

Standardorientierte Überwachung von Compliance Management-Systemen durch den Aufsichtsrat



Prof. Dr. Bartosz Makowicz, Europa-Universität Viadrina Frankfurt an der Oder und Compliance Academy Münster (www.ca-seminare.de)

Die Zeiten, als ein Compliance Management-System (CMS) ein nice-to-have war, sind längst vorbei. Heute wird ein CMS nicht nur vom Deutschen Corporate Governance Kodex (DCGK) mit seinen konkreten Elementen ausdrücklich empfohlen, sondern, vorausgesetzt seine Effektivität und Effizienz, von der Rechtsprechung und Verwaltung konkret belohnt. Es ist zwar die Aufgabe des Vorstands, für erfolgreiche Konzepte zu sorgen, der Aufsichtsrat ist jedoch verpflichtet, diese zu überwachen. Doch wie können sie das tun? Der nachfolgende Beitrag liefert einen praktischen Überblick über die Rolle des Aufsichtsrats bei der CMS-Überwachung und erläutert, auf welche konkreten Elemente im Sinne der Norm DIN ISO 19600 Compliance-Management-Systeme zu achten ist.

I. Vorteile des CMS und seiner standardbasierten Überwachung

Noch vor einigen Jahren behaupteten viele, bei der Compliance (= Einhaltung von Regeln) würde es sich um einen Modebegriff handeln. Mittlerweile ist diese Behauptung sowohl rechtlich, als auch faktisch widerlegt. Management-Systeme zur Einhaltung von Regeln (CMS) sind inzwischen nicht nur zum festen Bestandteil der deutschen Governance-Struktur geworden, sondern bewirken eine Reihe von rechtlichen und faktischen Vorteilen für die Unternehmen, die diese korrekt implementiert haben.

1. Rechtliche Vorteile

Von herausragender Bedeutung ist zunächst das Urteil des Bundesgerichtshofes aus dem vergangenen Jahr, in dem höchstrichterlich festgehalten wurde, dass sich ein effizientes CMS mindernd auf die Höhe der Sanktion gegen Unternehmen auswirken kann.¹ Die Bedeutung des Urteils ist enorm, zumal die Große

Koalition in ihrem aktuellen Koalitionsvertrag Sanktionen gegen Unternehmen i.H.v. 10 % des Jahresumsatzes in Aussicht gestellt hat. Mit dem erwähnten Urteil hat der BGH das sog. Compliance-Anreizmodell höchstrichterlich bestätigt. Auch abgesehen von dem Urteil werden effektive CMS aber schon längst belohnt: So kann die Verfolgung wegen Verfehlungen in der Außenwirtschaft ausbleiben, wenn der betroffene Verstoß durch Eigenkontrolle aufgedeckt und gemeldet wurde und angemessene Maßnahmen zur Verhinderung ähnlicher Verfehlungen in der Zukunft getroffen wurden. Gleiche Richtung schlägt das GWB in Bezug auf das neue Wettbewerbsregister und die Möglichkeit der sog. Selbstreinigung ein. Danach kann ein Unternehmen zum Ausschreibungsverfahren wieder zugelassen werden, wenn der verursachte Schaden ausgeglichen wurde, das Unternehmen kooperiert und konkrete technische, organisatorische und personelle Maßnahmen ergriffen hat, die geeignet sind, weiteres Fehlverhalten zu vermeiden. All das kann im Rahmen eines CMS umgesetzt werden. Damit können Unternehmen nicht nur die erwähnten Vorteile

INHALT

- I. Vorteile des CMS und seiner standardbasierten Überwachung
 - 1. Rechtliche Vorteile
 - 2. Sonstige Vorteile
- II. Aufsichtsrat zwischen Herausforderung und Verantwortung
 - 1. Verantwortung
 - 2. Herausforderung
 - 3. DIN ISO 19600 CMS als Orientierungsrahmen
- III. Grundprinzipien
- IV. Überwachungsleitfaden
 - 1. Rolle der Unternehmensleitung
 - 2. Informationsbeschaffung (Compliance-Risiko)
 - 3. Compliance-Politik
 - 4. Klare Rollenzuweisung, insbes. Compliance-Funktion
 - 5. Unterstützung
 - 6. Aufklärung, Ahndung und ständige Verbesserung
- V. Fazit

Keywords

Compliance; Compliance Management-System; Effektivität; Effizienz; Prüfung

erreichen, sondern setzen auch die Empfehlungen des DCGK um, der in seiner seit 2017 erweiterten Fas-

¹ Vgl. BGH, 9.5.2017 – 1 StR 265/16, BeckRS 2017, 114578.

sung auch Risiko-Management und Hinweisgebersysteme als konkrete CMS-Elemente erwähnt.

