

# Compliance Berater

11 / 2023

## Betriebs-Berater Compliance

26.10.2023 | 11.Jg  
Seiten 425–476

### EDITORIAL

**Greenwashing: Neue Herausforderung für Internal Investigations** | I

Dr. Martin Petrasch

### AUFSÄTZE

**Compliance für Wertpapierdienstleister mit der neuen EU Retail Investment Strategy** | 425

Anika Feger

**Das Hinweisgeberschutzgesetz in der Praxis von Banken und Finanzdienstleistern** | 432

Prof Dr. Dieter Krimphove

**DORA, internationaler Datentransfer und der „neue“ EU-US Datenschutzrahmen** | 436

Thomas Kahl und Charlotte Dreisigacker-Sartor

**10 Jahre MaRisk-Compliance** | 441

Markus Müller und Tabea Jarocki

**BAFA-Handreichung zur Zusammenarbeit in der Lieferkette** | 450

Dr. Lothar Harings, Stefanie Beermann und Dr. Julia Hörnig

**Berufsrecht-Compliance: Der neue § 31 BORA** | 455

Tim Günther

**Die Relevanzanalyse – Durchführung, Ablauf, Inhalt** | 459

Prof. Dr. Oliver Haag und Khadija Sandführ

### RECHTSPRECHUNG

**OLG Düsseldorf: Kartell-Geldbußen – Vorstand und Geschäftsführer haften nicht persönlich** | 465

Schwerpunktheft  
Finanz-Compliance

## CB-BEITRAG

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

# Die Relevanzanalyse – Durchführung, Ablauf, Inhalt

Um unternehmensspezifische Risiken zu erfassen ist die Risikoanalyse unumgänglich. Ihr ist wiederum eine Relevanzanalyse voranzustellen. Nachdem in CB 2023, 400 ff. die Grundlagen, Ziele, Anforderungen und Ansätze der Relevanzanalyse dargestellt wurden, widmet sich der nachfolgende Beitrag der Durchführung der Relevanzanalyse und gibt Hinweise zu deren Ablauf und Inhalt.

## I. Ablauf und Inhalt der Relevanzanalyse

Der grobe Ablauf der Relevanzanalyse gliedert sich in zwei Schritte. Zuerst werden im Rahmen der Inventarisierung die potenziell relevanten Themenfelder, die das Unternehmen betreffen könnten, identifiziert. Anschließend erfolgt im Rahmen der Bewertung eine Priorisierung der identifizierten Themenfelder. Mit diesem Ablauf kann das Unternehmen sicherstellen, dass das CMS entsprechend dem unternehmensindividuellen Risikostatus aufgestellt ist.<sup>1</sup> Nachfolgend werden die Methoden und Instrumente beschrieben, die nötig sind, die Inventarisierung und Bewertung durchführen zu können, und die zur Identifikation von Risiken genutzt werden, aber aufgrund der ähnlichen Vorgehensweise auch für die Identifikation der potenziellen Themenfelder der Relevanzanalyse geeignet sind.

### 1. Methoden zur Risikosammlung

Grundsätzlich existiert eine Vielzahl von Möglichkeiten in Form von Methoden und Instrumenten zur Risikosammlung und -identifikation. Dabei geht es um das Erfassen aller nicht gänzlich unwahrscheinlichen Themenfelder, wobei auch die Themenfelder einbezogen werden müssen, die durch Dritte und das Umfeld des Unternehmens relevant sein können.<sup>2</sup> Auch hier werden die Methoden angewandt, die bei der Risikoidentifikation, das heißt in einer späteren Phase des CRA vorkommen. Denn bei der Vorgehensweise in der Relevanzanalyse besteht eine Ähnlichkeit und die Methoden können somit auch auf sie angewandt werden.

#### a) Perspektiven

Damit alle potenziellen Themenfelder identifiziert und gesammelt werden können, ist es notwendig verschiedene Perspektiven einzunehmen, von denen in der Literatur überwiegend drei beschrieben werden, auch wenn es zahlreiche weitere gibt.<sup>3</sup> Dabei werden Themenfelder aus der internen, externen und analytischen Perspektive ausgewählt und betrachtet.

Die interne Perspektive umfasst die Geschäftsfelder und -modelle sowie die geschäftlichen Aktivitäten. Ebenso hervorzuheben sind besonders risikorelevante Unternehmenssparten, Funktionsbereiche und Abteilungen aufgrund der risikobezogenen Abläufe und Aktivitä-

ten wie beispielsweise der Vertrieb und die Vertriebswege. Die Standorte, Länderorganisationen und regionalen Organisationsbereiche sind ebenso bedeutsam. Innerhalb der internen Perspektive kann noch einmal die Perspektive in den Management-Kontext gewechselt werden, sodass auch Themen aus den Bereichen Strategie, Unternehmensziele, Risikotoleranz, Führung und vor allem die Unternehmenskultur von großer Bedeutung sind.<sup>4</sup>

Durch die externe Perspektive können Themenfelder wie Reputationsrisiken, Branchenrisiken oder auch länderspezifische Risiken erkannt werden. Auch Rechtsrisiken durch veränderte Gesetze und Regularien sowie Rechtsprechungsergebnisse können Auswirkungen auf die Identifikation relevanter Themenfelder haben.<sup>5</sup>

