DICO Standard

Compliance-Management-Systeme

Übergreifender Standard der DICO-Standard-Reihe

Autoren: Arbeitskreis Compliance Management Systeme

Wissenschaftliche Überarbeitung: Viadrina Compliance Center,
Europa-Universität Viadrina Frankfurt (Oder)

DICO
Deutsches Institut für Compliance

Viadrina
Compliance
Center

Stand: März 2021

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-Themen in der Unternehmenspraxis umzusetzen. Mit der Veröffentlichung eines DICO Standards ist die Diskussion des jeweiligen Themenkreises 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 DICO Standard Compliance-Management-Systeme wurde im Rahmen des Projektes „Compliance und Integrität – Kompetenzpaket“ am Viadrina Compliance Center unter Leitung von Prof. Dr. Bartosz Makowicz wissenschaftlich erstellt. Das Projekt wurde vom KBA Integrity Fund gefördert und umfasste die Entwicklung eines allgemeinen CMS-Standards sowie weiterer spezieller Compliance-Standards. Wir danken dem KBA Integrity Fund, Prof. Makowicz und seinem Team sowie den Mitgliedern des DICO Arbeitskreises Compliance Management und allen Compliance-Praktikern, die durch ihre Hinweise und Beiträge an der Entwicklung dieses DICO Standards mitgewirkt haben.

VORWORT 5

1. GRUNDLAGEN 6
1.1 Ziele und Aufgaben 6
1.1.1 Regelkonformität der Geschäftsaktivitäten 6
1.1.2 Haftungsvermeidung und Reputationsschutz 6
1.1.3 Weitere Ziele und Aufgaben 6
1.2 Prinzipien 7
1.2.1 Wertebasiertes Regelsystem und Compliance-Kultur 7
1.2.2 Risikoorientierung, Angemessenheit und Flexibilität 7
1.2.3 Praktische Wirksamkeit (Effektivität) 8
1.2.4 Integration 8
1.2.5 Dokumentation 8

2. ENTWICKLUNG UND UMSETZUNG 9
2.1 Planung und Grundlagen 10
2.1.1 Rolle der Unternehmensleitung 10
2.1.2 Compliance-Risiko-Analyse 10
2.1.3 Organisatorische Grundlagen 11
2.1.4 Anwendungsbereich des CMS 11
2.1.5 Aufgabenverteilung, insbes. Compliance-Funktion 12
2.2 Vorbeugen (Prevent) 14
2.2.1 Verhaltenskodex und Compliance-Richtlinien 14
2.2.2 Beratung 14
2.2.3 Kommunikation und Schulungen 15
2.2.4 Kompetenzsicherung 15
2.2.5 Themenspezifische CMS-Elemente 16

2.3 Entdecken (Detect) 16
2.3.1 Fortlaufende Überwachung (Compliance-Kontrollen) 16
2.3.2 Hinweisgebersystem und Aufklärung von Verdachtsfällen 17
2.4 Reagieren (Respond) 17
2.4.1 Interne Sanktionierung 17
2.4.2 Sonstige Remediation-Maßnahmen 18
2.4.3 Berichterstattung 18
2.4.4 Krisenmanagement 19
2.5 Regelmäßige Systemevaluierung und fortlaufende Optimierung 19

3. REFERENZSTANDARDS 21

4. BIBLIOGRAPHIE 22
4.1 Verwendete Literatur 22
4.2 Weiterführende Literatur 26

5. GLOSSAR 28

Vorwort

Unternehmen in Deutschland sehen sich in den letzten Jahren einer Vielzahl von Vorgaben zur Ausgestaltung von Compliance-Management-Systemen (CMS) gegenüber. Hinzu treten immer komplexere Vorgaben des Gesetzgebers und der Justiz. Das geplante Gesetz zur Stärkung der Integrität in der Wirtschaft,[1] mit dem ein neues Verbandssanktionengesetz (VerSanG) eingeführt wird, zielt nicht nur auf die Förderung von CMS ab, sondern sieht eine sanktionsmindernde Wirkung von CMS vor. Nicht nur große, sondern insbesondere mittelgroße und kleinere Unternehmen können mit der Implementierung dieser Vorgaben überfordert sein. DICO will den Unternehmen mit diesem Standard, ergänzt um weitere DICO Spezialstandards, eine praktische Hilfestellung geben.

Compliance ist kein statisches Thema. Entwicklungen im Bereich der künstlichen Intelligenz, der Kriminologie und Verhaltensforschung, der Digitalisierung wie auch neue Möglichkeiten der Unterstützung der Compliance-Arbeit durch den Einsatz von IT-Tools sind bei der Fortentwicklung eines CMS zu berücksichtigen. Vor allem der Digitalisierungsprozess ist aus Compliance-Perspektive in doppelter Hinsicht zu berücksichtigen: als Chance für eine effektive System-Unterstützung, aber auch als Quelle neuer Compliance-Risiken.

Der vorliegende Standard – CMS umfasst in knapper Form allgemeine Empfehlungen zur Ausgestaltung eines CMS. Er ist auf alle Unternehmensarten anwendbar, unabhängig von ihrer Größe, Struktur und Komplexität. Er bildet eine strukturelle Einheit mit den DICO Spezialstandards, die ausführliche Empfehlungen zur Gestaltung ausgewählter CMS-Elemente enthalten und von weiteren DICO Arbeitskreisen erarbeitet wurden. Ergänzt wird diese Struktur um weitere Leitfäden und Dokumente der DICO Arbeitskreise. Die neu erarbeiteten DICO Spezialstandards oder DICO Leitlinien werden in diesen Standard systematisch eingepflegt. Der Standard wird regelmäßig aktualisiert und fortentwickelt.

Der Standard – CMS berücksichtigt Vorgaben deutscher Gesetze in der Konkretisierung durch die Rechtsprechung und einzelne Gesichtspunkte ausgewählter ausländischer Rechtsquellen. Branchenspezifische Vorgaben (etwa für die Finanzindustrie) sind mit Ausnahme weiterführender Hinweise in Fußnoten nicht berücksichtigt. Er basiert auf den in der deutschen Literatur verbreitet vertretenen Meinungen sowie den in der Praxis überwiegend umgesetzten CMS. Die verwendeten Begriffe werden im Glossar am Ende des Dokuments erörtert; das angefügte Literaturverzeichnis soll einen raschen Zugriff auf Spezialliteratur zur vertieften Befassung mit ausgewählten Fragestellungen ermöglichen.

Die Erstfassung dieses Standards entstand als Ergebnis der Arbeit des DICO Arbeitskreises Compliance Management mit wissenschaftlicher Unterstützung des Viadrina Compliance Center im Rahmen des von Prof. Dr. Bartosz Makowicz geleiteten und vom KBA NotaSys Integrity Fund geförderten Drittmittelprojekts „Compliance & Integrity – Kompetenzpaket“.

1 Zum Zeitpunkt der Fertigstellung des vorliegenden Standards ist der Regierungsentwurf eines Gesetzes zur Stärkung der Integrität in der Wirtschaft am 16. Juni 2020 von der Bundesregierung beschlossen worden. Am 18. September 2020 beschloss der Bundesrat im weiteren Gesetzgebungsverfahren, dass weitere Änderungen im Entwurf notwendig seien. Der Ausgang des einschlägigen Gesetzgebungsverfahrens ist noch offen.

1. GRUNDLAGEN

Ein Compliance-Management-System (CMS) erfüllt diverse Ziele und Aufgaben (Ziff. 1.1)[2] und wird unter Beachtung wesentlicher Prinzipien (Ziff. 1.2) entwickelt und umgesetzt (Ziff. 2).

1.1 Ziele und Aufgaben

Da die Grenzen zwischen Zielen und Aufgaben eines Managementsystems oft unscharf verlaufen und ineinandergreifen, werden diese nachfolgend in Bezug auf ein CMS gebündelt betrachtet.

1.1.1 Regelkonformität der Geschäftsaktivitäten

Ein CMS soll primär dazu beitragen, dass das Unternehmen und seine Mitglieder im Einklang mit Recht, Gesetz und internen Regeln agieren. Die für rechtskonformes Handeln letztlich verantwortliche Unternehmensleitung und alle Unternehmensmitglieder sollen in der Ausübung ihrer unternehmerischen Tätigkeit unterstützt werden, so dass die vom Unternehmen hergestellten Produkte, angebotenen Dienstleistungen und andere Aktivitäten regelkonform sind.[3] Im Sinne der Risikoorientierung, Angemessenheit und Flexibilität (Ziff. 1.2.2) sollen Unternehmen individuell entscheiden, welche Compliance-Themenfelder vom Anwendungsbereich des CMS (Ziff. 2.1.4) umfasst und welche im Rahmen anderer Prozesse gesteuert werden.[4]

1.1.2 Haftungsvermeidung und Reputationsschutz

Ein weiteres wichtiges Ziel von CMS ist Haftungsvermeidung durch Präventionswirkung. Das CMS soll sicherstellen, dass es im besten Fall erst gar nicht zum Verstoß kommt. Zudem hat das CMS eine exkulpierende Wirkung. Wenn dennoch ein Compliance-Verstoß eintritt, haften das Unternehmen und seine Leitung nicht oder nur reduziert, weil mit dem CMS alles Zumutbare getan wurde, um Verstöße zu verhindern, bzw. zu erschweren und aufzuklären.[5] Neben der Haftungsvermeidung soll das CMS eine positive Auswirkung auf die Reputation des Unternehmens haben, indem es diese schützt oder sogar aktiv fördert.

1.1.3 Weitere Ziele und Aufgaben

Über die Regelkonformität, Haftungsvermeidung und den Reputationsschutz hinaus sollen im Rahmen eines CMS folgende Ziele und Aufgaben verfolgt werden:

- **Integrität:** Das CMS soll bezwecken, dass alle Unternehmensmitglieder die Compliance-Kultur des Unternehmens aktiv fördern und die in ihren Bereichen geltenden Regeln und Werte des Unternehmens kennen, sie verinnerlichen und mit ihnen konform handeln.[6]

- **Förderung des Unternehmenserfolgs und -wertes:** Langfristiger Unternehmenserfolg ist nur auf Basis gelebter Werte möglich. Das CMS soll den nachhaltigen Unternehmenserfolg und den Unternehmenswert fördern. Durch eine gelebte Compliance-Kultur kann das CMS den Wert eines Unternehmens für wichtige Anspruchs- oder Interessengruppen (*stakeholder value*) steigern

2 Vgl. auch bei *Schorn*, in: Hauschka/Moosmayer/Lösler, § 13, Rn. 24 ff.; *Löffler/Ahammer*, in: Barbist/Ahammer/Fabian/Löffler, S. 34 f.

3 *Weiß/Koch/Osterloh*, in: Jäger/Rödl/Campos Nave, S. 57 f.

4 *Löffler/Ahammer*, in: Barbist/Ahammer/Fabian/Löffler, S. 35.

5 Vgl. § 130 Abs. 1 S. 1 OWiG; *Hauschka/Moosmayer/Lösler*, in: Hauschka/Moosmayer/Lösler, § 1, Rn. 28 f.; *Jenne/Martens*, CCZ 2017, 285 (286 ff.); *Hoffmann/Schieffer*, NZG 2017, 401 (403 f.); *Wilsing/Goslar*, GmbHR 2017, 1202 (1203 f.).