2. Sonstige Vorteile

Ein effektives und effizientes CMS verfolgt darüber hinaus eine ganze Menge von weiteren Zielen, erfüllt diverse Funktionen und generiert somit verschiedene Vorteile nicht rechtlicher Art für Unternehmen und seine Mitglieder. Nur drei wesentliche davon sind zu erwähnen. Erstens wirkt heutzutage ein CMS als ein Wettbewerbsfaktor und wird als solcher auch von Unternehmen bewusst ausgespielt. Unternehmen mit CMS haben viel größere Chancen, einen Auftrag zu erlangen, als diejenigen ohne solche Systeme, da sie als zuverlässigere Geschäftspartner gelten. Zweitens tragen CMS nicht nur zum guten Ruf des Unternehmens bei, sondern schützen diese vor Schäden im Falle einer Verfehlung. Nicht zuletzt tragen CMS erheblich zur Integrität und zur nachhaltigen Compliance-Kultur im Unternehmen bei, die darin besteht, dass alle Mitglieder einer Organisation die Regel kennen und sie einhalten.

II. Aufsichtsrat zwischen Herausforderung und Verantwortung

All die erwähnten Vorteile wird ein CMS jedoch nur dann erzeugen können, wenn es effektiv und effizient umgesetzt worden ist. Doch welche Verantwortung trägt dabei der Aufsichtsrat und wie kann er seine diesbezüglichen Aufsichtspflichten ausrichten?

1. Verantwortung

Die Verantwortung des Aufsichtsrats für die Überwachung des CMS ergibt sich aus dem Gesetz und wird zutreffend in der Fachpresse kommentiert. Nach einer klaren Auslegung der Gesetzeslage gehört zu den Überwachungsaufgaben des Aufsichtsrates auch die Unternehmenskontrolle durch den Vorstand und sämtliche

Compliance-Aufgaben, die der Vorstand wahrzunehmen hat.² Der Aufsichtsrat ist verpflichtet, die Eignung und Effizienz von Compliance-Maßnahmen anlassunabhängig fortlaufend zu überprüfen.³ Er sollte somit kontrollieren, ob die Geschäftsführung ihren Compliance-Verpflichtungen nachkommt, wobei sich die Kontrolle jedoch zunächst regelmäßig auf die „System-Kontrolle“ beschränkt.⁴ Zwar sind die Berichte des Vorstands auf Grund der Berichtspflicht die wichtigsten Informationsquellen des Aufsichtsrats, er hat aber die Gesellschaft auch unabhängig zu überwachen und kann sich deshalb nicht allein auf die Vorstandsberichte als einzige Informationsquelle verlassen, sodass in der Hinsicht diverse weitere Instrumente empfohlen werden.⁵

2. Herausforderung

Sobald sich die Aufsichtsratsmitglieder ihrer Überwachungspflicht hinsichtlich des CMS bewusst sind, stehen sie schnell vor einer erheblichen Herausforderung hinsichtlich der Frage, worauf im Rahmen dieser Kontrollpflicht zu achten ist. Diese Herausforderung ist auch begründet. Compliance-Management-Systeme sind sehr heterogen ausgestaltet. Sie sollten im Idealfall das Spiegelbild der Risikolage des Unternehmens abbilden, was dazu führt, dass unterschiedliche Risiken durch unterschiedliche Maßnahmen adressiert und sich so unterschiedliche CMS ergeben können. Hinzu tritt noch, dass bei einem CMS gleich mehrere Fachdisziplinen zum Zuge kommen: Während die Ausgangslage, also Erfassung von einzuhaltenden Pflichten

von der Rechtswissenschaft dominiert ist, ist die Risikosteuerung von der BWL und die CMS-Umsetzung von Kommunikationswissenschaften oder Verhaltenspsychologie geprägt. Die Mischung aus diversen CMS-Arten und dem interdisziplinären Wesen der Compliance an sich, stellt Aufsichtsratsmitglieder vor eine große Herausforderung, wenn sie das hausinterne CMS überwachen sollten.