Die dritte Perspektive ist die analytische Perspektive, in der auf Auditergebnisse, Revisionsdaten und Controlling-Daten zurückgegriffen wird. Weiterhin können Erkenntnisse aus früherem Fehlverhalten im eigenen Unternehmen aber auch in anderen Unternehmen herangezogen werden, aus Compliance-Audits oder aus Ergebnissen aus der Beratungs- und Informationsfunktion des Compliance-Officers. Auch das Hinweisgebersystem und gegebenenfalls die Compliance-Ombudsfunktion können aufgrund der vorangegangenen Sachverhalte zur Risikosammlung beitragen.<sup>6</sup>

Die verschiedenen Perspektiven können bei der Identifikation und der Darstellung im Risikokatalog helfen, da diese eine Ordnung nach

1 Deutsches Institut für Compliance e.V., S09 – Compliance-Risikoanalyse (CRA), 2020, S. 10.

2 Pauthner, in: Ghassemi-Tabar/Pauthner/Wilsing, Corporate Compliance, 2016, S. 105.

3 Pauthner/Stephan, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, 3. Aufl. 2016, §16 Rn. 78 f.; Pauthner, in: Ghassemi-Tabar/Pauthner/Wilsing, Corporate Compliance 2016, S. 106.

4 Pauthner/Stephan, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, 3. Aufl. 2016, §16 Rn. 79.; Pauthner, in: Ghassemi-Tabar/Pauthner/Wilsing, Corporate Compliance 2016, S. 106.

5 Pauthner/Stephan, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, 3. Aufl. 2016, §16 Rn. 79.; Pauthner, in: Ghassemi-Tabar/Pauthner/Wilsing, Corporate Compliance 2016, S. 106.

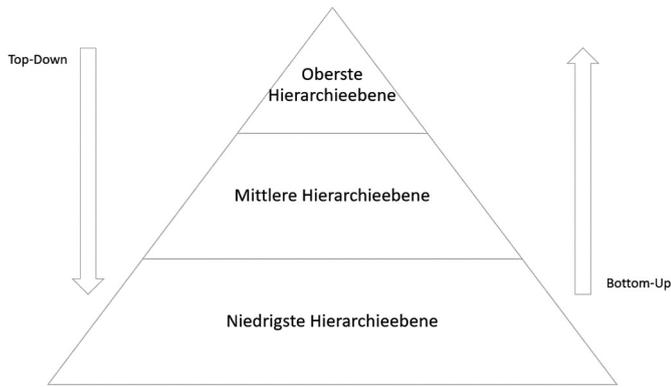
6 Pauthner/Stephan, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, 3. Aufl. 2016, §16 Rn. 79.; Pauthner, in: Ghassemi-Tabar/Pauthner/Wilsing, Corporate Compliance 2016, S. 106.

intern, extern und analytisch vorgeben. Weiterhin kann dies als Grundlage für die Anwendung der verschiedenen Methoden, wie beispielsweise dem Risikoworkshop, dienen.

**b) Top-Down und Bottom-Up Ansatz**

Je nach eingenommener Perspektive des Unternehmens können verschiedene Ansätze bei der Risikoidentifikation gewählt werden und hilfreich sein. Der Top-Down-Ansatz beginnt auf der obersten Hierarchieebene des Unternehmens, das heißt die oberste Managementebene beginnt mit der Identifizierung von potenziell relevanten Themenfeldern, bevor nachgelagerte Hierarchieebenen den Prozess fortsetzen.

**Abb. 1:** Top-Down und Bottom-Up-Ansatz<sup>7</sup>



Der Top-Down-Ansatz hat den Vorteil, dass potenziell relevante Themenfelder zügig und mit geringem Aufwand identifiziert werden können, da nur eine geringe Anzahl an Personen befragt werden muss. Zudem hat das Management eine erweiterte Sicht auf das Unternehmen sowie auf die Datenbasis wie relevante Unternehmensdaten, Geschäftspartner oder auch Compliance-Vorfälle, die durch die umfassende Sicht des Managements mit anderen Unternehmensbereichen verknüpft werden können, sodass dies zu Querbezügen, neuen Prozessen oder Projekten führen kann.<sup>8</sup> Allerdings kann die Top-Down-Vorgehensweise zu einem Nichterkennen von Abhängigkeiten verschiedener Risiken führen. Weiterhin dient der Top-Down Ansatz auch der Zusammenführung und Auswertung der in den verschiedenen Unternehmensbereichen gesammelten Bottom-Up-Ergebnisse durch die zentrale Compliance-Abteilung oder den zentralen Compliance-Verantwortlichen.<sup>9</sup>

Gegensätzlich dazu wird beim Bottom-Up-Ansatz auf der niedrigsten Hierarchieebene, das heißt in den operativen Einheiten des Unternehmens mit der Identifikation der potenziell relevanten Themenfelder begonnen und dann von den nachfolgenden Hierarchieebenen fortgesetzt. Dieses Vorgehen hat den Vorteil, dass die Personen in den operativen Einheiten an den risikorelevanten Abläufen beteiligt sind und so die Informationen zu potenziellen Themenfeldern eine hohe Qualität aufweisen. Wichtig dabei ist, dass die Compliance-Abteilung den Prozess koordiniert, sodass ein einheitliches Verfahren mit einem einheitlichen Grundverständnis zum Vorgehen und der Bewertung von potenziellen Themenfeldern gegeben ist.<sup>10</sup> Ein weiterer Vorteil des Bottom-Up-Ansatzes ist, dass wenn der Prozess auf der obersten Hierarchieebene endet, alle gesammelten Informationen zentral zusammengeführt werden können. Allerdings ist dieser Ansatz deutlich aufwendiger als der Top-Down-Ansatz und es fehlt an einer Abwägung aus der Gesamtperspektive des Unternehmens.<sup>11</sup>

Damit die Vorteile des jeweiligen Ansatzes genutzt und die Nachteile weitestgehend ausgeschlossen werden können, können beide Ansätze in Form des sogenannten Gegenstromverfahrens kombiniert werden. Hierbei wird die oberste Hierarchieebene genutzt, um potenziell relevante Themenfelder vorab zu identifizieren, die dann von den untersten Hierarchieebenen verifiziert und erweitert werden.<sup>12</sup> So kann die Expertise der operativen Einheit durch die Nähe zu risikorelevanten Themen genutzt werden und der Gesamtüberblick geht durch die Priorisierung und Aggregation nicht verloren.

