DICO
Deutsches Institut für Compliance

Viadrina Compliance Center

DICO STANDARD

S17 – AUFSICHTSRAT UND COMPLIANCE

AUTOREN: ARBEITSKREIS AUFSICHTSRAT & COMPLIANCE

WISSENSCHAFTLICHE ÜBERARBEITUNG: VIADRINA COMPLIANCE CENTER, EUROPA-UNIVERSITÄT VIADRINA FRANKFURT (ODER)

STAND 08/2022

Stand: August 2022

Disclaimer

DICO-Standards richten sich an Compliance-Praktiker. Sie sollen den Einstieg in ein Thema erleichtern und einen Überblick verschaffen. Sie folgen einer einheitlichen Metastruktur. Juristische Sonderfälle und Ausnahmeregelungen werden nicht behandelt. Ein DICO-Standard ersetzt auch nicht die ggf. erforderliche rechtliche Beratung im Einzelfall. Literaturangaben erheben keinen Anspruch darauf, die wissenschaftliche Diskussion vollständig abzubilden. Weiterführende Literatur ist in der Bibliographie zusammengefasst worden.

DICO-Standards formulieren praxistaugliche und umsetzbare Anforderungen zu ausgewählten Compliance-Themen. Dargestellt wird die weithin anerkannte und (jedenfalls in Deutschland) überwiegend angewandte bzw. angestrebte Art und Weise, Compliance-Management und Compliance-Themen in der Unternehmenspraxis umzusetzen. Mit der Veröffentlichung eines DICO-Standards ist die Diskussion des jeweiligen Arbeitskreises nicht abgeschlossen. Compliance-Praktiker und Wissenschaft sind aufgerufen, an der Weiterentwicklung der DICO-Standards durch Hinweise und Beiträge mitzuwirken. Senden Sie Ihre Anregungen und Beiträge an Standards@dico-ev.de.

Dank

Der vorliegende Standard wurde auf Basis der im April 2020 veröffentlichten DICO-Leitlinie vom Arbeitskreis „Aufsichtsrat und Compliance“ unter wissenschaftlicher Unterstützung des Viadrina Compliance Center erstellt. Dies erfolgte im Rahmen des vom KBA NotaSys Integrity Fund geförderten Projektes „Compliance und Integrität – ein Kompetenzpaket“. Das Projekt umfasste die Entwicklung eines allgemeinen CMS-Standards sowie weiterer spezieller Compliance-Standards. Wir danken den Mitgliedern des DICO-Arbeitskreises „Compliance und Aufsichtsrat“, dem KBA NotaSys Integrity Fund, Prof. Makowicz und seinem Team sowie allen Compliance-Praktikern, die durch ihre Hinweise und Beiträge an der Entwicklung dieses DICO-Standards mitgewirkt haben.

Vorwort

Compliance-Management-System[1] (CMS), also struktur- und prozessorientierte Maßnahmen zur Sicherstellung der Regeleinhaltung, werden mittlerweile zutreffend als zwingender Bestandteil guter Unternehmensführung angesehen, dessen Miss- oder Nichtbeachtung auch zur persönlichen Haftung der verantwortlichen Personen, darunter auch der Aufsichtsratsmitglieder, führen kann. Ein CMS gehört neben den anderen Funktionen im Unternehmen, wie Interne Kontrollsysteme, Risikomanagement oder interne Revision, zu den wesentlichen Elementen guter Governance und soll daher auch zu den ständigen Aufgaben des Aufsichtsrats gehören. CMS können zugleich eine Breite an Themenfeldern abdecken, etwa die Anforderungen an Lieferketten, Datenschutz, Geldwäsche- und Korruptionsprävention und andere.

Ein CMS ist jedoch inzwischen nicht nur aus der betrieblichen Perspektive wichtig. Auch rechtlich wird ein effektives CMS vielfältig belohnt und kann zu Minderung von Sanktionen führen. Dies bestätigte inzwischen der BGH, auch im kartellrechtlichen und geldwäschepräventiven Bereich sind solche Compliance-Anreize inzwischen vorhanden. Weitere aktuelle Entwicklungen bekräftigen die stetig wachsende Bedeutung von CMS. Erwähnt seien etwa die neuen Sorgfaltspflichten in den Lieferketten, die ebenfalls ein spezifisches CMS[2] erfordern, die für den Datenschutz nach der DSGVO notwendigen Managementsysteme, die sich aus dem Unionsrecht ergebende Pflicht zur Einrichtung von Hinweisgebersystemen, die ihrerseits Teil eines CMS sind oder die diversen Pflichten nach dem 2021 in Kraft getretenen Gesetz zur Stärkung der Finanzmarktintegrität und nicht zuletzt die nichtfinanzielle Berichterstattung.