6 *Schwarzbartl/Pyrcek*, S. 28 ff.; Schulz, BB 2017, 1475 (1476 ff.). Siehe auch DICO Leitlinie L07 – Hinweise und Kriterien zur Messung einer Unternehmenskultur.

und wesentlich zu seiner besseren Wettbewerbsfähigkeit beitragen. Im Innenverhältnis kann das CMS die Attraktivität als Arbeitgeber[7] erhöhen. Außerdem trägt das CMS zur Vermeidung des Risikos bei, dass geschäftliche (strategische oder transaktionale) Entscheidungen sachwidrig oder nicht im eigentlichen Unternehmensinteresse getroffen werden.

- **Optimierung und Innovation:** Ein CMS begleitet Innovationsprozesse im Unternehmen von Anfang an (Ziff. 1.2.4) und kann zur grundlegenden Optimierung der Unternehmensprozesse und -strukturen beitragen.[8] Durch Verankerung und Einbindung in Geschäftsprozesse, durch Synergien von Organisationsabläufen innerhalb des CMS und im Rahmen anderer Prozesse entstehen weitere Vorteile. So sollen auch entsprechende Innovationsabläufe unterstützt werden, die innerhalb des CMS, das selbst fortwährender Innovation unterliegt, als neuartige Maßnahmen integriert (Ziff. 1.2.4) werden oder in anderen Prozessen zum Einsatz kommen. Ein wirksames CMS soll gleichzeitig verhindern, dass vermeintlich zukunftsfähige Innovationen entwickelt werden, die aufgrund unverhältnismäßiger Compliance-Risiken aus rechtlichen oder unternehmerischen Gründen nicht tragfähig sind.

1.2 Prinzipien

Die nachfolgenden Prinzipien der CMS-Gestaltung sollen bei Entwicklung und Umsetzung (Ziff. 2) beachtet werden und nebeneinander Anwendung finden.

1.2.1 Wertebasiertes Regelsystem und Compliance-Kultur

Grundlage eines CMS sollen eine verantwortungsvolle Unternehmensführung im Sinne des Leitbilds des Ehrbaren Kaufmanns[9] und eine werteorientierte Compliance-Kultur (Ziff. 1.1.3)[10] sein, die über das CMS ethisches und verantwortungsvolles Handeln innerhalb und außerhalb des Unternehmens fördert.[11]

1.2.2 Risikoorientierung, Angemessenheit und Flexibilität

Das CMS und die dafür eingesetzten Ressourcen sollen für das jeweilige Risikoprofil, insbesondere unter Berücksichtigung von Größe, Struktur und Komplexität des konkreten Unternehmens, angemessen sein.[12] Die Governance des Unternehmens sowie die Ausgestaltung und Implementierung des CMS sollen bei geänderten Bedingungen[13] zeitnah angepasst werden, um einem veränderten Risikoprofil Rechnung zu tragen.[14]

---

7 Zum Zweck der besseren Lesbarkeit wird auf die geschlechtsspezifische Schreibweise verzichtet. Alle personenbezogenen Bezeichnungen in diesem Standard sind geschlechtsneutral zu verstehen.

8 *Eckert*, S. 60 f.

9 Präambel DCGK; *Obermayr*, in: Hauschka/Moosmayer/Lösler, § 44, Rn. 26 ff.

10 *Löffler/Ahammer*, in: Barbist/Ahammer/Fabian/Löffler, S. 32 ff.

11 *Schulz*, BB 2018, 1283 (1286 ff.); *Makowicz*, COMPLY. 3/17, 12 (13).

12 Vgl. Empfehlung A.2 DCGK; *Pauthner*, in: Ghassemi-Tabar/Pauthner/Wilsing, Kap. 1, Rn. 254 ff.; *Makowicz*, in: Makowicz, Kap. 1-10, Nr. 3.2; *Bings*, CCZ 2017, 118 (119).

13 Z. B. Größe, Struktur und Komplexität des Unternehmens, neue Produkte, Dienstleistungen, neue Märkte, technische Fortentwicklungen wie Digitalisierung, künstliche Intelligenz etc.; vgl. auch bei *Pyrcek*, BB 2017, 939 (939 ff.).

14 Vgl. §§ 3 Abs. 1 Nr. 2, 15 Abs. 1 Nr. 2, 35 Abs. 1 und Begr. S. 79 VerSanG-E; Ziff. 6.1 UKBA; Ziff. I. C, I. E, II. B., III. A. ECCP; *Martin/Ralston*, Compliance and Ethics Professional Magazine 10/2019, 50 (50 ff.); *Frank/Kerley*, New Law Journal UK, 01.05.2020, 13 (13 f.).

1.2.3 Praktische Wirksamkeit (Effektivität)

Das CMS soll so entwickelt und umgesetzt werden, dass es unternehmensbezogene Compliance-Verstöße soweit möglich tatsächlich verhindert. Im Einzelfall sollen Hinweise auf Verstöße zum Schutz des Unternehmens und zur Vermeidung künftiger Verstöße zuverlässig empfangen, aufgeklärt und adressiert werden.[15] Dies erfordert insbesondere, dass für die Tätigkeit jedes Unternehmensmitglieds risikoadäquate Aufsichtsmaßnahmen getroffen und umgesetzt werden.[16] Voraussetzung hierfür ist ferner eine angemessene Durchdringung des gesamten Unternehmens mit dem CMS im In- und Ausland (inkl. Beteiligungen und Joint Ventures).[17]

1.2.4 Integration

Das CMS soll mit den übrigen bestehenden Managementsystemen[18] über definierte Schnittstellen so verknüpft werden, dass eine integrierte Governance-Struktur gewährleistet ist.[19] Dabei soll sichergestellt werden, dass die Aufgaben- und Anwendungsbereiche der einzelnen Systeme so verzahnt sind, dass keine Lücken verbleiben.[20] In diesem Zuge kann es notwendig sein, Compliance-Maßnahmen in die Aufbau- und Ablauforganisation anderer Unternehmensbereiche zu integrieren.[21] Einzelheiten sollen bei der Bestimmung des Anwendungsbereiches des CMS festgelegt werden (Ziff. 2.1.4).

1.2.5 Dokumentation

Das CMS und die in seinem Rahmen umgesetzten Maßnahmen sollen angemessen dokumentiert werden.[22] Dokumentationsumfang und -tiefe sollen an der Bedeutung der jeweiligen Regelung oder Maßnahme orientiert sein. Dies gilt sowohl für Entscheidungen zu den organisatorischen Grundlagen des CMS (Ziff. 2.1.3) als auch für Einzelfallentscheidungen zu Sachverhalten mit Compliance-Relevanz (z. B. Verdachtsfälle, Ziff. 2.3.2). »

15 Ziff. II. B. ECCP; *Makowicz*, in: Makowicz, Kap. 1-10, Nr. 3.6; *Wiedmann/Greubel*, CCZ 2019, 88 (88); *Jüttner*, CCZ 2018, 168 (168 ff.).

16 Ziff. 5.1, 5.3., 7.2.1, 7.3 und 9.1.1 ISO 37301; Empfehlung D.3 DCGK; *Fissenewert*, Praxishandbuch CMS, S. 77.

17 *Ebner/Leone*, CCZ 2020, 7 (10 f.); *Chen*, COMPLY. 2/18, 16 (17).

18 Z. B. Risiko-, Qualitäts-, Personalmanagement etc.

19 *Daum*, in: Bay/Hastenrath, Kap. 3, Rn. 29 f.; *Klahold/Lochen*, in: Hauschka/Moosmayer/Lösler, § 37, Rn. 68 ff.; *Makowicz*, in: Makowicz, Kap. 1-10, Nr. 3.8.

20 Siehe zur systematischen Herangehensweise an das Risikomanagement insbesondere auch das sog. Three Lines Modell, vgl. *Obermayr*, in: Hauschka/Moosmayer/Lösler, § 44, Rn. 116 ff.

21 Z. B. wird eine technische Compliance-Prüfung in Prozesse der Produktentwicklung integriert.

22 Ziff. 7.5 ISO 37301; *Vetter*, in: Wecker/van Laak, S. 47; *Meckenstock*, in: Makowicz, Kap. 2-80; *Behringer*, in: Behringer, Compliance KMU, S. 259 f.

2. ENTWICKLUNG UND UMSETZUNG

Unternehmen haben bei Definition, Ausgestaltung, Umsetzung und Weiterentwicklung des CMS einen weiten unternehmerischen Beurteilungs- und Ermessensspielraum,[23] um die für das spezifische Unternehmen und seine Risiken angemessenen Maßnahmen zu treffen und damit unternehmensbezogene Rechts- und Richtlinienverstöße soweit möglich zu verhindern.[24] In der Praxis haben sich über die Jahre Vorgaben und Empfehlungen für einzelne Elemente und Methoden eines CMS herauskristallisiert, aus denen sich die im Folgenden beschriebene Vorgehensweise zur Entwicklung und Umsetzung des CMS ergeben.

Auf Basis einer Planung und grundlegender Maßnahmen (Ziff. 2.1) soll das CMS individuell erstellt und umgesetzt werden. Die Ausgestaltung der CMS-Elemente und ihre Operationalisierung sollen auf Basis des in der Praxis etablierten sog. Prevent – Detect – Respond (Vorbeugen – Entdecken – Reagieren)-Modells[25] erfolgen (Ziff. 2.2–2.4). Das CMS soll zudem regelmäßig evaluiert und fortlaufend verbessert werden (Ziff. 2.5). So soll sichergestellt werden, dass das CMS im Unternehmen in systematischer Weise als ein Qualitätsprozess betrieben wird.[26] Einzelne CMS-Elemente können mehrere Ziele und Aufgaben im CMS (Ziff. 1.1) erfüllen und in ihrer Anwendung sowohl präventiv als auch repressiv wirken.[27] Das Modell mit der hier gewählten Zuordnung der CMS-Elemente ist in der nachfolgenden Abbildung dargestellt.

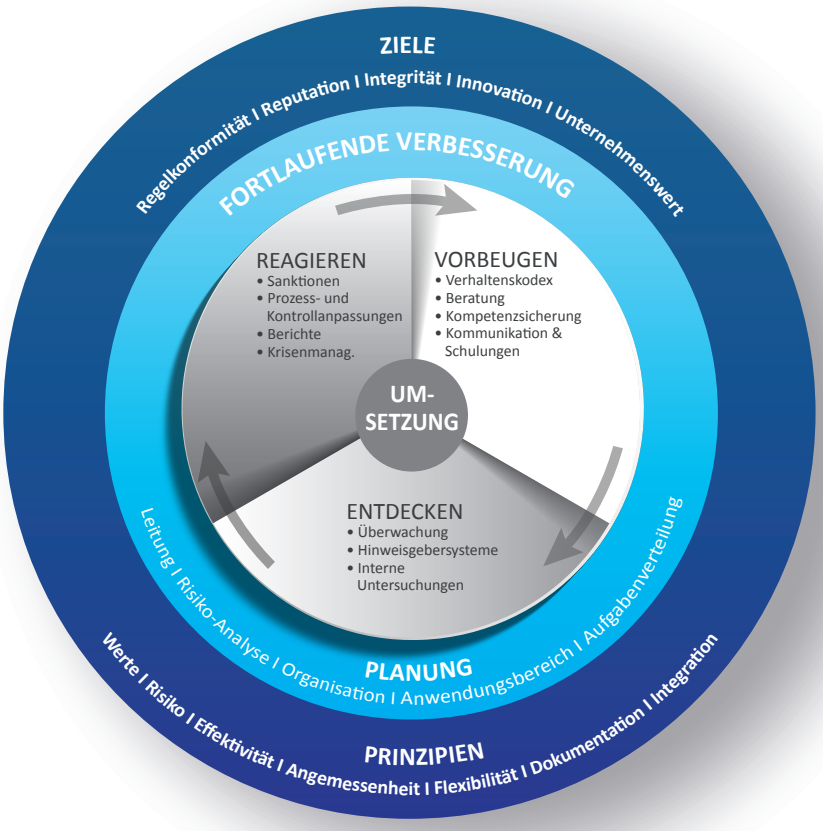

Abbildung: CMS-Modell gemäß DICO Standard 12 – CMS

23 *Kremer/Klahold*, in: Krieger/Schneider, Handbuch Managerhaftung, Rn. 25.3; *Seibt*, in: Schmidt/Lutter, § 76 AktG, Rn. 12.

