufrechtzuerhalten.

III. Wesentliche Prozesselemente des rechnungslegungsbezogenen internen Kontroll- und Risikomanagementsystems

Die Qualifikation der in den Rechnungslegungsprozess einbezogenen Mitarbeiter*innen wird durch geeignete Auswahlprozesse und Schulungen sichergestellt. Es gilt das „Vier-Augen-Prinzip“; zudem müssen Abschlussinformationen bestimmte Freigabeprozesse durchlaufen. Weitere Kontrollmechanismen sind Soll-Ist-Vergleiche sowie Analysen der inhaltlichen Zusammensetzung und Veränderungen der einzelnen Posten – sowohl der von Konzerneinheiten berichteten Abschlussinformationen als auch des Konzernabschlusses. Zum Schutz vor nicht autorisiertem Zugriff sind in Übereinstimmung mit unseren Bestimmungen zur Informationssicherheit in den rechnungslegungsbezogenen IT-Systemen Zugriffsberechtigungen definiert. Die oben genannten manuellen und systemseitigen Kontrollmaßnahmen gelten grundsätzlich auch für die Überleitung der Abschlussinformationen nach den International Financial Reporting Standards (IFRS) auf den Jahresabschluss des Unternehmens.

Quartalsweise findet ein interner Zertifizierungsprozess statt, bei dem das Management verschiedener Ebenen unserer Organisation – unterstützt durch Bestätigungen des Managements von Einheiten in ihrem Verantwortungsbereich – die Ordnungsmäßigkeit der an die Konzernzentrale berichteten Finanzdaten bestätigt und über die Wirksamkeit der entsprechenden Kontrollsysteme berichtet.

Der Head of Risk Management and Internal Control berichtet dem Vorstand quartalsweise über Angelegenheiten bezüglich der Umsetzung, Durchführung und Überwachung des Risikomanagement- und internen Kontroll-systems und unterstützt den Vorstand bei der Berichterstattung an den Prüfungsausschuss des Aufsichtsrats.

Der Group Compliance Officer berichtet vierteljährlich (und bei Bedarf ad hoc) an den Vorstand und den Prüfungsausschuss der Obergesellschaft Kennzahlen und wesentliche Inhalte des Compliance Management Systems - u.a. wesentliche Entwicklungen bei Compliance-Fällen, Statistiken zu durchgeführten Disziplinarmaßnahmen, Anzahl durchgeführter Schulungen, aktuelle Veränderungen im regulatorischen Umfeld.

Unser Management beurteilt zu jedem Geschäftsjahresende die (konzeptionelle sowie operative) Wirksamkeit des eingerichteten Kontrollsystems. Dazu verfügen wir über ein standardisiertes Verfahren, nach dem notwendige Kontrollen definiert, nach einheitlichen Vorgaben dokumentiert und regelmäßig auf ihre Wirksamkeit geprüft werden. Jedoch kann kein Kontrollsystem, auch wenn es als wirksam beurteilt wurde, alle unzutreffenden Angaben verhindern oder aufdecken.

Unser Konzernabschluss wird auf Basis eines zentral vorgegebenen konzeptionellen Rahmens erstellt. Es wird fortlaufend analysiert, ob eine Anpassung des konzeptionellen Rahmens aufgrund von Änderungen im regulatorischen Umfeld erforderlich ist. Quartalsweise werden die Rechnungswesenabteilungen über aktuelle Themen und einzuhaltende Termine informiert, die die Rechnungslegung und den Abschlusserstellungsprozess betreffen. Dies umfasst u.a. quartalsweise Durchsprachen der wesentlichen Compliance-Themen.

Unsere interne Revision beurteilt unter anderem die Integrität unserer Finanzberichterstattung, die Effektivität des Kontrollsystems und des Risikomanagementsystems sowie die Einhaltung unserer Compliance-Richtlinien. Im Anschluss daran erfolgt die Mandatierung durch unseren Vorstand und unseren Prüfungsausschuss.

Der Prüfungsausschuss ist in unser Kontrollsystem eingebunden. Er überwacht insbesondere die Rechnungslegung und den Rechnungslegungsprozess sowie die Wirksamkeit des internen Kontrollsystems, des Risikomanagementsystems und des internen Revisionssystems.

Darüber hinaus besteht die Möglichkeit, im Rahmen von Compliance-Beschwerden Meldungen zu tätigen, z. B. anonym und direkt im Rahmen des „Speak Up“-Systems oder über eine Ombudsperson.

IV. Schlussfolgerungen zur Angemessenheit und Wirksamkeit des Internen Kontroll- und Risikomanagementsystems

Die Aussage zur Angemessenheit und Wirksamkeit des internen Kontroll- und Risikomanagementsystems im Lagebericht ist das Ergebnis einer Gesamtschau der o.g. Prozesse und Informationsquellen. Bei der Überprüfung der Angemessenheit und Wirksamkeit unseres Internes Kontroll- und Risikomanagementsystems und bei der Formulierung der Schlussfolgerungen für den Lagebericht berücksichtigt der Vorstand – wie oben dargestellt - eine Vielzahl von Informationen, darunter

- Berichte über die Ergebnisse des rechnungslegungsbezogenenen Kontrollsystems,
- Berichte über die Ergebnisse des IC-Prozesses und Berichte über die Ergebnisse des ERM-Prozesses,
- Prüfungsberichte der internen Revision,

- Berichte über aktuelle Themen, die von unseren Rechts- und Compliance-Abteilungen identifiziert wurden,
- Bestätigungen über die Wirksamkeit des Risikomanagement- und Kontrollsystems durch die weltweit Prozessverantwortlichen,
- Bestätigungen der Umsetzung aller Konzernanforderungen zum Risikomanagement und Kontrollsystem von vollkonsolidierten Unternehmen (In Control Certifications).

