1. Teil
Grundlagen und Organisation

1. Kapitel
Bestandteile eines effektiven Compliance-Management-Systems

Literatur: *Buck-Heeb,* Wissenszurechnung und Informationsmanagement, in *Hauschka/Moosmayer/Lösler* (Hrsg), Corporate Compliance[3] (2016) § 2; *Busekist/Schlitt,* Der IDW PS 980 und die allgemeinen rechtlichen Mindestanforderungen an ein wirksames Compliance Management System, (2) – Risikoermittlungspflicht, CCZ 2012, 86; *Busekist/Uhlig,* Third Party Compliance, in *Hauschka/Moosmayer/Lösler* (Hrsg), Corporate Compliance[3] (2016); *Glage/Grötzner,* Unternehmensrisiken und Risikomanagement, in *Hauschka/Moosmayer/Lösler* (Hrsg), Corporate Compliance[3] (2016) § 14; *Grüninger/Jantz,* Möglichkeiten und Grenzen der Prüfung von Compliance-Management-Systemen, ZCG 2013, 131; *Hülsberg/Laue,* Compliance-Organisation in der Praxis, in *Inderst/Bannenberg/Poppe,* Compliance, Aufbau – Management – Risikobereiche[3] (2017) Kap 3; *Institut für Interne Revision Österreich* (Hrsg), Das unternehmensweite Risikomanagementsystem aus der Sicht der Internen Revision[2] (2014); *Jantz/Grüninger,* Prüfung von Compliance-Management-Systemen (Konstanz Institut für Corporate Compliance – KICG, Forschungspapiere Nr 7/2013) (2013); *Klahold/Lochen,* Compliance-Organisation, in *Hauschka/Moosmayer/Lösler* (Hrsg), Corporate Compliance[3] (2016) § 37; *Klingenstein,* Compliance Programm, in *Bay/Hastenrath,* Compliance-Management-Systeme[2] (2016) Kap 4; *Kustor* (Hrsg), Unternehmensinterne Untersuchungen – Handbuch für Internal Investigations (2010); *Moosmayer,* Compliance – Praxisleitfaden für Unternehmen[4] (2021); *Pollak,* Internal Investigations, in *Soyer* (Hrsg), Handbuch Unternehmensstrafrecht (2020) Kap 14; *Romeike,* Compliance-Organisation in der Praxis, in *Inderst/Bannenberg/Poppe,* Compliance, Aufbau – Management – Risikobereiche[3] (2017) Kap 3; *Ruhmannseder,* Unternehmensinterne Ermittlungen – rechtliche Fallstricke in Deutschland und Österreich, in FS Roxin (2012) 501; *Ruhmannseder,* Tax Compliance, in *Petsche/Mair,* Handbuch Compliance[3] (2019) 433; *Ruhmannseder,* Corporate Governance und Compliance, in *Ruhmannseder/Wess* (Hrsg), Handbuch Corporate Compliance (2022) Kap 1; *Ruhmannseder,* Compliance-Strategien, in *Soyer* (Hrsg), Handbuch Unternehmensstrafrecht (2020), Kap 13; *Ruhmannseder/Behr/Krakow* (Hrsg), Hinweisgebersysteme[2] (2021); *Ruhmannseder/Lehner/Beukelmann* (Hrsg), Compliance aktuell (2023); *Schönborn/Morwitzer* (Hrsg), Criminal Compliance (2023); *Schmidt,* Wirtschaftsprüfung und CMS-Prüfung, in *Hauschka/Moosmayer/Lösler* (Hrsg), Corporate Compliance[3] (2016) § 45; *Schulz/Galster,* Aufgaben im Unternehmen, in *Bürkle/Hauschka,* Der Compliance Officer (2015) § 4; *Soyer/Pollak* Criminal Compliance, in *Kert/Kodek* (Hrsg), Handbuch Wirtschaftsstrafrecht[2] (2022) 1127.

