DICO Leitlinie

L09 – Compliance Risikoanalyse (CRA)

Autoren: Arbeitskreis Compliance Risikoanalyse (CRA)

DICO
Deutsches Institut für Compliance

Stand: September 2017

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

Eine Compliance Risikoanalyse (CRA) ist die systematische Suche nach möglichen Ursachen und Auslösern für Compliance Vorfälle. Sie dient als Grundlage für die Entwicklung von Compliance Maßnahmen und sollte der Planung eines Compliance Programms vorgeschaltet sein. Ein Compliance Programm wird nur dann zielgerichtet und wirksam sein, wenn es auf die wesentlichen Compliance Risiken des Unternehmens ausgerichtet ist.

Dieser Leitfaden 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 und versucht sich daran, diesem vielschichtigen und in der Praxis sehr heterogen ausgestalteten Thema eine grundlegende Struktur zu geben.

Für den Compliance-Verantwortlichen, der die Compliance Risikoanalyse 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.

Auf den ersten Blick überraschend erscheint die Vielfältigkeit möglicher Compliance-Risiken, denen ein Unternehmen ausgesetzt sein kann. Hierzu zählen nicht nur die Themenfelder einer „klassischen“ Compliance-Abteilung wie Korruptionsbekämpfung, Kartellrecht oder Geldwäsche. Vielmehr können Compliance Risiken überall entstehen, wo es entsprechende rechtliche Vorgaben einzuhalten gilt: Steuerrecht, Umweltrecht, Datenschutz oder Arbeitsrecht als Beispiele zeigen bereits die inhaltliche Bandbreite des Compliance-Begriffs auf. An dieser Stelle wird auch klar, dass Compliance nicht die Aufgabe einer einzelnen zentralen Abteilung sein kann. Vielmehr ist sicherzustellen, dass es im Unternehmen klare Zuständigkeitsstrukturen gibt, die auch die Verantwortung für relevante Compliance-Themenfelder umfassen.

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. »

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