**c) Progressiver und retrograder Ansatz**

Ein weiterer Ansatz zur Identifikation von potenziell relevanten Themenfeldern innerhalb des Unternehmens liegt in der Nutzung des progressiven und des retrograden Ansatzes.

**Abb. 2:** Progressiver und Retrograder Ansatz<sup>13</sup>



Der progressive Ansatz geht von den Risikoquellen beziehungsweise Risikoursachen als Ansatz des Risikoprozesses aus und verfolgt die Risiken bis hin zu den definierten Zielen und der Strategie des Unternehmens. Dabei sollten die Bereiche im Unternehmen identifiziert werden, in denen potenziell relevante Themenfelder auftreten können. Daraufaufgehend werden die Ursachen der Themenfelder identifiziert und welche Auswirkungen diese auf die Ziele und die Strategie des Unternehmens haben können.<sup>14</sup> Je nach Größe, Branche und Struktur des Unternehmens ist es sinnvoll, dieses in verschiedene Bereiche wie zum Beispiel strategische Geschäftsfelder und Geschäftseinheiten, rechtliche Einheiten und Betriebsstätten, aufzuteilen, um Schritt für Schritt alle relevanten Themenfelder zu identifizieren. In der Praxis sollte dieser Ansatz mit der Analyse von zentralen und unentbehrlichen Unternehmensprozessen beginnen und alle Aktivitäten und Prozesse nach internen und externen potenziellen Themenfeldern durchsuchen. Mit der Durchführung dieses Ansatzes können nahezu alle Themenfelder des Unternehmens identifiziert werden, auch wenn der Ansatz aufwendig ist.<sup>15</sup> Die Unternehmensziele und die Strategie bilden beim retrograden Ansatz den Ausgangspunkt, wodurch potenzielle Themenfelder direkt

7 Eigene Darstellung in Anlehnung an *Knauf/Bender*, in: Mahnke/Rohlf's, Betriebliches Risikomanagement und Industrieversicherung, 2020, S. 22 f.  
 8 *Knauf/Bender*, in: Mahnke/Rohlf's, Betriebliches Risikomanagement und Industrieversicherung, 2020, S. 23; *Pauthner/Stephan*, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, 3. Aufl. 2016, §16 Rn. 59.  
 9 *Pauthner/Stephan*, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, 3. Aufl. 2016, §16 Rn. 59.  
 10 *Pauthner/Stephan*, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, 3. Aufl. 2016, §16 Rn. 57.  
 11 *Knauf/Bender*, in: Mahnke/Rohlf's, Betriebliches Risikomanagement und Industrieversicherung, 2020, S. 23; Deutsches Institut für Compliance e.V., S09 – Compliance-Risikoanalyse (CRA), 2020, S. 16.  
 12 *Kark*, Compliance-Risikomanagement, 2. Aufl. 2019, S. 171; *Knauf/Bender*, in: Mahnke/Rohlf's, Betriebliches Risikomanagement und Industrieversicherung 2020, S. 23 f.  
 13 Eigene Darstellung in Anlehnung an *Knauf/Bender*, in: Mahnke/Rohlf's, Betriebliches Risikomanagement und Industrieversicherung, 2020, S. 22 f.  
 14 *Diederichs*, Risikomanagement und Risikocontrolling, 4. Aufl. 2018, S. 95 f.; *Knauf/Bender*, in: Mahnke/Rohlf's, Betriebliches Risikomanagement und Industrieversicherung 2020, S. 22 f.  
 15 *Diederichs*, Risikomanagement und Risikocontrolling, 4. Aufl. 2018, S. 96.

identifiziert werden, die unmittelbare Auswirkungen auf die Ziele und Strategie haben. Hierzu müssen in einem ersten Schritt die Ziele des Gesamtunternehmens sowie der einzelnen Funktionsbereiche herangezogen werden und falls nicht vorhanden, müssen diese hergeleitet werden. Danach werden die Themenfelder untersucht, die einen negativen Einfluss auf die Zielerreichung haben können und in welchen Bereichen diese Risiken verursacht werden. Der Vorteil des retrograden Ansatzes liegt in der zielgerichteten Suche und Identifikation der Themenfelder und erlaubt eine exaktere Erkennung von Zusammenhängen. Weiterhin ist dieser Ansatz weniger aufwendig als der progressive Ansatz und kann dadurch in weniger Zeit durchgeführt werden.<sup>16</sup> Ebenso wie bei Top-Down und Bottom-Up sollten auch beim progressiven und retrograden Ansatz beide Ansätze miteinander kombiniert werden, um das bestmögliche Ergebnis zu erreichen. So kann nach einer retrograden Erkennung von potenziellen Themenfeldern die Vollständigkeit der Erfassung durch eine progressive Vorgehensweise überprüft und gegebenenfalls angepasst werden. In der Praxis haben daher beide Ansätze ihre Berechtigung und sollten im richtigen Maß angewendet werden.<sup>17</sup>