3. DIN ISO 19600 CMS als Orientierungsrahmen

Eine Abhilfe kann daher ein Orientierungsrahmen bieten. Solche sind in der Regel den Standards oder Normen zu entnehmen. Im Compliance-Bereich sind zwei Normen relevant: Zum einen handelt es sich um den Prüfungsstandard IDW PS 980, zum anderen um die DIN ISO 19600 CMS.⁶ Die beiden Normen unterscheiden sich grundlegend voneinander.⁷ Während PS 980 ein Prüfungsstandard (für die Wirtschaftsprüfer) ist und somit nur wenige inhaltliche Hinweise zur Ausgestaltung eines CMS enthält, handelt es sich bei der erwähnten ISO-Norm um eine generische Norm, die sich an Anwender richtet, umfangreiche Umsetzungsbeispiele und Hinweise enthält und als eine Check-box-Liste verwendet werden kann. ISO 19600 CMS ist vor einigen Jahren als eine DIN-Norm übernommen worden. Die DIN-Vorschriften kommen nach Rechtsprechung des Bundesverwaltungsgerichts als geeignete Quellen für die anerkannten „Regeln der Technik“ und als Ausdruck der fachlichen Mehrheitsmeinung in Betracht.⁸ Die Heranziehung des DIN ISO 19600 CMS als ein Referenzrahmen auch zu Zwecken der Überprüfung des CMS durch den Aufsichtsrat ist daher höchst empfehlenswert. Die Mitglieder des Aufsichtsrats sind so

2 Grundlegend dazu bei Rack, Die Verantwortung des Aufsichtsrates für das Compliance-Management-System im Unternehmen – Teil I, in: CB 2017, 59, 61 m.w.N.; von Busekist/Keuten, Zur Einrichtung eines Compliance-Ausschusses im Aufsichtsrat, CCZ 2016, 119, 120 ff.

3 von Busekist/Keuten, Fn. 2, S. 120.

4 Siepelt/Pütz, Die Compliance-Verantwortung des Aufsichtsrats, CCZ 2018, 78, 79.

5 Rack, Fn. 2, S. 61–62 und Derselbe, Die Verantwortung des Aufsichtsrats für das Compliance-Management-System im Unternehmen – Teil II, CB 2017, 105 ff.

6 Mehr unter: www.iso19600.info

7 Vergleich zum IDW PS 980 vgl. bei Withus/Kunz, Auswirkungen des neuen ISO 19600:2014 zu Compliance-Management-Systemen auf die Prüfung nach IDW PS 980, BB 2015, 685 ff.

8 BVerwG, Beschl. V. 30.9.1996, Az. 4 B 175/96, NVwZ-RR 1997, 213, 214 f.

auf der sicheren Seite, dass sie keine wesentlichen CMS-Elemente übersehen haben und können die Kontrolle anhand von objektiven und weltweit anerkannten Kriterien durchführen. Welche Elemente sind es nun aber?⁹

III. Grundprinzipien

Bevor auf die einzelnen CMS-Elemente im Sinne des DIN ISO 19600 CMS eingegangen wird, seien die wesentlichen Prinzipien kurz erläutert, die bei der Implementierung eines effizienten und effektiven CMS zu beachten sind. Diese Prinzipien sind in allen Stadien eines CMS zu beachten, sie spiegeln auch die Eigenart eines CMS wider. Danach soll dieses an die Größe, Struktur, Art und Komplexität der Organisation (Grundsatz der Flexibilität) angepasst und nach den Grundsätzen der Good Governance, der Verhältnismäßigkeit, der Transparenz und der Nachhaltigkeit umgesetzt werden.¹⁰ Auf einige dieser Prinzipien sei nun wegen ihrer Wichtigkeit im Einzelnen eingegangen.



