www.compliance-berater.de

Compliance Berater

4 / 2021

Betriebs-Berater Compliance

25.03.2021 | 9.Jg
Seiten 89–136

Fachmedien Recht und Wirtschaft | dfv Mediengruppe | Frankfurt am Main

CB-BEITRAG

Prof. Dr. Oliver Haag und Hannah Bindschädel, LL. M.

Das idealtypische Compliance Risk Assessment – Teil 2

Nachdem im 1. Teil des Beitrags (siehe CB 2021, 64) die wesentlichen zu berücksichtigenden Faktoren eines idealtypischen Compliance Risk Assessments (CRA) dargestellt wurden, sollen im nun folgenden 2. Teil Hinweise zur Vorbereitung und Durchführung eines unternehmensspezifischen CRA gegeben werden.

I. Vorbereitung des Risk Assessments

Eine sorgfältige Vorbereitung des CRA sichert eine systematische und strukturierte Durchführung und damit valide Ergebnisse. Im Rahmen der Vorbereitung sind die Rollen und Verantwortlichkeiten sowie der Scope des Risk Assessments festzulegen. Darüber hinaus ist zu bestimmen, welche Methode für die Durchführung verwendet wird.[1]

1. Festlegung von Rollen und Verantwortlichkeiten

Grundsätzlich trägt die Geschäftsführung die Verantwortung für das CRA sowie die Risikosteuerung. Sie sollte die Verantwortung für die Durchführung jedoch an die Compliance-Funktion bzw. den Compliance Officer übertragen.[2] Wichtig ist, dass der Compliance Officer oder eine andere, für das CRA verantwortliche Person, sowohl über die benötigte fachliche Eignung, als auch über vertiefte Unternehmenskenntnisse verfügt. Vor der Durchführung des Risk Assessments sollte außerdem eine Abstimmung mit der Risikomanagement-Abteilung stattfinden.[3] Fachabteilungen wie die Interne Revision, Controlling oder Recht sind einzubeziehen, da diese oftmals über risikorelevante Informationen verfügen. Um einen geregelten Austausch der Compliance-Funktion mit den relevanten Fachabteilungen zu gewährleisten, kann ein Risiko-Ausschuss eingerichtet werden.[4]

Außerdem sollten die Risikoverantwortlichen einzelner Organisationseinheiten oder Verantwortungsbereiche bei der Durchführung eines CRAs einbezogen werden. Des Weiteren sollten auch sonstige Führungskräfte und Mitarbeiter, die Kenntnisse über Geschäftsprozesse und diesbezügliche Compliance-Risiken haben, in den Risikoanalyse-Prozess integriert werden.[5] Existieren innerhalb eines Unternehmens keine Mitarbeiter, die über die nötige Fachkompetenz zur Durchführung von CRAs verfügen, sollten Externe mit dieser Aufgabe beauftragt werden.[6]

2. Festlegung des Scopes

Darüber hinaus muss im Rahmen der Vorbereitung der Scope des Risk Assessments bestimmt werden. Es muss jedenfalls grob analysiert und abgeschätzt werden, welche Themenfelder und Geschäftsaktivitäten in CRA einbezogen werden müssen. Basis der Relevanzanalyse können beispielsweise Risikoberichte der jeweiligen Branche oder Dokumente der Revision, der Rechtsabteilung oder des Risikomanagements bilden.[7] Das CRA sollte umfassend sein, d. h. ohne Einschränkungen auf bestimmte Rechtsquellen (z. B. Kartell- oder Datenschutzrecht), Unternehmensbereiche (z. B. Personal oder Einkauf) oder Jurisdiktionen. Aufgrund der Knappheit zeitlicher und finanzieller Ressourcen ist ein umfassendes CRA in der Praxis jedoch meist nicht umsetzbar. Wird die Reichweite des CRAs eingeschränkt, so sollte die Einschränkung daher zumindest sorgfältig erfolgen. Zur Bestimmung des Scopes werden meist Erfahrungswerte bezüglich der Risikogeneigtheit innerhalb der Gesellschaft oder der Branche herangezogen. Intransparente oder willkürliche Ausgrenzungen sollten vermieden werden, weil es dadurch zur Beeinträchtigung der haftungsreduzierenden Wirkung des CMS kommen könnte.[8]

Bei der Festlegung der Reichweite muss zum einen bestimmt werden, ob neben den gesetzlichen Vorgaben auch interne Richtlinien, freiwillige Selbstverpflichtungen sowie vertragliche Verpflichtungen einbezogen werden.[9] Darüber hinaus fokussieren viele Unternehmen ihr CRA aufgrund von Effizienz- und Praktikabilitätsgründen auf Risikobereiche deren tatsächlicher Eintritt drastische Folgen, wie z. B. hohe Bußgelder, die Strafbarkeit von Mitarbeitern, Reputationsschäden oder Auswirkungen auf das Geschäftsmodell, hat. Häufig sind dies typische Themenbereiche wie Korruption, Exportkontrolle, Datenschutz, Geldwäsche und Wettbewerbsrecht. Außerdem sind vor allem diejenigen Rechtspflichten von Bedeutung, deren Verstoß als Ordnungswidrigkeit oder Straftat geahndet wird. Neben der Eingrenzung der Risikobereiche wird das Risk Assessment oftmals auch hinsichtlich der einzubeziehenden Unternehmensteile beschränkt. Meist werden zentrale Unternehmenseinheiten sowie die Kerngebiete der geschäftlichen Tätigkeit einbezogen. Verbundene Unternehmen werden nur teilweise berücksichtigt. Dies liegt daran, dass davon aus-