#### d) Risikoindikatoren

Eine weitere Methode zur Risikosammlung und Risikoidentifikation ist das Vorgehen mit Hilfe von Risikoindikatoren.<sup>18</sup>

Risikoindikatoren sind Umstände und Merkmale, die auf potenzielle Risiken oder Themenfelder hinweisen können. Das Vorliegen eines Indikators ist jedoch kein direktes Indiz für ein Risiko, sondern eher ein Hinweis auf einen näheren Prüfungsbedarf des Sachverhalts. So kann dann überprüft werden, ob ein potenzielles oder ein tatsächliches Risiko beziehungsweise Risikothemenfeld vorliegt oder sogar ein tatsächliches Fehlverhalten identifiziert wurde. Risikoindikatoren sind zahlreich und können aus internen und externen Merkmalen wie der operativen Tätigkeit des Unternehmens oder Umfeldbedingungen abgeleitet werden. Risikoindikatoren im Compliance Bereich sind beispielsweise auffällige Gutschriften, unvollständige Vertragsdokumentation, häufige Umbuchungen, nicht ausgeräumte Interessenskonflikte oder auch der Einkauf zu nicht marktgerechten Preisen.<sup>19</sup> Damit die Identifikation mit Hilfe von Risikoindikatoren erfolgreich sein kann, muss das Unternehmen einen individuellen Katalog an Indikatoren aufbauen und kontinuierlich anpassen und erweitern, um die Wirksamkeit der Risikoidentifikation steigern zu können. Die Indikatoren sollten dann in Kategorien geordnet werden, wie zum Beispiel Länder, Deliktsarten oder Schadensarten. Allerdings sollte dies erst in einer späteren Phase der Identifikation zum Einsatz kommen, um eine zusätzliche Überprüfung der bereits gesammelten Themenfelder vorzunehmen und um die Risikosammlung nicht zu Beginn einzuschränken.<sup>20</sup>

Anhand der verschiedenen Methoden wird deutlich, dass die Risikosammlung ein eher aufwendiger Prozess ist und nur annähernd vollständig sein kann, wenn eine Kombination der Methoden und Ansätze gewählt wird. Dabei muss unternehmensindividuell bewertet werden, welche Methoden und Ansätze für das jeweilige Unternehmen von Bedeutung sind. Damit die Risikosammlung und Identifizierung von Risiken vollumfänglich und systematisch sichergestellt werden kann, sollten neben den Methoden zur Risikosammlung auch Instrumente zur Identifizierung angewandt werden.

## 2. Instrumente zur Identifizierung

Es gibt eine Vielzahl an verschiedenen Instrumenten zur Identifizierung von potenziell relevanten Themenfeldern, die bei entsprechender An-

wendung und Kombination für die Unternehmen sehr hilfreich sein können. Darunter fallen zum Beispiel Fragebögen, Checklisten, Interviews mit Experten und/oder Mitarbeitern, Brainstorming, Entscheidungsbäume und -tabellen, SWOT-Analysen (Strengths, Weaknesses, Opportunities, Threats) oder auch Workshops.<sup>21</sup> Nachfolgend werden die Instrumente dargestellt, die eine strukturierte und systematische Identifikation mit einer gewissen Objektivität ermöglichen, für die Relevanzanalyse relevant sind und die sich in der Praxis bewährt haben.

#### a) Fragebögen

Das methodische Vorgehen durch Fragebögen bei der Identifizierung von Themenfeldern dient als eigenes Instrument, kann aber auch als Grundlage für weitere Instrumente dienen.

Fragebögen eignen sich vor allem, um innerhalb kurzer Zeit eine Einschätzung zu bekommen. Dabei muss in einem ersten Schritt überlegt werden, welche Fragen und damit Themenfelder Inhalt des Fragebogens sein sollen. Die Fragen werden anhand der vorhandenen Informationsquellen entwickelt. Empfehlenswert ist, eine Art Masterfragebogen zu erstellen, der alle denkbaren Fragen enthält und dann auf die jeweilige Fachabteilung und Anforderung abgeändert werden kann. Dabei sollten rund 70–80% des Fragebogens als Basis gleichbleiben und „nur“ die restlichen 20–30% variieren können, um der Individualität der verschiedenen Abteilungen gerecht zu werden.<sup>22</sup> Die relevanten Fachbereiche erhalten den Fragebogen von der Compliance-Abteilung oder dem Compliance-Verantwortlichen und beschreiben ihre Themenfelder und machen Vorschläge für Gegenmaßnahmen, die aus ihrer Sicht sinnvoll sein können, um das Risiko zu minimieren.<sup>23</sup> Damit der Fragebogen so viele Themenfelder wie möglich abdeckt, sollte am Ende jedes Fragebogens eine offene Fragestellung stehen, bei der die verschiedenen Abteilungen Themen eintragen können, die der Fragebogen bisher nicht berücksichtigt hat, die aber ein Compliance-Risiko darstellen können. Auch wenn ein Fragebogen nie abschließend sein kann, wird so verhindert, dass relevante und spezifische Themen einer Abteilung übersehen werden.<sup>24</sup> Eine weitere Voraussetzung für den Erfolg der Informationssammlung anhand von Fragebögen ist eine leicht verständliche Fragestellung, da bei Unklarheiten nicht direkt Rückfragen gestellt werden können. Weiterhin muss beachtet werden, dass der Fragebogen ernsthaft beantwortet wird und von den Abteilungen nicht als lästige Zusatzaufgabe angesehen wird, die schnell während der Arbeitszeit erledigt werden muss, denn sonst sind die Ergebnisse nicht valide und erfüllen nicht die Anforderungen einer qualitativ hochwertigen Analyse.<sup>25</sup>

16 *Knauf/Bender*, in: Mahnke/Rohlf, Betriebliches Risikomanagement und Industrieversicherung, 2020, S. 22 f.; Diederichs, Risikomanagement und Risikocontrolling, 4. Aufl. 2018, S. 96.

