www.compliance-berater.de

Compliance Berater

10 / 2023

Betriebs-Berater Compliance

28.9.2023 | 11.Jg
Seiten 381–424

Fachmedien Recht und Wirtschaft | dfv Mediengruppe | Frankfurt am Main

CB-BEITRAG

Prof. Dr. Oliver Haag und Khadija Sandführ, LL. M.

Die Relevanzanalyse – Grundlagen, Ziele, Anforderungen

Ordnungsgemäße Unternehmensführung ohne adäquates Risiko- und Compliance-Management ist kaum noch vor- und darstellbar. Rechtsprechung, Literatur, Politik und Gesellschaft stellen (mehr oder weniger) klare Anforderungen an ordnungsgemäßes unternehmerisches Verhalten und sanktionieren tatsächliche (und vermeintliche) Regelverstöße. Um die unternehmensspezifischen Risiken zu erfassen ist die Durchführung einer Risikoanalyse (Compliance Risk Assessment – CRA) unumgänglich[1]. Der eigentlichen Risikoanalyse ist eine Relevanzanalyse voranzustellen, um sich der bei unternehmerischen Aktivitäten naturgemäß nahezu unüberschaubaren potenziellen Risikomenge anzunähern und diese „abarbeitbar" zu erfassen. Wird diese Relevanzanalyse professionell und strukturiert durchgeführt und dokumentiert, so kann sie einen wertvollen Beitrag zum Schutz und zur Hilfe gegen Compliance-Verstöße und deren Sanktionierung leisten. Der nachfolgende Beitrag stellt die Grundlagen, Ziele, Anforderungen und Ansätze der Relevanzanalyse dar. In einem weiteren Beitrag (erscheint in CB 11/2023) werden sich die Autoren der Durchführung der Relevanzanalyse widmen und Hinweise zu deren Ablauf und Inhalt geben.

I. Definition und Ziele der Relevanzanalyse

Die Relevanzanalyse oder auch Scoping oder Screening genannt, ist „eine erste, von allgemeinen und einfach zugänglichen Informationen ausgehende Einschätzung von Themenfeldern und Geschäftsaktivitäten des Unternehmens, in denen es am ehesten zu Compliance-Vorfällen kommen kann"[2]. Sie dient der Festlegung des Umfangs und der Ziele des Compliance Risk Assessments (CRA). Die potenziellen Themenfelder, die das Unternehmen betreffen könnten, müssen identifiziert werden, um das Ziel der Relevanzanalyse erfüllen zu können. Das Ziel liegt im Erreichen eines effektiven und effizienten Konzepts und der Implementierung eines wirksamen Compliance-Management-Systems (CMS), da die Relevanzanalyse mit der Risikoidentifikation die Grundlage des CMS darstellt.[3]
Weder in der Literatur noch in Standards oder gesetzlichen Vorgaben wird eine wissenschaftliche Methodik zur Vorgehensweise bei der Relevanzanalyse genannt. Dies macht es für Unternehmen beschwerlich, die richtige Auswahl an Methoden und Instrumenten zu finden, da stets eine gewisse Unsicherheit bezüglich der Richtigkeit der Vorgehensweise und damit auch des gesamten Risikoanalyseprozesses besteht.
Nichtsdestotrotz hat sich in der Praxis die nachfolgend beschriebene Vorgehensweise bewährt.

Eine erste Einschätzung über relevante Themenfelder kann durch eine sogenannte Betroffenheitsanalyse erreicht werden. Hierbei wird der Rechtsrahmen der Gesetze, gegen die das Unternehmen verstoßen kann, erfasst, um die Identifikation der Risiken zu erleichtern. Hier geht es nicht darum, eine vollständige Liste aller denkbaren Vorschriften zu erstellen, sondern die relevanten branchen- und unternehmensspezifischen Besonderheiten zu erfassen, sodass die spätere Identifikation der Compliance-Risiken erleichtert wird.[4] Ebenso können Risikoberichte der Branche, oder auch unternehmensinterne Dokumente beziehungsweise Unternehmensfunktionen eine Hilfestellung bei der Relevanzanalyse darstellen. Darauffolgend können die Themen- und Rechtsgebiete, sowie die Bereiche und Prozesse im Unternehmen identifiziert werden, in denen wesentliche Risiken angenommen werden, das heißt Risiken, die signifikant für das Unternehmen sind.[5] Diese Auswahl und Priorisierung der Themenbereiche unterliegt einer stetigen Hinterfragung, ebenso wie die Vorgehensweise, die bei Anpassungsbedarf geändert werden muss.[6]
Es geht also um die Sammlung aller relevanten, nicht gänzlich unwahrscheinlichen Compliance-Risikogebiete als Risikogesamtheit, wobei mögliche Schadensauswirkungen für das Unternehmen noch nicht berücksichtigt werden.[7] Dabei erfolgt der grobe Ablauf der