1 *Wermelt*, CB 2014, 109, 111 f.
2 Konstanz Institut für Corporate Governance (KICG), Empfehlungen für die Ausgestaltung und Beurteilung von Compliance-Management-Systemen, Leitlinie 3, 2014, S. 32.
3 *Busekist/Schlitt*, CCZ 2012, 86, 91.
4 KICG (Fn. 2), Leitlinie 3, S. 32.
5 *Wermelt*, CB 2014, 109, 111 f.
6 *Busekist/Schlitt*, CCZ 2012, 86, 91.
7 Deutsches Institut für Compliance e. V., S09 – Compliance-Risikoanalyse (CRA), 2020, S. 15.
8 *Busekist/Schlitt*, CCZ 2012, 86, 88.
9 *Busekist/Schlitt*, CCZ 2012, 86, 88.

gegangen wird, dass die Geschäftsführung des verbundenen Unternehmens für die Einhaltung der gesetzlichen Vorgaben und internen Regelungen innerhalb ihrer Gesellschaft sorgt. Randaktivitäten sowie kleine Landesgesellschaften werden im Rahmen des CRAs ebenfalls oftmals nicht berücksichtigt.[10] Es ist jedoch zu empfehlen, dass die einzelnen Konzerngesellschaften, unabhängig von ihrem Sitz, ihrer Größe oder ihren Aktivitäten, zumindest innerhalb eines festgelegten Rhythmus bei der Durchführung der CRAs berücksichtigt werden.[11]

3. Auswahl der Methode

Neben der Festlegung der Verantwortlichkeiten und Rollen sowie des Scopes muss eine geeignete Methode für das CRA ausgewählt werden. Bei der Auswahl der Methode muss entschieden werden, ob ein manuelles oder ein smartes CRA durchgeführt wird. Bei der Auswahl der Methode ist zu bedenken, dass es grundsätzlich Ziel des CRAs ist, einen möglichst hohen Output zu erzielen und dabei Ressourcen schonend einzusetzen. In der Praxis ist der Aufwand für ein manuelles Risk Assessment jedoch oftmals hoch. Dies ist damit zu begründen, dass das operative Geschäft durch eine Vielzahl von Workshops, Interviews etc. belastet wird. Vor allem internationale Konzerne mit vielen Akteuren und Tochtergesellschaften haben mit dieser Problematik zu kämpfen. Trotz der genannten Nachteile kann auf das klassische CRA nicht verzichtet werden, denn es ermöglicht notwendige und unverzichtbare Informationen zu generieren. Um die Nachteile des manuellen Risk Assessments auszugleichen und eine effizientere Risikoanalyse zu gewährleisten, wurde das smarte CRA entwickelt. Die smarte Risikoanalyse wird zweistufig durchgeführt, die erste Stufe bildet dabei das sog. „Screening". Im Rahmen des Screenings werden operative Einheiten durch elektronische Unterstützung ausgewählt, die auf der zweiten Stufe näher analysiert werden. Nachdem das von jeder Tochtergesellschaft ausgehende Risiko ermittelt wurde, werden durch einen internen oder externen Vergleich oder durch absolute Auswahlkriterien diejenigen Gesellschaften und Einheiten bestimmt, die risikogeneigt sind und daher auf der zweiten Stufe genauer analysiert werden müssen. Die zweite Stufe bildet die sog. Dialogebene. Hier werden genauso wie beim manuellen CRA interaktive Dialoge in Form von Interviews, Workshops etc. geführt.[12]

II. Durchführung des Risk Assessments

Nachdem das CRA sorgfältig vorbereitet und eine systematische Vorgehensweise festgelegt wurde, kann es durchgeführt werden. Grundsätzlich kommen für die Durchführung der Risk Assessments verschiedene Ansätze in Frage. Des Weiteren kann die Durchführung in drei wesentliche Schritte untergliedert werden. In einem ersten Schritt werden die bestehenden Compliance-Risiken identifiziert, in einem zweiten Schritt werden sie analysiert. Zuletzt werden sie bewertet.[13]

Abb. 1: Ablauf des CRAs[14]

1. Mögliche Ansätze

Im Rahmen der Durchführung des Risk Assessments kommen verschiedene Ansätze in Betracht. Zu den möglichen Ansätzen zählen der Top-down und der Bottom-up-Ansatz sowie eine Kombination beider Ansätze. Unabhängig davon, welcher Ansatz ausgewählt wird, sollte die Compliance-Abteilung einheitliche Vorgaben und Anforderungen an die Durchführung des Risk Assessments bereitstellen, an denen sich die einzelnen Abteilungen und Geschäftseinheiten orientieren können.[15] Beim Top-down-Ansatz handelt es sich um eine zentrale Durchführung des Risk Assessments. Dabei werden die Compliance-Risiken von der obersten Hierarchiestufe durch die Betrachtung der Organisation und Prozesse identifiziert und bewertet. Beim Bottom-up-Ansatz wird die Top-down-Vorgehensweise auf den Kopf gestellt. Die Risiken werden hierbei innerhalb einzelner organisatorischer und/ oder geographischer Unternehmensteile, also dezentral, identifiziert und bewertet. Die Risikoidentifikation erfolgt direkt durch die Risiko- und Prozesseigner. Die identifizierten Risiken werden nach oben weitergegeben und von der zentralen Compliance-Funktion gesammelt.[16] Neben der Anwendung des Top-down oder Bottom-up-Ansatzes ist auch eine Kombination beider Ansätze möglich. Einerseits werden die Ergebnisse der Bottom-up-Analyse durch die zentralen Compliance- oder Risikomanagementbereiche zusammengeführt und ausgewertet. Andererseits führen die zentralen Fachbereiche eigene Risk Assessments in ausgewählten Unternehmensbereichen durch. Dadurch wird eine wiederholte, systematische Prüfung kritischer Bereiche gewährleistet.[17]

