Q&A zum DICO Risikokatalog

Autoren: Arbeitskreis Compliance Risikoanalyse I Stand: August 2024

1. Wozu dient eine Compliance Risikoanalyse (CRA)?

Die Compliance Risikoanalyse (CRA) ist die Grundlage eines wirksamen Compliance Management Systems (CMS). Die systematischen Erfassung und Bewertung der für eine Organisation bzw. ein Unternehmen relevanten Compliance Risiken ermöglicht erst die zielgerichtete und damit auch ressourceneffiziente Definition von risikoreduzierenden Maßnahmen und internen Kontrollen (= Compliance Programm). Anders gesprochen: Ohne eine wirksame Compliance Risikoanalyse kann keine Aussage zur Angemessenheit und Wirksamkeit eines Unternehmens-CMS vorgenommen werden.

Ziel der CRA ist es, Compliance-Risiken möglichst umfassend zu identifizieren, zu selektieren und realistisch zu bewerten, um schließlich adäquate und zielgerichtet risikomindernde Maßnahmen zu ergreifen. Sie ist damit Grundlage sowohl des “Ob” als auch des “Wie” von Compliance-Maßnahmen.

2. Welche DICO Produkte stehen für eine Compliance Risikoanalyse zur Verfügung?

- Der DICO-Arbeitskreis Compliance Risikoanalyse hat im Februar 2020 einen an die Praxis gerichteten **Standard zur Compliance Risikoanalyse (S09 – Compliance-Risikoanalyse (CRA))** herausgegeben, in dem wesentliche Anforderungen, Grundelemente und Beispiele für eine CRA zusammengetragen und strukturiert wurden. Das Ziel ist, Unternehmensangehörigen den Einstieg in das Thema zu erleichtern und konkrete Hilfestellungen für die praktische Umsetzung bereitzustellen. Juristische Sonderfälle und Ausnahmeregelungen werden nicht behandelt. Der DICO Standard ersetzt auch nicht die ggf. erforderliche rechtliche Beratung im Einzelfall.

- Der Standard wird durch den **DICO Risikokatalog** ergänzt, der ein umfassendes Risikouniversum möglicher Compliance-Themenfelder darstellt. Diese Zusammenstellung möglicher Rechtsgebiete kann für ein Unternehmen Ausgangspunkt der sogenannten Relevanzanalyse sein. Dabei werden die für das jeweilige Unternehmen relevanten Themenfelder identifiziert und anschließend priorisiert.

DICO
Deutsches Institut für Compliance

3. Was sind die ersten Schritte im Rahmen einer Compliance Risikoanalyse (CRA)?

Für eine CRA sollte in einem ersten Schritt eine umfassende Bestandsaufnahme und ggf. erste Priorisierung der für das jeweilige Unternehmen relevanten Compliance-Themenfelder erfolgen. Dabei sind die individuellen Gegebenheiten im Unternehmen einzubeziehen, wie Branche, Größe, Standort, wirtschaftliche Faktoren. Diese Bestandsaufnahme wird in der Praxis häufig „Relevanzanalyse“ oder „horizontale Risikoanalyse“ genannt. Der DICO Risikokatalog kann als Startpunkt zur Relevanzanalyse dienen, um einen Überblick über mögliche Risikofelder im Unternehmen zu erlangen. Im Anschluss folgt dann die (vertikale) Operationalisierung, d.h. die Ableitung von konkreten Risikoszenarien, deren Verortung in Geschäftsprozessen und die Bewertung der Compliance-Risiken.

DICO
Deutsches Institut für Compliance