Abb. 1: Die vier wesentlichen CMS-Grundsätze.

Von entscheidender Bedeutung bei der Überwachung eines CMS ist, ob dieses „maßgeschneidert“ ist. Ein CMS kann nicht als eine Standardlösung von einem anderen Unternehmen kopiert werden. Vielmehr muss es an die Größe, Struktur und

insbes. die Risikolage des Unternehmens angepasst werden. Diese Anforderungen sind mit dem Grundsatz der Flexibilität gemeint.

Darüber hinaus sollten verhältnismäßige Lösungen implementiert werden. Zu überwachen ist in der Hinsicht, ob die im Rahmen des CMS implementierten Maßnahmen überhaupt geeignet sind, die mit ihnen verfolgten Ziele zu fördern und ob die damit generierten Vorteile die möglicherweise mitverursachten Nachteile überwiegen. Ein CMS sollte weder übertrieben sein oder gar das operative Geschäft behindern, noch darf die in der Praxis nicht selten vorkommenden Situation eintreffen, dass eine Compliance-Maßnahme selbst einen Compliance-Verstoß verursacht.

Wie jedes andere System, sollte auch ein CMS möglichst überschaubar bleiben. Die Mitarbeiter müssen seine Funktionsweise kennen und wissen, welche Personen wofür zuständig sind. Die damit gemeinte Transparenz kann durch entsprechende offene Kommunikation und begleitende Materialien gefördert werden.

Schließlich soll ein CMS nachhaltig wirken. Gemeint ist damit insbes. die Förderung einer nachhaltigen Kultur der Regeleinhaltung, der sog. Compliance-Kultur, die auch als eines der Hauptziele eines CMS bezeichnet werden kann. Zur Etablierung und Stärkung der nachhaltigen Compliance-Kultur werden in der ISO-Norm diverse Schritte empfohlen. Zwar wird dabei von einem aktiven, sichtbaren, konsistenten und nachhaltigen Bekenntnis von Unternehmensleitung, Topmanagement und Management ausgegangen,¹¹ doch viel weiter in die operative Compliance geht der sich daran anschließende Katalog an Handlungsempfehlungen,¹² welche die Compliance-Kultur fördern können. Nur einige von diesen Maßnahmen seien hier erwähnt: Zum einen soll das Unternehmen einen

Wertekatalog aufstellen, angemessene Prüfung der Bewerber betreiben, einheitliche Behandlung der Mitarbeiterinnen und Mitarbeiter im Falle eines Verstoßes sicherstellen, fortlaufende und stets aktualisierte Compliance-Schulungen durchführen, fortlaufende Kommunikation der Compliance-Themen einplanen, sichtbare Anerkennung der Compliance-Erfolge kommunizieren und einen klaren Zusammenhang zwischen der Strategie der Organisation und der Rolle der Einzelnen darin unter Betonung der wesentlichen Funktion der Compliance für Erreichung der Ziele herstellen.¹³

IV. Überwachungsleitfaden

Während die obigen Grundsätze allgemeine Regeln für die Implementierung eines CMS zusammenfassen, die Mitglieder des Aufsichtsrats im Hinterkopf behalten sollten, geht es bei dem nachfolgenden Katalog um die wesentlichen CMS-Elemente, die nach der DIN ISO 19600 CMS unter Beachtung ebendieser Grundsätze in einem Unternehmen implementiert werden können. Auch an der Stelle ist zu betonen, dass es sich lediglich um einen Orientierungsrahmen handelt, an dem sich eine Aufsichtsplanung und Durchführung, vorausgesetzt ausreichender Informationen, orientieren können.¹⁴

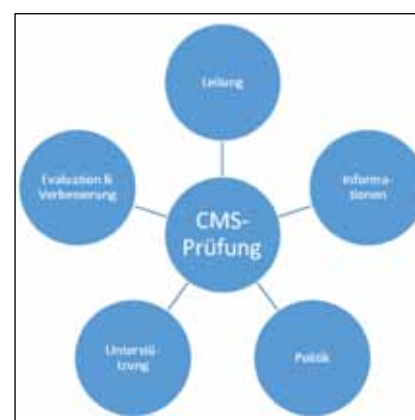


Abb. 2: Elemente der CMS-Prüfung durch den Aufsichtsrat.