2. Risikoidentifikation

Die Identifikation der Compliance-Risiken ist entscheidend für die Qualität des CRAs. Es ist von Bedeutung, dass der für das CRA Verantwortliche im Rahmen einer systematischen Vorgehensweise Zugang zu jeglichen Informationen über Compliance-Risiken innerhalb des Unternehmens erhält.[18] Die Risikoidentifikation kann auf verschiedenen Ebenen erfolgen. Sie ist z. B. auf Ebene der Geschäftseinheiten oder -felder, auf Abteilungsebene oder auf Prozessebene möglich. Neben den eigentlichen Risiken sollten die Risikoverantwortlichen (sog. Risk Owner) des jeweiligen Einzelrisikos bestimmt werden.[19] Im Rahmen der Risikoidentifikation ist es von Bedeutung, ein umfassendes Bild über die Risikosituation des Unternehmens zu bekommen. Dazu müssen Informationen aus den unterschiedlichsten Quellen vernetzt werden.[20] Dabei ist zu beachten, dass Daten, die innerhalb des Unternehmens bereits erhoben wurden, wie z. B. statistische Daten über die Geschäftsentwicklung, unbedingt genutzt werden sollten.[21] Darüber hinaus ist es illusorisch zu denken, dass im Rahmen der Risikoidentifikation alle Compliance-Risiken aufgedeckt werden können. Vielmehr sollte das Ziel verfolgt werden, die bedeutendsten Risiken zu identifizieren.[22] Eine Identifikation aller Com-

10 *Grunert*, CCZ 2020, 71, 75.
11 *Vogelsang*, CB 2016, 463, 464.
12 *Stork/Ebersoll*, CB 2015, 57 ff.
13 *Kark*, Compliance-Risikomanagement, 2. Aufl. 2019, Rn. 646 ff.
14 *Kark*, Compliance-Risikomanagement, 2. Aufl. 2019, Rn. 646 ff.
15 KICG (Fn. 2), Leitlinie 3, S. 31.
16 Deutsches Institut für Compliance e. V., S09 – Compliance-Risikoanalyse (CRA), 2020, S. 16.
17 *Pauthner/Stephan*, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, 3. Aufl. 2016, § 16 Rn. 59 f.
18 *Kark*, Compliance-Risikomanagement, 2. Aufl. 2019, Rn. 646 ff.
19 *Potinecke*, in: Behringer, Compliance für KMU, 2. Aufl. 2016, S. 224 f.
20 *Kark*, Compliance-Risikomanagement, 2. Aufl. 2019, Rn. 692.
21 Deutsches Institut für Compliance e. V., S09 – Compliance-Risikoanalyse (CRA), 2020, S. 19.
22 *Krisor*, Compliance-Risikoanalyse: Von der praktischen Umsetzung bis hin zur automatisierten Lösung, CB 2019, 25, 26.

pliance-Risiken wäre auch schon deshalb nicht sinnvoll, da sie einer wirtschaftlichen und effizienten Risikoerhebung entgegenstehen würde.[23] Um bei der Risikoidentifikation ein qualitativ hochwertiges Ergebnis zu erzielen, ist neben einer systematischen Vorgehensweise außerdem die Unternehmenskultur, aber vor allem eine gelebte Risikokultur von Bedeutung. Darüber hinaus sollte die Geschäftsführung ausreichende Ressourcen und qualifiziertes Personal bereitstellen, um die Risiken innerhalb des gesteckten Rahmens aufdecken zu können.

a) Instrumente

Innerhalb der regulatorischen Vorgaben für das CMS sind keine konkreten Instrumente zur Identifikation von Compliance-Risiken zu finden.[24] Zur Identifikation der Risiken kann daher eine Vielzahl verschiedener Instrumente verwendet werden. Diese können bei entsprechender Verwendung und Kombination sehr hilfreich sein.[25] Welche Instrumente für ein Unternehmen die Richtigen sind, ist einzelfallabhängig. Es kommt hierbei darauf an, welche Methoden für das jeweilige Unternehmen zumutbar sind und wie die Unternehmenskultur ist.[26]

Eines der Instrumente, welches beispielsweise zur Identifikation von Compliance-Risiken verwendet werden kann, ist der Risikokatalog bzw. die Risikocheckliste. Beim Risikokatalog handelt es sich um ein Instrument mit kollektivistischem Charakter, da im Rahmen dieser Methode neuartige Risiken nur eingeschränkt erfasst werden können.[27] Innerhalb des Risikokatalogs sind potenzielle Risiken pro Compliance-Themenfeld bzw. Risikobereich aufgelistet.[28] Zu den Compliance-Themenfeldern zählen beispielsweise das Datenschutz-, Umwelt- oder Steuerrecht.[29]

Darüber hinaus kann der interaktive Risikodialog zur Identifikation der Compliance-Risiken genutzt werden. Dieser wird üblicherweise im Rahmen von Interviews durchgeführt.[30] Innerhalb des interaktiven Risikodialogs können sowohl offensichtliche, als auch bisher unbekannte Risiken identifiziert werden.[31] Vorteilhaft am interaktiven Risikodialog ist, dass ein direkter Austausch stattfindet und Unklarheiten sofort geklärt werden können.[32]