24 §§ 30, 130 OWiG; *Makowicz*, in: Makowicz, Kap. 1-10, Nr. 4.1; *Volz*, in: Teichmann, Kap. 1, Rn. 35 ff.

25 Siehe etwa *Kahlenberg/Schäfer/Schieffer*, in: Busch/Hoven/Pieth/Rübenstahl, Kap. 33, Rn. 36 ff.; *Moosmayer*, Rn. 364 ff.; *Seyfarth*, ZGR-Sonderheft 22/2020, 87 (97); *Schieffer*, in: Minkoff/Sahan/Wittig, § 28 Rn. 48 ff.

26 Die Vorgehensweise entspricht weitestgehend dem für Managementsystemstandards etablierten PDCA-Zyklus, vgl. etwa ISO 37301 Compliance Management Systems, ISO DIN 37001 Anti-Bribery Management Systems, ISO DIN 9001 Qualitätsmanagement-Systeme.

27 Siehe Ziff. II. C. ECCP; *Makowicz*, in: Makowicz, Kap. 1-10, Nr. 2.4.1-3; *Schwarzbartl/Pyrcek*, S. 35 ff. sowie S. 67 ff.; *Makowicz*, BB 2018, 556 (559.).

2.1 Planung und Grundlagen

Planung und Grundlagen bilden den Ausgangspunkt für die Einrichtung der einzelnen CMS-Elemente und ihre Umsetzung (Ziff. 2.2–2.4).[28]

2.1.1 Rolle der Unternehmensleitung

Compliance-Management ist als Teil der Legalitätskontrollpflicht primär Aufgabe der Unternehmensleitung. Die Verantwortung trifft das jeweilige Leitungsgremium gemeinschaftlich.[29] In der grundlegenden Phase des CMS-Aufbaus kommt der Unternehmensleitung eine besondere Bedeutung zu. Sie hat zunächst die Aufgabe, eine Compliance-Risiko-Analyse (Ziff. 2.1.2) durchzuführen bzw. zu veranlassen.[30] Aus dieser soll sich ergeben, ob und inwieweit das Risikoprofil des Unternehmens strukturierte Elemente im Sinne eines CMS verlangt. Auf dieser Basis werden von der Unternehmensleitung anschließend die organisatorischen Grundlagen des CMS festgelegt (Ziff. 2.1.3) und sein Anwendungsbereich definiert (Ziff. 2.1.4). Zu dieser Phase gehören auch die Aufgabenverteilung sowie die Einrichtung und Ausgestaltung der Compliance-Funktion, einschließlich ihrer angemessenen sachlichen, finanziellen und personellen Ausstattung (Ziff. 2.1.5).

Die Unternehmensleitung soll die Umsetzung des CMS im Unternehmen kontinuierlich unterstützen[31] sowie die praktische Wirksamkeit des CMS fortlaufend überwachen und in hinreichenden Zeitabständen evaluieren lassen (Ziff. 2.5).[32] Sie soll sich darüber hinaus ausdrücklich zur Compliance-Kultur bekennen (sog. tone from the top) und das Bekenntnis durch aktive Unterstützung des CMS als Prozess und dessen wiederkehrende Thematisierung bekräftigen.[33] Innerhalb der Unternehmensleitung kann die Zuständigkeit für die konkrete Ausgestaltung und Umsetzung des CMS einem Mitglied des Leitungsgremiums zugewiesen werden; insoweit wird die Verantwortlichkeit der übrigen Mitglieder dann zu einer Überwachungspflicht (horizontale Delegation).[34]

2.1.2 Compliance-Risiko-Analyse

Grundlage für die Entwicklung und Umsetzung des CMS und ein ganz wesentlicher Bestandteil soll die Analyse der Risiken von Regelverstößen, die sog. Compliance-Risiko-Analyse (CRA)[35] (Ziff. 1.2.2), sein, aus der sich die zu beachtenden Compliance-Themenfelder ergeben. Dabei soll beachtet werden, dass die CRA in ein bestehendes Enterprise Risk Management (ERM) integriert sein oder daneben funktionieren kann. So viele Unternehmensarten es gibt, so unterschiedlich sind die von ihnen angebotenen Produkte und Dienstleistungen, und so unterschiedlich die Märkte sind, in denen die Unternehmen tätig sind, so unterschiedlich werden auch die Compliance-Risiken sein, die im Rahmen des CMS gesteuert werden sollen.[36]

---

28 *Fissenewert*, Praxishandbuch CMS, S. 107 ff.

29 § 93 Abs. 2 AktG, § 43 Abs. 2 GmbHG.

30 *Harz/Weyand/Reiter/Methner/Noa*, S. 34 ff.

31 *Schulz*, BB 2019, 579 (579 f.).

32 LG München I, Urt. v. 10.12.2013 – Az. 5 HK O 1387/10, BeckRS 2014, 1998, im Weiteren als „Neubürger-Urteil".

33 Ziff. 5.1.1 ISO 37301; Principle 2 UKBA; Ziff. II. A. ECCP; *Vetter*, in: Wecker/van Laak, S. 43; */Freiler-Waldburger*, in: Sartor/Freiler-Waldburger, S. 30 ff.; *Makowicz*, in: Makowicz, Kap. 1-10, Nr. 4.1.1; *Löffler/Ahammer*, in: Barbist/Ahammer/Fabian/Löffler, S. 32 ff.; *Weiß/Koch/Osterloh*, in: Jäger/Rödl/Campos Nave, S. 61 ff.

34 *Klahold/Lochen*, in: Hauschka/Moosmayer/Lösler, § 37, Rn. 18; *Hoffmann/Schieffer*, NZG 2017, 401 (405); *Schulz*, BB 2019, 579 (581 f.); *Gomer*, S. 115.

35 § 93 AktG und § 43 GmbHG; „Neubürger"-UrtBegr. S. 13, siehe Fn. 33; Begr. S. 79 VerSanG-E; Principle 3 UKBA; Ziff. I. A. ECCP; *Borowa*, in: Bay/Hastenrath, Kap. 5, Rn. 87 ff.; *Löffler/Ahammer*, in: Barbist/Ahammer/Fabian/Löffler, S. 35; *Grunert*, CCZ 2020, 71 (75 ff.); *Vetter/Harting*, in: Moosmayer, Kap. 2, Rn. 31 ff.

36 Vorgaben zur Durchführung einer Risikoanalyse können etwa abgeleitet werden aus § 130 OWiG, Empfehlung A.2 DCGK sowie – soweit anwendbar – aus § 5 GwG, § 25g Abs. 1 KWG; § 25a i. V. m. Ziff. 4.4.2 MaRisk; „Basel III"; vgl. auch *Behringer*, in: Behringer, Compliance KMU, S. 257 ff.

Diese können sich aus diversen inländischen, ausländischen, unionsrechtlichen und internationalen Rechtsvorschriften ergeben, die im Rahmen der CRA systematisch und regelmäßig erfasst und analysiert werden.[37] Im Ergebnis sollen die organisatorischen Grundlagen sowie der Anwendungsbereich festgelegt und Aufgaben zugeordnet werden, damit auf der Basis angemessene CMS-Elemente (Ziff. 2.2–2.4) entwickelt und umgesetzt werden. Für Einzelheiten zur Erstellung und Durchführung der CRA wird auf den DICO Spezialstandard verwiesen.

2.1.3 Organisatorische Grundlagen

Die grundlegenden Bestimmungen zum CMS sollen von der Unternehmensleitung festgelegt und in geeigneter Form als organisatorische Grundlagen dokumentiert werden.[38] Diese Festlegung kann in Gestalt eines Dokuments oder in aufeinander abgestimmten Einzeldokumenten erfolgen. Die Kohärenz mit anderen Governance-Dokumenten (z. B. für die Bereiche „Risiko“ oder „Strategie“) soll sichergestellt werden. Folgende Aspekte sollen bei der Konzipierung der organisatorischen Grundlagen berücksichtigt werden:[39]

- Ziele und Aufgaben des CMS (Ziff. 1.1);
- Art und Umfang der Compliance-Dokumentation (Ziff. 1.2.5);
- finanzielle und personelle Ressourcen, die für das CMS zur Verfügung gestellt werden (Ziff. 2.1.1);
- Methodik und Turnus der Compliance-Risiko-Analyse (Ziff. 2.1.2);
- Anwendungsbereich des CMS (Ziff. 2.1.4) und Definition seiner Elemente (Ziff. 2.2–2.4);
- Aufgaben- und Rollenbeschreibungen zur Sicherstellung von Compliance und Implementierung des CMS auf Ebene der Leitung, der Compliance-Funktion und der operativ Verantwortlichen;
- Verpflichtung jeder Unternehmenseinheit und aller Unternehmensmitglieder, die Regeleinhaltung in ihren Bereichen sicherzustellen (Ziff. 2.1.5);
- Einrichtung und Ausgestaltung der Compliance-Funktion (Ziff. 2.1.5), einschließlich ihrer Schnittstellen zu anderen Unternehmensfunktionen, wie Risikomanagement oder interner Revision (Ziff. 1.2.4);
- Rolle von Verhaltenskodex und Compliance-Richtlinien (Ziff. 2.2.1);
- Berichtslinien und Frequenzen für die Compliance-Berichterstattung (Ziff. 2.4.3).

In festgelegten Zeitabschnitten sowie bedarfsabhängig soll eine Aktualisierung der organisatorischen Grundlagen erfolgen.

2.1.4 Anwendungsbereich des CMS

Im Rahmen des CMS soll die Regeleinhaltung innerhalb eines risikoadäquat bestimmten sachlichen und organisatorischen Anwendungsbereichs sichergestellt und überwacht werden. Dieser soll klar festgelegt werden; abhängig von der Größe, Struktur und Komplexität des Unternehmens variiert der Anwendungsbereich.[40]

37 Ziff. 4.1 und 4.4 ISO 37301; *Tabbert*, CCZ 2020, 46 (47 f.); Bei Finanzdienstleistungsunternehmen müssen zusätzlich die möglichen Auswirkungen von Änderungen des Rechtsumfeldes (Rechtsänderungsrisiken) berücksichtigt werden (vgl. § 29 Abs. 2 S. 2 VAG; MaGo Rn. 91; MaComp BT 1.2.2, Ziff. 6). Siehe auch DICO Standard 09 „Compliance-Risiko-Analyse“.

38 *Pauthner*, in: Ghassemi-Tabar/Pauthner/Wilsing, Kap. 1, Rn. 413 ff.; *Vetter*, in: Wecker/van Laak, S. 45-46; *Makowicz*, in: Makowicz, Kap. 1-10, Nr. 4.3; *Löffler/Ahammer*, in: Barbist/Ahammer/Fabian/Löffler, S. 36-37; *Montag*, S. 47 ff.; *Schulz*, BB 2017, 1475 (1479 ff.); *Schulz*, BB 2019, 579 (580 ff.).

39 Weitere Beispiele in Ziff. 5.2 ISO 37301; *Zentes*, S. 173 ff.; *Grützner/Boerger/Momsen*, CCZ 2018, 50 (59 ff.); *Dittmers*, S. 144 ff.