17 *Diederichs*, Risikomanagement und Risikocontrolling, 4. Aufl. 2018, S. 96.

18 *Wind*, Leitfaden Compliance, 2018, S. 47.

19 *Pauthner/Stephan*, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, 3. Aufl. 2016, §16 Rn. 89 ff.

20 *Pauthner/Stephan*, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, 3. Aufl. 2016, §16 Rn. 92 ff.

21 *Haag/Bindschädel*, CB 2021, 112, 114; *Philippi*, in: Bay/Hastenrath, Compliance-Management-Systeme, 3. Aufl. 2022, § 3 Rn. 50; *Straßer/Koch*, in: Zenke/Schäfer/Brocke, Corporate Governance, 2. Aufl. 2020, S. 45.

22 *Vogelsang*, CB 2016, 463 ff.

23 *Kark*, ZRFC 2019, S. 254, 258.

24 *Vogelsang*, CB 2016, 463, 466.

25 *Otremba*, in: Wieland/Steinmeyer/Grüninger, Handbuch Compliance-Management, 3. Aufl. 2020, S. 440 f.

Grundsätzlich ist ein Fragebogen ein vergleichsweise unkompliziertes Instrument zur Risikosammlung, das sehr effiziente Ergebnisse in relativ kurzer Zeit liefern kann.

### b) Interviews

Interviews können auf verschiedene Art und mit verschiedenen Personen durchgeführt werden. Sie können an Fragebögen oder Leitfäden orientiert sein oder mit Experten außerhalb des Unternehmens durchgeführt werden.

Zunächst bietet sich allgemein das bilaterale Interview an, bei dem ein Fragebogen oder Leitfaden als Grundlage des Gesprächs herangezogen wird, um das Instrument des Interviews strukturiert, mit Systematik, Einheitlichkeit und Vergleichbarkeit der Ergebnisse, durchführen zu können. Der Fragebogen oder Leitfaden dient dabei als Orientierung und soll sicherstellen, dass keine wichtigen Aspekte übersehen werden. Der Fragebogen kann vor dem Interview versendet werden, damit sich der Empfänger mit dem Thema vertraut machen kann und das Gespräch zu sinnvollen Ergebnissen führt. Kennzeichnend ist, dass offen formulierte Fragen zum Einsatz kommen, auf die der Befragte frei antworten kann und soll. Der Interviewer kann somit auch entscheiden, ob und bei welchen Fragen er noch einmal detaillierter nachfragt und wann er zum Fragebogen oder Leitfaden zurückkehrt.<sup>26</sup> Experteninterviews eignen sich vor allem, um neue Denkanstöße zu Themenfeldern durch Spezialwissen zu erlangen und so auch in Zukunft selbst Risiken besser identifizieren zu können. Durch das Spezialwissen der Experten sind diese Interviews sehr effektiv bei der Risikosammlung in einem klar definierten Themengebiet. Aus diesem Grund ist es wichtig, verschiedene Experten mit unterschiedlichem Spezialwissen zu befragen und neben Experteninterviews auch unternehmensinterne Interviews durchzuführen, um nicht auf bestimmte Themengebiete begrenzt zu sein, da Experten nicht an alle unternehmensinternen Gegebenheiten denken können.<sup>27</sup>

Auch wenn ein Interview aufwendiger ist als ein Fragebogen, führt das Interview meist zu fundierten Ergebnissen, da sich beide Seiten intensiv mit dem Thema Risiken beschäftigen. Gleichzeitig erfährt das Thema der Risikoanalyse eine höhere Sensibilität in den Abteilungen, sodass der Erkenntnisgewinn für beide Seiten, also Fachabteilung sowie Compliance-Abteilung, besteht. Der Dialog bietet zudem die Möglichkeit, nach der Identifizierung von Themenfeldern auch adäquate Lösungen zu finden, sodass die Umsetzung derer von beiden Funktionen entwickelt und getragen wird. Durch die Kombination der Identifikation der Risiken und dem Finden der passgenauen, individuellen Lösungen für die Compliance-Steuerung, bietet ein Interview die Chance, die Lösungen und Maßnahmen zuverlässig umzusetzen und deren Akzeptanz durch die Abteilungen und ihr Mitwirken zu steigern.<sup>28</sup>

### c) Compliance-Risiko-Workshops

Ein Compliance-Risiko-Workshop ist der multilaterale Austausch über Compliance-Risiken zwischen zwei Parteien, in diesem Fall der Compliance-Abteilung beziehungsweise dem Compliance-Verantwortlichen mit den relevanten und sachkundigen Personen der Fachabteilungen des Unternehmens. Ebenso wie bei den bereits genannten Instrumenten ist auch beim Workshop auf einen strukturierten und systematischen Ablauf zu achten, der eine Einheitlichkeit und Vergleichbarkeit der Ergebnisse gewährleistet.<sup>29</sup>