1 Vgl. hierzu *Haag/Bindschädel*, CB 2021, 64 ff. und 112 ff.
2 Deutsches Institut für Compliance e. V., S09 – Compliance-Risikoanalyse (CRA), 2020, S.15.
3 Deutsches Institut für Compliance e. V., S09 – Compliance-Risikoanalyse (CRA), 2020, S.10; Withus, ZRFC 2015, 170, 172.
4 *Ozip-Philippsen*, ZRFC 2013, 203, 206.
5 Deutsches Institut für Compliance e. V., S09 – Compliance-Risikoanalyse (CRA), 2020, S.15.
6 *Bartuschka*, in: Schulz, Compliance Management im Unternehmen, 2. Aufl. 2021, 10. Kap. Rn. 51 ff.
7 *Pauthner/Stephan*, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, 3. Aufl. 2016, §16 Rn. 77.

Relevanzanalyse in zwei Schritten. In einem ersten Schritt, der sogenannten Inventarisierung, werden die potenziellen Themenfelder, die das Unternehmen betreffen könnten, identifiziert. In einem nächsten Schritt werden die gesammelten relevanten Themenfelder priorisiert, es erfolgt also die sogenannte Bewertung, ob die Themenfelder für das Unternehmen von Bedeutung sind und in die CMS-Beschreibung aufgenommen werden sollten.[8]

II. Erforderlichkeit und Anforderungen der Relevanzanalyse

Compliance-Risiken können grundsätzlich überall entstehen, wo es entsprechende rechtliche Vorgaben gibt, die eingehalten werden müssen.[9] Dabei kann es nicht nur in den „klassischen" Themenfeldern wie Kartellrecht, Korruption oder Geldwäsche zu Verstößen kommen, sondern in einer Vielzahl von Themengebieten wie beispielsweise im Steuerrecht, Umweltrecht, Datenschutz, in der Lieferkettensorgfaltspflicht oder auch im Bereich der Nachhaltigkeit durch Environment Social Governance.[10]

Die Relevanzanalyse kann einen ersten Überblick über die wesentlichen Risiken beziehungsweise Themengebiete verschaffen und so auch als Grundlage jedes weiteren Vorgehens dienen.[11]

Aus diesem Grund ist es erforderlich, der eigentlichen Risikoanalyse die Relevanzanalyse vorzuschalten, um die Themenfelder zu identifizieren, in denen grundsätzlich Compliance-Verstöße vorkommen können und um diese dann zu priorisieren, das heißt zu überprüfen, ob diese für das Unternehmen von Bedeutung sind. Dabei sollte noch unbeachtet bleiben, ob die Themenfelder wesentliche oder unwesentliche Risiken vermuten lassen, denn die Bewertung, ob ein Risiko wirklich beachtenswert ist oder nicht, fällt in einen anderen Schritt des CRA.[12] Erforderlich ist die Relevanzanalyse und ihre Dokumentation auch im Falle eines Verstoßes. Kommt es im Unternehmen zu einem Compliance-Verstoß in einem abseitigen oder kaum vorhersehbaren Themenbereich, dient die Dokumentation der systematisch durchgeführten Relevanzanalyse mit Priorisierung zur Verteidigung, denn das Unternehmen kann seine Einschränkungen im CRA nachvollziehbar darlegen.[13] Die Qualität der Relevanzanalyse bestimmt die Effektivität und Effizienz der weiteren Prozessschritte des CRA, da sie den Kern und damit den Anfang darstellt.[14]

Damit die Qualität der Relevanzanalyse gewährleistet werden kann, sind einige Anforderungen an die Ermittlung der Themengebiete und deren Sammlung zu stellen.