Übersicht

I. Einleitung

1.1 Grundlage für ein maßgeschneidertes und effizientes Compliance-Management-System (CMS) ist die umfassende und systematische **Identifizierung sowie Bewertung der Compliance-Risiken** im Unternehmen, wobei Umfang und Schwerpunkt der Risikoanalyse insb von Größe, Struktur und Branche sowie von den Geschäftspraktiken der Geschäftspartner des Unternehmens abhängen. Im Anschluss daran ist in Abhängigkeit der festgestellten Risiken ein entsprechendes **Compliance-Programm aufzusetzen** und eine adäquate **Compliance-Organisation aufzustellen.**[1] Dabei steht und fällt der Erfolg eines Compliance-Programms mit der Überzeugung der Unternehmensleitung von der Notwendigkeit eines solchen Programms und ihrem Einsatz bei der Einführung und Implementierung. Erforderlich ist daher ein klares, vorbehaltloses und glaubwürdiges **Bekenntnis zur Rechtstreue,** dass sowohl von der Unternehmensleitung als auch von den Angehörigen des mittleren Managements abgegeben werden muss („Tone from the Top“ und „Tone from the Middle“) sowie eine **Unternehmenskultur,** die durch vorbehaltlose Botschaften zum Thema Compliance geprägt ist. Ziel ist dabei die **Vermeidung systematischen Fehlver**haltens im Unternehmen.[2]

1 *Ruhmannseder* in *Ruhmannseder et al,* Compliance aktuell, Fach O1010 Rz 4.
2 Vgl hierzu auch *Soyer/Pollak* in *Kert/Kodek,* HB Wirtschaftsstrafrecht[2] Rz 28.16.

Um das Ziel funktionstüchtiger, unternehmensinterner Compliance-Strukturen zu erreichen, kommt eine Vielzahl von Maßnahmen in Betracht, die etwa von Vorgaben und Handlungsempfehlungen in Form von Verhaltensrichtlinien und Stellungnahmen oder Anweisungen bis hin zur Vorgabe von bestimmten Elementen innerhalb der Geschäftsabläufe reichen. Weiterer zentraler Baustein einer funktionstüchtigen Compliance-Organisation ist ein **effektives Informationsmanagement** (Kommunikation, Schulung, Beratung), das die Informationsbeschaffung und den Informationsfluss sowohl nach innen zu den Mitarbeitern als auch nach außen gegenüber Dritten (zB Kunden oder sonstige Geschäftspartner) berücksichtigt. **1.2**

Um prüfen zu können, ob das Compliance-Programm effektiv ist und um etwaige Umgehungen der unternehmensinternen Vorgaben oder bewusste Rechtsverstöße möglichst frühzeitig aufdecken und rasch abstellen zu können, müssen darüber hinaus in regelmäßigen Abständen **Kontrollen** durchgeführt werden, die präventiv und nach bestimmten Prüfmustern erfolgen. Hiervon zu unterscheiden sind interne Untersuchungen, die aufgrund eines bestimmten Verdachts auf ein Fehlverhalten eingeleitet werden.[3] Werden im Zusammenhang von Kontrollen oder Untersuchungen Verfehlungen von Mitarbeitern oder Dritten aufgedeckt, bedarf es einer angemessenen Reaktion, ggf einer arbeits- und zivilrechtlichen **Sanktionierung,** die erkannten Defizite in der Compliance-Organisation sind durch geeignete Maßnahmen abzustellen. **1.3**

Einen wichtigen Bestandteil stellt schließlich die **Dokumentation** von Compliance-Vorgängen dar, die insb gemeldete Compliance-Vorfälle, aber auch sämtliche Maßnahmen zur Aufklärung, Schulung, Beratung und der Wirksamkeits- und Effizienzkontrolle umfasst. Auf diese Weise ist es der Unternehmensleitung auch nach längerer Zeit noch möglich, den Nachweis der Einhaltung ihrer Sorgfaltspflichten in der Vergangenheit erbringen zu können.[4] Nachfolgende Ausführungen stellen die Grundätze und möglichen Bestandteile eines **effektiven CMS** dar. Hierzu werden die Ausführungen in sieben Elemente unterteilt, die bei der Umsetzung von Compliance-Strategien in der Praxis eine wesentliche Rolle einnehmen. **1.4**

II. Compliance-Kultur

Ausgangspunkt für die Implementierung eines erfolgreichen CMS sollte stets der Entschluss sein, eine **Compliance-Kultur** im Unternehmen zu verankern, die gemeinsam von der Unternehmensleitung und den Mitarbeitern getragen wird. Grundvoraussetzung hierfür ist, dass die Unternehmensleitung ein **klares Bekenntnis zur Rechtstreue** abgibt, welches von den Mitarbeitern als glaubwürdig empfunden und dementsprechend als Handlungsmaxime akzeptiert wird. Die Unternehmensspitze wie auch Führungskräfte aller Managementebenen müssen hierzu verdeutlichen, dass sie geschlossen hinter dem vorgegebenen Ziel stehen, systematisches Fehlverhalten innerhalb des Unternehmens und gegenüber Geschäftspartnern zu verhindern. Geschäftsleiter und Führungskräfte sollten sich daher vorbehaltlos und uneingeschränkt zur Bekämpfung bestehender Miss- **1.5**