Der Risiko-Workshop ist ein wirksames und bewährtes Instrument zur Risikoidentifikation, da er zu einem besseren Risikoverständnis der

Beteiligten führt und wichtige Erkenntnisse über Zusammenhänge zwischen Risikoindikatoren und Einzelrisiken und Themenfeldern gewonnen werden können. Der Workshop kann in allen Unternehmensbereichen eingesetzt werden und kann sowohl Top-Down als auch Bottom-Up durchgeführt werden und so noch wirksamer sein.<sup>30</sup> Zu Beginn des Workshops wird der Anlass des Workshops erörtert sowie die im Vorfeld grob gesammelten Themenfelder diskutiert. Zusätzlich werden die Teilnehmer ermutigt, weitere für ihre Abteilung spezifische Themenfelder zu identifizieren. Dabei kann in einer Art Brainstorming alles zusammengetragen werden, sodass durch eine offene Diskussion auch neu aufkommende Themen berücksichtigt werden können. In einem nächsten Schritt werden die identifizierten Themenfelder beschrieben und gegebenenfalls priorisiert und die Teilnehmer können auch Maßnahmen zur Minimierung vorschlagen.<sup>31</sup>

Für die Wirksamkeit des Workshops ist eine gute Vorbereitung unerlässlich, weshalb das Instrument des Risiko-Workshops einen hohen organisatorischen Aufwand aufweist und ebenso zeitintensiv ist, vor allem im Vergleich zu den anderen Instrumenten.<sup>32</sup> Wichtig sind eine klare Zielsetzung und Ausrichtung auf bestimmte Ergebnisse, um den Fokus korrekt zu setzen. Auch die Anzahl und Auswahl der Teilnehmer ist entscheidend: Sind zu viele Teilnehmer anwesend, können die einzelnen Perspektiven nicht ausreichend beschrieben und beleuchtet werden. Daher hat sich in der Praxis eine Teilnehmeranzahl von mindestens drei bis maximal acht Teilnehmern als praktikabel und wirksam herausgestellt. Bei der Auswahl der Teilnehmer ist darauf zu achten, dass von jedem relevanten Prozess und Risiko mindestens ein Vertreter anwesend ist. Die Teilnehmer werden vor dem Workshop vorbereitet, indem sie wichtige Informationen zum Ablauf, der eingesetzten Instrumente und der Ziele des Risiko-Workshops erhalten. Personen, die nicht am Workshop teilnehmen, aber dennoch über relevante Informationen verfügen könnten, werden durch ein Vorgespräch abgefragt.<sup>33</sup>

Die Compliance-Abteilung beziehungsweise der Compliance-Verantwortliche sollte als Moderator oder Schriftführer Teil des Risiko-Workshops sein. Falls ein Geschäftsleitungsmitglied am Workshop teilnimmt, sollte vorab besprochen werden, wer Moderator des Workshops ist. Der Moderator sollte nicht zu stark eingreifen, sondern eher eine lenkende Funktion einnehmen. Aus diesem Grund sollten auch Moderation und Schriftführung personell getrennt sein, da der Schriftführer für das Verlaufsprotokoll zuständig ist und somit die Diskussion nicht durchgehend aufmerksam verfolgen kann.<sup>34</sup> Weiterhin sollte die

26 Ebersoll/Stork, Smart Risk Assessment, 2016, S. 125 f.; Mayer, Interview und schriftliche Befragung, 6. Aufl. 2013, S. 37.

27 Knauf/Bender, in: Mahnke/Rohlf, Betriebliches Risikomanagement und Industrieversicherung 2020, S. 28.

28 Otremba, GRC-Management als interdisziplinäre Corporate Governance, 2016, S. 178; Otremba, in: Wieland/Steinmeyer/Grüniger, Handbuch Compliance-Management, 3. Aufl. 2020, S. 441.

29 Ebersoll/Stork, Smart Risk Assessment, 2016, S. 125; Kark, ZRFC 2019, S. 254, 258.

30 Pauthner, in: Ghassemi-Tabar/Pauthner/Wilsing, Corporate Compliance, 2016, S. 107 f.

31 Klasen/Buljko, in: Wieland/Steinmeyer/Grüniger, Handbuch Compliance-Management, 3. Aufl. 2020, S. 503 f.

32 Pauthner, in: Ghassemi-Tabar/Pauthner/Wilsing, Corporate Compliance, 2016, S. 107 f.; Ebersoll/Stork, Smart Risk Assessment, 2016, S. 125.

33 Pauthner, in: Ghassemi-Tabar/Pauthner/Wilsing, Corporate Compliance, 2016, S. 107 f.

34 Pauthner, in: Ghassemi-Tabar/Pauthner/Wilsing, Corporate Compliance, 2016, S. 109 ff.; Bendrich, CCZ 2019, 145, 146.

verantwortliche Stelle eine kurze Agenda aufstellen, um den Workshop grob zu strukturieren und um einen allgemeinen Zeitrahmen festzulegen. Dieser sollte nicht unter zwei Stunden angesetzt werden, um einen zweckmäßigen Workshop zu gestalten. Zur Unterstützung der Agenda und sonstigen Unterlagen kann es sinnvoll sein einige Dateien oder PowerPoint-Folien vorzubereiten. So können komplizierte Themen durch eine Visualisierung vereinfacht werden oder auch mit möglichen Top-Risiken der vorausgehenden Periode ausgestattet sein. Allerdings sollte eine zu detaillierte Vorabinformation oder Unterstützung durch Themenfelder der Vorperiode vermieden werden, um der freien Diskussion Raum zu lassen und um die Themenfelder nicht durch eine Vorauswahl einzuschränken.<sup>35</sup>