Die erste und wichtigste Anforderung bildet die Aktualität, denn nur bei frühzeitiger Identifikation relevanter Themengebiete können rechtzeitig Steuerungsmaßnahmen eingeleitet werden. Weitere Anforderungen sind die Vollständigkeit und Richtigkeit. Diese fordern eine möglichst detaillierte und lückenlose Risikosammlung, denn nur wenn die Risiken beziehungsweise Themengebiete vollumfänglich identifiziert werden, können sie gesteuert werden. Hierbei geht es um aktuelle, also bestehende Risikothemengebiete und um potenzielle Risikothemengebiete, die sowohl inhaltlich als auch formal richtig aufgedeckt werden. Die inhaltliche Richtigkeit beschreibt die Zuverlässigkeit der Aufdeckung und die formale Richtigkeit beschreibt die Genauigkeit, mit welcher Themengebiete identifiziert werden sollen.[15]

Weiterhin besteht eine Anforderung in der Systematik der Erfassung, was bedeutet, dass bei der Identifizierung von Themengebieten ein systematischer, standardisierter und kontinuierlicher Prozess zu etablieren ist, der auch für Dritte nachvollziehbar ist. Hierbei gilt es zu beachten, nicht die Flexibilität zu verlieren, da sonst möglicherweise neue Themengebiete und damit einhergehende Risiken nicht erkannt werden können. Dies kann durch ein flexibles Instrumentarium und eine flexible Anwendung der Methodik gesichert werden. Zuletzt ist die Anforderung der Akzeptanz zu beachten. Mitarbeiter und jegliche in den Prozess involvierte Personen müssen die Instrumente und Methoden verstehen und akzeptieren, um sich aktiv am Prozess beteiligen zu können.[16] Dabei ist auch die Motivation und Intuition der Mitarbeiter von großer Bedeutung, sodass die gelebte Risikokultur und -strategie auch hier eine übergeordnete Rolle spielen.[17] Im Zusammenhang mit der Akzeptanz ist auch die Belastbarkeit der Informationen zu nennen, die überwiegend von unternehmensinternen Personen stammen. Alle an der Informationssammlung beteiligten Personen müssen ein einheitliches Verständnis des Compliance-Risikos haben und wie sie dieses einzuschätzen haben.[18]

Alle zuvor genannten Anforderungen können in Konkurrenz zueinanderstehen und meist ist es nicht möglich, allen gerecht zu werden. Aus diesem Grund müssen auch unternehmensspezifische Rahmenbedingungen mit in Betracht gezogen werden, um eine für das Unternehmen individuell passende Auswahl an Anforderungen zu erhalten.[19]

III. Ansätze der Relevanzanalyse

Welche Themenfelder für ein Unternehmen relevant sind, wird oft aus der Erfahrung heraus bestimmt oder es werden typische Branchenrisiken herangezogen. Die Relevanzanalyse bleibt daher oft im Ungefähren, sodass eher eine Art Schleppnetz ausgeworfen wird, in dem die wichtigsten Risiken hängen bleiben, anstatt eines systematischen Ansatzes.[20] Aus diesem Grund werden nachfolgend verschiedene Ansätze und Sichtweisen der Relevanzanalyse bezogen auf die Informationsgewinnung und Durchführung derselben beschrieben. Dabei soll auch die Frage beantwortet werden, welche unternehmensinternen und -externen Informationsquellen geeignet sind, um die relevanten Themengebiete identifizieren zu können.