40 In größeren Unternehmen werden regelmäßig einzelne Compliance-Themenfelder von gesonderten (Teil-) CMS abgedeckt (z. B. Steuern, technische Compliance, Datenschutz etc.); *Wiedmann/Greubel*, CCZ 2019, 88 (90); *Makowicz*, BB 2018, 556 (559 f.).

Bei der Bestimmung:

- des **sachlichen Anwendungsbereichs** soll insbesondere eine Festlegung der Zuständigkeiten für die wesentlichen Compliance-Themenfelder erfolgen, die im Rahmen des CMS gesteuert werden, und die Abgrenzung und Schnittstellen zu weiteren Managementsystemen[41] und Unternehmensfunktionen[42] mit einer klaren Zuständigkeitszuweisung durch die Unternehmensleitung (Delegation) definiert werden; dabei soll sichergestellt werden, dass insbesondere die im Rahmen der Compliance-Risiko-Analyse (Ziff. 2.1.2) identifizierten Compliance-Themenfelder klar adressiert sind;

- des **organisatorischen Anwendungsbereichs** des CMS soll – soweit nach dem konkreten Unternehmensaufbau relevant – insbesondere geregelt werden, welche Unternehmensteile bzw. welche Konzerngesellschaften umfasst sind und wie nicht-konsolidierte Beteiligungsunternehmen sowie gesellschafts- bzw. länderübergreifende Geschäftstätigkeiten zugeordnet werden.[43]

2.1.5 Aufgabenverteilung, insbes. Compliance-Funktion

Die Aufgaben zur Umsetzung des CMS sollen einzelnen Unternehmenseinheiten bzw. Funktionsträgern und den sonstigen Unternehmensmitgliedern unter Berücksichtigung der Größe, Struktur und Komplexität des Unternehmens in dokumentierter Form zugewiesen werden.[44]

Die nachfolgende Aufstellung soll lediglich als Beispiel verstanden werden; andere Modelle können ebenfalls umgesetzt werden, soweit sie nach Größe, Struktur und Komplexität des Unternehmens adäquat sind.[45]

- **Unternehmensleitung**: Der Unternehmensleitung kommt die entscheidende Rolle für das CMS zu (Ziff. 2.1.1).[46]

- **Aufsichtsrat:** Unternehmen, die über einen Aufsichtsrat verfügen, sollen dessen Rolle bei der Ausgestaltung des CMS, insbesondere bei der Berichterstattung sowie für den Fall, dass sich Compliance-Vorwürfe gegen Mitglieder der Unternehmensleitung richten, berücksichtigen.[47]

- **Mittleres Management und sonstige Führungskräfte** sollen das CMS aktiv anwenden und unterstützen. Dazu sollen sie Vorbild für Compliance sein und die Unternehmenswerte in besonderer Weise vorleben. Sie sollen ferner die ihnen unterstehenden Unternehmensmitglieder für die Regeleinhaltung sensibilisieren, ihnen Handlungsorientierung geben und sicherstellen, dass die CMS-Elemente in ihrem Verantwortungsbereich auf die spezifischen Prozesse und Risiken angepasst werden und die definierten Kontrollprozesse wirksam sind. Sie sollen zudem fortlaufend und vertrauensvoll mit der Compliance-Funktion kooperieren.[48]

---

41 Z. B. Risiko- oder Qualitätsmanagement etc.

42 Z. B. Personalabteilung, interne Revision, Audit etc.

43 *Makowicz*, in: Makowicz, Kap. 1-10, Nr. 4.2.2.

44 *Behringer*, in: Behringer, Compliance KMU, S. 247 ff.; *Hastenrath*, CB 2017, 325 (326 f.)

45 *Bürkle*, in: Hauschka/Moosmayer/Lösler, § 36, Rn. 76 ff; *Grüninger/Butscher*, in: Wieland/Steinmeyer/Grüninger, Kap. 1.5.4, Rn. 32 ff.; *Bicker*, ZWH 2013, 473 (473 ff.); *Schneider*, ZIP 2016, S070 (S071); *Habersack*, AG 2014, 1 (3 ff.); *Hoffmann/Schieffer*, NZG 2017, 401 (402 f.); *Laue/Brandt*, BB 2016, 1002 (1006 f.); *Merkt*, ZIP 2014, 1705 (1711 ff.).

46 Neubürger"-UrtBegr. S. 15, siehe Fn. 33; Principle 2 UKBA; Ziff. II. A. ECCP; *Behringer*, in: Behringer, Compliance kompakt, S. 281.

47 Empfehlung D.6 DCGK; *Eckert*, S. 58; *Behringer*, in: Behringer, Compliance kompakt, S. 292 ff.; *Bachmann*, COMPLY. 4/18, 60 (61 ff.); *Kremer/Klahold*, in Krieger/Schneider, Handbuch der Managerhaftung, Rn. 25.18; *Eichner/Leukel*, AG 2020, 513 (515 ff.).
Siehe auch DICO Leitlinie L03 – Compliance-Leitfaden für den Aufsichtsrat.

48 Siehe auch DICO Kompendium „Compliance als Führungsaufgabe – Ein Kompendium von Werkzeugen, Methoden und innovativen Ansätzen".

- **Alle Unternehmensmitglieder:** Alle Unternehmensmitglieder sollen die in ihren Bereichen bestehenden Regeln kennen und ausreichend zu deren Anwendung geschult sein. Sie sollen ein Verständnis dafür entwickeln, neue oder bislang unbekannte Compliance-Risiken und Hinweise auf Regelverstöße oder Auffälligkeiten, über die sie Kenntnis erlangen, transparent zu machen (sog. „Speak-up-Kultur"). Sie sollen ferner die grundlegende Funktionsweise des CMS kennen und in der Lage sein, die sie betreffenden CMS-Elemente entsprechend zu nutzen und umzusetzen.[49] Dies soll auf Basis konkreter Rollen- und Aufgabenbeschreibungen erfolgen. Ziel ist, dass die Unternehmensmitglieder aus eigener Motivation und Überzeugung in ihrem Verantwortungsbereich zur Compliance und zur angemessenen Umsetzung des CMS beitragen. Dabei gilt: Je besser das CMS von den operativ tätigen Unternehmensmitgliedern verstanden und umgesetzt wird, desto mehr kann sich die Compliance-Funktion auf Gestaltungs-, Steuerungs- und Kontrollaufgaben sowie auf wesentliche Einzelfragen konzentrieren.

- **Compliance-Funktion:** Die Zuständigkeit unterhalb der Unternehmensleitung für die Entwicklung, Ausgestaltung und Umsetzung des CMS soll in ihrem Kern bei der Compliance-Funktion liegen, die zur Erfüllung dieser Kernaufgaben mit anderen Funktionen und Abteilungen zusammenarbeitet.[50] Für die identifizierten Compliance-Themenfelder sollen von der Compliance-Funktion möglichst konkrete Vorgaben und Handlungspflichten definiert werden, die in den relevanten Organisationseinheiten und -bereichen bekannt gemacht werden sollen und deren Einhaltung durch geeignete Prozesse sichergestellt werden soll.[51] Bei der Ausgestaltung der Compliance-Funktion sollen folgende Faktoren umgesetzt werden:[52]

  - **Unabhängige und angemessene Stellung:** Der Compliance-Funktion soll für die Gewährleistung der Wirksamkeit des CMS (Ziff. 1.2.3) eine ausreichende Unabhängigkeit von anderen Funktionen/Abteilungen/der Unternehmensleitung gewährt werden. Dies soll auch die Einbeziehung in strategische und operative Entscheidungsprozesse umfassen.[53]

  - **Angemessene Ressourcen:** Die Compliance-Funktion soll mit angemessenen finanziellen und personellen Ressourcen ausgestattet werden, was zu Effektivität und Effizienz (Ziff. 1.2.3) des CMS beitragen soll.[54]

  - **Erforderliche Kompetenzen:** Die Ausstattung der Compliance-Funktion mit erforderlichen Zugängen zu Personen und Informationen (z. B. internen Berichten), Qualifikation und Kompetenz von personellen Ressourcen soll so weit gehen, dass diese die Funktionsfähigkeit des CMS sicherstellen kann.[55]
    Im Übrigen wird auf den DICO Spezialstandard über die Ausgestaltung der Compliance-Funktion verwiesen.

---

49 *Daum*, in: Bay/Hastenrath, Kap. 3, Rn. 67; Frankenberger, COMPLY. 4/19, 34 (34 f.).

50 Ziff. 5.3.2 ISO37301; „Neubürger"-UrtBegr. S. 15, siehe Fn. 33; § 3 Abs. 1 Nr. 2 VerSanG-E; Ziff. 2.4 UKBA; *Klahold*/*Lochen*, in: Hauschka/Moosmayer/Lösler, § 37, Rn. 28 ff.; s. a. *Makowicz*, in: Makowicz, Kap. 1-10, Nr. 4.4.2; *Volz*, in: Teichmann, Kap. 1, Rn. 44 ff.; *Dittmers*, S. 161 ff.

51 *Hoffmann*/*Schieffer*, NZG 2017, 401 (404 ff.).

52 Ziff. II. B. ECCP.

53 Ziff. II. B. ECCP: Das US DoJ fasst diese Anforderung unter dem Begriff „Stature" zusammen.

54 *Volz*, in: Teichmann, Kap. 1, Rn. 42; *Eckert*, S. 44; *Klahold*/*Lochen*, in: Hauschka/Moosmayer/Lösler, § 37, Rn. 46.

55 *Klahold*/*Lochen*, in: Hauschka/Moosmayer/Lösler, § 37, Rn. 57.

Andere Abteilungen/Funktionen: Es soll ebenfalls festgelegt werden, welche Themen der Verantwortung anderer Abteilungen/Funktionen zugeordnet werden und welche konkreten Aufgaben bei der Überwachung des CMS andere Abteilungen/Funktionen übernehmen sollen.[56] Entscheidend ist, dass in der Gesamtschau alle in der CRA identifizierten wesentlichen Compliance-Themenfelder (Ziff. 2.1.2) klar zugeordnet und effektiv adressiert werden.

2.2 Vorbeugen (Prevent)

Die folgenden CMS-Elemente sollen nach ihrer schwerpunktmäßigen Zielsetzung der Säule „Prevent" zugeordnet werden:

2.2.1 Verhaltenskodex und Compliance-Richtlinien

Der Verhaltenskodex soll auf den Unternehmenswerten (Ziff. 1.2.1) basieren und das Bekenntnis der Unternehmensleitung zu Compliance (Ziff. 2.1.1) in konkrete Handlungsanweisungen für die Unternehmensmitglieder übersetzen.[57] Inhaltlich soll der Verhaltenskodex die Ergebnisse der CRA (Ziff. 2.1.2) berücksichtigen. Er soll um Verweise auf weiterführende themenspezifische Compliance-Richtlinien ergänzt werden, soweit solche im Unternehmen bestehen.[58]

Der Verhaltenskodex soll allen Unternehmensmitgliedern und relevanten Dritten zugänglich gemacht und in Compliance-Schulungen erläutert werden.[59] Damit sollen das Verständnis seiner Bestimmungen und zugleich ihre Akzeptanz gefördert werden. Der Verhaltenskodex soll schließlich einer fortlaufenden Aktualisierung und Verbesserung unterliegen und in das allgemeine CMS-Kommunikationskonzept integriert werden.[60]

Für die Einzelheiten der Ausgestaltung des Verhaltenskodex wird auf den DICO Spezialstandard verwiesen.