9 Als ein Prüfungsleitfaden auch für Mitglieder des Aufsichtsrats geeignet: Makowicz, Globale Compliance Management Standards, München 2018.
10 Vgl. Ziff. 1 DIN ISO 19600 CMS.

11 Vgl. Ziff. 7.3.2.3 DIN ISO 19600 CMS.
12 Vgl. den vollständigen Katalog in Ziff. 7.3.2.3 DIN ISO 19600 CMS.

13 Vollständiger Katalog in Ziff. 7.3.2.3 DIN ISO 19600 CMS.
14 Die nachfolgende Zusammenstellung orientiert sich am DIN ISO 19600 CMS.

1. Rolle der Unternehmensleitung

Entscheidend bei jedem CMS ist die Rolle der Organisationsleitung. Diese sollte sich nicht nur zu Compliance effektiv bekennen, sondern das CMS entsprechend ermöglichen, indem ausreichende personelle und finanzielle Ressourcen bereitgestellt werden. Die Vorbildfunktion für die Mitarbeiter wird auch in der Fachpresse hervorgehoben.¹⁵ Diese Maßnahme wird jedoch in der Praxis oft falsch verstanden, weswegen bei der Prüfung durch den Aufsichtsrat Vorsicht geboten ist. Es geht nämlich nicht nur darum, dass der Vorstand einmal das einschlägige Bekenntnis abgegeben hat, von nun an für Compliance zu sorgen. Dem Bekenntnis müssen vielmehr konkrete Taten folgen. Die Leitung muss das CMS aktiv und fortlaufend unterstützen, der Compliance-Funktion entsprechende Unabhängigkeit und Zuständigkeiten gewähren und die Effektivität und Effizienz des CMS regelmäßig überprüfen.

2. Informationsbeschaffung (Compliance-Risiko)

Ist ein CMS von der Unternehmensleitung im obigen Sinne überhaupt ermöglicht worden, so kann es im nächsten Schritt mit der Informationsbeschaffung weitergehen. Bei der Beaufsichtigung dieses CMS-Elements ist darauf zu achten, dass geeignete Maßnahmen zur Erfassung, Bewertung und Steuerung des unternehmenseigenen Compliance-Risikos bestehen. Auch der 2017 reformierte DCGK empfiehlt die Maßnahme nun ausdrücklich. Das Ziel ist es, ausreichende Informationen über die Organisation, ihre Stakeholder, Produkte, Dienstleistungen, Partner, Mitarbeiter und sonstiges Umfeld zu sammeln, um auf der Basis das Compliance-Risikoportfolio zu erarbeiten. Hierzu gehören insbes. auch die Compliance-Pflichten der Organisation, die lücken-

los erfasst und regelmäßig aktualisiert werden sollten. Zwar sollte hierzu in der Regel ein Risk-Management-System eingerichtet werden, doch insbes. im Mittelstand werden auch alternative Methoden der Informationsbeschaffung ausreichen, wie etwa Schulungen, Flurgespräche, etc. Entscheidend ist jedenfalls, dass die Risikolage als Grundlage für weitere Schritte erfasst, korrekt bewertet und fortlaufend aktualisiert wird. Hiervon hängen nämlich weitere Maßnahmen ab.

3. Compliance-Politik

Auf der Basis der ermittelten Informationen kann durch die Unternehmensleitung, gemeinsam mit der Compliance-Funktion und sonstigen Organisationsmitgliedern die sog. Compliance-Politik erarbeitet werden. Diese enthält die Grundbestimmungen über die Compliance-Strategie der Organisation. Sie sollte in einer einfachen Sprache verfasst, allen Mitarbeiterinnen und Mitarbeitern gegenüber effektiv kommuniziert und erklärt sowie ständig aktualisiert werden. Innerhalb der Compliance-Politik sollten die Ziele des CMS und des Unternehmens erwähnt, die konkreten CMS-Maßnahmen festgehalten und insbes. der Anwendungsbereich des CMS ansich festgelegt werden. Für den Aufsichtsrat hat die Compliance-Politik einen doppelten Charakter. Zum einen wird sie eine wichtige Informationsquelle über den CMS darstellen, anhand der dieses auch überprüft werden kann. Andererseits sollte auch die Compliance-Politik als solche auf ihre Vollständigkeit und formell effektive Umsetzung überwacht werden.

