DICO Leitlinie

L02 – Kriterien zur internen Qualitätssicherung von CM-Systemen

Autoren: Arbeitskreis Zertifizierung und Qualitätsmanagement

DICO
Deutsches Institut für Compliance

Stand: Dezember 2016

Disclaimer

DICO Leitlinien richten sich an Compliance-Praktiker. Sie sollen einen Einstieg in das Thema erleichtern und einen Überblick verschaffen. Es wird daher bewusst darauf verzichtet, juristische Sonderfälle und Ausnahmeregelungen aufzuzeigen.

DICO Leitlinien bieten dem geneigten Leser praxistaugliche und umsetzbare Empfehlungen für ausgewählte Compliance-Themen. Mit Veröffentlichung einer Leitlinie soll zugleich eine Diskussion zum jeweiligen Themenkreis angestoßen werden mit dem Ziel, darauf aufbauend einen Standard zu entwickeln, der von Compliance-Praktikern anerkannt wird.

Senden Sie Ihre Anregungen und Beiträge an Leitlinien@dico-ev.de. Wir freuen uns auf eine lebhafte Diskussion und bedanken uns für Ihre konstruktive Unterstützung!

Vorwort

Dass Unternehmen und deren Organe im Einklang mit gesetzlichen Vorgaben handeln müssen, ist eine Selbstverständlichkeit. Die Praxis zeigt, dass die Unternehmen sich dem Thema proaktiv und systematisch stellen und Compliance-Management-Systeme (CMS) als Ausprägung guter Corporate Governance implementieren.

Zur Ausgestaltung von CMS haben die Rechtsprechung sowie die juristische und betriebswirtschaftliche Literatur klare Mindestanforderungen formuliert, nachzulesen zum Beispiel im Urteil des LG München I vom 10.12.2013, dem Gesetzgebungsvorschlag für eine Änderung der §§ 30, 130 des Ordnungswidrigkeitengesetzes (OWiG) des Bundesverbands der Unternehmensjuristen e. V. (BUJ) und im Gesetzesvorschlag des Deutschen Instituts für Compliance e. V. (DICO) für ein Gesetz zur Schaffung von Anreizen für Compliance-Maßnahmen in Betrieben und Unternehmen (CompAG).

Unstreitig ist, dass die mangelhafte Einrichtung sowie unzureichende Überwachung des CMS eine Verletzung der Pflichten der Geschäftsleitung bedeutet. Ganz praktisch stellt sich nunmehr die Frage, wie die Angemessenheit und Wirksamkeit der implementierten CMS überwacht und kontinuierlich verbessert werden kann, damit Geschäftsleitung und Aufsichtsorgan die Organisations- und Überwachungspflichten effizient ausfüllen können.

Der DICO-Arbeitskreis „Zertifizierung und Qualitätsmanagement“ hat sich zum Ziel gesetzt, einen Beitrag zur Diskussion über die inhaltliche Ausgestaltung des Begriffs „Überwachung von CMS“ durch die Geschäftsleitung und das Aufsichtsorgan zu leisten.

Um einen einheitlichen terminologischen Rahmen zu schaffen, wird das juristisch geprägte Verständnis von einer „Wirksamkeitskontrolle“ des CMS mit dem betriebswirtschaftlichen Modell zur Überwachung von Systemen zusammengeführt. Dies bietet den Vorteil, dass dadurch interdisziplinäre Diskussionen zur inhaltlichen Ausgestaltung der Überwachung von CMS unterstützt werden.

Im Hinblick auf die Ausgestaltung der Überwachung eines CMS lässt sich unterscheiden, ob die Überwachung als Teil des CMS angelegt ist oder ob sie systemunabhängig durchgeführt wird. Hierbei soll die systeminterne Überwachung als „Qualitätsmanagement von CM-Systemen“ und die systemexterne Überwachung als „Prüfung“ bezeichnet werden.