8 Deutsches Institut für Compliance e. V., S09 – Compliance-Risikoanalyse (CRA), 2020, S.15.
9 *Oeder/Havers/Barra Taladriz/Biaesch*, CB 2021, 159; *Pauthner*, in: Ghassemi-Tabar/Pauthner/Wilsing, Corporate Compliance, 2016, S.116.
10 *Passarge*, CNL 2022, 3, https://www.ruw.de/news/media/2/Online-Zeitschrift-Compliance-Mrz-2022 –15563.pdf.
11 *Schefold*, ZRFC 2021, 209, 211.
12 *Kark*, Compliance-Risikomanagement, 2.Aufl. 2019, S.125.
13 Deutsches Institut für Compliance e. V., S09 – Compliance-Risikoanalyse (CRA), 2020, S.15.
14 *Vanini/Rieg*, Risikomanagement, 2. Aufl. 2021, S.199.
15 *Diederichs*, Risikomanagement und Risikocontrolling, 4. Aufl.2018, S. 93 f.; *Vanini/Rieg*, Risikomanagement, 2. Aufl. 2021, S.200.
16 *Diederichs*, Risikomanagement und Risikocontrolling, 4. Aufl. 2018, S.93 f.; *Vanini/Rieg*, Risikomanagement, 2. Aufl. 2021, S. 200.
17 *Diederichs*, Risikomanagement und Risikocontrolling, 4. Aufl. 2018, S.93 f.; *Vanini/Rieg*, Risikomanagement, 2. Aufl. 2021, S. 200.
18 *Reichert*, ZRFC 2012, 111, 114.
19 *Diederichs*, Risikomanagement und Risikocontrolling, 4. Aufl. 2018, S. 94.
20 *Haag/Bindschädel*, CB 2021, 112, 114 f.; *Eggers*, CB 2021, 286, 287.

1. Informationsgewinnung

In der Literatur werden für die Identifikation von Compliance-Risiken und im Fall der Relevanzanalyse von Themenfeldern vergleichbare Quellen wie im klassischen Risikomanagement benutzt.[21]

a) Mitarbeiter als Quelle

Einleitend sind daher die eigenen Mitarbeiter im Unternehmen zu nennen. Diese besitzen ein Rechts- und Unrechtsempfinden, sind zudem nah am operativen Geschäft und können tätigkeitsbezogene Themenfelder oder potenzielle Verstöße erkennen, einer Würdigung unterziehen und diese melden. Sie erkennen vor allem Unregelmäßigkeiten in Bezug auf die Einhaltung interner Richtlinien oder auch in der Tätigkeit benachbarter Bereiche und Abteilungen.[22]

b) Führungskräfte

Führungskräfte und Mitglieder der Geschäftsleitung sind gesondert zu nennen, da sie im Rahmen ihrer hervorgehobenen Stellung andere Informationen und Einblicke in das Unternehmen erhalten. Außerdem haben sie, vor allem auch aus eigenem Interesse, eine bessere Kenntnis über die Compliance-Situation ihres Bereiches und kennen die Stellen, die zu potenziellen Verstößen führen können.

c) Interne Revision

Eine weitere Quelle zur Identifikation von Compliance-Themenfeldern ist, sofern im Unternehmen vorhanden, die interne Revision. Die Erkenntnisse der internen Revision können Schwachstellen der Prozesse in Geschäftsbereichen und anderen Bereichen im Unternehmen identifizieren und sind in Revisionsberichten dokumentiert. Daher ist es ratsam, dass die Compliance-Abteilung beziehungsweise der Compliance-Verantwortliche zusammen mit Personen der internen Revision die Berichte analysiert.[23]

d) Weitere unternehmensinterne Ressourcen

Prinzipiell sollten alle internen Quellen genutzt werden, die zur Informationssammlung geeignet sind, denn so lassen sich unternehmensinterne Ressourcen in personeller aber auch zeitlicher und finanzieller Sicht schonen. Daher sind weitere wichtige Quellen, falls vorhanden, das Hinweisgebersystem beziehungsweise die Whistleblower-Hotline oder das interne Kontrollsystem, die bei der Identifikation von Themenfeldern hilfreich sein können. Durch Prüfung und Nachgehen der eingegangenen Hinweise und möglicher Verstöße können Rückschlüsse auf spezielle Themenfelder im gemeldeten Bereich oder auch in anderen Unternehmensbereichen sowie zum Stand des gesamten CMS gezogen werden.[24]

e) Externe Quellen

Auch unternehmensexterne Quellen können zur Identifikation von Themenfeldern genutzt werden. So können beispielsweise Rechtsanwaltskanzleien neben der unternehmensinternen Rechtsabteilung Gesetzesänderungen oder das Unternehmen betreffende Urteile und daraus entstehende Risikofelder frühzeitig identifizieren. Außerdem kann in der Rechtsabteilung als Schnittstelle zu anderen Abteilungen eine Identifikation der Themenfelder in vielen operativen Abteilungen des Unternehmens gewährleistet werden.[25]

