DICO Standard

S09 – Compliance-Risikoanalyse (CRA)

Autoren: Arbeitskreis Compliance-Risikoanalyse (CRA)

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

DICO
Deutsches Institut für Compliance

Viadrina Compliance Center

Stand: Februar 2020

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 S09 Compliance-Risikoanalyse (CRA) basiert auf der 2017 veröffentlichten DICO Leitlinie L09 Compliance-Risikoanalyse (CRA). Diese wurde im Rahmen des Projektes „Compliance und Integrität – Kompetenzpaket“ am Viadrina Compliance Center unter Leitung von Prof. Dr. Bartosz Makowicz wissenschaftlich überarbeitet und ergänzt. Das Projekt wurde vom KBA Integrity Fund gefördert und umfasste die Entwicklung eines allgemeinen CMS-Standards sowie weiterer speziellen Compliance-Standards. Wir danken dem KBA Integrity Fund, Prof. Makowicz und seinem Team sowie den Mitgliedern des DICO Arbeitskreises Compliance-Risikoanalyse (CRA) und allen Compliance-Praktikern, die durch ihre Hinweise und Beiträge an der Entwicklung dieses DICO Standards mitgewirkt haben.

Abkürzungsverzeichnis

AktG	Aktiengesetz
BGH	Bundesgerichtshof
CCZ	Corporate Compliance Zeitschrift
CMS	Compliance-Management-System
CPI	Corruption Perception Index
CRA	Compliance-Risikoanalyse
DICO	Deutsches Institut für Compliance e.V.
DIN	Deutsches Institut für Normung e.V.
DOJ	US Department of Justice
FCPA	Foreign Corrupt Practices Act
GwG	Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (Geldwäschegesetz)
GRC	Governance, Risk & Compliance
ISO	International Organization for Standardization
KWG	Kreditwesengesetz
LG	Landgericht
PDCA	Plan-Do-Check-Act
UK	United Kingdom
UKBA	UK Bribery Act 2010
US	United States
USA	United States of America

Abbildungsverzeichnis

Abbildungen

Tabellen

Vorwort

Eine Compliance-Risikoanalyse (CRA) ist die systematische Suche nach möglichen Ursachen und Auslösern von potentiellen Compliance-Vorfällen (Compliance-Risiken). Sie dient als Grundlage für die Ausgestaltung und weitere Entwicklung des Compliance-Management-Systems (CMS). Ein CMS wird nur dann zielgerichtet und wirksam sein, wenn es auf die wesentlichen Compliance-Themenfelder und -Risiken des Unternehmens ausgerichtet ist.

Dieser Standard soll dazu dienen, wesentliche Rahmenbedingungen und Anforderungen an die Organisation und Durchführung einer CRA zu erläutern. Er fasst das gesammelte Wissen der Mitglieder des gleichnamigen DICO Arbeitskreises zusammen, berücksichtigt die einschlägigen Fachquellen und versucht sich daran, diesem vielschichtigen und in der Praxis sehr heterogenen Thema eine grundlegende Struktur zu geben.

Für den Compliance-Verantwortlichen, der die CRA verantwortet, wird die Ausgestaltung der CRA oft eine Herausforderung sein: Hier spielen die jeweiligen Gegebenheiten wie das von seinem Unternehmen verfolgte Geschäftsmodell, die Branche, die Unternehmensgröße, internationale und damit unterschiedliche regulatorische Vorgaben, aber auch der Erfahrungshorizont einer Unternehmensorganisation (insbesondere der Compliance- und Rechtsabteilungen, der Internen Revision oder des Risikomanagements) eine entscheidende Rolle.[1]

Entsprechend vielfältig sind die Ansätze zur Risikoanalyse: Die CRA eines kommunalen Versorgungsunternehmens wird grundsätzlich anders aussehen als die eines globalen Industriekonzerns. Ebenso wird sich die Analyse von Risiken aus der Einhaltung umweltrechtlicher Vorgaben wesentlich von der Analyse datenschutzrechtlicher Risiken unterscheiden. »

1 *Pape*, Corporate Compliance – Rechtspflichten zur Verhaltenssteuerung von Unternehmensangehörigen in Deutschland und den USA, S. 119.

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