3 Näher dazu etwa *Pollak* in *Soyer,* HB Unternehmensstrafrecht Rz 14.5 ff; *Ruhmannseder* in FS Roxin 501 mwN.

4 *Ruhmannseder* in *Ruhmannseder et al,* Compliance aktuell, Fach O1010 Rz 5.

stände bekennen und klarstellen, dass systematische Regelverstöße kein adäquates Mittel zur Erreichung der Unternehmensziele sind, weshalb unlautere Praktiken, auch wenn sie für das Unternehmen auf den ersten Blick als „wirtschaftlich nützlich" erscheinen, **nicht geduldet** werden (sog „Mission Statement").[5]

1.6 Ein derartiges Mission Statement sollte neben dem Appell an die Mitarbeiter, sich an die bestehenden Vorschriften zu halten, auch einen **Hinweis auf die Risiken** enthalten, denen das Unternehmen, dessen Organe und auch die betreffenden Mitarbeiter selbst **im Falle von Zuwiderhandlungen** ausgesetzt sind. Dies dient va dazu, jedem Unternehmensangehörigen verständlich zu machen, dass die Einhaltung der Regeln unmittelbar im Unternehmens- und auch im Eigeninteresse liegt. Idealerweise hat dies zur Folge, dass Compliance nicht als „aufoktroyierte Vorgabe" der Unternehmensleitung empfunden, sondern im gemeinsamen Interesse von Unternehmen und Mitarbeitern als Verhaltensmaxime akzeptiert wird.

1.7 Klare Botschaften der Unternehmensleitung („Tone from the top") allein genügen indes nicht, die Mitarbeiter dafür zu gewinnen, Compliance zu einem akzeptierten Teil der Unternehmenskultur zu machen – vielmehr müssen die Entscheidungsträger ihre Grundhaltung nicht nur unmissverständlich kommunizieren, sondern **sich selbst entsprechend verhalten** und somit die eigenen Vorgaben konsequent umsetzen, um damit ihrer **Vorbildfunktion** gerecht zu werden.[6]

III. Compliance-Ziele

1.8 Die Angemessenheit der in einem CMS enthaltenen Maßnahmen hängt von den mit dem CMS verfolgten Zielen bzw dem Zielekanon ab. Hierzu legen die gesetzlichen Vertreter auf der Grundlage der allgemeinen Unternehmensziele die maßgeblichen Compliance-Ziele fest – insofern besteht folglich eine **„Definitionspflicht"** der Geschäftsleitung.[7]

1.9 Die Beschreibung der Ziele muss **eindeutig und klar verständlich** sein. Hier wird ein allgemein formuliertes Ziel wie etwa „Korruption wird im Unternehmen nicht geduldet" nicht ausreichen. Eine unscharfe Definition der Compliance-Ziele kann sowohl zu organisatorischer Unsicherheit bei der Verantwortlichkeit der Teilbereiche als auch zu Unsicherheit bei der Prävention und ggf Sanktionierung von Verstößen sein.[8] Im Rahmen der Festlegung der Ziele zu beachtende Anforderungen sind insb

- die Konsistenz,
- Verständlichkeit und Praktikabilität der unterschiedlichen Ziele,
- die Messbarkeit des Zielerreichungsgrades (keine „moving targets") sowie
- die Abstimmung mit den verfügbaren Ressourcen.

5 *Ruhmannseder* in *Soyer,* HB Unternehmensstrafrecht Rz 13.24.

6 Vgl zum Ganzen auch *Ruhmannseder* in *Ruhmannseder/Wess,* HB Corporate Compliance Rz 1.143 ff; *Schönborn/Morwitzer,* HB Criminal Compliance Rz 1.58 f.

7 Vgl auch *Hülsberg/Laue* in *Inderst et al,* Compliance[3] Kap 3 Rz 165; *Schmidt* in *Hauschka et al,* Compliance[3] § 45 Rz 28.

8 *Ruhmannseder* in *Ruhmannseder/Wess,* HB Corporate Compliance Rz 1.105.