Auf der Grundlage der oben genannten Informationen wird untersucht, ob eine kritische internen Kontrollschwäche vorliegen könnte. Kritische interne Kontrollschwächen sind entweder einzelne interne Kontrollschwächen, die mit kritischen Auswirkungen identifiziert wurden, oder Gruppierungen ähnlicher interner Kontrollschwächen, die in ihrer Gesamtheit kritische Auswirkungen haben können. Zu den Faktoren, die bei unserer Beurteilung eine Rolle spielen, gehören unter anderem, ob eine Schwachstelle das Erreichen eines wichtigen Unternehmensziels (strategisch, operativ, finanziell, Compliance, Klima) ernsthaft beeinträchtigen oder verhindern könnte, oder ob eine Schwachstelle die Reputation der Organisation ernsthaft schädigen könnte, oder ob eine Schwachstelle eine wesentliche Auswirkung auf die Rechnungslegung haben könnte.

C. 2. Praxisbericht DAX-40 Großkonzern (Automotive): Compliance Reifegradmodell zur Bewertung der Angemessenheit und Wirksamkeit des CMS

I. Einleitung

Börsennotierte Gesellschaften sind nach § 91 Abs. 3 AktG verpflichtet, ein im Hinblick auf den Umfang der Geschäftstätigkeit und die Risikolage des Unternehmens angemessenes und wirksames CMS (als Bestandteil des internen Kontrollsystems (IKS) bzw. Risikomanagementsystems (RMS)) einzurichten. Im Lagebericht sollen nach A. 5 des Deutschen Corporate Governance Kodex (DCGK) dessen wesentliche Merkmale beschrieben und es soll (als Teil einer Gesamtaussage zum IKS/RMS) zur Angemessenheit und Wirksamkeit des CMS Stellung genommen werden.

Es stellt sich für die Compliance Funktion die Frage, auf welcher Basis diese Stellungnahme strukturiert abgeleitet werden kann. Dabei geht es zum einen um die (externe) gesamthafte Stellungnahme zu IKS und RMS nach A.5 im Lagebericht und zum anderen um die vorgelagerte (interne) Bewertung des CMS gegenüber Vorstand und Aufsichtsrat/Prüfungsausschuss.

II. Anforderungen und Begriffe

Die Pflicht zur Einführung eines angemessenen und wirksamen CMS gibt den Unternehmen bei der Ausgestaltung des Systems bzw. der einzelnen Compliance Programme ein breites Organisationsermessen. Die folgenden Leitplanken sind dabei zu beachten:

- Es gibt keine Pflicht zur Einrichtung eines allumfassenden CMS. Es sind nur solche Maßnahmen zu treffen, die im Sinne der Angemessenheit zulässig, objektiv zumutbar und erforderlich sind.
- Zulässigkeit und objektive Zumutbarkeit setzen insbesondere bei Kontroll- und Überwachungsmaßnahmen Grenzen vor Eingriffen in Mitbestimmungsrechte und Datenschutz und schützen die Mitarbeitenden und das Betriebsklima vor überzogenen, von Misstrauen oder Willkür geprägten Aufsichtsmaßnahmen.
- Erforderlichkeit beurteilt sich nach Umfang der Geschäftstätigkeit und Risikolage des Unternehmens. Zur Auswahl und konkreten Ausgestaltung der einzelnen Maßnahmen

empfiehlt sich die Orientierung an Branchen- und Industriestandards, wie etwa dem DICO Standard CMS.
- Zur angemessenen Ausgestaltung des CMS gehört auch eine geeignete Aufbau- und Ablauforganisation mit eindeutigen Zuständigkeiten, ausreichenden Sach- und Personalmitteln sowie Prozessen zur Operationalisierung des Systems und der einzelnen Maßnahmen.
- Wirksam ist das CMS bereits dann, wenn es zur Aufdeckung, Steuerung und Bewältigung aller wesentlichen Risiken geeignet ist. Maßgeblich sind die Umstände des Einzelfalls, zu denen auch gehört, dass die vom CMS umfassten Vorgaben und Maßnahmen im Unternehmen auch tatsächlich umgesetzt sind und nicht nur auf dem Papier stehen.
- Aus einzelnen Verstößen kann nicht zwingend auf die fehlende Wirksamkeit des CMS geschlossen werden. Erforderlich ist aber eine Ursachen- und Fehleranalyse, nebst entsprechenden Maßnahmen, um das Risiko vergleichbarer Vorgänge bzw. die Wiederholungsgefahr wirksam zu reduzieren.

III. Drei Bausteine für drei Kernaspekte (3x3-Ansatz) zur Beurteilung der Angemessenheit und Wirksamkeit des CMS

Zur Beurteilung der Angemessenheit und Wirksamkeit des CMS werden in der nachfolgenden Case Study **drei wesentliche Bausteine** herangezogen. Damit wird der Mehrdimensionalität, die dieser Beurteilung zu Grunde liegt, Rechnung getragen und sichergestellt, dass das CMS anhand der folgenden **drei Kernaspekte** analysiert wird:

(i) Dimensionierung und programmatische und organisatorische Ausgestaltung,
(ii) Umsetzung in den verschiedenen Einheiten und Tochtergesellschaften des Unternehmens und
(iii) Kontrollmaßnahmen, identifizierte Verstöße und Potentiale zur Weiterentwicklung.

