

L02 – KRITERIEN ZUR INTERNEN QUALITÄTSSICHERUNG VON CM-SYSTEMEN

HIGH



QUALITY
LEVEL

AUTOREN:

ARBEITSKREIS ZERTIFIZIERUNG &
QUALITÄTSMANAGEMENT

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 geeigneten 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	5
EINLEITUNG	6
QM FÜR CMS-ELEMENTE	7
1. COMPLIANCE OFFICER/ORGANISATION	8
1.1 Ausstattung Compliance Organisation	
1.2 Verankerung im Unternehmen	
1.3 Kompetenz der Mitarbeiter / Compliance Officer	
2. COMPLIANCE RISIKOANALYSE	11
2.1 Prozess & Organisation	
2.2 Umfang und Methodik	
2.3 Maßnahmen	
3. REPORTING	13
3.1 Nutzen & Ziele	
3.2 Adressaten	
3.3 Quellen	
3.4 Frequenz	
4. COMPLIANCE BERATUNG	15
4.1 Bekanntheit / Erreichbarkeit	
4.2 Qualität der Antworten	
4.3 Prozessdurchlauf	
4.4 Kompetenz	
5. HINWEISGEBERSYSTEM	17
5.1 Anwendergerechtes „System“	
5.2 Bekanntheit / Erreichbarkeit	
5.3 Prozessdurchlauf	

6. CODE OF CONDUCT/RICHTLINIEN	19
6.1 Thematische Abdeckung	
6.2 Anwendbarkeit	
6.3 Rechtsverbindliche Implementierung	
6.4 Formalanforderungen	
6.5 Kompetenz	
7. UNTERSUCHUNGEN UND KONSEQUENZEN	22
7.1 Eindeutiger Prozess	
7.2 Kompetenz und Ressourcen	
7.3 Vergleichbarkeit	
7.4 Nachhaltigkeit	
8. KOMMUNIKATION	24
8.1 Eindeutiger Prozess	
8.2 Adressatenkreis	
8.3 Kommunikationsmittel	
9. TRAINING	26
9.1 Strategie und Inhalte	
9.2 Mittel	
9.3 Kontrolle und Reporting	
SCHLUSSBEMERKUNG	28

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. »

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

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