4. Klare Rollenzuweisung, insbes. Compliance-Funktion

Mit Sicherheit von erheblicher Bedeutung für die Effizienz eines jeden CMS ist, dass jede Mitarbeiterin und jeder Mitarbeiter des Unternehmens weiß, welche Rolle sie oder er für Compliance hat. Denn jede einzelne

Person unterliegt bestimmten Pflichten, die einzuhalten sind. Generell lässt sich der ISO-Norm die Tendenz entnehmen, dass je höher die Position, umso wichtiger ist die Rolle der sie bekleidenden Person für Compliance.

Im Mittelpunkt eines CMS steht in dem Sinne die Compliance-Funktion (sog. Compliance Officer oder Compliance-Beauftragter), die entweder als eine zusätzliche Stelle eingerichtet oder einer anderen Funktion, etwa dem Leiter der Personalabteilung, zugewiesen werden kann. Die zuletzt erwähnte Methode wird insbes. im Mittelstand praktiziert. Für die Compliance-Funktion finden Grundsätze von Good Governance Anwendung, d.h. sie sollte den Direktzugang zur Organisationsleitung haben, mit ausreichenden Befugnissen und Ressourcen ausgestattet werden und eine unabhängige Stellung genießen. Bei der Überwachung ist daher darauf zu achten, wer die Compliance-Funktion hat, welche Mittel dieser Person zur Verfügung stehen und wie sie ausgestattet ist.

Während die Compliance-Funktion für das CMS, sind alle Mitglieder einer Organisation für Compliance verantwortlich. Diese Botschaft muss nicht nur an alle Beschäftigten effektiv kommuniziert werden, womit auch die entsprechende Sensibilisierungsarbeit erfolgt. Vielmehr muss die Verantwortung für Compliance an allen Ebenen mit den jeweiligen Verantwortungsbereichen verknüpft werden. So können alle Abteilungsleiter die Compliance-Risiken in deren Bereichen effektiv ermitteln und das CMS fördern. Die Mitarbeiter sollten das CMS effektiv nutzen und sich insbes. deren Verantwortung für Compliance bewusst sein.

Jedes Unternehmen sollte im Idealfall über einen Katalog der Compliance-Zuständigkeiten verfügen. Diese können entweder in der Compliance-Politik festgehalten werden oder sie können auf die Beschreibungen der allgemeinen Aufgaben der Mitarbeiter verweisen, wo auch die Compli-

¹⁵ Vgl. Jux/Saby, Top Management und Compliance: Top oder Flop, CB 2017, 353, 355.

ance-Aufgaben mit aufgenommen werden.

5. Unterstützung

Das Herzstück des DIN ISO 19600 CMS bilden die operativen Compliance-Maßnahmen. Die ISO-Norm bezeichnet diese als die das CMS unterstützenden Maßnahmen. Es lässt sich schwer pauschal festlegen, welche Maßnahmen zur Systemunterstützung zu ergreifen sind. Diese hängen nämlich wiederum von der Größe, Struktur und Natur der Organisation und mithin auch von der konkreten Risikolage ab. Zentrale Rolle spielt hier in jedem Fall ein effektives Compliance-Kommunikationskonzept, das in der Regel auch Compliance-Schulungen mitumfasst. Als besonders hilfreich in vielen Unternehmen haben sich auch sog. Verhaltenskodizes erwiesen, in denen die wesentlichen Verhaltensweisen systematisiert und in einer einfach verständlichen Sprache zusammengefasst werden. Die ISO-Norm erwähnt in der Hinsicht auch die regelmäßige Prüfungen des Kompetenzniveaus der Mitarbeiter, da auch darin ein Compliance-Risiko gesehen wird.