Die **drei Bausteine** sind:

- Regelmäßige Befragungen auf Ebene der Compliance Funktion,
- Jährliche Befragung der operativ Verantwortlichen,
- Weitere Erkenntnisquellen, z.B. Prüfungen der internen Revision und ggf. externer Stellen, Mitarbeiterbefragungen etc.

Die ersten beiden Bausteile bilden das sog. **Compliance Reifegradmodell**. Der dritte Baustein komplettiert das Reifegradmodell und ermöglicht eine gesamte Einschätzung zur Angemessenheit und Wirksamkeit, in die auch Erkenntnisse der internen Revision und externer Stellen sowie aus Mitarbeiterbefragungen etc. einfließt.

IV. Compliance Reifegrad Modell

1. Ausgangslage

Compliance Themen liegen im Unternehmen häufig nicht nur in der Zuständigkeit einer Abteilung (etwa der zentralen Compliance Funktion), sondern sind auf verschiedene Abteilungen verteilt. So können etwa die Themen Steuern, Datenschutz, Kapitalmarkt Compliance, Produkt Compliance, HR Compliance etc. je nach Unternehmensorganisation nicht zentral bei der Compliance Funktion/Abteilung gebündelt sein. Gleichwohl ist nicht auszuschließen, dass Vorstand und Aufsichtsrat/Prüfungsausschuss vom Chief Compliance Officer als Leiter der zentralen Compliance

Funktion eine gesamthafte Aussage zur Angemessenheit und Wirksamkeit des CMS und der einzelnen ihm zugeordneten Compliance Programme erwarten. Das umfasst dann sowohl die Themen (wie etwa Korruptionsbekämpfung, Exportkontrolle und Kartellrecht) die der zentralen Compliance Funktion zugewiesen sind, als auch z.B. die Produkt Compliance, auch wenn die Zuständigkeit dafür etwa beim Qualitätsmanagement liegt.

Auch für den Fall, dass die Compliance Funktion lediglich eine Aussage zu den Themen treffen möchte bzw. soll, für die sie auf Ebene der 2nd Line selbst unmittelbar Verantwortung trägt, eignet sich der nachfolgende Ansatz. Denn auch in diesem Fall stellt sich die Frage, der angemessenen Ausgestaltung, der Umsetzungskontrolle im Unternehmen sowie der Wirksamkeit des CMS.

2. Lösungsansatz

Inhaltlich basiert das Reifegrad Modell auf dem Prevent-Detect-Respond Ansatz, d.h. die Analyse der Angemessenheit und Wirksamkeit des CMS wird in jeder der drei Säulen (und deren Einzelelemente) durchgeführt. Hinzu kommen als übergeordnete Bestandteile die Analyse der Compliance Kultur und der Compliance Organisation Ein **Schwerpunkt** der Analyse liegt auf den durchgeführten **Kontrollmaßnahmen** auf den verschiedenen Ebenen. Dabei geht es um die Frage,

- welche Kontrollen existieren (manuell, automatisiert/systemgestützt etc.);
- ob diese mit Blick auf das identifizierte Risiko angemessen konzipiert sind, einschließlich entsprechender Kontroll-Testings;
- ob und von wem die Kontrollen durchgeführt wurden;
- sofern die Kontrolldurchführung durch die 1st Line erfolgt ist, ob die effektive Durchführung einem Monitoring durch die 2nd Line unterzogen wurde.

3. Jährliche Befragung der maßgeblichen operativ Verantwortlichen

Die für Compliance in den lokalen Einheiten sowie in zentralen Unternehmensbereichen **operativ verantwortlichen Führungskräfte** (z.B. Leiter der Einkaufs-, Vertriebs- und Entwicklungsabteilungen, Leiter der Stabsstellen, Geschäftsführer von Tochterunternehmen etc.) werden themenspezifisch geclustert über einen IT-gestützten Prozess jährlich zu ihrer Einschätzung der Ausgestaltung, Umsetzung und Wirksamkeit des CMS befragt. Dazu gehören insgesamt rund **15-20 Fragen**, u.a. zur **Compliance Kultur** und zur Compliance Awareness, zu ihrem eigenen Tone from the Top, Einschätzungen zu Compliance **Risikofeldern**, zur Wirksamkeit von **Schulungen** und zur Funktionalität von spezifischen IT-Compliance Tools (etwa zur Third Party Due Diligence). Im Ergebnis erhält man eine **subjektive**, aber dennoch konkrete und umfassende **Einschätzung der sog. 1st Line** zum Compliance Status bzw. dem Grad der Verankerung von Compliance bei den Mitarbeitern und zu möglichen Verbesserungspotenzialen.

4. Regelmäßige Einschätzung von Vertretern der Compliance Funktion und anderer Governance Funktionen

Diese jährliche Befragung der 1st Line wird durch ein **Reifegrad Assessment** auf Ebene der **Compliance Funktion** und anderer Governance Funktionen (2nd Line) ergänzt:

Auf Basis des **Prevent-Detect-Respond-Ansatzes** werden für **alle Compliance Programme** (Kartellrecht, Korruptionsbekämpfung, Produkt Compliance etc.) die übergeordnete strategische Ausrichtung sowie die Compliance Ziele definiert. Die Compliance Programme sind zur besseren Operationalisierung in einzelne **Compliance Elemente** eingeteilt, die im Wesentlichen mit den

Compliance-Kernaufgaben korrespondieren. Die Ausgestaltung der einzelnen Elemente kann sich etwa aufgrund unterschiedlicher rechtlicher Anforderungen sowie Risiko- und Organisationsstrukturen in ihrer detaillierten inhaltlichen Ausprägung von Programm zu Programm unterscheiden.