Außerdem ist es im Rahmen von Risiko-Workshops möglich Compliance-Risiken zu identifizieren. Der Risiko-Workshop ist ein typisches Instrument des Bottom-up Risk Assessments.[33] Zur Reduzierung der Komplexität sollten die Workshops thematisch und/ oder personenbezogen eingegrenzt werden. Um die Effektivität der Workshops zu gewährleisten, sollten sie sorgfältig vorbereitet werden. Die Ergebnisse der Vorbereitung sollten im Rahmen des Workshops kritisch überprüft werden.[34]

Weitere Instrumente, die zur Identifikation von Compliance-Risiken genutzt werden können, sind Besichtigungen oder Betriebsbegehungen, Dokumenten- und Kennzahlenanalysen, die Analyse von Schadensstatistiken und eingetretenen Schadensfällen im Unternehmen[35] sowie die SWOT (Stärken-Schwächen-Chancen-Risiken)-Analyse.[36] Darüber hinaus können Szenario-Analysen oder Fehler-Ursachen-Analysen zur Risikoidentifikation herangezogen werden.[37]

b) Informationsquellen

Zur Identifikation von Compliance-Risiken kann eine Vielzahl interner und externer Informationsquellen herangezogen werden. Es muss bedacht werden, dass im Rahmen der Risikoidentifikation in die Zukunft geblickt werden muss. Die Risikoidentifikation beinhaltet zwangsläufig „subjektive Bewertungselemente künftiger Entwicklungen."[38] Darüber hinaus muss berücksichtigt werden, dass die Herausforderung bei der Verwendung der verschiedenen Informationsquellen vor allem darin besteht, die geeigneten Quellen auszuwählen und mit den Verantwortlichen die Inhalte, das Format sowie den Zeitpunkt der Übergabe der Informationen abzustimmen.[39]

aa) Interne Informationsquellen

Innerhalb eines Unternehmens existieren verschiedene Abteilungen und Funktionen, die unterschiedliche Blickwinkel auf die potenziellen Risiken des Unternehmens haben. Um Informationen über Compliance-Risiken zu gewinnen, ist es deshalb wichtig das breit gefächerte Spezialwissen der einzelnen Akteure des Unternehmens zu nutzen.[40] Darüber hinaus ist es im Rahmen der Risikoidentifikation durch interne Informationsquellen von Bedeutung, Anreize zur Förderung einer Risikokultur zu schaffen. Dadurch werden die Unternehmensakteure bestärkt, Kenntnisse über Risiken offenzulegen. Sie müssen sicher sein können, Risiken zu melden, ohne dadurch Sanktionen zu befürchten, anderenfalls könnte sich eine Risikoidentifikation durch interne Informationsquellen schwierig gestalten.[41]

aaa) Mitarbeiter

Eine der wichtigsten Informationsquellen zur Identifikation von Compliance-Risiken bilden die Mitarbeiter eines Unternehmens. Durch das Wissen und die Erfahrung in ihrem jeweiligen Aufgabenbereich besitzen sie in der Regel Detailkenntnisse und erkennen problematische Gegebenheiten. Darüber hinaus erlangen sie im Rahmen der Zusammenarbeit mit anderen Abteilungen Informationen darüber, wo außerhalb ihres Tätigkeitsbereichs Risiken bestehen.

bbb) Führungskräfte und Mitglieder der Geschäftsführung

Neben den Mitarbeitern bilden Führungskräfte sowie die Mitglieder der Unternehmensleitung eine bedeutende Informationsquelle bei der Identifikation von Compliance-Risiken. Sie verfügen über andere Informationen als die Mitarbeiter, da sie umfangreichere Möglichkeiten zur Vernetzung haben.[42] Bei der Auswahl der Teilnehmer der Risikoidentifikation ist wichtig, dass diese auskunftsfähig sind und ausreichende Kenntnisse über Unternehmensabläufe haben. Dies

23 *Glage/Grötzner*, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, 3. Aufl. 2016, § 14 Rn. 59.
24 Deutsches Institut für Compliance e. V., S09 – Compliance-Risikoanalyse (CRA), 2020, S. 17.
25 *Klingenstein*, in: Bay/Hastenrath, Compliance-Management-Systeme, 2. Aufl. 2016, Kap. 4 Rn. 44.
26 *Busekist/Schlitt*, CCZ 2012, 92.
27 *Romeike*, Risikomanagement, 2018, S. 62.
28 *Krisor*, CB 2019, 25, 26.
29 Deutsches Institut für Compliance e. V., Risikokatalog, 2020, S. 10.
30 *Stork/Ebersoll*, CB 2015, 57, 60.
31 *Romeike*, Risikomanagement, 2018, S. 67.
32 *Vogelsang*, CB 2016, 463, 466.
33 *Pauthner/Stephan*, in: Hauschka/Moosmayer/Lösler, § 16 Rn. 57.
34 *Pauthner/Stephan*, in: Hauschka/Moosmayer/Lösler, § 16 Rn. 96 f.
35 *Klingenstein*, in: Bay/Hastenrath, Compliance-Management-Systeme, 2. Aufl. 2016, Kap. 4 Rn. 45.
36 *Romeike*, in: Inderst/Bannenberg/Poppe, Compliance, Aufbau-Management-Risikobereiche, 2. Aufl. 2013, Kap. 4 Rn. 277.
37 *Romeike*, Risikomanagement, 2018, S. 56.
38 *Kark*, Compliance-Risikomanagement, 2. Aufl. 2019, Rn. 438.
39 Deutsches Institut für Compliance e. V., Risikokatalog, 2020, S. 19.
40 Deutsches Institut für Compliance e. V., Risikokatalog, 2020, S. 17.
41 *Kark*, Compliance-Risikomanagement, 2. Aufl. 2019, Rn. 430 f.
42 *Kark*, Compliance-Risikomanagement, 2. Aufl. 2019, Rn. 429.