Der Risiko-Workshop wird anhand eines Ergebnisprotokolls dokumentiert, in dem Ergebnisse, aber auch die Gründe für die Gewichtung beziehungsweise Priorisierung der Themenfelder sowie die Dauer und der Verlauf der Diskussion dargestellt werden. Durch Rücksprache mit den Abteilungen, können klärungsbedürftige Themenfelder noch einmal aufgegriffen werden, sodass der Workshop vollständige Ergebnisse liefert.<sup>36</sup>

#### d) Dokumentation

Unabhängig von den gewählten Instrumenten ist es entscheidend, dass vergleichbare und reproduzierbare Ergebnisse erfasst werden, die für Dritte nachvollziehbar und datensicher dokumentiert sind. Dies ist nicht nur für den Fall eines Compliance-Verstoßes und der damit verbundenen Nachweispflicht gegenüber Behörden, der eigenen Organisationspflicht nachgekommen zu sein, entscheidend, sondern auch, weil dies die Grundlage für den weiteren CRA-Prozess darstellt. Die Dokumentation ist somit unumgänglich.<sup>37</sup> Weiterhin ist für alle Instrumente eine sorgfältige Auswahl der Teilnehmer von hoher Relevanz, da sie eine gewisse Verantwortlichkeit für das Risiko haben und auskunftsfähig sein müssen. Es müssen die Mitarbeiter ausgewählt werden, unabhängig von der Führungsebene, die vom Risiko betroffen sind und damit eine Orts- und Sachnähe aufweisen. Zudem muss eine angemessene Vorbereitungszeit beziehungsweise Bearbeitungszeit bei Fragebögen eingeräumt werden. Diese Anforderungen entsprechen dem Grundsatz der sorgfältigen Auswahl der Beschäftigten, welche zu den Hauptpflichten des Betriebsinhabers nach § 130 OWiG gehören, wonach ein strukturiertes und transparentes Verfahren zur Auswahl neuer Mitarbeiter erforderlich ist. Dieser Auswahlpflicht kommt auch im Rahmen der Relevanzanalyse und damit auch im Rahmen des CRA eine große Bedeutung zu, denn die identifizierten Themenfelder sind nur dann geeignet, wenn sie angemessene, und der gehörigen Aufsicht gemäß § 130 OWiG entsprechende Aufsichtsmaßnahmen nach sich ziehen und damit der tatsächlichen Risikolage des Unternehmens entsprechen.<sup>38</sup>

Die vorherig beschriebenen Instrumente können erfolgreich durchgeführt werden, wenn sie je nach Unternehmenskultur angewendet werden. Bei einer eher verschlossenen Unternehmenskultur bringen anonyme Fragebögen einen größeren Erfolg als Workshops, während es bei einer offenen Unternehmenskultur bei Workshops oder Interviews zu besseren Ergebnissen kommen wird. So kann für jedes Unternehmen ein anderes Instrument von Erfolg gekrönt sein, oder auch eine Kombination aus diesen.<sup>39</sup>

### 3. Risikogliederung und -priorisierung

Die zahlreichen potenziellen Themenfelder, die durch die verschiedenen Methoden und Instrumente identifiziert wurden, müssen in einem nächsten Schritt strukturiert werden, um eine Priorisierung der The-

menfelder vornehmen zu können.<sup>40</sup> Das Ergebnis der Identifikation der relevanten Themenfelder, das Risikoinventar oder auch ein Risikokatalog, ist eine strukturierte Darstellung aller identifizierten und relevanten Themenfelder. Diese kann zum Beispiel in Form einer Liste oder in Form einer Risikolandschaft, ähnlich wie der DICO-Risikokatalog, dargestellt werden.<sup>41</sup> Da im Rahmen der Relevanzanalyse Themenfelder betrachtet werden und nicht Einzelrisiken, ist es oft nicht sinnvoll, diese nach Geschäftsbereichen, Ursachen oder auch Auswirkungen zu gliedern. Um dennoch einen besseren Überblick über die Themenfelder zu bekommen, können diese in verschiedene Gruppen gegliedert werden, die einen Überbegriff, wie beispielsweise selbstgesetzte Standards, haben.

Aus dieser großen Menge sind dann in einem ersten Schritt die Themenfelder zu identifizieren, in denen wesentliche Risiken für das Unternehmen vermutet werden. Voraussetzung für diese Auswahl ist, dass die Risikostrategie des Unternehmens bekannt ist, sodass Themenfelder als weniger relevant eingestuft werden können, die bewusst im Rahmen der geschäftlichen Aktivität eingegangen werden müssen.<sup>42</sup> In einem nächsten Schritt folgt dann die Priorisierung der identifizierten Themenfelder, indem überprüft wird, ob die identifizierten Themenfelder auch wirklich wesentlich beziehungsweise signifikant für das Unternehmen sind. Diese Priorisierung ist nötig, um die Ressourcen des Unternehmens effektiv und effizient zu steuern und einzusetzen.<sup>43</sup>