2.2.2 Beratung

Das CMS soll Beratungsangebote zu relevanten Compliance-Themenfeldern bereitstellen. Die Beratung soll dabei über geeignete Kanäle erfolgen, z. B. durch persönliche Ansprechpartner und Online-Angebote im Intranet (FAQ-Listen, Leitfäden etc.), welche jedem Unternehmensmitglied bekannt und leicht zugänglich sind.[61] Das Beratungsangebot soll in Bezug auf die Compliance-Themenfelder umfassend und aktuell sein; die abgegebenen Bewertungen und Empfehlungen sollen qualitativ hochwertig, konkret und praktikabel sein. Die Compliance-Funktion soll die Qualität und Konsistenz der Beratungspraxis durch geeignete Maßnahmen sicherstellen, wie z. B. durch:

- Vorgabe einheitlicher Beratungsleitlinien;
- Weiterbildung der zuständigen Unternehmensmitglieder oder auch
- entsprechende Feedbackmöglichkeiten der Unternehmensmitglieder.[62]

56 *Klahold/Lochen*, in: Hauschka/Moosmayer/Lösler, § 37, Rn. 68 ff.
57 Ziff. 2.4 UKBA; Ziff. I. B. ECCP; Daum, in: Bay/Hastenrath, Kap. 3, Rn. 50 ff.; Pauthner, in: Ghassemi-Tabar/Pauthner/Wilsing, Kap. 1, Rn. 601 ff.; *Iglhauser/Schönauer*, in: Sartor/Freiler-Waldburger, S. 54 ff.
58 *Löffler/Ahammer*, in: Barbist/Ahammer/Fabian/Löffler, S. 34 f.
59 Der Verhaltenskodex soll in der Hauptsprache des Unternehmens zur Verfügung gestellt und ggf. in unterschiedliche Sprachversionen übersetzt werden.
60 *Vetter*, in: Wecker/van Laak, S. 44.
61 *Klahold/Lochen*, in: Hauschka/Moosmayer/Lösler, § 37, Rn. 58 f.
62 *Fissenewert*, Compliance Mittelstand, S. 219 ff.

Für die erbrachte Beratung gilt in besonderem Maße die Anforderung einer vollständigen und aussagekräftigen Dokumentation (Ziff. 1.2.5).

2.2.3 Kommunikation und Schulungen

Für die Förderung der Ziele und Erfüllung seiner Aufgaben (Ziff. 1.1) soll im Rahmen des CMS ein effektives Kommunikationskonzept erarbeitet und umgesetzt werden.[63] Die Compliance-Kommunikation spielt im Rahmen des CMS eine entscheidende Rolle, da zu seinen Hauptzielen die Einhaltung von Regeln (Ziff. 1.1.1) und die Schaffung einer nachhaltigen Compliance-Kultur (Ziff. 1.2.1) gehören.[64] Beide erwähnten Ziele betreffen das Verhalten der Unternehmensmitglieder, welches von Informationen beeinflusst wird, die über verschiedene Kommunikationskanäle verbreitet werden.[65] Das Kommunikationskonzept soll von der Compliance-Funktion (Ziff. 2.1.5) unter Beteiligung der Unternehmensleitung (Ziff. 2.1.1) sowie der Kommunikationsabteilung entwickelt werden. Die im Unternehmen bestehenden Kommunikationswege und -maßnahmen sollen mitverwendet werden (Ziff. 1.2.4), um prozessbezogene Synergien und Optimierungseffekte zu nutzen. Bezüglich der möglichen Compliance-Kommunikationskonzepte und -maßnahmen wird auf den DICO Spezialstandard verwiesen.

Schulungen sollen entsprechendes Wissen über Compliance-Themenfelder in diversen Bereichen sowie Kenntnis im Umgang mit ihnen und dem CMS vermitteln.[66] Sie sollen daher der Compliance-Sensibilisierung und der Förderung einer nachhaltigen Compliance-Kultur (Ziff. 1.2.1) dienen. Im Rahmen der Schulungen können der Verhaltenskodex (Ziff. 2.2.1) sowie das CMS als solches erläutert werden. Die Konzeption, Form, Häufigkeit und Inhalte der Compliance-Schulungen sollen im Sinne der Angemessenheit (Ziff. 1.2.2) stets unter Berücksichtigung der Größe, Struktur und Komplexität des Unternehmens festgelegt werden.[67] Im Sinne der Flexibilität (Ziff. 1.2.2) soll eine fortlaufende Anpassung erfolgen. Im Hinblick auf die konkreten Möglichkeiten der Ausgestaltung von Compliance-Schulungen wird auf den DICO Spezialstandard verwiesen.

2.2.4 Kompetenzsicherung

Fehlende oder lückenhafte Kompetenz kann nicht nur Ursache für Schlechtleistung, sondern auch für Compliance-Verstöße sein. Die für die Ausübung der zugewiesenen Aufgaben erforderliche Kompetenz aller Unternehmensmitglieder sollte daher fortlaufend geprüft werden.[68]

Ein wichtiges CMS-Element liegt dabei auf der Schnittstelle zwischen Personal- und Compliance-Abteilung. Insbesondere bei der Auswahl und Aufgabenzuweisung von bzw. an Mitglieder(n) der Unternehmensleitung und Führungskräfte(n) sowie für Unternehmensmitglieder in besonders risikoexponierten Positionen sollen daher die Relevanz von Compliance, ihre Bedeutung für die Unternehmenswerte und die spezifischen Aufgaben des (künftigen) Stelleninhabers in Bezug auf das CMS thematisiert werden.

63 Ziff. 7.2, 7.3 und 7.4 ISO 37301; „Neubürger"-UrtBegr. S. 5, siehe Fn. 33; Principle 5 UKBA; Ziff. I. C. ECCP; *Löffler/Ahammer*, in: Barbist/Ahammer/Fabian/Löffler, S. 37 f.; *Makowicz*, in: Makowicz, Kap. 1-10, Nr. 4.5.3

64 *Vetter*, in: Wecker/van Laak, S. 44; Löffler/Ahammer, in: Barbist/Ahammer/Fabian/Löffler, S. 32 ff.

65 *Bauer/Sartor*, in: Sartor/Freiler-Waldburger, S. 74 ff.

66 Ziff. 7.2.3 ISO 37301; Principle 5 UKBA; Ziff. I. C. ECCP; *Schmahl*, in: Makowicz, Kap. 2-70, Nr. 2.1 ff.; *Klahold/Lochen*, in: Hauschka/Moosmayer/Lösler, § 37, Rn. 60 ff. Siehe auch DICO Standard 05 – Zielgruppenorientiertes Schulungskonzept.

67 Zentes, S. 201 ff.

68 Ziff. 7.2 ISO19600; „Neubürger"-UrtBegr. S. 5; Ziff. 2.4 UKBA; Ziff. II. B. ECCP; vgl. auch *Gösswein*, CCZ 2017, 43 (43 ff.).

Zudem soll ein Prozess definiert werden, inwieweit diese Erörterung (ggf. unterstützt durch Selbstauskünfte und, soweit geboten und rechtlich zulässig, durch sog. Background Checks) im Rahmen des regulären Einstellungs- und Beförderungsprozesses erfolgen kann und unter welchen Voraussetzungen die Compliance-Funktion hinzuzuziehen ist (etwa sofern es in früheren Positionen zu Compliance-Vorfällen gekommen ist oder begründete Zweifel an der Integrität bzw. am Bekenntnis zu Compliance bestehen). Organisatorisch (Ziff. 2.1.3) soll insbesondere geregelt sein:

- welche Abteilung[69] für Durchführung und Überwachung der Kompetenzprüfung zuständig ist;
- wann und wie die Kompetenzprüfung erfolgen soll und welche Maßnahmen im Falle der Feststellung von Mängeln durchgeführt werden.

2.2.5 Themenspezifische CMS-Elemente

Themenspezifische CMS-Elemente sollen nach Bedarf entwickelt und umgesetzt werden. Die Themen sollen stets auf der Basis der CRA (Ziff. 2.1.2) bestimmt und die Prozessausgestaltung im Sinne der Angemessenheit und Flexibilität an Größe, Struktur und Komplexität des Unternehmens ausgerichtet und bei Veränderungen des Geschäftsportfolios oder des Risikoprofils dynamisch angepasst werden (Ziff. 1.2.2). Zu diesen themenspezifischen CMS-Elementen zählen etwa die Überprüfung von Geschäftspartnern, Prozesse zum Umgang mit Geschenken, Unterhaltung und Bewirtung, Sponsoring und Spenden, die Einhaltung des Datenschutzes, kartellrechtliche Vorgaben zum Verhalten in Branchenverbänden, die Prüfung von Sanktionslisten und Maßnahmen aus dem Bereich der Exportkontrolle sowie Compliance-bezogene Prüf- und Integrationsprozesse für M&A-Transaktionen.[70]

Die Verantwortung für diese Aufgaben und ihre prozessseitige Implementierung soll dabei innerhalb der Compliance-Funktion oder anderen Fachabteilungen/Funktionen zugeordnet werden (Ziff. 2.1.5). Soweit im Kern operative Prozesse und Aufgaben betroffen sind, soll die primäre Zuständigkeit bei den jeweiligen Abteilungen (etwa Einkauf oder Vertrieb bei der Geschäftspartnerprüfung) verbleiben.

2.3 Entdecken (Detect)

CMS-Elemente, die im Schwerpunkt dazu dienen, Schwachstellen des CMS zu identifizieren und Compliance-Verstöße aufzudecken, sollen in der Säule „Detect“ angesiedelt werden. In dieser Säule sollen auch Prozesskontrollen verortet werden.

2.3.1 Fortlaufende Überwachung (Compliance-Kontrollen)

Das CMS soll Elemente enthalten, mit denen die Einhaltung von Regeln in den identifizierten Compliance-Themenfeldern fortlaufend überwacht wird.[71] Im Sinne des Prinzips der Integration (Ziff. 1.2.4) sollen die Prozesse des CMS mit dem internen Kontrollsystem ineinandergreifen (evtl. sogar integriert werden) und die Schnittstellen klar definiert werden.[72]

---

69 In der Regel werden hier eine Zuweisung an die Personalabteilung, eine enge Abstimmung mit der Compliance Abteilung und eine Aufnahme in das Regelprüfprogramm der internen Revision zweckmäßig sein.

70 Siehe auch DICO Standard 01 – Geschäftspartner-Compliance, DICO Leitlinien und Arbeitspapiere „Sanktionslistenprüfungen und Exportkontrolle“ (L08, A07 und A06). Die aufgeführten DICO Spezialstandards decken nicht alle themenspezifischen CMS-Elemente ab und werden fortlaufend ergänzt.

71 *Klahold/Lochen*, in: Hauschka/Moosmayer/Lösler, § 37, Rn. 82; *Fissenewert*, Praxishandbuch CMS, S. 27 ff.

72 Ziff. 6.4, 8 und 9 ISO 37301; *Weiß/Koch/Osterloh*, in: Jäger/Rödl/Campos Nave, S. 75 ff; *Makowicz*, in: Makowicz, Kap. 1-10, Nr. 4.6.