Die konkreten Inhalte der zehn Compliance Elemente werden in folgender Abbildung dargestellt und hier nicht näher erläutert. Sie sind einem typischen CMS Standard, wie etwa dem **DICO Standard für Compliance Management Systeme** nachempfunden.

Auf dieser Basis ergibt sich die konzeptionelle Grundstruktur des Reifegrad Modells, bestehend aus den 10 Compliance Elementen und ergänzt um die Elemente „Werte & Kultur" und „Organisation & Strukturen".

Compliance Element	Compliance Programm 1	Compliance Programm 2	Compliance Programm n
Compliance Risk Assessment			
Verhaltenskodex und Compliance Regelungen			
Compliance Kommunikation und Trainings			
Compliance IT-Systeme und Prozesse			
Compliance Beratung			
Compliance Monitoring			
Hinweisgeberkanal und Compliance Untersuchungen			
Compliance Audits			
Compliance Reporting			
Risikoreduzierende Compliance Maßnahmen („Remediation"), inklusive Sanktionierung			
Werte & Kultur			
Organisation & Strukturen			

Im eigentlichen Assessment wird dann sowohl die **Wahrnehmung des Interview-Partners** (2nd Line) zum **eigenen Verantwortungsbereich** abgefragt, als auch seine Einschätzung zum **Gesamtunternehmen**. Als ein Experte auf dem Gebiet Compliance ist davon auszugehen, dass diese Einschätzung fundiert und umfassend erfolgt. Wichtig zu berücksichtigen ist, dass der Fokus explizit auf Angemessenheit und Effektivität liegt und insbesondere die Reife der CMS Implementierung anhand der dargestellten Elemente eruiert werden soll.

Hinsichtlich der **Operationalisierung** der Einschätzungsbewertungen können unterschiedliche Ansätze gewählt werden. So kann beispielsweise bewusst auf **vordefinierte Skalen** verzichtet werden, um den Charakter eines offenen Interviews nicht zu verlieren und auch der Gefahr eines zu großen Formalismus entgegenzuwirken.

Auf der anderen Seite können vordefinierte Skalen hilfreich sein, wenn es darum geht, einen Gesamteindruck der Implementierung in der 2nd Line zu erhalten bzw. auch um Vergleiche zu ermöglichen oder zeitliche Veränderungen darzustellen. Eine in der Praxis gängige Skala, ist die **Einstufung von 1 (sehr gering) bis 5 (sehr hoch)** und kann auf den vorliegenden Kontext sehr gut übertragen werden. In einer weiteren Ausbaustufe ist es denkbar, die einzelnen Skalenniveaus mit entsprechenden Ausprägungskriterien anzureichern. So wird sichergestellt, dass die Einschätzungen der Befragten hinreichend valide und vergleichbar sind.

Sobald alle Assessments mit der 2nd Line durchgeführt wurden, können diese zentral gesamthaft ausgewertet und konsolidiert werden und fließen schließlich als ein Baustein – wie eingangs erwähnt – als Input für die Ableitung einer Einschätzung zur Beurteilung der Angemessenheit und Wirksamkeit des CMS ein. Der Fokus liegt auf einer Einschätzung der angemessenen **Ausgestaltung/Dimensionierung** und der **Umsetzungskontrolle** sowie auf der Relevanz festgestellter **Verstöße** und **Verbesserungspotentiale** im Unternehmen.

V. Weitere Erkenntnisquellen, insbesondere Prüfungen der internen Revision

Hinzu kommen weitere Erkenntnisquellen außerhalb der Compliance Funktion bzw. Community. Dazu gehören insbesondere **Prüfungsberichte der internen Revision**, und zwar sowohl zur CMS Implementierung in Einzelbereichen und Tochterunternehmen, als auch **durchgeführte Systemprüfungen**. Ferner können Erkenntnisse aus der **Anwendung des IKS** mit Compliance Bezug herangezogen werden (etwa zur durchgängigen Anwendung des 4-Augen-Prinzips oder zur Implementierung von Compliance Prozesskontrollen). Auch **externe Einschätzungen** zum CMS bzw. von Teilaspekten, etwa durch den **Abschlussprüfer**, aus **Sonderprüfungen** oder im Rahmen einer **externen anwaltlichen Prüfung** können dazu gehören. Schließlich geben Ergebnisse von **Mitarbeiterbefragungen** Hinweise auf die Compliance Kultur, die Sichtbarkeit/Akzeptanz der Compliance Funktion und der Durchdringungstiefe des CMS.

VI. Ausgewählte Einzelaspekte und jährliche Analyseschwerpunkte

Optional können die Aussagen zur Angemessenheit und Wirksamkeit des CMS durch **ausgewählte Analyseschwerpunkte** zusätzlich abgestützt werden. Dabei werden wechselnde **Einzelaspekte** untersucht, wie etwa das Vergütungs- oder das Incentivierungssystem des Unternehmens. Auf diese Weise können etwa wichtige externe Impulse, wie die aktuellen Empfehlungen des

US-Justizministeriums DOJ aus dem **sog. Monaco Memorandum** (z.B. zur Vergütungsstruktur) kurzfristig und pragmatisch berücksichtigt werden.

VII. Stärkung der Angemessenheit und Wirksamkeit des CMS durch übergeordnete Governance Maßnahmen

Die Angemessenheit und Wirksamkeit des CMS wir schließlich auch von übergeordneten bzw. **übergreifenden Governance Maßnahmen** unterstützt, auf die hier nicht näher eingegangen werden soll. Gleichwohl ist die Bedeutung der Corporate Governance auf Ebene der Vorstand/Aufsichtsrat, einer ordnungsgemäßen Aufbau- und Ablauforganisation unter Wahrung der Delegationsgrundsätze sowie verzahnter Kontroll- und Governancessysteme für ein ordnungsgemäßes CMS nicht zu unterschätzen.