Ebenso ist die Tätigkeit der Wirtschaftsprüfungsgesellschaften von großer Bedeutung, denn diese prüfen nicht nur den Jahresabschluss, sondern auch das CMS und kennen somit durch meist langjährige Tätigkeiten auch die Unternehmensprozesse und deren Qualität. Auch durch Gespräche abseits der Prüfungsgespräche können Anhaltspunkte für die Themenfelder erkannt werden, wenn der Prüfer zum Beispiel aufgrund seiner Erfahrung in anderen Unternehmen vergleichbarer Größe und bei branchenunabhängigen Themenfeldern Empfehlungen geben kann, ohne dass erkennbar ist, für welche Unternehmen er noch tätig ist.[26]

f) Wettbewerbsanalyse

Eine weitere Informationsquelle für die Identifikation von Themenfeldern ist die Wettbewerbsanalyse. Dabei lässt das komplette Unternehmensumfeld Rückschlüsse auf Themenfelder zu, sodass sowohl die Analyse von Wettbewerbern mit einer ähnlichen Compliance-Situation durchgeführt werden sollte, als auch eine Analyse von anderen Unternehmen anderer Größe und anderer Branchen, die aber beispielsweise dieselben Kunden beliefern. Ebenso kann das weitere Wettbewerbsumfeld durch Informationsblätter von Fachverbänden, Compliance-Studien von Verbänden oder Beratungsunternehmen, Gespräche am Rande von Tagungen oder mit ehemaligen Kollegen und Kommilitonen, oder auch durch Meldungen in der Presse der Identifikation von Themenfeldern dienen.[27]

g) Regulatorische Anforderungen

Auch neue gesetzliche und regulatorische beziehungsweise behördliche Anforderungen und der Fokus der Strafverfolgungs- und Kartellbehörden müssen betrachtet werden, um alle Informationsquellen zu nutzen.[28]

2. Identifikation relevanter Themenfelder

All diese Informationen aus unterschiedlichen Quellen können Compliance-Themenfelder beinhalten und identifizieren. Sie ergeben zwar keinen kompletten Überblick über alle möglichen Themenfelder, stellen aber jedenfalls die gravierendsten und dringlichsten Themenfelder dar.[29] Bei der Nutzung all dieser Daten besteht die Herausforderung darin, die geeigneten Quellen für die Informationen zu finden und mit den Verantwortlichen die Übergabe zu vereinbaren. Außerdem müssen die Informationen abschließend noch für die eigentliche Analyse entsprechend aufbereitet werden.[30]

John beschreibt den Ansatz der Relevanzanalyse als Vorauswahl der für das Unternehmen relevanten Themenfelder, die aufgrund der Branche, des Geschäftsmodells und der Internationalität ein Gefahrenpotenzial darstellen. Dabei muss auch das Geschäftsumfeld beobachtet und analysiert werden, ob Veränderungen Auswirkungen auf den rechtlichen Rahmen haben, beispielsweise Themen wie die

21 *Kark*, Compliance-Risikomanagement, 2. Aufl. 2019, S. 128; *Pauthner*, in: Ghassemi-Tabar/Pauthner/Wilsing, Corporate Compliance, 2016, S. 71 ff.; *Ebersoll/Stork*, Smart Risk Assessment, 2016, S. 80 f.

22 *Wind*, Leitfaden Compliance, 2018, S. 46 f.; *Kark*, Compliance -Risikomanagement, 2. Aufl. 2019, S. 128.

23 *Kark*, Compliance-Risikomanagement, 2. Aufl. 2019, S.129 f., *Reichert*, ZRFC 2012, 111, 114.

24 *Pauthner*, in: Ghassemi-Tabar/Pauthner/Wilsing, Corporate Compliance, 2016, S. 74.

25 *Kark*, Compliance-Risikomanagement, 2. Aufl. 2019, S. 130.

26 *Kark* Compliance-Risikomanagement, 2. Aufl. 2019, S.130 f.