IV. Compliance-Risikoanalyse

1.10 Ein zwingender erster Schritt auf dem Weg zu einem effektiven CMS ist die **umfassende, systematische Identifikation und Bewertung** bestehender rechtlicher Risiken.[9] Umfang und Schwerpunkt der Risikoanalyse sind vor allem von der Größe und Struktur des Unternehmens, der Branchenzugehörigkeit sowie den für das jeweilige Geschäftsmodell maßgeblichen (ggf internationalen) Märkten abhängig.[10] Problematisch gestaltet sich regelmäßig insb die im Rahmen der Risikobewertung erforderliche Prognose von Schadenswahrscheinlichkeiten und möglichen Schadenshöhen („Risikoquantifizierung"). Dabei ist zu beachten, dass – jenseits besonderer, gesetzlich bzw regulatorisch geregelter Fälle – keine allgemeine Risikovermeidungspflicht existiert. Vielmehr ist unternehmerisches Handeln stets mit Risiken verbunden, deren bewusstes Eingehen in der Regel unvermeidbar ist, um überhaupt ökonomische Erfolge erreichen zu können. Das ökonomische Erfolgsstreben ist jedoch bei den meisten Unternehmen im Regelfall darauf auszurichten, nachhaltige Erlöse trotz bestehender Risiken – auch durch gezielte Präventionsmaßnahmen – zu erreichen. Bei der Implementierung eines CMS geht es nicht darum, rechtlich missbilligtes Verhalten der Unternehmensorgane und -mitarbeiter gänzlich auszuschließen. Ziel kann bei realistischer Betrachtungsweise lediglich (aber immerhin) die Vermeidung systematischen Fehlverhaltens durch der jeweiligen Risikolage angemessene Präventivmaßnahmen sein.[11]

A. Definition Risiko sowie Abgrenzung zu Chance und Schaden

1.11 Im Rahmen der Identifizierung von Compliance-Risiken lässt sich als **„Risiko"** ein ungewisses, zukünftiges Ereignis mit potenziell negativer Auswirkung bezeichnen.[12] **Abzugrenzen** ist das Risiko einerseits zum **Schadensfall:** Ein Ereignis, das bereits zu einem Schaden geführt hat, ist im Rahmen eines reaktiven **Krisenmanagement-Systems** aufzugreifen.[13] Abzugrenzen ist das Risiko andererseits zur **Chance:**[14] Im gegebenen Kontext der Compliance-Risiken ist es sinnvoll, ausschließlich Ereignisse mit potenziell negativer Auswirkung auf Erwartungs- bzw Planwerte zu betrachten, während künftige unsichere Ereignisse im Allgemeinen sowohl positiv als auch negativ von erwarteten Entwicklungen abweichen.[15]

B. Unterscheidung zwischen internen und externen Risiken

1.12 **Interne Risiken** können sich aus der strategischen Positionierung, aus Organisationsdefiziten oder aus finanzwirtschaftlichen Positionierungen ergeben. Durch geeignete Gegenmaßnahmen können derartige Risiken grundsätzlich vom Unternehmen beeinflusst

9 Vgl nur *Ruhmannseder* in *Soyer,* HB Unternehmensstrafrecht Rz 13.29; *Schönborn/Morwitzer,* Criminal Compliance Rz 1.49.

10 Vgl *Ruhmannseder* in *Petsche/Mair,* Compliance[3] 452.

11 Vgl *Moosmayer,* Compliance[4] Rz 71; *Ruhmannseder* in *Petsche/Mair,* Compliance[3] 452.

12 Ausführlich zum Risikobegriff *Romeike* in *Inderst et al,* Compliance[3] Kap 3 Rz 247 ff, 257; vgl auch *Busekist/Schlitt,* CCZ 2012, 86 und 89.

13 *Klingenstein* in *Bay/Hastenrath,* Compliance[2] Kap 4 Rz 22.

14 Vgl zum Ganzen auch *Institut für Interne Revision Österreich,* Risikomanagementsystem[2] 21 und 49 f.

15 *Ruhmannseder* in *Ruhmannseder/Wess,* HB Corporate Compliance Rz 1.109.

und begrenzt werden. Demgegenüber erwachsen **externe Risiken** aus nicht antizipierten Entwicklungen im Unternehmensumfeld, die nicht direkt durch Entscheidungen bzw Handlungen des Unternehmens beeinflusst werden können. Unternehmen können auf externe Risiken vor diesem Hintergrund entweder nur reagieren oder allenfalls gegensteuernde Maßnahmen ergreifen, mit denen potenzielle Auswirkungen begrenzt werden.[16]

1.13 Eine weitere Kategorisierung der Risiken kann **wirkungsbezogen** (Vermögens-, Liquiditäts- und Ertragsrisiken) oder **nach der Ursächlichkeit** (finanzielle, operationelle und strategische Risiken) erfolgen.[17]

C. Risikoträger (Risk Owner)

1.14 Neben der Risikokategorie ist jedem identifizierten Einzelrisiko auch ein **Risikoträger** bzw Risikoverantwortlicher **(Risk Owner)** zuzuordnen. Hierunter versteht man eine Person oder Stelle mit der Verantwortung und Befugnis hinsichtlich eines Risikos zu handeln.[18]