VIII. Zusammenfassung

Zusammenfassend kann festgehalten werden, dass es für die Beurteilung der **Angemessenheit und Wirksamkeit eines CMS** wichtig ist, die Mehrdimensionalität der Problemstellung zu berücksichtigen. Einfache, nicht belegbare Aussagen bergen immer eine Gefahr der fehlenden Glaubwürdigkeit bzw. zu großer Subjektivität. Daher werden in vorliegender Case Study **unterschiedliche Erkenntnisquellen** wie auch unterschiedliche **Informationsarten** berücksichtigt, um die jeweiligen Aussagen unter dem Strich zu objektivieren. Im Ergebnis ergibt sich eine belastbare Aussage zur Angemessenheit und Wirksamkeit des CMS mit Schwerpunkt auf die **drei Kernaspekte**:

(i) Dimensionierung und programmatische und organisatorische Ausgestaltung,
(ii) Umsetzung in den verschiedenen Einheiten und Tochtergesellschaften des Unternehmens und
(iii) Kontrollmaßnahmen, identifizierte Verstöße und Potentiale zur Weiterentwicklung.

Nachfolgende Abbildung stellt die Bewertung der Angemessenheit und Wirksamkeit eines CMS inkl. des vorgestellten Reifegradmodells wie beschrieben dar.

BEWERTUNG ANGEMESSENHEIT UND WIRKSAMKEIT DES CMS.

*vgl. Erklärung zur Unternehmensführung gem. §§ 289f, 315d HGB .

D. 3. Praxisbericht: Mittelgroßes DAX-40 Unternehmen (Handel) zur Angemessenheit und Wirksamkeit des Internen Kontroll- und Risikomanagementsystems (einschließlich Compliance)

I. Von Einzelelementen zur Gesamtschau

In vielen Konzernen wird sich vor allem die Herausforderung stellen, Schnittstellen einzelner bereits bestehender Experten- und Governance-Funktionen in einer Weise zusammenzubringen, dass alle erforderlichen Themen allokiert sind, ein hinreichender fortlaufender Austausch über die gewonnen Erkenntnisse erfolgt und dem Senior Management eine realistische Gesamtschau berichtet werden kann.

In der hier vorgestellten SE und ihrer Töchter (die „Gruppe“) wurde zunächst im Rahmen einer Gap-Analyse geklärt, welche Ressourcen und Prozesse, aber auch Schnittstellen noch fehlen, um genau diese Gesamtschau zu erreichen. So wurde u.a. zum Thema Non-Financial ICS auf Management-Ebene beraten und Vorschläge hierzu mit dem Prüfungsausschuss des Aufsichtsrates intensiv diskutiert. Dabei standen inhaltliche Fragen genauso wie eine effiziente Governance und kontinuierliches Monitoring auf der Agenda. Der Moment war günstig, auch die Aufgaben und die Zusammenarbeit der einzelnen Governance-Funktionen der Gruppe zu durchdenken.

1. Zuständigkeiten und Zusammenarbeit

Das **Risikomanagement** und ebenso die **Interne Revision** wurden im Ergebnis ohne größere inhaltliche Änderungen beibehalten, allerdings durch **Investitionen in Systeme** stärker automatisiert. Dadurch werden die Ergebnisse auch für die verschiedenen Business- und Governance Funktionen transparenter gemacht, und dynamische Entwicklungen können besser abgebildet werden. Beide Funktionen sind gruppenweit zentral und beim CFO geführt. Aus regulatorischen Gründen hat eine für Zahlungsdienstleistungen lizenzierte Tochter aus der Gruppe ein eigenes Risiko-Team und berichtet entsprechend den speziellen Anforderungen.

Eine **neue IKS-Funktion** wurde hingegen im Bereich Finance geschaffen, um das financial und non-financial ICS zusammenführen, wobei das Team **Nachhaltigkeit** (in anderer Berichtslinie) allerdings wesentliche Daten hierfür zusammenstellt und entsprechende Projekte verantwortet.

Der **Compliance-Bereich** umfasst alle Aspekte eines Corporate Compliance CMS – u.a. die Bereiche Richtlinienmanagement, Schulungen, Geschäftspartnerprüfungen sowie Beschwerdemanagement und interne Untersuchungen. Angesiedelt sind dort zudem Expertenfunktionen z.B. zum Außenwirtschaftsrecht und die Geldwäscheprävention.

Der Compliance Officer führt mit dem Corporate Compliance Team die entsprechenden Funktionen in einem **monatlichen Austausch** zusammen und **berichtet dem Vorstand** und dem **Prüfungsausschuss** entsprechend. Diese Möglichkeit hat selbstverständlich auch der Leiter der Internen Revision. Der formelle Austausch erfolgt mindestens quartalsweise; darüber hinaus werden z.B. bestimmte Audits oder Projekte in dieser Runde besprochen.

Als Committees besteht ein **Compliance Committee** zur Entscheidungsfindung bei dem Verdacht schwerwiegender Compliance-Verstöße, sowie ein **Ad-hoc-Committee**.