Die Legalitätskontrollpflicht,[3] d. h. die Pflicht dafür zu sorgen, dass das Unternehmen und seine Mitarbeitenden Recht und Gesetz einhalten und somit u. a. die obigen Entwicklungen entsprechend beachtet werden, wird jedoch häufig nur als Verantwortung des Vorstands, bzw. der Geschäftsleitung wahrgenommen. Die Einhaltung von Regeln (Compliance) und die Einrichtung eines effektiven CMS richtet sich aber nicht nur an diese, sondern stellt auch den integralen Bestandteil der Arbeit im Aufsichtsrat, der die Wirksamkeit des umgesetzten CMS überwachen soll.[4]

Dabei soll sich der Aufsichtsrat hinsichtlich des CMS und Compliance mit drei wesentlichen Fragenkomplexen beschäftigen, die entsprechend in diesem Standard abgebildet werden: Zum einen soll der Aufsichtsrat selbst die für seine Mitglieder geltenden Regeln einhalten und damit ein gutes Beispiel geben (**Teil 1:** Aufsichtsrat-CMS, kurz AR-CMS), was auch unter tone from the top bekannt ist. Des Weiteren soll der Aufsichtsrat wissen, welche Kontrollpflichten bezogen auf das CMS ihm obliegen und wie sie umgesetzt werden können (**Teil 2:** Umsetzung der Kontrollpflichten). Drittens soll der Aufsichtsrat wissen, worauf bei der Kontrolle des CMS zu achten ist (**Teil 3:** Leitplanken eines CMS), damit eine effektive Aufsicht des unternehmerischen CMS überhaupt möglich ist. Treten in einem der drei Aspekte Unzulänglichkeiten auf, so droht dem Aufsichtsrat im schlimmsten Fall eine eigene Haftung aufgrund eines Organisations- und Überwachungsverschuldens.

1 Singular: ein System mit verschiedenen Programmen, vgl. § 91 Abs. 3 AktG; DCGK.
2 Dieses ist zwar im Gesetz als Risikomanagement bezeichnet, es weist aber alle typischen Elemente eines CMS auf.
3 Vgl. *Koch*, in Hüffer/Koch, § 93, Rn. 17: wichtiger Unterschied, da Legalitätspflicht absolut und Legalitätskontrollpflicht risikobezogen umzusetzen ist. Dieser Unterschied wird auch in der aktuellen Entscheidung des OLG Nürnberg (OLG Nürnberg, 30.03.2022 – 12 U 1520/19, NZG 2022, 1058) nicht gemacht.
4 Vgl. Grundsatz 6 DCGK.

Vor diesem Hintergrund richtet sich dieser Standard vornehmlich an Mitglieder von Aufsichtsräten sowie deren Berater.

Mit diesem Standard wird nicht die Absicht verfolgt, die „allein richtige Praxis“ darzustellen. Vielmehr sollen für die Aufsichtsratsarbeit praxistaugliche und umsetzbare Anforderungen dargestellt werden, welche gleichzeitig auch den Einstieg in das Thema CMS und Aufsichtsrat ermöglichen sowie einen guten Überblick über die mit dem Thema einhergehenden Anforderungen verschaffen sollen. Eine ggf. erforderliche rechtliche Beratung im Einzelfall kann hierdurch nicht ersetzt werden.