erfordert eine gewisse Unternehmenszugehörigkeit. Vor allem bei Großunternehmen oder Konzernen sollten die Befragungsteilnehmer Orts- oder Sachnähe zu der Niederlassung oder Tochtergesellschaft haben. Die Auswahl der Teilnehmer sollte repräsentativ sein, sie sollte aus Mitarbeitern der Unternehmensebenen bestehen, die vom Risiko betroffen sind.[43]

ccc) Interne Revision

Außerdem können aus den Prüfungsergebnissen der Audits der Internen Revision, falls ein Unternehmen über eine solche verfügt, Hinweise auf Risiken gewonnen werden. Im Normalfall werden im Rahmen von Audits sehr unterschiedliche Unternehmensbereiche geprüft, die gewonnenen Informationen über identifizierte Risiken können dadurch oftmals für andere Unternehmensbereiche von Bedeutung sein und auf ähnliche Sachverhalte übertragen werden.[44]

ddd) Interne Kontrollsysteme

Verfügt eine Gesellschaft über ein internes Kontrollsystem (IKS), so kann auch dieses als Informationsquelle herangezogen werden. Aus den Fehlermeldungen des IKS können Schwachpunkte in der Unternehmensorganisation und in den Prozessabläufen abgeleitet werden, welche sich wiederum zu Risiken entwickeln können. Informationen aus dem IKS sind besonders hilfreich, da die einzelnen Prozessschritte genau dokumentiert sind. Risiken können dadurch effizient identifiziert werden.[45]

bb) Externe Informationsquellen

Neben den internen, können außerdem externe Informationsquellen für die Identifikation sowie die Analyse und Bewertung von Compliance-Risiken herangezogen werden.

aaa) Compliance-Verstöße und -Risiken anderer Unternehmen

Eine mögliche externe Informationsquelle die zur Risikoidentifikation herangezogen werden kann bilden Compliance-Verstöße, die bei Wettbewerbern und anderen Marktteilnehmern aufgetreten sind. Zwar ist die Risikosituation jedes Unternehmens individuell, jedoch können sich zumindest durch eine Tätigkeit in der gleichen Branche ähnliche Risiken ergeben.[46] Des Weiteren können Compliance-Risiken von Wettbewerbern, Zulieferern und Kunden im Rahmen der Risikoidentifikation berücksichtigt werden.[47]

bbb) Hinweise von Wirtschaftsprüfern

Darüber hinaus können Wirtschaftsprüfer im Rahmen der Jahresabschlussprüfung als Informationsquelle dienen. Da sie eine unabhängige Sicht auf das Unternehmen sowie Erfahrungen aus anderen Prüfungen haben, kann dies dazu führen, dass sie Risiken identifizieren, die innerhalb der Gesellschaft nicht wahrgenommen wurden.[48]

ccc) Statistiken

Als externe Informationsquelle können außerdem Statistiken, die außerhalb des Unternehmens erhoben wurden, herangezogen werden. Hierzu gehören beispielsweise Compliance-Umfragen oder –Berichte von Wirtschaftsprüfungsgesellschaften, von Transparency International, der World Bank sowie Global Integrity.[49]

ddd) Markt- und Wettbewerbsdaten

Zur Identifikation von Compliance-Risiken können außerdem Markt- und Wettbewerbsdaten herangezogen werden. Informationen über die allgemeine Marktentwicklung können beispielsweise durch das Bruttoinlandsprodukt, die Inflation oder Arbeitslosenquote gewonnen werden. Wettbewerbsdaten können durch die Betrachtung des Wettbewerbsumfelds, z. B. ob ein Oligopol oder Monopol besteht, gesammelt werden.[50]

3. Risikoanalyse

Nachdem die Risiken identifiziert wurden, können sie analysiert werden. Im Rahmen der Risikoanalyse werden die Ergebnisse der Risikoidentifikation geordnet und kategorisiert. Die Ordnung und Kategorisierung ermöglicht es Fehler wie z. B. Doppelnennungen zu erkennen. Außerdem können Synergieeffekte zwischen einzelnen Risiken aufgedeckt werden. Dies ist von Bedeutung, da einzelne Risiken oftmals harmlos erscheinen, durch entsprechende Synergieeffekte kann es jedoch zu einem erheblichen Risiko für das Unternehmen kommen. Des Weiteren können durch die Risikoanalyse Kumulationen von Gefahrenquellen aufgespürt werden. Genauso wie Synergieeffekte können auch Kumulationen dazu führen, dass kleine, unter Umständen unbedeutende Risiken zusammen zu einer erheblichen Gefahr führen.[51]

Es bietet sich an, die Compliance-Risiken z. B. nach regionalen Gesichtspunkten, nach den Geschäfts- oder Funktionsbereichen in denen sie auftreten oder nach den einzelnen Stufen der Wertschöpfungskette zu gliedern. Neben den genannten Möglichkeiten zur Kategorisierung existieren viele weitere Möglichkeiten unternehmensspezifische Compliance-Risiken zu kategorisieren. Unabhängig davon, welche Art der Kategorisierung letztendlich gewählt wird, ist es vor allem wichtig, dass durch Quervergleiche Defizite innerhalb des Risikoidentifikations-Prozesses aufgedeckt werden können.[52]