27 *Kark*, Compliance-Risikomanagement, 2. Aufl. 2019, S. 132 f.; *Ebersoll/Stork*, Smart Risk Assessment, 2016, S. 82.; *Schefold*, ZRFC 2012, 209, 210 f.

28 Deutsches Institut für Compliance e. V., S09 – Compliance-Risikoanalyse (CRA), 2020, S. 20.

29 *Kark*, Compliance-Risikomanagement, 2. Aufl. 2019, S.133.

30 Deutsches Institut für Compliance e. V., S09 – Compliance-Risikoanalyse (CRA), 2020, S. 19.

Pandemie, Digitalisierung, Wettbewerbssituation der Kunden und Lieferanten oder auch die gesellschaftlichen Erwartungen.[31] Hieraus lässt sich ein beispielhafter Risikokatalog erstellen, der in Themenbereiche und dazugehörige Themenfelder gegliedert ist. Die Relevanzanalyse und die Auswahl der Themenfelder sind ausführlich zu dokumentieren und zu begründen, weshalb Entscheidungen und Eingrenzungen wie erfolgt getroffen wurden. Damit kann im Falle eines Compliance-Verstoßes die Dokumentation als Hilfsmittel für die Aufklärung und als Abwehr von Vorwürfen dienen.

Abb. 1: Beispielhafte Risikolandschaft[32]

Auch das Konstanz Institut für Corporate Governance (KICG) beschreibt in seiner Leitlinie wie die Identifikation von Themenfeldern ablaufen sollte.[33] Die Verantwortung liegt demnach bei der Compliance-Abteilung oder den Compliance-Verantwortlichen und ist für die Identifikation auf die Informationen und Rückmeldungen der verschiedenen Fachbereiche und Geschäftseinheiten, wie interne Revision, Controlling oder auch die Rechtsabteilung, angewiesen. Dabei erfolgt die Identifikation zentral und dezentral, das heißt die regelmäßige Identifikation erfolgt in allen zentralen und dezentralen Geschäftseinheiten hinsichtlich der Compliance-Themenfelder und die Ergebnisse werden dann zentral zusammengeführt. Das KICG beschreibt dabei folgende Quellen und Methoden zur Identifikation: Erkenntnisse aus Revisionstätigkeit und dem internen Kontrollsystem, Erkenntnisse aus Compliance-Fällen, Ergebnisse der Abschluss- und Wirtschaftsprüfer, Management-Befragungen, Umfeldanalyse, Expertenbefragungen, Studien und Umfragen aus dem Bereich Compliance-Management und Compliance-Risiken sowie die systematische Auswertung sonstiger Branchen-, Börsen-, und Medien- Informationen. Die möglichen Themenfelder sind laut KICG insbesondere Korruption, Kartellabsprachen und Vermögensschädigung des Unternehmens, beispielsweise durch Untreue oder Betrug. Weiterhin sind je nach Unternehmen und Branche besondere Themenfelder zu beachten, die sich aus der Geschäftstätigkeit ergeben oder auch aus der Zusammenarbeit mit internationalen Geschäftspartnern.[34]

Wind verweist in seiner Darstellung der Identifikation von Compliance-Risiken und der Risikofaktoren des jeweiligen Unternehmens auf die Compliance-Themenfelder und Faktoren, die das KICG beschreibt. Er betont jedoch, dass jedem Einzelrisiko ein Themenfeld beziehungsweise eine Kategorie und ein Risikoverantwortlicher zugeordnet werden muss. Dieser Verantwortliche hat dann die Aufgabe, sein Risikothemenfeld durch geeignete Kennzahlen und Indikatoren fortlaufend zu überwachen.[35] Welche Indikatoren oder Kennzahlen dazu genutzt werden sollen, wird nicht erläutert.