2. Schriftliche Niederlegung

In schnittstellen-intensiven Bereichen können schriftliche Dokumentationen besonders hilfreich sein. Sie sind selbstverständlich auch die Basis für eine Auditierung (dazu sogleich). Daher sind die Bereiche Risiko, Compliance und Internal Audit in Handbüchern bzw. Beschreibungen niedergelegt. Hierbei hat es sich nach den Erfahrungen der berichtenden SE sehr bewährt, Dokumentationen in (mindestens) drei unterschiedliche Kategorien aufzuteilen, um diese nicht zu überfrachten: i) Grundsatzdokumente wie die Handbücher, die z.B. Aufgabenbereich und Ziele der Compliance- oder Risikoabteilung beschreiben – die sind insbesondere an die Governance-Funktionen selbst und Auditoren adressiert ii) Policies und ggf. darauf aufbauende Prozessbeschreibungen, die aufzeigen, wie im Arbeitsalltag die Compliance-Ziele erreicht werden sollen und wer für welchen Schritt konkret zuständig ist und – diese sind an Mitarbeiter:innen adressiert, die mit der jeweiligen Thematik in Berührung kommen und werden bei Audits selbstverständlich mitgeprüft iii) einfache „Do's and Don't" als einfache Kommunikationsmaterialien, die schnell zu erfassen sind.

3. Monitoring

Wirksamkeit von Kontrollen können nur bewertet werden, wenn diese fortlaufend überprüft werden. Als vorbereitungsintensiv und nicht trivial hat sich der Ausbau des entsprechenden Monitorings erwiesen. Denn die Erhebung der entsprechenden Daten, um Kontrollziele abzugleichen, erfordert unternehmensinterne abteilungsübergreifende Abstimmung, teilweise aber auch Änderungen an den bestehenden Systemen bzw. Einrichtung von Schnittstellen. Der weitere Ausbau angemessener Dashboards für den weiteren Anwenderkreis wird aktuell noch fortgeführt. Denn nur auf der Basis eines gemeinsamen Verständnisses können Trends erkannt und ggf. Anpassungen in den Gegenmaßnahmen effektiv erfolgen; auch dies gehört zu einem integrierten System des Risikomanagements.

4. Auditing

Um Schwächen in der Wirksamkeit von Kontrollen zu erkennen, ist die interne Revision zentral. Der mit dem Prüfungsausschuss abgestimmte Audit-Plan umfasst dabei sehr unterschiedliche Prüfungsbereiche, sowohl inhaltlich als auch geographisch. Seng engmaschig werden auch Governance-Funktionen selbst auditiert.

Eine **externe Auditierung nach IDW PS Standard** ist sowohl für den Compliance- als auch für den Risiko-Bereich erfolgt. Die externe Auditierung wird in der Gruppe als besonders hilfreiches Instrument angesehen. Die Taktung der Prüfungen erfolgt dabei auf eine Art, die es erlaubt, dass die jüngst auditierte Funktion bei der Abarbeitung etwaiger Empfehlungen durch die anderen Governance-Funktionen unterstützt werden kann (es erfolgt also keine Gleichzeitigkeit der Auditierung bzw. ihrer Wiederholung, sondern eine „Staffelung" von Audits über die verschiedenen Funktionen im Rahmen eines übergreifenden Plans).

E. Management der Angemessenheit und Wirksamkeit des CMS durch ein „Active Risk Assessment“ (Fallbericht aus Compliance Beratung)

Für den verantwortungsvollen Umgang mit den Risiken der Geschäftstätigkeit fordert Grundsatz 4 des DCKG 2022 ein angemessenes und wirksames internes Kontrollsystem (IKS) und Risikomanagementsystem (RMS). Diese umfassen nach Grundsatz 5 auch ein an der Risikolage des Unternehmens ausgerichtetes Compliance Management System (CMS). Darüber hinaus stellt Grundsatz 4 fest, dass die Angemessenheit und Wirksamkeit von IKS, RMS und CMS im Rahmen der internen Überwachung regelmäßig zu überprüfen sind.

Ergänzt werden diese Aspekte noch mit der Anforderung, dass der Vorstand den Aufsichtsrat regelmäßig, zeitnah und umfassend über alle für das Unternehmen relevanten Fragen insbesondere der Strategie, der Planung, der Geschäftsentwicklung, der Risikolage, des Risikomanagements und der Compliance informiert. (Grundsatz 16).

Daraus ergibt sich für das CMS insgesamt die Anforderung, dass Angemessenheit und Wirksamkeit nicht nur beim Aufbau des CMS zu berücksichtigen sind, sondern dass diese Grundsätze im CMS laufend überwacht und das Management bzw. die Organe des Unternehmens hierüber regelmäßig informiert werden müssen.

Im Übrigen folgt der DCKG in seinem Update mit der Betonung von Angemessenheit und Wirksamkeit eines CMS einer internationalen Entwicklung, die sich bereits seit einiger Zeit abzeichnet. So haben Vertreter des DoJ in den USA bspw. zuletzt im Frühjahr 2022 die Bedeutung von „Testings“ weiter in den Mittelpunkt der Beurteilung der Wirksamkeit von CMS gerückt. Die sogenannte „CCO Certification“ der Wirksamkeit des CMS und deren erstmaliger Umsetzung als Bestandteil der Einigung mit Glencore im Sommer 2022 ist eine direkte Folge daraus.

I. Bekannte Methoden zur Überwachung des CMS

Die Überwachung (oder das Monitoring) ist im Grunde nichts Neues, sondern wird bereits als Kernbestandteil eines CMS verstanden - auch international von Instanzen wie dem DoJ in den Guidelines zur „Evaluation of Corporate Compliance Programs“ oder dem SFO in den „Six Principles“ zum UKBA.