In diesen Zusammenhang fallen ferner weitere das CMS und seine Verankerung in der Governance-Struktur betreffende Maßnahmen. So sollten die einzelnen CMS-Maßnahmen entsprechend den gesetzlichen Anforderungen dokumentiert werden, um beweisfeste Unterlagen vorhalten zu können, schließlich sind eine geordnete Berichterstattung und Feedback von großer Bedeutung. Auch an der Stelle ergeben sich weitere Materialien für die Aufsichtsräte, die von zwei Seiten geprägt sind: Zum einen können sie als Quellen für die Überwachungsaufgaben verwendet werden, zum anderen sollten Aufsichtsräte bei der Prüfung auch darauf achten, ob die Dokumentation angemessen ist und die Compliance-Berichte an sich

formal korrekt und die Berichtswege richtig sind.

Im Bereich der Unterstützung wird der Aufsichtsrat mit Sicherheit auf die größten Herausforderungen in seiner Aufsichtstätigkeit stoßen, denn auch hier sind die größten unternehmerischen Spielräume vorhanden, die durch Implementierung von passenden Maßnahmen effektiv und effizient zu nutzen sind.

6. Aufklärung, Ahndung und ständige Verbesserung

Schließlich seien zwei Aspekte deutlich betont: Zum einen wird kein CMS der Welt den absoluten Schutz vor Non-Compliance gewährleisten. Aufgabe des CMS liegt somit auch darin, alle Verdachtsfälle zu identifizieren und ihnen mit reaktiven Maßnahmen zu begegnen. Auch hier bewirkt ein CMS, dass Unternehmen nicht nur auf den Ernstfall, sondern auch auf den Besuch von staatlichen Ermittlern vorbereitet sind. Zu achten ist daher bei der Prüfung durch den Aufsichtsrat, ob geeignete Krisenmanagementkonzepte vorhanden sind und insbes., ob angemessene Kommunikationswege, darunter insbes. Hinweisgebersysteme implementiert wurden, um den Mitarbeiterinnen und Mitarbeitern eine geschützte Mitteilung zu ermöglichen. Auch diese Maßnahme wird von dem novellierten DCGK empfohlen.

Ferner sollte das CMS selbst regelmäßig auf Effektivität und Effizienz untersucht werden. Insbes. bei Non-Compliance sollte geprüft werden, ob diese nicht durch einen systemischen Fehler ermöglicht wurde. In jedem Falle sollte das CMS als ein Managementsystem verstanden werden, das regelmäßiger Verbesserung unterliegt. DIN ISO 19600 CMS bedient sich hier des PDCA-Modells¹⁶ aus der

16 Plan > Do > Check > Act = Planen > Umsetzen > Prüfen > Verbessern.

Qualitätssicherung, das zum Ziel hat, den Prozess ständig zu verbessern.

V. Fazit

Ein Compliance Management-System ist von der Governance-Struktur deutscher und ausländischer Unternehmen nicht mehr wegzudenken. Ist ein CMS effektiv und effizient implementiert worden, kann es eine Reihe von erheblichen rechtlichen und sonstigen Vorteilen für Unternehmen und ihre Belegschaft erzeugen. Insbesondere die rechtliche Bedeutung von CMS ist in den letzten Jahren wesentlich gestiegen und wird in den kommenden Jahren weiter steigen, beachtet man die Festlegungen im aktuellen Koalitionsvertrag. Aus diesen Gründen sollte der Aufsichtsrat die Effizienz und Effektivität eines CMS fortlaufend überwachen. Da die CMS unterschiedlich gestaltet werden können, stehen Mitglieder eines Aufsichtsrats jedoch oft vor großer Herausforderung, wenn sie das hauseigene CMS unter die Lupe nehmen. Dabei kann die anerkannte Norm DIN ISO 19600 CMS einen verlässlichen, leicht verständlichen und überschaubaren Referenzrahmen bieten. Sie enthält allgemeine Grundsätze und konkrete Umsetzungsregeln, auf die Aufsichtsräte achten sollten, wenn sie sich sicher sein möchten, dass die jeweiligen CMS-Maßnahmen entsprechend den allgemein anerkannten Regeln und dem aktuellen „Stand der Technik“ implementiert wurden. Damit erfüllen die Aufsichtsräte nicht nur ihre eigenen Überwachungspflichten, sondern tragen zur Effektivität und Effizienz des CMS und damit zur nachhaltigen Compliance-Kultur im Unternehmen bei.