2.3.2 Hinweisgebersystem und Aufklärung von Verdachtsfällen

Im Rahmen des CMS soll sichergestellt werden, dass alle Unternehmensmitglieder auf Verdachtsfälle und bereits erfolgte Unregelmäßigkeiten geschützt und anonym hinweisen können.[73] Eingehende Informationen sollen sorgfältig verifiziert werden, bevor sie als Initialpunkt für die Durchführung von internen Untersuchungen verwendet werden. Die Ausgestaltung von Hinweisgebersystemen soll an die Größe, Struktur und Komplexität des Unternehmens angepasst werden (Ziff. 1.2.2).[74] Darüber hinaus sollen Hinweisgebersysteme gleichzeitig in die Konzeption der Compliance-Kommunikation (Ziff. 2.2.3) aufgenommen werden. Hinsichtlich der Ausgestaltungsmöglichkeiten von Hinweisgebersystemen wird auf den DICO Spezialstandard verwiesen.[75]

Im Rahmen des CMS soll Verdachtsfällen in Unternehmen nachgegangen werden.[76] Verdachtsfälle können sich entweder durch konkrete Hinweise von Unternehmensmitgliedern oder Dritten oder durch spezifische Compliance-Kontrollen[77] bzw. Revisionsprüfungen ergeben. Unternehmen sollen für die Durchführung von internen Untersuchungen entweder eigene Kapazitäten und Teams bereithalten oder mit sorgfältig gewählten externen Anbietern eng zusammenarbeiten.[78] Ziel von internen Untersuchungen soll die Aufklärung des Sachverhaltes und die angemessene Reaktion (Ziff. 2.4) sein. Hinsichtlich der Einzelheiten zur Durchführung von internen Untersuchungen wird auf den DICO Spezialstandard verwiesen.[79]

2.4 Reagieren (Respond)

Ein wirksames CMS erfordert konsequente Reaktionen auf Compliance-Verstöße (Ziff. 2.4.1–2.4.2), identifizierte Prozess- oder Kontrollschwächen und andere relevante Entwicklungen.[80] Sowohl aus den präventiven als auch aus den aufklärenden bzw. identifizierenden Elementen des CMS kann sich dabei konkreter Handlungsbedarf ergeben, der – etwa im Bereich von Personalmaßnahmen – regelmäßig der Einbindung der Unternehmensleitung oder anderer Abteilungen bedarf. Das Berichtswesen (Ziff. 2.4.3) soll als Basis für jede Form einer von der Unternehmensleitung getragenen Reaktion schwerpunktmäßig ebenfalls der dritten Säule „Respond“ zugeordnet werden, genau wie das Krisenmanagement (Ziff. 2.4.4).

2.4.1 Interne Sanktionierung

Nachgewiesene Compliance-Verstöße darf das Unternehmen schon aus Rechtsgründen nicht tolerieren. Unternehmen sollen daher im Rahmen der organisatorischen Grundlagen (Ziff. 2.1.3), und/oder des Verhaltenskodexes sowie der Compliance-Richtlinien (Ziff. 2.2.1) ein unternehmensweit einheitliches Sanktionierungskonzept entwickeln,[81] das zu einer Unternehmens- und Compliance-Kultur (Ziff. 1.2.1) beitragen soll, in der Compliance-Verstöße nicht toleriert und das Aufdecken von Compliance-Verstößen gefördert werden.

---

73 Ziff. 8.3 ISO 37301; Ziff. 2.3 UKBA; Ziff. I. D. ECCP; *Waldzus*, in: Behringer, Compliance kompakt, S. 233 ff.

74 Empfehlung A.2 DCGK; Ziff. 1.7 UKBA; Näheres dazu in der EU-Richtlinie zum Schutz von Hinweisgebern (EU) 2019/1937, die zum Zeitpunkt der Fertigstellung des vorliegenden Standards noch nicht umgesetzt wurde.

75 Siehe auch DICO Standard 11 – Hinweisgebersysteme.

76 „Neubürger“-UrtBegr. S. 13, siehe Fn. 33; *Klahold/Lochen*, in: Hauschka/Moosmayer/Lösler, § 37, Rn. 89 ff.; *Lohmeier/Shahhosseini*, in: Umnuß, Kap. 7, Rn. 1 ff.; Eckert, S. 56 f.

77 Vgl. zu sog. Compliance Audits: *Kremer/Klahold*, in: Krieger/Schneider, Handbuch Managerhaftung, Rn. 25.40.

78 Ziff. 10.1 ISO 37301; § 16 und § 17 VerSanG-E; Principle 6 UKBA; Ziff. III. B. ECCP.

79 Siehe auch DICO Standard 04 – Interne Untersuchungen.

80 Frank, Compliance Week, 11.03.2020, https://www.complianceweek.com/opinion/10-tips-to-meet-government-expectations-of-remediation-programs/28584.article (abgerufen am 14.12.2020).

81 Ziff. 1.7 UKBA.

Besonderes Augenmerk soll auf der adäquaten, konsequenten und nicht-diskriminierenden Umsetzung der festgelegten disziplinarischen Maßnahmen gelegt werden.[82]

Die Unternehmensleitung soll sich dabei ausdrücklich zu der konsequenten Verfolgung von Compliance-Verstößen und zur Verhängung angemessener Sanktionen bekennen.[83] Das Sanktionierungskonzept soll:

- abteilungsübergreifend festgelegt sein (insbesondere Compliance-, Rechts- und Personalabteilung);
- die Kriterien definieren, die zur Ermittlung einer angemessenen Sanktion heranzuziehen sind und
- interne Zuständigkeiten und Verantwortungsbereiche klar definieren.

Aufgetretene Compliance-Verstöße und die infolgedessen vom Unternehmen verhängten Disziplinarmaßnahmen sollen dokumentiert werden (Ziff. 1.2.5).

2.4.2 Sonstige Remediation-Maßnahmen

Neben Disziplinarmaßnahmen kann sich in der Aufarbeitung von Compliance-Verstößen sowie von durch Compliance-Kontrollen (Ziffer 2.3.1) identifizierten Prozess- oder Kontrollschwächen weiterer Handlungsbedarf zeigen. Zu nennen sind hier beispielsweise die Überarbeitungen des Regelwerks, Anpassung/Entwicklung einzelner Organisationseinheiten, Prozessverbesserungen und Schulungsmaßnahmen für bestimmte Zielgruppen. Die getroffenen Maßnahmen sollen dokumentiert, mit klaren Verantwortlichkeiten versehen und die Umsetzung durch die Compliance- Funktion nachverfolgt werden.

2.4.3 Berichterstattung

Die Compliance-Berichterstattung dient dazu, die Unternehmensleitung regelmäßig über Inhalte und die Funktionsweise des CMS zu informieren, so dass sie ihren Aufsichtspflichten für die an die Compliance-Funktion delegierte Zuständigkeit zur Sicherstellung eines effektiven CMS nachkommen kann.[84] Dabei sollen die organisatorischen Grundlagen (Ziff. 2.1.3) Regelungen zur angemessenen, zeitnahen und regelmäßigen Compliance-Berichterstattung an die Unternehmensleitung und ggf. die Aufsichtsorgane enthalten.[85] Die Basis dafür soll eine interne unternehmensweite Compliance-Berichterstattung sein, die die kontinuierliche Entwicklung des CMS in allen Unternehmensteilen (Teilkonzerne, Tochtergesellschaften, Länder, Regionen etc.) transparent macht.

Zu den wesentlichen Elementen einer regelmäßigen Compliance-Berichterstattung gehören:

- relevante Rechtsentwicklungen (z. B. Rechtsänderungen, Compliance-Anforderungen);
- Ergebnisse der CRA, insbesondere identifizierte Compliance-Themenfelder (Ziff. 2.1.3);
- themenspezifische CMS-Elemente (Ziff. 2.2.5)[86] und entsprechende Aktivitäten;
- Evaluation der Compliance-Funktion im Hinblick auf unabhängige und angemessene Stellung, angemessene Ressourcen, erforderliche Kompetenzen etc. (Ziff. 2.1.5);

82 Wird auch als sog. zero-tolerance policy in Bezug genommen, vgl. Principle 2.3 UKBA; Ziff. II. C. ECCP; *Wiedmann/Greubel*, CCZ 2019, 88 (91); *Schulz*, BB 2017, 1475 (1481).

83 Principle 2.3 und 5.4 UKBA; vgl. Ziff. II. A. ECCP; *Vetter*, in: Wecker/van Laak, S. 43; *Makowicz*, in: Makowicz, Kap. 1-10, Nr. 4.1.1; *Löffler/Ahammer*, in: Barbist/Ahammer/Fabian/Löffler, S. 32 ff.

84 Ziff. 5 ISO 37301; Ziff. II. B. ECCP; *Daum*, in: Bay/Hastenrath, Kap. 3, Rn. 35 f.; *Wiedmann/Greubel*, CCZ 2019, 88 (90 f.); *Kunkel/Kunkel*, jurisPR-Compl 2/2017 Anm 3; *Rau*, in: Schulz, Kap. 11, Rn. 24; Gomer, S. 115.

85 Ziff. 9.1.4 ISO 37301; Empfehlung D.3 DCGK; Principle 6 UKBA; Ziff. II. B. ECCP.

86 Vgl. DICO Standard 09 – Compliance Risikoanalyse (CRA), S. 29.

- festgestellte bzw. vermutete Regelverstöße (nebst Untersuchungsergebnissen, personellen Konsequenzen sowie getroffenen Maßnahmen und Systemverbesserungen, Ziff. 2.4.1–2.4.2);[87]
- Ergebnisse der fortlaufenden Compliance-Überwachung (Ziff. 2.3.1), der regelmäßigen Systemevaluierung (Ziff. 2.5) und entsprechender Maßnahmen zur Verbesserung des CMS.

Dabei sollen folgende Formen vorgesehen werden:[88]

- Standardberichte: Sie sollen Informationen (einschließlich quantitativer und qualitativer Daten) in gleichbleibender Art, regelmäßig (z. B. jährlich oder quartalsweise) nach vorgegebenen Standards und Prozessen liefern.
- Bedarfs- oder Ad-hoc-Berichte: Sie sollen die Unternehmensleitung bei speziellen Sachverhalten informieren, z. B. beim Auftreten von Regelverstößen, Schwachstellen im CMS, wesentlichen neuen Compliance-Risiken oder Rechtsänderungen.[89]

Analog soll auf Ebene von Teilkonzernen, Tochtergesellschaften und Niederlassungen jeweils an die zuständige Unternehmensleitung über die für sie relevanten Themen berichtet werden.

2.4.4 Krisenmanagement

Im Rahmen des CMS oder des unternehmensweiten Krisenmanagementsystems soll ein Konzept für den Umgang mit Compliance-Krisen entwickelt werden.[90] Dort soll insbesondere festgehalten werden:

- wie eine Compliance-Krisensituation für das jeweilige Unternehmen definiert wird,
- welche internen und externen Maßnahmen ergriffen werden,
- wie die Krisensituation intern aufgearbeitet wird und
- was im Falle des Kontakts mit Externen zu beachten ist.

Zum Krisenmanagement sollen ferner Festlegungen und entsprechende Maßnahmen zur potenziellen Offenlegung des Verstoßes gegenüber Behörden sowie die mit dem Krisenfall verbundenen Berichtspflichten gehören, wenn diese nicht bereits im Rahmen der Compliance-Berichterstattung (Ziff. 2.4.3) berücksichtigt worden sind.[91] Darüber hinaus können situationsabhängig weitere risiko- und bedarfsbezogene Reaktions-Maßnahmen umgesetzt werden.[92] Hinsichtlich der Ausgestaltung des Compliance-Krisenmanagements wird auf den DICO Spezialstandard verwiesen.