Um dieses Monitoring durchzuführen, gibt es verschiedene bekannte Ansätze: z.B. die interne Prüfung des CMS oder einzelner Bestandteile durch die Interne Revision im Rahmen eines Compliance Audits oder das externe Assessment nach einem gängigen Standard (bspw. IDW PS 980 oder ISO 37301). Auch eine regelmäßig durchgeführte Compliance Risikoanalyse (CRA) dient abhängig von der jeweilig genutzten Methodik dem Monitoring eines CMS.

Diese Ansätze haben sich in vielerlei Hinsicht in der Praxis bewährt. Sie bieten aber in der Regel nur eine recht statische Beurteilung des CMS zu einem definierten Stichtag und für einen zuvor festgelegte Prüfungsperiode. Darüber hinaus können diese Prüfungen je nach Methode, Scope und Betrachtungszeitraum sehr aufwendig in der Umsetzung sein und die Kapazitäten einer Compliance Abteilung und anderer Unternehmensbereiche über einen längeren Zeitraum stark beanspruchen.

Darüber hinaus bieten diese Ansätze in der Regel auch nicht die Möglichkeit, fortlaufend oder kurzfristig Entwicklungen zu erkennen, darauf zu reagieren und bspw. gezielte Maßnahmen in einer Region oder einem Unternehmensbereich einzuleiten und danach den Effekt messbar darzustellen.

Das Ziel eines effizienten Managements von Angemessenheit und Wirksamkeit des CMS, vielleicht sogar in Echtzeit, ist mit diesen Methoden daher nicht oder nur bedingt möglich.

II. Das Active Risk Assessment als moderne Alternative für ein CMS-Monitoring

Versetzen wir uns einmal in die Lage des CCO eines börsennotierten, internationalen Industrieunternehmens. Bereits vor einigen Jahren wurde mit dem Aufbau eines CMS begonnen und die Maßnahmen entfalten auch in den ausländischen Tochtergesellschaften Schritt für Schritt ihre Wirkung. Einen heftigen Vorfall mit Beteiligung einer ausländischen Behörde gab es bisher nicht. Die Entwicklung des CMS kann daher einer selbstgewählten Geschwindigkeit folgen.

Der Vorstand hat unserem CCO den Auftrag erteilt, die Angemessenheit und Wirksamkeit des CMS regelmäßig zu monitoren und über die Ergebnisse zu berichten. Darüber hinaus haben Vorstand und CCO gemeinsam folgende interne Ziele für das Monitoring festgelegt:

Risiken managen und reduzieren - Sammlung von Informationen über Risiken im Zusammenhang mit der Einhaltung von Rechtsvorschriften und die Entwicklung von geeigneten Kontrollen und Maßnahmen, um das Risiko von Strafen für das Unternehmen in Form von Geldbußen, anderen rechtlichen Sanktionen und Rufschädigung zu mindern und nach Möglichkeit zu verringern.

CMS kontinuierlich verbessern - Qualitätskontrolle des CMS durch Überwachung von Veränderungen im Risikoumfeld, Implementierung von Verbesserungen, um auf veränderte Umstände zu reagieren und damit sicherzustellen, dass das CMS weiterhin zweckmäßig ist.

Zur Kosteneffizienz beitragen - Investitionen in die Einhaltung von Compliance-Vorgaben und anderen Vorschriften werden dort getätigt, wo sie benötigt werden. Die operative Zielsetzung des CMS orientiert sich an den realen, rechtlichen Risiken, mit denen die Organisation konfrontiert ist.

Zusammenarbeit mit dem Management erleichtern – transparente und faktenbasierte Zusammenarbeit mit dem lokalen Management, die die Anerkennung der Risikolandschaft des Unternehmens durch das lokale Management einfordert und die Unterstützung der Umsetzung von CMS-Elementen und Maßnahmen zur Risikominderung verbessert.

In seinen Überlegungen, welcher Ansatz für das Monitoring geeignet sein könnte, stellt sich unser CCO vor, er wäre in der Lage das Compliance-Risikoprofil in seinem Unternehmen für eine Region, oder einen Unternehmensbereich oder sogar auf Ebene einer Einzelgesellschaft auf Basis aktueller Informationen aus dem Unternehmen abrufen zu können. Er stellt sich weiter vor, er könnte auf dieser Basis gezielt in einer Einzelgesellschaft gemeinsam mit dem lokalen Management Maßnahmen umsetzen, um ein erkanntes Risiko zu managen. Und nach Umsetzung dieser Maßnahme könnte er einige Zeit später in dem Risikoprofil der betreffenden Gesellschaft auch die Wirkung der Maßnahme sichtbar machen.

Wenn wir zu dieser Vorstellung unseres CCO noch die Begriffe „laufend“ und „in Echtzeit“ ergänzen, dann kommen wir zur Beschreibung der Vorteile eines datengesteuerten Active Risk Assessments.

III. Von einer umfragegesteuerten, periodisierten (bspw. jährlichen) Risikobewertung zu einer datengesteuerten Echtzeit-Risikobewertung mit dem Active Risk Assessment

Grundlage für das Active Risk Assessment ist die Berechnung eines Risiko-Scores, der auf die bestehende Risiko-Library aufsetzt, die jeweiligen risiko-relevanten Kriterien beinhaltet und dann in Form eines Score-Matrix-Systems im Unternehmen abgebildet wird.

Das Konzept des Active Risk Assessments und das Instrument des Compliance-Risiko-Scores ermöglichen unserem CCO auch, die richtigen Ziele und Maßnahmen zur Umsetzung im Unternehmen zu definieren.

Auf Basis dieser Methode kann unser CCO den individuellen (gewünschten) Risiko-Score einer Unternehmenseinheit (Segment, Region, Gesellschaft etc.) als Key Performance Indikator (KPI) mit dem zuständigen Management vereinbaren.