Bei einer Vielzahl potenzieller Risiken und Themenfelder, kann die Identifikation erfolgreicher sein, wenn eine formale Gliederung erfolgt. Diese Gliederung kann anhand verschiedener Kriterien wie zum Beispiel kurz- oder langfristige Auswirkungen, interne oder externe Ursachen, Compliance-Ziele oder auch nach Organisationsaspekten wie Ländern, Abteilungen oder Standorten erfolgen. Diese Ordnung in Risikokatalogen ist vor allem für die frühe Phase der Risikoidentifikation, insbesondere zum Aufdecken von Wirkungszusammenhängen oder schlicht zur Übersicht gut geeignet.[36] Aufgrund der großen Bedeutung in der frühen Phase der Risikoidentifikation, ist die Ordnung der potenziellen Themenfelder für die Relevanzanalyse von besonderer Wichtigkeit. Bei der Identifizierung von Themenfeldern hat sich in der Praxis eine Art Best Practice etabliert, indem die Identifizierung in meist rechtlich kodifizierte Risikokataloge geclustert wird, um die identifizierten Themenfelder systematisch darzustellen und in einem nächsten Schritt priorisieren zu können.[37]

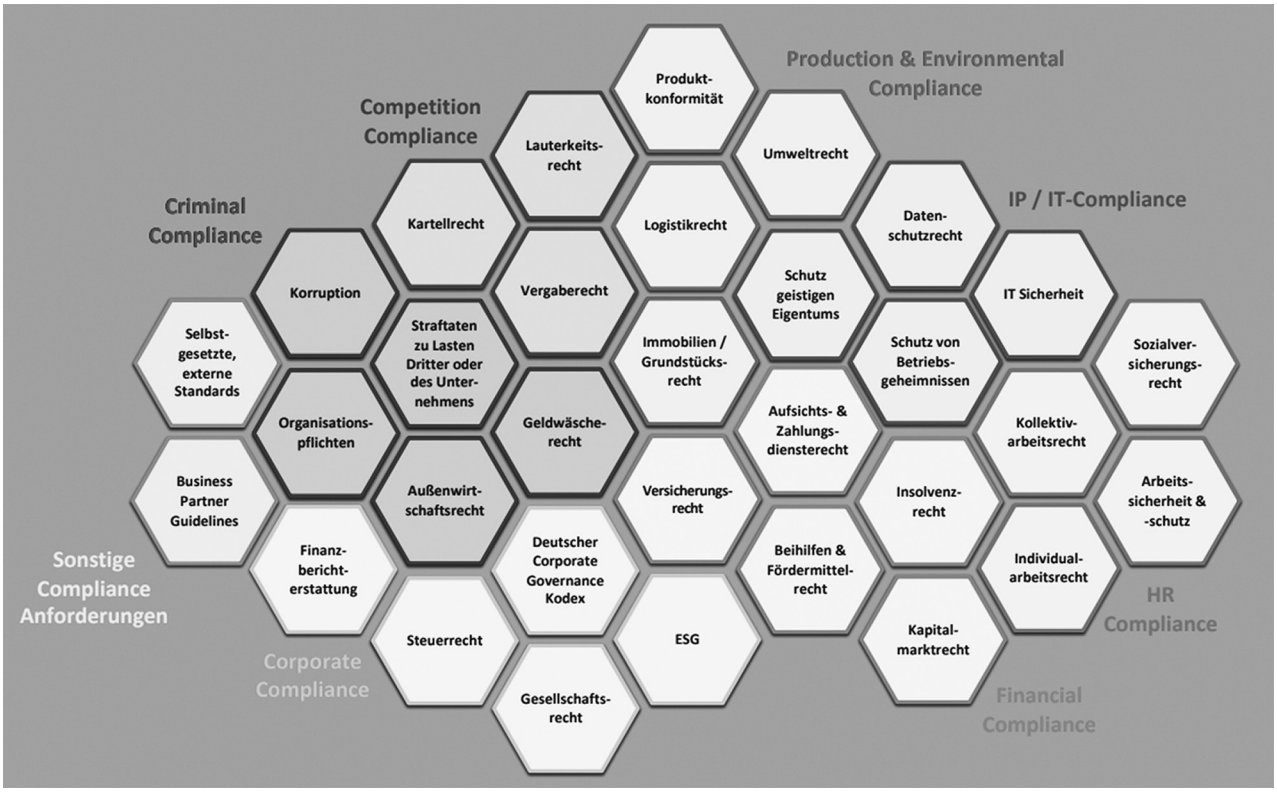
Für einen ersten Überblick kann ein Unternehmen ebenso den DICO-Risikokatalog, das sogenannte DICO-Wabenmodell, als Hilfestellung und übergeordneten, flexiblen Ordnungsrahmen anwenden. Hierbei können die 32 Themen, die als Waben dargestellt sind, als Ausgangsbasis für eine Bestandsaufnahme und damit für den ersten Schritt der Relevanzanalyse dienen.[38]