1.15 Risikoträger sind für die praktische Umsetzung des Risikomanagement Prozesses von der Identifizierung, Priorisierung und Bewertung bis zur Steuerung und Überwachung ihrer Risiken maßgeblich verantwortlich. In der Regel sind dies die operativen Einheiten in den Unternehmensbereichen bzw Abteilungen, die in der Lage sind, die jeweiligen Risiken bestmöglich zu steuern und deren Risikomanagement-Aktivitäten am wirkungsvollsten sind.[19]

D. Compliance-Risikomanagement-Prozess

1.16 **Vor** dem eigentlichen Risikomanagement-Prozess ist von der Unternehmensführung eine **klare Risikostrategie zu definieren** und dafür die erforderlichen organisatorischen Maßnahmen im Unternehmen zu etablieren (Schaffung einer Risikomanagement-Organisation).[20]

1. Risikostrategie

1.17 Die Risikostrategie ist regelmäßig von der individuellen Unternehmensstrategie abzuleiten und bei allfälligen Veränderungen letzterer an diese anzupassen.[21] Die Risikostrategie dient als Leitfaden für den Umgang mit Risiken und damit der Sicherstellung des langfristigen Unternehmenserfolgs. Dabei sind **auch rechtliche Risiken (Compliance-Risiken)** zu berücksichtigen. Die Entwicklung einer Geschäfts- und Risikostrategie liegt **im nicht delegierbaren Aufgabenbereich der Unternehmensführung.** Die im Zuge der Risikostrategie festgelegten Rahmenbedingungen, Ziele und unternehmensinternen Risiko-

16 *Klingenstein* in *Bay/Hastenrath,* Compliance[2] Kap 4 Rz 26.
17 Vgl dazu auch *Romeike* in *Inderst et al,* Compliance[3] Kap 3 Rz 262 ff.
18 *Ruhmannseder* in *Petsche/Mair,* Compliance[3] 452.
19 Vgl hierzu nur *Institut für Interne Revision Österreich,* Risikomanagementsystem[2] 22 und 33; *Klingenstein* in *Bay/Hastenrath,* Compliance[2] Kap 4 Rz 47.
20 *Klingenstein* in *Bay/Hastenrath,* Compliance[2] Kap 4 Rz 36; *Romeike* in *Inderst* et al, Compliance[3] Kap 3 Rz 273 ff.
21 *Glage/Grötzner* in *Hauschka et al,* Compliance[3] § 14 Rz 49.

definitionen sollten mindestens einmal pro Jahr überprüft und ggf angepasst werden. Auf die Konsistenz zwischen Geschäfts- und Risikostrategie ist dabei stets zu achten.[22]

2. Risikotragfähigkeit

1.18 Unter Risikotragfähigkeit versteht man die Fähigkeit des Unternehmens Schaden, Verluste und Strafen aus Risiken **zu tragen, ohne** dass hieraus der **Fortbestand** des Unternehmens **unmittelbar gefährdet** ist.[23] Zur Ermittlung der Risikotragfähigkeit ist zu beurteilen ob das Eigenkapital für eine Fortführung des Geschäftsbetriebs auch dann noch ausreichend wäre, wenn vom verfügbaren Eigenkapital derjenige – hierzu zu quantifizierende – Verlust abgezogen wird, der bei einem risikoinduzierten „Maximalschaden" zu erwarten wäre.[24]

1.19 Dieser **„Maximalschaden"** wird üblicherweise unter bewusster Akzeptanz eines mit einer (geringen) Restwahrscheinlichkeit eintretenden noch größeren („katastrophalen") Schadens, bei dem eine Unternehmensfortführung ohne externe Kapitalzufuhr[25] nicht mehr möglich wäre, bestimmt. Das dadurch bestimmte „Sicherheitsniveau" wird auch als (einseitiges) Konfidenzniveau bezeichnet. Bspw bedeutet ein Konfidenzniveau von 95%, dass in maximal 5% aller denkbaren Fälle ein Verlust auftreten würde, der eine Fortführbarkeit des Unternehmens ohne externe Kapitalzufuhr nicht mehr zuließe. Der größte fiktive Verlust, bei dessen Eintritt die Fortführbarkeit des Unternehmens ohne Kapitalzufuhr gerade noch gegeben wäre, wird auch als „Money at Risk" oder „Value at Risk" (VaR) bezeichnet.[26]