4. Risikobewertung

Nachdem die Risiken identifiziert und analysiert wurden, können sie nach ihrer Schadenshöhe und Eintrittswahrscheinlichkeit beurteilt werden.[53] Zur Bewertung der Risiken können grundsätzlich die gleichen Instrumente und Informationsquellen, die bereits im Rahmen der Risikoidentifikation verwendet wurden, genutzt werden.[54] Bei der Bewertung der Risiken muss in Bruttorisiko, d. h. das Risiko ohne Berücksichtigung von Maßnahmen wie Schulungen oder Richtlinien, und Nettorisiko, d. h. das Risiko mit Berücksichtigung der tatsächlich eingeleiteten Maßnahmen, unterschieden werden.[55] Es muss festgelegt werden, ob das Netto- oder Bruttorisiko oder beide Risikoarten evaluiert werden.[56] Vorteilhaft an der Berücksichtigung beider Risikoarten ist, dass das tatsächliche Ausmaß der Risiken ermittelt und die Wirksamkeit der bestehenden Maßnahmen festgestellt werden kann.[57] Die ausschließliche Berücksichtigung des Nettorisikos bietet sich für Unternehmen an,

43 *Busekist/Schlitt*, CCZ 2012, 86, 92.
44 *Kark*, Compliance-Risikomanagement, 2. Aufl. 2019, Rn. 432.
45 *Kark*, Compliance-Risikomanagement, 2. Aufl. 2019, Rn. 434.
46 *Kark*, Compliance-Risikomanagement, 2. Aufl. 2019, Rn. 430.
47 Deutsches *Institut für Compliance e. V.*, Risikokatalog, 2020, S. 20.
48 *Kark*, Compliance-Risikomanagement, 2. Aufl. 2019, Rn. 433.
49 *Hansen*, in: Moosmayer, Compliance-Risikoanalyse, 2015, § 5 Rn. 33.
50 *Hansen*, in: Moosmayer, Compliance-Risikoanalyse, 2015, § 5 Rn. 36.
51 *Kark*, Compliance-Risikomanagement, 2. Aufl. 2019, Rn. 440 ff.
52 *Kark*, Compliance-Risikomanagement, 2. Aufl. 2019, Rn. 707 ff.
53 *Grunert*, CCZ 2020, 71, 76.
54 *Romeike*, Risikomanagement, 2018, S. 61 ff.
55 *Wermelt*, CB 2014, 109, 112.
56 *Glage/Grötzner*, in: Hauschka/Moosmayer/Lösler, § 14 Rn. 63.
57 *Klingenstein*, in: Bay/Hastenrath, Compliance-Management-Systeme, 2. Aufl. 2016, Kap. 4 Rn. 57.

die bereits ein etabliertes CMS mit hohem Reifegrad haben. Grund dafür ist, dass der Fokus bei dieser Bewertungsweise auf die Risiken gelegt werden kann, die zusätzliche Gegenmaßnahmen erfordern.[58]
Die Risikobewertung kann sowohl von der Compliance-Organisation,[59] als auch dezentral von einzelnen Geschäftseinheiten durchgeführt werden. Wird die Risikobewertung dezentral durchgeführt, so müssen die Ergebnisse der einzelnen Risikobewertungen zentral zusammengeführt werden. Dadurch wird eine Gesamtbewertung ermöglicht.[60]

a) Bewertungskriterium: Eintrittswahrscheinlichkeit

Die Analyse der Eintrittswahrscheinlichkeit basiert auf der Auswertung möglicher Risikoursachen. Es ist die Frage zu stellen, welche Aspekte dazu beitragen, dass ein bestimmtes Risiko innerhalb eines festgelegten Zeitraums tatsächlich real wird. Die Eintrittswahrscheinlichkeit eines Risikos kann sowohl objektiv, d. h. auf Basis vergangenheitsbezogener Daten z. B. in Form von statistischen Untersuchungen, Studien oder internationalen Rankings wie dem CPI (Corruption Perception Index), als auch auf Grundlage subjektiver Einschätzungen erfolgen.[61] Hierbei ist es illusorisch zu denken, dass die Bewertung der Eintrittswahrscheinlichkeit auf einem mathematisch präzisen Verfahren beruht.[62] Vielmehr erfolgt die Einschätzung der Eintrittswahrscheinlichkeit über verschiedene Klassifizierungsstufen. Je mehr Klassifizierungsstufen es gibt, desto detaillierter kann die Eintrittswahrscheinlichkeit bestimmt werden. In der Praxis sind drei (z. B. niedrig, mittel, hoch) bis sechs (z. B. unmöglich, unwahrscheinlich, möglich, wahrscheinlich, sehr wahrscheinlich und sicher) Klassifizierungsstufen üblich. Nachdem die Klassifizierungsstufen bestimmt wurden, werden ihnen prozentuale Eintrittswahrscheinlichkeiten zugeordnet.[63] Vorteilhaft an der Festlegung von Klassifizierungsstufen ist, dass der Bearbeiter nicht einen bestimmten prozentualen Wert, sondern lediglich eine Größenordnung bestimmen muss.[64]

Abb. 2: Beispiel für die Klassifizierung der Eintrittswahrscheinlichkeiten[65]