2.5 Regelmäßige Systemevaluierung und fortlaufende Optimierung

Ist das CMS entsprechend geplant (Ziff. 2.1) und sind die einzelnen CMS-Elemente definiert und umgesetzt (Ziff. 2.2-2.4) worden, soll es als ein Managementsystem in regelmäßigen Zeitabständen (und nicht nur anlassbezogen) evaluiert werden.[93]

87 „Neubürger"-UrtBegr. S. 9, 15 und 19, siehe Fn. 33; vgl. DICO Standard 04 – Interne Untersuchungen , S. 36 f.
88 *Klahold*/*Lochen*, in: Hauschka/Moosmayer/Lösler, § 37, Rn. 52 ff.; *Fissenewert*, Praxishandbuch CMS, S. 160 ff.
89 *Schwarzbartl*/*Pyrcek*, S. 90.
90 Ziff. 10 ISO 37301; „Neubürger"-UrtBegr. S. 14 und 16, siehe Fn. 33; Principle 6 UKBA; Ziff. III. C. ECCP; Eckert, S. 59 f.; *Schwarzbartl*/*Pyrcek*, S. 87 f.
91 Vgl. § 17 VerSanG-E.
92 Vgl. § 15 Abs. 3 Nr. 7 VerSanG-E.
93 Ziff. 8 und 9 ISO 37301; „Neubürger"-UrtBegr. S. 14 (siehe auch S. 6, 9, 15 und 17), siehe Fn. 33; Ziff. 1.6 und Principle 6 UKBA; Ziff. III. A. ECCP; *Kahlenberg*/*Schäfer*/*Schieffer*, in: Busch/Hoven/Pieth/Rübenstahl, Kap. 33, Rn. 115 ff.; *Löffler*/*Ahammer*, in: Barbist/Ahammer/Fabian/Löffler, S. 38-39; *Bauer*/*Schwab*, in: Sartor/Freiler-Waldburger, S. 140 ff.; *Behringer*, in: Behringer, Compliance KMU, S. 262 f.; *Schmidt*/*Eibelshäuser*, COMPLY. 3/17, 20 (21 ff.)

Durch die Evaluierung soll sichergestellt werden, dass das CMS seine Ziele fördern und Aufgaben (Ziff. 1.1) erfüllen kann, d. h. insbesondere, dass es angemessen dimensioniert, im Anwendungsbereich adäquat definiert und wirksam (Ziff. 1.2.3) ist.[94] Die Evaluierung dient zugleich der Erfüllung der Überwachungspflicht der Unternehmensleitung.

Art und Häufigkeit der Evaluierungsmaßnahmen[95] sollen von der Größe, Struktur und Komplexität des Unternehmens abhängen. Die Evaluierung soll durch prozessunabhängige Stellen stattfinden. Dies können etwa unternehmensinterne (regelmäßig die Interne Revision oder auch die Compliance-Abteilung in Bezug auf Compliance-Themenfelder, die sie nicht unmittelbar selbst verantwortet) oder unternehmensexterne Prüfungsinstanzen (z. B. Wirtschaftsprüfer, Rechtsanwälte, sonstige unternehmensexterne Gutachter und Sachverständige) sein.

Mit der Evaluierung soll die fortlaufende Verbesserung des CMS verknüpft werden.[96] Hat sie ergeben, dass im Hinblick auf bestimmte CMS-Elemente (Ziff. 2.2–2.4) Optimierungsbedarf besteht, sollen diese umgehend verbessert werden.[97] Ein identifiziertes unzureichendes CMS-Element wird entsprechend anders geplant, anschließend umgesetzt und erneut geprüft. Damit wird die notwendige Qualitätssicherung in Bezug auf das CMS sichergestellt.

Optimierungspotenzial kann zudem durch Entwicklungen im Bereich der Digitalisierung realisiert werden. Soweit CMS-Elemente im Sinne der Prinzipien der Integration (Ziff. 1.2.4) und Dokumentation (Ziff. 1.2.5) automatisiert und durch den Einsatz von IT-Tools in ihrer Wirksamkeit verstärkt und vereinfacht werden können, erhöht dies gleichzeitig die Akzeptanz im Unternehmen.[98]

94 *Wiedmann/Greubel*, CCZ 2019, 88 (92); *Schlegel*, COMPLY. 3/18, 12 (13 ff.).

95 Maßnahmen zur Evaluierung der Wirksamkeit können insbesondere umfassen: Surveys/Fragebögen (z. B. zur Evaluierung der Wahrnehmung der Compliance-Kultur), Überprüfung der Umsetzung von Compliance-Maßnahmen (bspw. Richtlinien, Trainingsumsetzung, Prozesskontrollen etc.) sowie Datenanalysen und/oder Befragungen von Unternehmensmitgliedern und Dritten zur Überprüfung der Wirksamkeit relevanter Kontrollen.

96 Ziff. 9 ISO 37301; „Neubürger"-UrtBegr. S. 14 und 16, siehe Fn. 33; Ziff. III. A. ECCP; *Löffler/Ahammer*, in: Barbist/Ahammer/Fabian/Löffler, S. 38-39; *Fissenewert*, Praxishandbuch CMS, S. 167 ff.

97 *Eckert*, S. 60 f.

98 *Kahlenberg/Schäfer/Schieffer*, in: Busch/Hoven/Pieth/Rübenstahl, Kap. 33, Rn. 87 f.

3. REFERENZSTANDARDS

In diesem Standard wurden nachfolgende Referenzstandards berücksichtigt:

- DIN ISO 37301 (ex. 19600): Compliance Management Systems (Stand: Entwurf Juni 2020),
- DIN ISO 37001: Anti-Bribery Management Systems,
- IDW PS 980: Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen,
- DCGK: Deutscher Corporate Governance Kodex (in der Fassung vom 16.12.2019),
- UKBA: Leitlinien zum UK Bribery Act 2010 (The Bribery Act 2010 – Guidance),
- ECCP: Leitfaden des U.S. Department of Justice, Criminal Division, Evaluation of Corporate Compliance Programs (Stand: June 2020 Guidance).

4. BIBLIOGRAPHIE

4.1 Verwendete Literatur

Barbist, Johannes/*Ahammer*, Michael/*Fabian*, Tibor/*Löffler*, Helge (Hrsg.), Compliance in der Unternehmenspraxis, 2. Aufl., Wien 2015
Zit.: Bearbeiter, in: Barbist/Ahammer/Fabian/Löffler, S.

Bachmann, Bernhard, Compliance Management-Systeme als Mittel effektiver Kontrolle, COMPLY. 4/18, 60 ff.

Bay, Karl-Christian/*Hastenrath*, Katharina, Compliance-Management-Systeme, 2. Aufl., München 2016
Zit.: Bearbeiter, in: Bay/Hastenrath, Kap., Rn.

Behringer, Stefan (Hrsg.), Compliance für KMU. Praxisleitfaden für den Mittelstand, 2. Aufl., Berlin 2016
Zit.: Bearbeiter, in: Behringer, Compliance KMU, S.

Behringer, Stefan (Hrsg.), Compliance kompakt, Berlin 2010
Zit.: Bearbeiter, in: Behringer, Compliance kompakt, S.

Bicker, Eike, Corporate Compliance – Pflicht und Ermessen, ZWH 2013, 473 ff.

Bings, Sophie Luise, Änderungen des DCGK betreffen Compliance Management Systeme, CCZ 2017, 118 ff.

Busch, Markus/*Hoven*, Elisa/*Pieth*, Mark/*Rübenstahl*, Markus (Hrsg.), Antikorruptions-Compliance, Heidelberg 2020
Zit.: Bearbeiter, in: Busch/Hoven/Pieth/Rübenstahl, Kap., Rn.

Chen, Hui, Sieben Anzeichen für ineffektive Compliance-Programme, COMPLY. 2/18, 16 ff.

Dittmers, Claudia, Werteorientiertes Compliance-Management, Leipzig 2018

Ebner, Stephan M./*Leone*, Susanne, J.D., International Compliance – Deutsche Small and Medium Enterprises in den USA, CCZ 2020, 7 ff.

Eckert, Tilman, Praxiswissen Compliance, Freiburg 2014

Fissenewert, Peter, Compliance für den Mittelstand, 2. Aufl., München 2018
Zit.: Fissenewert, Compliance Mittelstand, S.

Fissenewert, Peter, Praxishandbuch internationale Compliance-Management-Systeme, Berlin 2015
Zit.: Fissenewert, Praxishandbuch CMS, S.

Frank, Jonny, 10 Tips to Meet Government Expectations of Remediation Programs, Compliance Week, 11.03.2020, https://www.complianceweek.com/opinion/10-tips-to-meet-government-expectations-of-remediation-programs/28584.article (abgerufen am 14.12.2020).

Frank, Jonny/*Kerley*, Annabel, Compliance Matters: Meeting SFO Expectations, New Law Journal UK, 01.05.2020, 13 f.

Frankenberger, Sabine, Die drei Ks des Integritäts- und Compliance-Managements, COMPLY. 4/19, 34 f.

Ghassemi-Tabar, Nima/*Pauthner*, Jürgen/*Wilsing*, Hans-Ulrich, Corporate Compliance, Düsseldorf 2016
Zit: Bearbeiter, in: Ghassemi-Tabar/Pauthner/Wilsing, Kap., Rn.

Gomer, Maxim, Die Delegation von Compliance-Zuständigkeit des Vorstands einer Aktiengesellschaft, Berlin 2020

Gösswein, Georg, Die Führungskräfte im Zentrum eines funktionierenden Compliance Management Systems, CCZ 2017, 43 ff.

Grunert, Eike, Verbandssanktionengesetz und Compliance-Risikoanalyse, CCZ 2020, 71 ff.

Grützner, Thomas/*Boerger*, Björn/*Momsen*, Carsten, Die „Dieselaffäre“ und ihre Folgen für Compliance-Management-Systeme – Evolution durch Einbeziehung des Bereichs Produkt Compliance in ein CMS (z. B. zum Zweck der Prävention produktbezogener Täuschungen), CCZ 2018, 50 ff.

Habersack, Mathias, Grund und Grenzen der Compliance-Verantwortung des Aufsichtsrats der AG, AG 2014, 1 ff.

Harz, Michael/*Weyand*, Raimund/*Reiter*, Julius F./*Methner*, Olaf/*Noa*, Daniel, Mit Compliance Wirtschaftskriminalität vermeiden, Stuttgart 2012

Hastenrath, Katharina, Das neue obiter dictum des BGH (Az: 1 StR 265/16): CMS im Unternehmen lohnt sich!, CB 2017, 325 ff.

Hauschka, Christoph/*Moosmayer*, Klaus/*Lösler*, Thomas (Hrsg.), Corporate Compliance. Handbuch der Haftungsvermeidung im Unternehmen, 3. Aufl., München 2016
Zit: Bearbeiter, in: Hauschka/Moosmayer/Lösler, §, Rn.

Hoffmann, Andreas C./*Schieffer*, Anita, Pflichten des Vorstandes bei der Ausgestaltung einer ordnungsgemäßen Compliance-Organisation, NZG 2017, 401 ff.

Jäger, Axel/*Rödl*, Christian/*Campos Nave*, José A. (Hrsg), Praxishandbuch Corporate Compliance, Weinheim 2009
Zit: Bearbeiter, in: Jäger/Rödl/Campos Nave, S.

Jenne, Moritz/*Martens*, Jan Henning, Compliance-Management-Systeme sind bei der Bußgeldbemessung nach § 30 OWiG zu berücksichtigen – Anmerkung zu BGH, Urteil vom 9.5.2017 – 1StR 265/16, CCZ 2017, 285 ff.

Jüttner, Markus, Die 42 der Compliance – Das Kriterium der Wirksamkeit eines Compliance Management Systems, CCZ 2018, 168 ff.

Krieger, Gerd/*Schneider*, Uwe H. (Hrsg.), Handbuch Managerhaftung, 3. Aufl., Köln 2017
Zit.: Bearbeiter, in: Krieger/Schneider, Handbuch Managerhaftung, Rn.