3. Risikoappetit

1.20 Der **Risikoappetit** bzw die Risikotoleranz **der Unternehmensführung** ist „rechnerisch" durch die Festlegung des (einseitigen) Konfidenzniveaus definiert, zu dem der Value at Risk ermittelt wird. Faktisch ist der Risikoappetit durch die Bereitschaft geprägt, innerhalb des festgelegten maximalen Verlustrahmens tatsächlich quantifizierbare (!) Risiken einzugehen. Hierzu **legt die Unternehmensleitung** eines Unternehmens in der Praxis einen maximalen Verlustbetrag fest, der **unterhalb** der vorstehend definierten Risikotragfähigkeitsgrenze liegt (Sicherheitspuffer). Da ein Unternehmen im Allgemeinen verschiedenen Risiken ausgesetzt ist, die sich schlimmstenfalls alle gleichzeitig realisieren können bzw deren Eintritt zumindest teilweise nicht unabhängig voneinander erfolgen kann, muss die Risikotoleranz bzw der „Risikoappetit" bezogen auf das Einzelrisiko deutlich unter der Gesamtrisikobereitschaft liegen, so dass auch kumulierte Verluste tragbar wären.[27] Unabhängig davon sollten auch nicht unmittelbar quantifizierbare (Folge-)Schäden – bspw **Reputationsschäden** – bei der Festlegung der Risikotoleranz Berücksichtigung finden.[28]

---

22 *Klingenstein* in *Bay/Hastenrath,* Compliance² Kap 4 Rz 37.
23 *Klingenstein* in *Bay/Hastenrath,* Compliance² Kap 4 Rz 38.
24 *Ruhmannseder* in *Soyer,* HB Unternehmensstrafrecht Rz 13.40.
25 Unter Berücksichtigung der Möglichkeit einer Thesaurierung erwirtschafteter Erträge.
26 Vgl *Institut für Interne Revision Österreich,* Risikomanagementsystem² 51 f.
27 Vgl auch *Romeike* in *Inderst et al,* Compliance³ Kap 3 Rz 289 f; *Klingenstein* in *Bay/Hastenrath,* Compliance² Kap 4 Rz 39.
28 Vgl etwa *Klingenstein* in *Bay/Hastenrath,* Compliance² Kap 4 Rz 39.

4. Risikoidentifikation

1.21 Das Eingehen von Risiken ist ein notwendiges Merkmal und Grundprämisse unternehmerischen Handelns. Ein verantwortungsvoller Umgang mit Risiken ist dann, und nur dann, gegeben, wenn diese bewusst eingegangen und – soweit möglich – begrenzt werden. Hierfür sind zunächst alle relevanten Risiken zu identifizieren (interne/externe; strategische/operationelle/finanzielle; kurz-/mittel-/langfristige; der Schadenshöhe nach unbedeutende bis bestandsgefährdende).[29]

5. Risikobewertung

1.22 Zur Festlegung einer angemessenen Risikostrategie ist eine Bewertung aller maßgeblichen Risiken vorzunehmen. Hierzu sind für jedes Risiko die Eintrittswahrscheinlichkeit innerhalb eines Prognosehorizonts sowie die potenzielle Schadenshöhe (ausgelöst durch den Eintritt des Risikos) abzuschätzen. Zur Beurteilung der Risikotragfähigkeit ist ein „Gesamtrisiko" zu ermitteln, indem die quantifizierten Risiken unter Berücksichtigung abgeschätzter Korrelationen zwischen verschiedenen Risiken aggregiert werden.[30]

1.23 Anhand der beiden Kriterien Schadenshöhe (qualitativ und quantitativ) und Eintrittswahrscheinlichkeit lassen sich wesentliche Risiken dadurch erkennen, dass die zu erwartende Schadenshöhe, die Eintrittswahrscheinlichkeit oder gar beide Kriterien einen bestimmten Schwellenwert (die von der Geschäftsleitung festgesetzte Risikotoleranz des Unternehmens) überschreiten. Schadenshöhe und Eintrittswahrscheinlichkeit sind im Rahmen der Risikobewertung **jeweils** sowohl für das sog „Bruttorisiko" als auch für das sog „Nettorisiko" eines jeden Einzelrisikos zu erfassen.[31] Das **Bruttorisiko** bildet dabei nur das hypothetische Compliance-Risiko ab, indem es sämtliche tatsächlich existierende und das Risiko **reduzierende Maßnahmen** des Unternehmens **ausblendet.** Dementsprechend stellt das **Nettorisiko** das Compliance-Risiko dar, das **nach Einbeziehung bestehender risikoreduzierender Maßnahmen** des Unternehmens verbleibt.[32] Eine Bewertung unter zusätzlicher Berücksichtigung weiterer geplanter Risikosteuerungsmaßnahmen muss ein **vertretbares Restrisiko** zum Ergebnis haben. Das Restrisiko ist vertretbar, wenn es die Grenze der durch die Geschäftsleitung festgesetzten und zulässigen Risikotoleranz („Risikoappetit") des Unternehmens nicht überschreitet.