„Prüfungen“ des CMS werden regelmäßig sowohl durch unternehmensinterne Instanzen (z. B. die Interne Revision) als auch durch unternehmensexterne Experten durchgeführt (z. B. nach dem Prüfungsstandard IDW PS 980).

Die vorliegende Leitlinie zum „Qualitätsmanagement von CM-Systemen“ dient als Hilfestellung zur Ausgestaltung der systeminternen Überwachung als zentralem Aspekt eines wirksamen CMS. »

Einleitung

In einem modernen Compliance Management System (CMS) spielt das Qualitätsmanagement (QM) eine zentrale Rolle. Die Gründe hierfür sind vielfältig: Zum einen gilt es, permanent Schwachstellen im CMS zu identifizieren und zu beseitigen. Auf der anderen Seite fordern neue Standards und Gesetze ein regelmäßiges QM in der Compliance.

Generell wird unter Qualitätsmanagement die Erhöhung der Effektivität und Effizienz von Management-Aufgaben, Geschäftsprozessen etc. oder die Erhaltung und Steigerung der Qualität von Produkten und Dienstleistungen verstanden. Auch die Einhaltung von inhaltlichen und zeitlichen Nebenbedingungen kann unter QM subsumiert werden.

Qualitätsmanagement meint dabei die internen, d.h. vom jeweils Verantwortlichen initiierten, gesteuerten und überwachten Maßnahmen. Das QM grenzt sich so gegen von externen Prüfinstituten o.ä. durchgeführte Prüfungen / Zertifizierungen ab.

Auf den Bereich Compliance bezogen bedeutet QM die Überwachung und Steigerung der Wirksamkeit, Effektivität und Effizienz der Elemente des Compliance Management Systems eines Unternehmens. Dies sollte einhergehen mit der Berücksichtigung bestehender und sich ggf. ändernder externer Vorgaben (Recht, Standards, etc.).

Die Qualitätssicherung findet auf der Ebene der einzelnen CMS-Elemente statt und wird aus diesem Grund im weiteren Verlauf nicht als CMS-Element nochmals gesondert erwähnt. Zwar gibt es keine ganzheitlich verbindlichen Vorgaben, welche Elemente ein CMS enthalten muss. Die folgenden Elemente gelten jedoch als sinnvoll und stimmen mit den einschlägigen Regularien und Standards (u. a. UK Bribery Act, IDW PS 980) überein.

Es sind dies:

- Compliance Officer / Organisation
- Compliance Risk Assessment
- Reporting
- Compliance Beratung
- Hinweisgebersystem
- Code of Conduct & Richtlinien
- Untersuchungen und Konsequenzen
- Kommunikation
- Training

Diese Elemente beschreiben ein „Basis-CMS“, sind jedoch je nach Unternehmen und dessen „Compliance-Bedarf“ nicht vollständig bzw. unterschiedlich ausgeprägt. Weitere Compliance Prozesse, die durch Compliance gesteuert bzw. durchgeführt werden, werden ggf. in einer zweiten Auflage dieser Broschüre berücksichtigt. Zu nennen sind hier etwa Integrity Checks bzgl. Geschäftspartnern oder die Compliance Due Diligence bei M&A Transaktionen.

Für jedes der genannten Elemente lassen sich qualitätssichernde Aktivitäten definieren, bewerten und umsetzen. Ziel des Leitfadens ist eine praktische, auf das eigene Unternehmen zugeschnittene Handreichung für die Umsetzung des QM in der Compliance. Bezüglich der Überwachung von Compliance Management Systemen sei auf das gleichnamige DICO Arbeitspapier verwiesen.

Voraussetzung für die nachfolgenden Ausführungen ist denknotwendig, dass ein Unternehmen / Konzern bereits ein CMS eingeführt hat, welches grundsätzlich seine Anforderungen abdeckt. »

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.

DICO – Deutsches Institut für Compliance

Chausseestraße 13

D-10115 Berlin

info@dico-ev.de

www.dico-ev.de