Ein Hilfsmittel zur Priorisierung der relevanten Themenfelder kann ein Entscheidungsbaum und/oder eine Entscheidungstabelle sein.<sup>44</sup> Durch diese können bestimmten Themenfeldern ausgewählte und unternehmensindividuelle Kriterien zugeordnet werden, durch die eine systematische und nachvollziehbare Priorisierung zustande kommt. Die Kriterien können zum Beispiel auf die Folge eines Verstoßes zielen, sodass eine Wesentlichkeit bei einem Reputationsschaden, eine Erlösschmälerung, eine Organhaftung, eine Geldbuße, die größer ist als eine unternehmensintern gesetzte Grenze oder auch der Entzug der Teilnahme an Ausschreibungen als Kriterium dienen kann. Hierbei können auch Verstöße aus der Vergangenheit oder in der Branche berücksichtigt werden.<sup>45</sup>

Weiterhin ist es üblich, die Ergebnisse noch einmal auf Plausibilität zu prüfen, indem sie mit Experten beziehungsweise fachkundigen Mitarbeitern des Unternehmensbereiches oder Rechtsgebietes validiert und falls nötig diskutiert werden.<sup>46</sup> Auf dieser Grundlage hat die

35 Pauthner, in: Ghassemi-Tabar/Pauthner/Wilsing, Corporate Compliance, 2016, S. 109 ff.; Bendrich, CCZ 2019, 145, 146.

36 Pauthner, in: Ghassemi-Tabar/Pauthner/Wilsing, Corporate Compliance, 2016, S. 112 f.

37 Otremba, in: Wieland/Steinmeyer/Grüniger, Handbuch Compliance-Management, 3. Aufl. 2020, S. 442; Pauthner, in: Ghassemi-Tabar/Pauthner/Wilsing, Corporate Compliance, 2016, S. 107.

38 von Busekist/Schlitt, CCZ 2012, 86, 93.

39 von Busekist/Schlitt, CCZ 2012, 86, 92.

40 Pauthner, in: Ghassemi-Tabar/Pauthner/Wilsing, Corporate Compliance, 2016, S. 114.

41 Knauf/Bender, in: Mahnke/Rohlf, Betriebliches Risikomanagement und Industrieversicherung, 2020, S. 37 f.

42 Pauthner/Stephan, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, 3. Aufl. 2016, §16 Rn. 111.

43 Pauthner/Stephan, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, 3. Aufl. 2016, §16 Rn. 111 ff.

44 Straßer/Koch, in: Zenke/Schäfer/Brocke, Corporate Governance, 2. Aufl. 2020, S. 46.

45 Wermelt, CB 2014, 109, 110.

46 von Busekist/Schlitt, CCZ 2012, 86, 95.

Unternehmensleitung zu entscheiden, welche signifikanten Themenfelder in das CMS aufgenommen werden müssen. Die Entscheidungsfindung zur Festlegung der relevanten und signifikanten Themenfelder sollte gut dokumentiert werden, denn nur so kann belegt werden, dass die Relevanzanalyse mit integrierter Signifikanzprüfung systematisch und nicht willkürlich vorgenommen wurde.<sup>47</sup>

Eine Priorisierung mit Hilfe einer Risikomatrix, Tabelle oder als Säulendiagramm ist für Einzelrisiken sinnvoll, da eine Rangordnung festgelegt werden kann, welche Risiken zuerst gesteuert werden müssen.<sup>48</sup> Allerdings ist das für die Priorisierung als Teil der Relevanzanalyse nicht von Bedeutung, da es hier um die Sammlung möglicher Themenfelder geht, die durch die Priorisierung konkretisiert werden, sodass als Ergebnis keine Rangordnung entstehen soll, sondern eine Sammlung relevanter und signifikanter Themenfelder für das Unternehmen. Die Priorisierung ist letztlich im Rahmen der Relevanzanalyse durch das Unternehmen anhand eigens erstellter bzw. gewählter Hilfsmittel, Methoden, Instrumente oder Kriterien vorzunehmen, um die unternehmensindividuell relevanten und signifikanten Themenfelder zu identifizieren.

Der Prozess der Priorisierung sollte ebenso wie die Risikoidentifikation beziehungsweise der komplette CRA-Prozess nicht einmalig, sondern in regelmäßigen Abständen wiederholt werden, denn es werden sich neue relevante und signifikante Themenfelder für das Unternehmen ergeben und die Risikostrategie des Unternehmens wird sich durch neue Gegebenheiten anpassen müssen. Die Effektivität des CRA und der Relevanzanalyse lebt von einem kontinuierlichen Prozess der Informationsbeschaffung.<sup>49</sup>

## II. Zusammenfassung

Auch wenn es für die Relevanzanalyse noch keine anerkannte wissenschaftliche Methodik gibt, kann durch die verschiedenen aufgezeigten Ansätze, Instrumente und Methoden ein methodischer Ablauf der Relevanzanalyse im Unternehmen etabliert und damit eine systematische und methodische Identifikation von Themenfeldern garantiert werden. Damit ist eine entsprechend professionell und struk-

turiert durchgeführte Relevanzanalyse Grundlage des sich anschließenden CRA und steigert und verbessert dessen Effektivität und Effizienz ebenso wie die Sicherheit des auf Basis des CRA zu etablierenden CMS. Auch wenn dies mit Aufwand verbunden ist, sollte daher der Relevanzanalyse als wertvollem Instrument zur Risikominimierung hinreichend Aufmerksamkeit gewidmet werden.

---

### 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.

---

47 Wermelt, CB 2014, 109, 110.

48 Haag/Bindschädel, CB 2021, 112, 117; Kark, Compliance-Risikomanagement, 2. Aufl. 2019, S. 83 f.

49 Philippi, in: Bay/Hastenrath, Compliance-Management-Systeme, 3. Aufl. 2021, §3 Rn. 63.