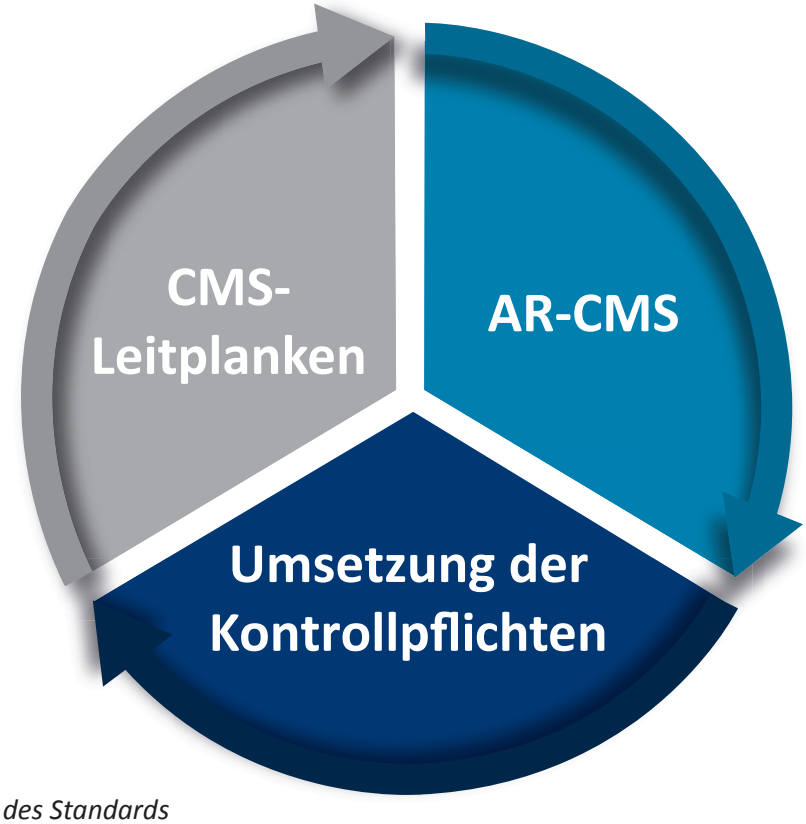

Abb. 1: Struktur des Standards

Der Standard richtet sich an Aufsichtsratsmitglieder, die ihre Vorkenntnisse im Bereich Compliance und CMS erweitern möchten und nicht in einer herausgehobenen Verantwortung zu CMS stehen, wie etwa die Mitglieder eines Prüfungsausschusses. Er konzentriert sich vielmehr auf solche Fragen, die sich jedes Aufsichtsratsmitglied zum Thema Compliance und CMS und seiner damit in Zusammenhang stehenden Kontrollfunktion stellt oder stellen soll.

Über DICO:

DICO – Deutsches Institut für Compliance e.V. wurde im November 2012 in Berlin auf Betreiben führender Compliance-Praktiker und -Experten gegründet und hat als gemeinnütziger Verein Mitglieder aus allen Branchen in Deutschland, darunter namhafte DAX-Unternehmen, Wirtschaftsprüfungs- und Beratungsgesellschaften sowie aus der Wissenschaft. DICO versteht sich als unabhängiges interdisziplinäres Netzwerk für den Austausch zwischen Wirtschaft, Wissenschaft, Politik und Verwaltung und sieht sich als zentrales Forum für die konsequente und praxisbezogene Förderung und Weiterentwicklung von Compliance in Deutschland.

DICO fördert Compliance in Deutschland, definiert in diesem Bereich Mindeststandards, begleitet Gesetzgebungsvorhaben und unterstützt zugleich die praktische Compliance-Arbeit in privaten und öffentlichen Unternehmen, fördert Aus- und Weiterbildung und entwickelt Qualitäts- sowie Verfahrensstandards.

Über VCC:

Das VCC verfolgt das Ziel der wissenschaftlich-kritischen Auseinandersetzung mit dem Phänomen der Compliance, Integrität und Wirtschaftsethik in Deutschland und weltweit. Die Themen werden am VCC vollumfänglich aus der Perspektive verschiedener Disziplinen behandelt. Immer mehr Organisationen führen Compliance-Management-Systeme mit dem Ziel ein, ihre Integrität und Zuverlässigkeit bewusst zu stärken und damit einen nachhaltigen Mehrwert für die Organisation selbst und für die Gesellschaft, der sie eingegliedert ist, zu generieren. Diese Compliance-Entwicklung hat bereits einen wesentlichen Beitrag zur Transparenzerhöhung in der deutschen Wirtschaft, zur Bekämpfung von Wirtschaftskriminalität sowie zur Förderung einer wertebasierten nachhaltigen Unternehmensführung geleistet. Das VCC behandelt Compliance aus einer wissenschaftlichen und fachübergreifenden Perspektive. Es verbindet diesbezügliche Erkenntnisse aus der Rechtswissenschaft, der Betriebswirtschaftslehre und der Soziologie in einem Think Tank miteinander und hält enge Kontakte zu allen Beteiligten.

DICO – Deutsches Institut für Compliance
Bergstraße 68
D-10115 Berlin
info@dico-ev.de
www.dico-ev.de

Viadrina Compliance Center
Europa-Universität Viadrina
Große Scharrnstr. 59
15230 Frankfurt (Oder)
compliance@europa-uni.de
www.compliance-academia.org