6. Risikosteuerung

1.24 Im Anschluss an die Identifizierung und Bewertung der Compliance-Risiken muss über geeignete Steuerungsmaßnahmen entschieden werden.[33] Die Risikosteuerung sollte dabei mit den in der Risikostrategie definierten Zielen sowie den allgemeinen Unternehmenszielen übereinstimmen.[34]

---

29 Ausführlich zum Ganzen *Klingenstein* in *Bay/Hastenrath,* Compliance[2] Kap 4 Rz 42 ff.

30 Näher zur Ermittlung der Eintrittswahrscheinlichkeit und der Schadenshöhe *Ruhmannseder* in *Ruhmannseder/Wess* HB Corporate Compliance Rz 1.123 ff.

31 *Ruhmannseder* in *Soyer,* HB Unternehmensstrafrecht Rz 13.49.

32 Vgl *Institut für Interne Revision Österreich,* Risikomanagementsystem[2] 51.

33 Zu den Einzelheiten siehe etwa *Institut für Interne Revision Österreich,* Risikomanagementsystem[2] 58 ff.

34 *Romeike* in *Inderst et al,* Compliance[3] Kap 3 Rz 292.

a) Risikovermeidung

1.25 Die **Risikovermeidung** setzt an der Ursache des Risikos an und führt zur **vollständigen Beseitigung des Risikos,** die lediglich dadurch erreicht werden kann, dass die risikobehaftete Aktivität aufgegeben wird. Sie führt damit auch zur Nichtwahrnehmung der damit verbundenen Chancen und stellt folglich die extremste Variante der Risikosteuerung dar.[35]

b) Risikoverminderung

1.26 Im Rahmen der **Risikoverminderung** wird versucht, durch geeignete technische, organisatorische oder personelle Präventivmaßnahmen (zB prozessinterne Kontrollen, Maßnahmen zur Erhöhung der Arbeitssicherheit sowie zum Brandschutz) die Eintrittswahrscheinlichkeit und bzw oder das Schadensausmaß zu reduzieren.[36]

c) Risikoüberwälzung

1.27 Bei der **Risikoüberwälzung** wird versucht, das entsprechende Risiko auf Dritte zu übertragen.[37] Ein klassisches Beispiel ist etwa der Abschluss einer Versicherung (zB Haftpflicht- oder Transportversicherung).[38]

d) Risikotragung

1.28 Schließlich bleibt die Möglichkeit, das Risiko und damit einen möglichen Schaden **selbst zu tragen.** Diese Maßnahme kommt aufgrund des Umstands der hierfür erforderlichen Risikofinanzierung allerdings nicht für identifizierte bestandsgefährdende Risiken in Betracht. Demgegenüber kann es wirtschaftlich sinnvoll sein, Risiken, deren Schadensausmaß und Eintrittswahrscheinlichkeit als gering einzustufen sind oder deren Verminderung mit zu hohen Kosten verbunden wäre, nicht aktiv zu steuern, sondern bewusst zu akzeptieren.[39]

7. Risikoüberwachung

1.29 Im Rahmen der **Compliance-Risikoüberwachung** werden die identifizierten Risiken in ihrer Entwicklung verfolgt und dadurch die Grundlage für eine wirksame Risikosteuerung gelegt.[40] Dabei gilt es auch, Abhängigkeiten bzw Interaktionen zwischen einzelnen Risiken zu erkennen und zu beachten.[41]

1.30 Es bedarf der Identifikation bzw Definition von geeigneten Kennzahlen und Indikatoren, die **Verantwortung** hierfür liegt bei den **Risiko-Ownern.**[42] Eine bewusste und aktive

35 Vgl auch *Glage/Glötzner* in *Hauschka et al,* Compliance[3] § 14 Rz 65; *Institut für Interne Revision Österreich,* Risikomanagementsystem[2] 58.
36 *Institut für Interne Revision Österreich,* Risikomanagementsystem[2] 59.
37 *Glage/Glötzner* in *Hauschka et al,* Compliance[3] § 14 Rz 66.
38 *Institut für Interne Revision Österreich,* Risikomanagementsystem[2] 59.
39 Vgl hierzu auch *Glage/Glötzner* in *Hauschka et al,* Compliance[3] § 14 Rz 66; *Institut für Interne Revision Österreich,* Risikomanagementsystem[2] 59; *Romeike* in *Inderst et al,* Compliance[3] Kap 3 Rz 294 ff.
40 *Glage/Glötzner* in *Hauschka et al,* Compliance[3] § 14 Rz 68.
41 *Klingenstein* in *Bay/Hastenrath,* Compliance[2] Kap 4 Rz 93.
42 Näher hierzu etwa *Klingenstein* in *Bay/Hastenrath,* Compliance[2] Kap 4 Rz 82 ff.