Stufe	Wahrscheinlichkeit	Erläuterung	Quantifizierung
1	unmöglich	Risiko kann nicht eintreten	0%
2	unwahrscheinlich	Risiko wird nach praktischer Vernunft nicht eintreten	< 5%
3	möglich	Risiko wird in weniger als der Hälfte der Fälle eintreten	5% bis < 50%
4	wahrscheinlich	Risiko wird in mehr als der Hälfte der Fälle eintreten	50% bis < 95%
5	sehr wahrscheinlich	Risiko wird nach praktischer Vernunft eintreten	95% bis < 100%
6	sicher	Risiko wird definitiv eintreten	100%

b) Bewertungskriterium: Schadenshöhe

Das zweite Bewertungskriterium bildet die Schadenshöhe bei Eintritt des jeweiligen Risikos.[66] Sie kann sowohl quantitativ als auch qualitativ bewertet werden. Im Rahmen der quantitativen Bewertung wird ein finanzieller Schaden, z. B. eine Strafzahlungsverpflichtung bei einem Compliance-Verstoß oder der Wegfall einzelner Produkte, evaluiert.[67] Die Schadenshöhe orientiert sich an der individuellen Vermögens-, Finanz- und Ertragslage des jeweiligen Unternehmens.[68] Innerhalb der qualitativen Bewertung erfolgt die Evaluierung auf Basis unternehmensindividueller Kriterien. Die Schadenskategorie „finanzieller Schaden" kann qualitativ durch die Kategorien „Reputationsschäden" oder „Sanktionen" ergänzt werden. Beispielweise kann die Bewertung der Reputationsschäden anhand des Umfangs der Berichterstattung evaluiert werden. In der Praxis werden meist beide Verfahren parallel angewendet, denn bei der Bewertung von Compliance-Risiken besteht häufig das Problem, dass sich diese nicht oder nur schwer quantifizieren lassen. Ist eine quantitative Bewertung jedoch möglich, so sollte diese bevorzugt werden.[69] Zur Bewertung der Schadenshöhe sollten genauso wie bei der Bewertung der Eintrittswahrscheinlichkeit ein mehrstufiges Bewertungssystem verwendet werden.[70] Die Untergliederung sollte in drei bis sechs Schadensklassen (z. B. gering, bedeutend oder bestandsgefährdend) erfolgen. Für jede Schadensklasse müssen quantitative und qualitative Bewertungskriterien festgelegt werden.[71]

Abb. 3: Beispiel für die Klassifizierung der Schadenshöhe[72]

		quantitativ	qualitativ	
Stufe	**Schadens-klasse**	**finanzieller Schaden**	**Reputationsschaden**	**Sanktionen**
1	unbedeutend	< 40 T €	keiner	Verwarnung
2	gering	40 - < 150 T €	Berichterstattung in lokalen Medien	geringe Sanktionen
3	bedeutend	150 T € - < 2 Mio. €	Berichterstattung in nationalen Medien	wesentliche Sanktionen
4	kritisch	500 T € - < 2 Mio. €	intensive nationale und geringe internationale Berichterstattung	vorübergehende Einstellung des Geschäftsbetriebes
5	bestands-gefährdend	> 2 Mio. €	intensive Berichterstattung in nationalen und internationalen Medien	Einstellung des Geschäftsbetriebes

c) Visualisierung der Ergebnisse

Die Ergebnisse der Risikobewertung können sowohl in einer Risikomatrix, als auch in einem Säulendiagramm oder einer Tabelle visualisiert werden.[73] In der Praxis hat sich die Darstellung der Ergebnisse in einer Risikomatrix durchgesetzt. In dieser werden alle Risiken auf zwei Achsen unter Berücksichtigung der Bewertung ihrer Eintrittswahrscheinlichkeit und Schadenshöhe dargestellt.[74] Innerhalb der Risikomatrix wird das Gesamtrisiko übersichtlich visualisiert und bildet

58 Deutsches Institut für Compliance e. V., Risikokatalog, 2020, S. 25.
59 *Stork/Ebersoll*, CB 2015, 57, 60.
60 KICG (Fn. 2), Leitlinie 3, S. 34.
61 *Klingenstein*, in: Bay/Hastenrath, Compliance-Management-Systeme, 2. Aufl. 2016, Kap. 4 Rn. 58.
62 LexisNexis Risk Solutions, Risk Assessment und Korruptionsprävention – Weißbuch, 2014, S. 11.
63 *Klingenstein*, in: Bay/Hastenrath, Compliance-Management-Systeme, 2. Aufl. 2016, Kap. 4 Rn. 59.
64 *Kark*, Compliance-Risikomanagement, 2. Aufl. 2019, Rn. 446.
65 *Klingenstein*, in: Bay/Hastenrath, Compliance-Management-Systeme, 2. Aufl. 2016, Kap. 4 Rn. 60.
66 LexisNexis Risk Solutions, S. 11.
67 *Klingenstein*, in: Bay/Hastenrath, Compliance-Management-Systeme, 2. Aufl. 2016, Kap. 4 Rn. 62 ff.
68 Deutsches Institut für Compliance e. V., Risikokatalog, 2020, S. 26.
69 *Klingenstein*, in: Bay/Hastenrath, Compliance-Management-Systeme, 2. Aufl. 2016, Kap. 4 Rn. 62 ff.
70 LexisNexis Risk Solutions, S. 11.
71 *Klingenstein*, in: Bay/Hastenrath, Compliance-Management-Systeme, 2. Aufl. 2016, Kap. 4 Rn. 65.
72 *Klingenstein*, in: Bay/Hastenrath, Compliance-Management-Systeme, 2. Aufl. 2016, Kap. 4 Rn. 66.
73 *Kark*, Compliance-Risikomanagement, 2. Aufl. 2019, Rn. 447.
74 *Glage/Grötzner*, in: Hauschka/Moosmayer/Lösler, § 14 Rn. 64.

damit einen wichtigen Teil der Risikoberichterstattung. Außerdem kann die Risikomatrix dazu verwendet werden eine Rangordnung festzulegen, welchen Einzelrisiken zuerst durch entsprechende Maßnahmen entgegengesteuert werden muss. Dabei ist der Fokus auf Risiken mit hoher Eintrittswahrscheinlichkeit und Schadenshöhe zu legen. Auch Risiken mit niedriger Eintrittswahrscheinlichkeit, aber einem hohen Schaden dürfen nicht vernachlässigt werden, da diese bei einem tatsächlichen Eintritt die Existenz des Unternehmens gefährden können. Darüber hinaus ist zu beachten, dass Synergieeffekte verschiedener Risiken innerhalb der Risikomatrix nicht beachtet werden.[75] Durch eine zusätzliche Analyse der einzelnen Risiken können Wechselwirkungen jedoch erkannt werden.[76]