Der Risikokatalog gilt für eine Vielzahl von Unternehmen, sodass er nicht alle Themenfelder für alle Unternehmen abdecken kann. Zudem sind Unternehmen immer neuen Regelungen und Situationen ausgesetzt wie zum Beispiel dem Lieferkettensorgfaltspflichtengesetz oder wie aktuell den weltweit verhängten Sanktionspaketen im Zusammenhang mit der russischen Invasion in die Ukraine.[39] Aus diesem Grund dient der Risikokatalog als erster Überblick und muss im Einzelfall auf Geschäftsmodell, -tätigkeit und -prozesse des jeweiligen Unternehmens angepasst und gegebenenfalls um eigene spezifische Themenfelder erweitert werden.[40]

Die Literatur beschreibt zusammenfassend verschiedene Möglichkeiten der Risikosammlung in Risikokatalogen durch die Sammlung geeigneter Informationen aus verschiedenen Quellen. Dabei werden überwiegend dieselben Themenfelder und Methoden genannt, sodass zumindest bei der Sammlung ein Anhaltspunkt besteht, wie diese bestmöglich durchgeführt werden kann. Allerdings gibt es nur wenige Anhaltspunkte wie die Relevanzanalyse in der Praxis oder nach einer Art Best Practice durchgeführt werden sollte.

31 *John*, Compliance ist keine Selbstverständlichkeit, 2021, S. 67.
32 Eigene Darstellung in Anlehnung an *John*, Compliance ist keine Selbstverständlichkeit, 2021, S. 67.
33 Konstanz Institut für Corporate Governance (KICG), Empfehlungen für die Ausgestaltung und Beurteilung von Compliance-Management-Systemen, CMS Guidance zu den Leitlinien 1 bis 4, 2014, S. 32 f.
34 Konstanz Institut für Corporate Governance (KICG), Empfehlungen für die Ausgestaltung und Beurteilung von Compliance-Management-Systemen, CMS Guidance zu den Leitlinien 1 bis 4, 2014, S. 32 f.
35 *Wind*, Leitfaden Compliance, 2018, S. 46 ff.
36 *Pauthner/Stephan*, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, 3. Aufl. 2016, § 16 Rn. 108.
37 *Jüttner/Artinger/Keller/Petersen*, CCZ 2019, 225.
38 Deutsches Institut für Compliance e. V., S09 – Compliance-Risikoanalyse (CRA), 2020, S.15; *Oeder/Havers/Barra Taladriz/Biaesch*, CB 2021, 159, 160.
39 *Bäumges/Jürgens*, CCZ 2022, 119.
40 Deutsches Institut für Compliance e. V., Risikokatalog – Hinweise und Erläuterungen zur Verwendung, 2022, S. 1.

Abb. 2: DICO-Risikokatalog[41]



IV. Ausblick

Ein weiterer Beitrag, der in CB 11/2023 erscheint, wird sich der Durchführung der Relevanzanalyse widmen und Hinweise zu deren Ablauf und Inhalt geben.

AUTOREN

Prof. Dr. Oliver Haag, *ist neben seiner Tätigkeit als Hochschullehrer an der HTWG Konstanz mit den Schwerpunkten Gesellschaftsrecht, Handelsrecht, Arbeitsrecht, Compliance und Corporate Governance als Direktor des Instituts für Unternehmensrecht sowie als Of-Counsel einer auf Unternehmensrecht spezialisierten Anwaltskanzlei tätig.*

Khadija Sandführ, *LL. M., ist als Wirtschaftsjuristin im Bereich Compliance und Risikomanagement in einem führenden Handelsunternehmen tätig. Zuvor studierte sie an der HTWG Konstanz Wirtschaftsrecht mit dem Schwerpunkt Corporate Compliance sowie Legal Management. Sie verfügt unter anderem über fundierte Kenntnisse in der Ausgestaltung von Compliance-Relevanzanalysen und -Risikoanalysen.*

41 Deutsches Institut für Compliance e. V., Risikokatalog, 2022.