Die zur Erreichung eines KPI erforderlichen Maßnahmen (z. B. Schulungen, Umsetzung von Richtlinien, Kontrollen oder Änderungen von Prozessen) werden dann ebenfalls gemeinsam mit dem zuständigen Management festgelegt. Wenn diese umgesetzt werden, lässt sich eine direkte und unmittelbare Auswirkung auf den individuellen Risiko-Score darstellen.

Als Informationsquelle für die Bestimmung der KPIs dienen unserem CCO vorrangig die technischen Systeme des Unternehmens, die bereits vorhanden sind. Dabei werden möglichst alle Daten über Schnittstellen automatisiert und kontinuierlich erfasst, um eine datengesteuerte Bewertung in Echtzeit zu realisieren.

Folgende technische Systeme kommen hierfür im Unternehmen in Frage:

- Compliance-Plattformen wie Hinweisgebersystem, Gifts & Hospitality App, Business Partner Due Diligence Tool, Antitrust-Datenbank, Integrity Survey, etc.
- HR-Systeme wie Learning-Management-System, statistische Personaldaten (Headcount, Fluktuation, etc.)
- Governance-Systeme wie Risikomanagement, Interne Revision, Policy-Management, Vertragsmanagement
- Kaufmännische ERP-Systeme der Bereiche Controlling und Finance, CRM, Einkauf, Warenwirtschaft, etc.

Den Möglichkeiten sind hierbei aber im Grunde keine Grenzen gesetzt. Abhängig von den verwendeten KPI und den hierfür erforderlichen Daten kann unser CCO die verschiedensten internen und auch externen Quellen nutzen, sofern technische Datenschnittstellen etabliert werden können. Voraussetzung ist auch, dass die jeweiligen Daten kontinuierlich und in geeigneter Qualität zur Verfügung stehen.

IV. Aktives Management der erkannten Risiken

Die Berechnung der KPIs und des resultierenden Risiko-Scores erfolgt für eine Region, ein Segment oder bis auf Ebene einer einzelnen Gesellschaft. Je nachdem wie detailliert das Score-Matrix-Model des Unternehmens aufgebaut ist und in welcher Tiefe und Qualität die Datenquellen jeweils zur Verfügung stehen.

Die Erfassung und Auswertung der Daten sowie die Darstellung der Ergebnisse wird idealer Weise mit Hilfe einer gängigen Datenanalysesoftware realisiert. Auf dieser Basis erfolgt auch der Austausch mit

dem zuständigen, lokalen Management zur Vereinbarung von KPIs und zur Festlegung von geeigneten Maßnahmen. Mit einem Vergleich der Risiko-Scores über den Zeitverlauf, lässt sich dann die Wirkung von Maßnahmen transparent abbilden.

In dieser Form verfügt unser CCO dann auch über sehr wirkungsvolle Möglichkeiten der Berichterstattung an den Vorstand und die Organe des Unternehmens. Fragen nach der Wirksamkeit und Angemessenheit des CMS und einzelner Maßnahmen kann er nun regelmäßig und transparent beantworten.

V. Fazit

Die Umsetzung eines datengesteuerten, Active Risk Assessments ermöglicht unserem CCO die fortlaufende Überwachung von Angemessenheit und Wirksamkeit des CMS. Damit trägt er einen wichtigen Beitrag zur Umsetzung des DCKG 2022 im Unternehmen bei und erfüllt damit auch wesentliche internationale Anforderungen an das Monitoring eines CMS.

Die Entwicklung des Risk-Score-Modells zwingt unseren CCO außerdem dazu, zu entscheiden, wie die einzelnen Elemente und Maßnahmen des CMS überhaupt im Unternehmen wirken sollen und wie diese Wirkung objektiv messbar gemacht werden kann. Die darauf basierende Darstellung von Veränderungen in den KPIs und dem Risk-Score über den Zeitverlauf als Resultat von eingeleiteten Maßnahmen, ermöglicht dann erst die Beurteilung der Wirksamkeit und Angemessenheit einzelner Maßnahmen und des CMS als Ganzem. Wenn die erforderlichen Daten dazu auch noch aus technischen Systemen im Unternehmen (und aus externen Datenbanken) automatisiert gesammelt werden, erfolgt dieses Monitoring sogar laufend und in Echtzeit. Ein Quantensprung im Vergleich zu den bisher gängigen zumeist statischen und stichtagsbezogenen Überprüfungen eines CMS.

F. Ausgewählte Literatur zu § 91 Abs. 3 AktG und A.5 DCGK

Backhaus, NZG 2023, 253 ff., Die Stellungnahme zur Angemessenheit und Wirksamkeit des internen Kontroll- und Risikomanagementsystems - zur Auslegung der Empfehlung A.5 Hs. 2 DCGK 2022

Bartuschka, BB 2022, 1387 ff., Angemessenheit und Wirksamkeit von Systemen der internen Unternehmensüberwachung im Kontext von FISG und DCGK 2022

Fischer/***Schuck*** NZG 2021, 534 ff., Die Einrichtung von Corporate Governance-Systemen nach dem FISG

Ghassemi-Tabar, Deutscher Corporate Governance Kodex: DCGK, 2. Aufl. 2023

Kopp, CCZ 2023, 125 ff., Praktische Umsetzung von A.5 DCGK – Beschreibung und Stellungnahme zu Angemessenheit und Wirksamkeit von internen Systemen zur Risikovermeidung

Naumann, FAZ vom 23.01.2023 „Unternehmen besser führen“

Sack, Präsentation des IDW auf der DAI Konferenz „Corporate Governance & Gesellschaftsrecht“ am 14.03.2023