5. Erstellung eines Risikoinventars

Die im Rahmen des CRAs identifizierten und bewerteten Risiken sollten in ein Risikoinventar aufgenommen werden. Innerhalb des Risikoinventars sind gewöhnlich die identifizierten Risiken und deren Bewertung, die Beurteilung risikopolitischer Maßnahmen, Empfehlungen für die Verbesserung des Status quo sowie eine Priorisierung der Maßnahmen zu finden. Es dient zu einer systematischen Darstellung der Risiken. Grund für die Erstellung eines Risikoinventars ist es, vor allem Entscheidungsträgern einen komprimierten Überblick über die Risikosituation des Unternehmens zu verschaffen.[77]

III. Inhalt des Abschlussdokuments

Nachdem ein CRA durchgeführt wurde, sollten alle im Rahmen der Analyse gewonnenen Erkenntnisse sowie das Vorgehen beim CRA einfach und verständlich in einem Abschlussdokument zusammengefasst werden.[78] Darüber hinaus sollten die Entscheidungsgründe für oder gegen eine Beschränkung des Risk Assessment aufgeführt werden.[79] Durch die Dokumentation wird zum einen ein Überblick über die Gesamtheit der Compliance-Risiken innerhalb eines Unternehmens geschaffen.[80] Das Dokument erleichtert die praktische Umsetzung der Erkenntnisse und gewährleistet diese über Jahre hinweg nachvollziehen zu können.[81] Zum anderen kann durch das Dokument nachgewiesen werden, dass das CRA sorgfältig und systematisch durchgeführt wurde. Dies ist von Bedeutung, wenn es zu einem tatsächlichen Compliance-Verstoß im Unternehmen gekommen ist und dient der Entlastung der Unternehmensleitung. Durch das Dokument kann die Unternehmensleitung beweisen, dass auf Basis der identifizierten Risiken erforderliche und zumutbare Aufsichtsmaßnahmen umgesetzt wurden und das tatsächlich eingetretene Risiko nicht vorhersehbar war. Ein sorgfältig dokumentiertes CRA ist Voraussetzung dafür, dass es bei einem Compliance-Verstoß zu einer Haftungsreduzierung kommen kann.[82]

IV. Häufigkeit der Durchführung

Ein CRA ist kein einmaliges Ereignis, sondern sollte regelmäßig, ca. alle ein bis drei Jahre, durchgeführt werden. Darüber hinaus sind Risk Assessments durchzuführen, wenn es interne oder externe Entwicklungen gibt, die sich auf die Risikosituation des jeweiligen Unternehmens auswirken.[83] Hierzu zählen Faktoren wie die Veränderung des rechtlichen Umfeldes durch Gesetzesänderungen oder durch die Ausdehnung oder Einschränkung der unternehmerischen Tätigkeit auf bestimmte Jurisdiktionen.[84] Außerdem ist die Erschließung neuer Geschäftsfelder, konkret neuer Branchen, Länder, Kunden, Produkte oder Geschäftsmodelle, Änderungen der Management-Strukturen und Zuständigkeiten, der Erwerb neuer Gesellschaften, neue Geschäftspartner in Form von Vertriebsmittlern oder Kooperationspartnern sowie deutliche Änderungen der Mitarbeiterzahl oder des Umsatzes von Bedeutung.[85]

V. Zusammenfassung

Die sorgfältige Vorbereitung, Durchführung und Dokumentation sind unerlässliche Faktoren für ein erfolgreiches, nutzenmaximierendes und zugleich risikenminimierendes CRA. Statt der Anwendung von standardisierten Mustern sollte der zwar aufwendigere aber dafür eben auch zielführendere Weg des unternehmensindividuellen Vorgehens gewählt werden. Nur ein unternehmensspezifisches und damit idealtypisches CRA führt zum gewünschten Ziel der Risikoerkennung, Risikominimierung und letztlich Haftungsreduzierung.

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.*

Hannah Bindschädel, *LL.M., ist als Wirtschaftsjuristin in der Rechtsabteilung eines mittelständischen Distributionsunternehmens mit den Schwerpunkten Compliance und Vertragsmanagement tätig. Zuvor hat sie an der HfWU Nürtingen-Geislingen Wirtschaftsrecht sowie an der HTWG Konstanz Legal Management studiert. Sie verfügt unter anderem über fundierte Kenntnisse in der Ausgestaltung von Compliance-Risikoanalysen.*

75 *Klingenstein*, in: Bay/Hastenrath, Compliance-Management-Systeme, 2. Aufl. 2016, Kap. 4 Rn. 67.
76 *Kark*, Compliance-Risikomanagement, 2. Aufl. 2019, Rn. 449.
77 *Reichling/Bietke/Henne*, Praxishandbuch Risikomanagement und Rating, 2007, S. 218 f.
78 *Wermelt*, CB 2014, 109, 112.
79 *Busekist/Schlitt*, CCZ 2012, 86, 89.
80 *Vogelsang*, CB 2016, 463, 467.
81 *Grunert*, CCZ 2020, 71, 76.
82 *Wermelt*, CB 2014, 109, 112.
83 *Vogelsang*, CB 2016, 463, 464.
84 *Busekist/Schlitt*, CCZ 2012, 86, 95.
85 *Grunert*, CCZ 2020, 71, 77.