Risikosteuerung ist nur möglich, wenn die Risikoursachen vom Risiko-Owner **fortlaufend** überwacht und bei entsprechender Veränderung **frühzeitig** an das Compliance-Risikomanagement berichtet werden, um sich mit diesem bezüglich der Durchführung von Maßnahmen zur Adressierung der Compliance-Risiken abzustimmen.[43] An der Ursache-Wirkungskette des Unternehmens ansetzende **Frühwarnindikatoren** sollen zu jedem Zeitpunkt darüber Auskunft geben, ob ein Risiko in naher Zukunft eintreten wird.[44]

1.31 Die **Durchführung** der Maßnahmen zur Risikosteuerung muss ebenfalls **kontrolliert** werden. Das entsprechende **Monitoring** zielt darauf ab, durch eigene Kontrollmaßnahmen zu überprüfen, ob die vor dem Hintergrund der identifizierten und bewerteten Risiken ergriffenen Compliance-Risikosteuerungsmaßnahmen auch tatsächlich wirkungsvoll sind (Beobachtung der termingemäßen Durchführung der notwendigen Tätigkeiten[45]; Validierung der eingeführten Risikosteuerungsmaßnahmen)[46].

8. Risikoberichterstattung

1.32 Eine **standardisierte Berichterstattung,** soll der Geschäftsleitung (und ggf dem Aufsichtsrat) ein übersichtliches Bild über vorhandene Risiken (und Chancen) sowie deren Bewältigung vermitteln.[47] Hierbei kommen Standardberichte im Rahmen der Regelberichterstattung (in vierteljährlichen bis jährlichen Intervallen), ein Limit-gesteuertes Berichtswesen oder Ad-hoc-Meldungen aufgrund besonderer Veranlassung in Betracht.[48]

V. Compliance-Organisation

1.33 Die Reduzierung von Compliance-Risiken und die Einhaltung der rechtlichen Pflichten im Unternehmen beginnen auf der Grundlage der identifizierten Risiken mit der Implementierung einer angemessenen Aufbau- und Ablauforganisation.

1.34 Eine angemessene Aufbauorganisation macht insb eine **klare Festlegung von Verantwortlichkeiten** sowie die **Bereitstellung von Ressourcen und Hilfsmitteln** für die Entwicklung und Umsetzung der Compliance-Struktur erforderlich.[49] Hierzu ist eine horizontale und vertikale Delegation von Aufgaben und die Einhaltung aller Anforderungen an eine ordnungsgemäße Aufgabenteilung notwendig. Die Mitarbeiter, die mit Compliance-Aufgaben betraut sind, müssen sorgfältig ausgewählt, eingewiesen und überwacht werden. Vor diesem Hintergrund empfiehlt es sich, die Delegation von Organpflichten schriftlich zu fixieren – etwa durch Organisationspläne (Organigramme) und Stellenbeschreibungen. Ferner sind dem jeweiligen Aufgabenträger die zur Aufgabenerfüllung erforderlichen Sachmittel zur Verfügung zu stellen.

---

43 *Klingenstein* in *Bay/Hastenrath,* Compliance[2] Kap 4 Rz 82, 87, 91.
44 *Glage/Glötzner* in *Hauschka et al,* Compliance[3] § 14 Rz 69.
45 Vgl dazu auch *Klingenstein* in *Bay/Hastenrath,* Compliance[2] Kap 4 Rz 94 ff.
46 *Klingenstein* in *Bay/Hastenrath,* Compliance[2] Kap 4 Rz 96.
47 *Institut für Interne Revision Österreich,* Risikomanagementsystem[2] 60.
48 *Glage/Glötzner* in *Hauschka et al,* Compliance[3] § 14 Rz 70; im Rahmen der Überwachung von Risikolimits erfolgt die Limit-gesteuerte Berichterstattung bei Abweichungen bzw beim Überschreiten dieser Wertgrenzen.
49 Vgl dazu und zu Folgendem *Ruhmannseder* in *Petsche/Mair,* Compliance[3] 453.