Kunkel, Carsten/*Kunkel*, Olga, Kein Schutz vor strafrechtlicher Haftung durch bloße Einführung eines Compliance Management Systems, jurisPR-Compl 2/2017 Anm 3.

Laue, Jens C./*Brandt*, Verena, Möglichkeiten und Grenzen des Outsourcing von Compliance-Aufgaben, BB 2016, 1002 ff.

Makowicz, Bartosz, Governance und Compliance, COMPLY. 3/17, 12 ff.

Makowicz, Bartosz, Integration neuer normativer, judikativer und administrativer Anforderungen in ein Compliance-Management-System, BB 2018, 556 ff.

Makowicz, Bartosz (Hrsg.), Praxishandbuch Compliance Management – Praxishandbuch Compliance, Köln 2020
Zit: Bearbeiter, in: Makowicz, Kap., Nr.

Martin, Stephen/*Ralston*, Toby, Best Practices for Developing and Executing a Successful Risk Assessment, Compliance and Ethics Professional Magazine 10/2019, 50 ff.

Merkt, Hanno, Compliance und Risikofrüherkennung in kleinen und mittleren Unternehmen, ZIP 2014, 1705 ff.

Minkoff, Andreas/*Sahan*, Oliver/*Wittig*, Petra (Hrsg.), Konzernstrafrecht, München 2020
Zit.: Bearbeiter, in: Minkoff/Sahan/Wittig, §, Rn.

Montag, Pia, Risikomanagement und Compliance im Mittelstand, Berlin 2016

Moosmayer, Klaus, Compliance Praxisleitfaden für Unternehmen, 3. Aufl., München 2015

Pyrcek, Andreas, Veränderungen der Unternehmenskultur und von Geschäftsmodellen durch Digitale Transformation – Auswirkungen auf das Compliance-Management, BB 2017, 939 ff.

Sartor, Roman/*Freiler-Waldburger*, Johannes (Hrsg.), Praxisleitfaden Compliance, Wien 2015
Zit: Bearbeiter, in: Sartor/Freiler-Waldburger, S.

Schlegel, Walter, Der Weg zur Compliance-Management-Zertifizierung, COMPLY. 3/18, 12 ff.

Schmidt, Stefan/*Eibelshäuser*, Beate, Die Prüfung von Corporate Governance-Systemen, COMPLY. 3/17, 20 ff.

Schmidt, Karsten/*Lutter*, Marcus (Hrsg.), Aktiengesetz, 4. Aufl., Köln 2020
Zit.: Bearbeiter, in: Schmidt/Lutter, §, Rn.

Schneider, Uwe H., Konflikte zwischen Unternehmensleitung und Aufsichtsrat über die Compliance, ZIP 2016, S070 ff.

Schulz, Martin (Hrsg.), Compliance-Management im Unternehmen, Frankfurt am Main 2017
Zit.: Bearbeiter, in: Schulz, Kap., Rn.

Schulz, Martin R., Compliance-Management im Unternehmen – Grundfragen, Herausforderungen und Orientierungshilfen, BB 2017, 1475 ff.

Schulz, Martin R., Compliance-Management im Unternehmen – Wirtschaftsfaktor „Compliance-Kultur", BB 2018, 1283 ff.

Schulz, Martin R., Compliance-Management im Unternehmen – Compliance-Strategie als (Dauer-)Aufgabe der Unternehmensleitung, BB 2019, 579 ff.

Schwarzbartl, Matrin/*Pyrcek*, Andreas, Compliance Management, Wien 2013

Seyfarth, Georg, Handlungspflichten der Konzernverwaltung im nachgeordneten Bereich am Beispiel Compliance im Konzern, ZGR-Sonderheft 22/2020, 87 ff.

Tabbert, Henning, Internationale Standards und Leitfäden zum Compliance Risikomanagement – eine Analyse des gemeinsamen Nenners für fortlaufendes Monitoring, CCZ 2020, 46 ff.

Teichmann, Christian (Hrsg.), Compliance, München 2014
Zit: Bearbeiter, in: Teichmann, Kap., Rn.

Umnuß, Karsten (Hrsg.), Corporate Compliance Checklisten, 4. Aufl, München 2020
Zit.: Bearbeiter, in Umnuß, Kap., Rn.

Wecker, Gregor/*van Laak*, Hendrik (Hrsg.), Compliance in der Unternehmerpraxis, 2. Aufl., Wiesbaden 2009
Zit.: Bearbeiter, in: Wecker/van Laak, S.

Wiedmann, Michael/*Greubel*, Marco, Compliance Management Systeme – Ein Beitrag zur effektiven und effizienten Ausgestaltung, CCZ 2019, 88 ff.

Wieland, Josef/*Steinmeyer*, Roland/*Grüninger*, Stephan (Hrsg.), Handbuch Compliance-Management, 3. Aufl., Berlin 2020
Zit.: Bearbeiter, in: Wieland/Steinmeyer/Grüninger, Kap., Rn.

Wilsing, Hans-Ulrich/*Goslar*, Sebastian, Die Berücksichtigung von Compliance-Management-Systemen bei der Bußgeldbemessung nach § 30 OwiG, GmbHR 2017, 1202 ff.

Zentes, Uta Christina, Das Sieben-Säulen-Modell der Korruptionsprävention, Wiesbaden 2017

4.2 Weiterführende Literatur

Bühr, Daniel Lucien/*Petsche*, Alexander/*Tolar*, Martin, ISO 19600 – Compliance Management Systems, Wien 2016

Dolata, Uwe, Compliance contra Wirtschaftskriminalität: Korruption im Wandel der Zeit, Hamburg 2014

Inderst, Cornelia/*Bannenberg*, Britta/*Poppe*, Sina (Hrsg.), Compliance, 3. Aufl., Heidelberg 2017

Institut der Wirtschaftsprüfer in Deutschland (IDW) (Hrsg.), Praxisleitfaden Governance, Risk und Compliance, Düsseldorf 2017

Kark, Andreas, Compliance-Risikomanagement, München 2013

Kleine, Maxim, Nicht effiziente Compliance Management Systeme sind bußgelderhöhend zu berücksichtigen, CCZ 2017, 241 ff.

KPMG Wirtschaftsprüfungsgesellschaft, Das wirksame Compliance-Management-System, 2. Aufl., Herne 2014

Makowicz, Bartosz/*Maciuca*, Florian, Prüfung von Compliance-Management-Systemen im Lichte neuer ISO-Standards, WPg 2020, 73 ff.

Menner, Stefan/*Bexa*, Kristina, Praktische Vorgehensweise bei der Einführung eines Tax Compliance Management Systems im Unternehmen, CCZ 2019, 129 ff.

Mittendorf, Martina, Compliance Management System als Haftungsbegrenzungsinstrument in der mittelständischen Wirtschaft, Berlin 2017

Moosmayer, Klaus, Compliance-Risikoanalyse, München 2015

Napokoj, Elke, Risikominimierung durch Corporate Compliance, Wien 2010

Nietsch, Michael (Hrsg.), Unternehmenssanktionen im Umbruch, Baden-Baden 2016

Pape, Jonas, Corporate Compliance – Rechtspflichten zur Verhaltenssteuerung von Unternehmensangehörigen in Deutschland und den USA, Berlin 2011

Rathgeber, Christian, Criminial Compliance, München 2012

Reiff, Rüdiger, Von kleinen Aufmerksamkeiten und großen Geschenken – was ist erlaubt? – „Eine Tasse Kaffee? Nein danke!" – Wo fängt Korruption an?, CCZ 2018, 194 ff.

Renz, Hartmut T./*Frankenberger*, Melanie, Aufgaben einer Compliance-Organisation im Rahmen des Internen Kontrollsystems (IKS), CB 2015, 420 ff.

Röhrich, Raimund (Hrsg.), Methoden der Korruptionsbekämpfung, Berlin 2008

Romeike, Frank/*Hager*, Peter, Erfolgsfaktor Risiko-Management 2.0, Wiesbaden 2009

Sonnenberg, Thomas, Compliance-Systeme in Unternehmen, JuS 2017, 917 ff.

Spindler, Gerald, Unternehmensorganisationspflichten, Berlin 2001

Teichmann, Fabian, Korruptionsbekämpfung durch Anreize – Ein Erfolgsmodell?, ZRFC 6/17, 267 ff.

Teicke, Tobias/*Matthiesen*, Reemt, Compliance-Klauseln als sinnvoller Bestandteil eines Compliance-Systems, BB 2013, 771 ff.

Troßbach, Stephanie, Geschäftspartner-Compliance – Wichtig wie nie zuvor, aber wie etabliert mein Unternehmen einen angemessenen Prozess?, CCZ 2017, 216 ff.

5. GLOSSAR

- **Angemessenheit** = Ein ausgewogenes Verhältnis zwischen der getroffenen Maßnahme und den Zielen, die mit ihnen verfolgt werden (Abwägung zwischen Vor- und Nachteilen), Relevanz u. a. für: Ziff. 1.2.2.
- **Compliance** = Einhaltung von Rechtsvorschriften und internen Regeln durch das Unternehmen und die Unternehmensmitglieder.
- **Compliance-Funktion** = Person oder Gruppe von Personen (Compliance-Abteilung, Compliance-Komitees), die für das CMS zuständig ist / sind, Relevanz u. a. für: Ziff. 2.1.5.
- **Organisatorische Grundlagen** = Festlegungen über Ziele, Aufgaben und weitere Aspekte des CMS, Relevanz u. a. für: Ziff. 2.1.3.
- **Compliance-Richtlinien** = Dokument / mehrere Dokumente, in denen Compliance-Themenfelder und Handlungsanweisungen speziell adressiert werden, Relevanz u. a. für: Ziff. 2.2.1.
- **Compliance-Management-System** = Zusammenhängende Elemente (bezogen auf Prozesse und Strukturen), die zur Erreichung von Compliance-Zielen und Erfüllung von Compliance-Aufgaben entwickelt und umgesetzt werden.
- **Compliance Officer** = Person, die die Compliance-Funktion innehat, Relevanz u. a. für: Ziff. 2.1.5.
- **Integrität** = Handeln nach Außen in Übereinstimmung mit den inneren (auch von Unternehmen vorgegebenen und von Unternehmensmitgliedern verinnerlichen) Werten, Relevanz u. a. für: Ziff. 1.1.3.
- **Interne Untersuchungen** = Aktivitäten, die zur Aufklärung von Verdachtsfällen in Unternehmen vorgenommen werden, Relevanz u. a. für: Ziff. 2.3.2.
- **Elemente** = Aktivitäten, die sich auf Prozesse und/oder Strukturen beziehen können und die im Rahmen der operativen Phase des CMS (Vorbeugen, Entdecken und Reagieren) umgesetzt werden, Relevanz u. a. für: Ziff. 2.2.
- **Themenfelder** = Risikobereiche, die im Rahmen der CRA festgestellt werden, Relevanz u. a. für: Ziff. 2.1.2.
- **Unternehmensmitglieder** = alle Personen, die mit dem Unternehmen aufgrund arbeitsvertraglicher oder vergleichbarer Grundlage verbunden sind, Relevanz u. a. für: Ziff. 2.1.5.
- **Unternehmensleitung** = Person oder Gruppe von Personen, die das Unternehmen faktisch und rechtlich leiten, Relevanz u. a. für: Ziff. 2.1.1.
- V**erhaltenskodex** = Festlegungen über Compliance-Themenfelder und die dort geltenden Handlungsanweisungen, Relevanz u. a. für: Ziff. 2.2.1. »

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
Chausseestraße 13
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