



A12 – Compliance-Baukasten für den Mittelstand

Autoren: Ausschuss Mittelstand

DICO

Deutsches Institut für Compliance

Stand: Mai 2018

Disclaimer

DICO Arbeitsmaterialien richten sich an Compliance-Praktiker. Sie sollen einen Einstieg in das Thema erleichtern und einen Überblick verschaffen. Es wird daher bewusst darauf verzichtet, juristische Sonderfälle und Ausnahmeregelungen aufzuzeigen. Daher erheben sie nicht den Anspruch auf Vollständigkeit. **DICO Arbeitsmaterialien ersetzen nicht den Rechtsrat im Einzelfall. DICO übernimmt keine Verantwortung für Entscheidungen, die sich auf Ausführungen in DICO Arbeitsmaterialien stützen.**

Senden Sie Ihre Anregungen und Beiträge an Leitlinien@dico-ev.de. Wir freuen uns auf eine lebhafte Diskussion und bedanken uns für Ihre konstruktive Unterstützung!



VORWORT	4
1. COMPLIANCE-KULTUR	5
2. COMPLIANCE- ZIELE	11
3. COMPLIANCE-RISIKEN	15
4. COMPLIANCE - PROGRAMM	20
5. COMPLIANCE- ORGANISATION	36
6. COMPLIANCE-KOMMUNIKATION	52
7. COMPLIANCE-ÜBERWACHUNG	70

Vorwort

Immer mehr mittelständische Unternehmen stehen vor der Herausforderung, ein Compliance Management System (CMS) einzuführen und zu entwickeln und dabei ihr Unternehmensumfeld und die eigene Geschäftstätigkeit zu berücksichtigen. Gefragt sind praxistaugliche und schlanke Compliance-Ansätze unter der Beachtung von Mindestanforderungen an ein CMS.

Die Fragestellung dabei ist: Was ist angemessen? Was ist bereits vorhanden und reicht dies aus? Was muss noch geschaffen werden?

Da gibt es keine Standard-Lösung für alle, jedes Unternehmen ist einzigartig und muss für sich auch ein individuelles System entwickeln. Das CMS muss nicht nur als „Tone from the Top“ durch das Top-Management vorgelebt und unterstützt werden, auch das Verständnis und vor allem die Akzeptanz der Belegschaft sind von zentraler Bedeutung. Hilfreich ist dabei immer, bereits bestehende Systeme und Instrumente mitzunutzen, z.B. Qualitätsmanagementsysteme, Interne Kontrollsysteme, Risikomanagementsysteme, Umfragen, Veranstaltungen, etc.

Dieses Arbeitspapier soll als Praxishilfe und Orientierung für mittelständische Unternehmen dienen, um genau diese Fragen zu beantworten. Es wurde von Praktikern für Praktiker geschrieben. Die Mitglieder im Ausschuss Mittelstand von DICO haben die eigenen Erfahrungen und das gesammelte Wissen bei der Einführung, Aufrechterhaltung und Weiterentwicklung eines CMS zusammengetragen und in dem vorliegenden Baukasten mit den einzelnen Bausteinen beschrieben. Der Baukasten orientiert sich an der Gliederung des IDW Prüfungsstandard: Grundsätze ordnungsgemäßer Prüfung von Compliance-Management-Systemen (IDW PS 980) und soll einen umfassenden Überblick zur möglichen Erfüllung geben. Dabei erhebt er keinen Anspruch auf Vollständigkeit oder auf eine vollständige Konformität mit dem IDW PS 980, bei dem es sich im Übrigen um einen Prüfungsstandard handelt.

In jedem Baustein werden die einzelnen Themen und Instrumente kurz beschrieben, teilweise mit Vorteilen und zu beachtenden Rahmenbedingungen bewertet und praxisnahe Empfehlungen zur Umsetzungsstrategie gegeben. Damit liegen für jeden Baustein schnelle, brauchbare Lösungsansätze vor. Oft sind die einzelnen Bausteine inhaltlich miteinander verbunden und ergänzen sich.

So können mittelständische Firmen von den Erfahrungen anderer profitieren und müssen sich nicht erst mühsam in die Themen einarbeiten. »

1. Compliance-Kultur

1.1 Tone from the Top

1. Beschreibung:

Der „Tone from the Top“ ist die Grundvoraussetzung für eine nachhaltig gelebte Unternehmenskultur. Ganz einfach besagt der Begriff, das oberste Management (Unternehmensführung, Führungskräfte) muss mit „gutem Beispiel vorangehen“, wobei hier Taten entscheidender sind als Worte.

Das Management gibt das Ziel und den gemeinsamen Weg vor und spricht dabei klar aus, was erlaubt und nicht erlaubt ist. Dies wird zumeist in einem „Code of Conduct/Verhaltenskodex“ verschriftlicht. Für die Implementierung einer Compliance-Kultur stellt ein Verhaltenskodex eine wichtige Komponente dar (siehe dazu 1.2.).

Für eine nachhaltig gelebte Compliance Kultur gilt es dann, dem „Tone from the Top“ folgend, diesen im betrieblichen Alltag zu berücksichtigen/anzuwenden und „mit gutem Beispiel“ voranzugehen. Der „Tone from the Top“ zeigt der Belegschaft, dass das oberste Management hinter einem Thema bzw. einem System steht, was erheblich zu dessen Beachtung und Akzeptanz beiträgt. Hierbei muss ein klares Statement ins Unternehmen hineingetragen werden, aber auch nach außen sichtbar erfolgen.

*„Mit gutem Beispiel voranzugehen, ist nicht nur der beste Weg,
andere zu beeinflussen, es ist der einzige.“*

(Albert Schweitzer)

2. Vorteile und zu beachtende Rahmenbedingungen:

Vorteile	Zu beachten
• Stärkt das Thema Compliance • Fördert die Akzeptanz im Unternehmen • Unterstreicht die Wichtigkeit und gibt der Belegschaft Sicherheit und Orientierung	• Das Management muss nachhaltig und ausnahmslos hinter der Compliance-Kultur stehen, damit diese nicht den Charakter eines Feigenblattes hat

3. Umsetzungsstrategie:

Das Management muss sich klar positionieren und das Thema flächendeckend kommunizieren, um im Unternehmen Akzeptanz zu schaffen z.B. als ein Punkt auf der Agenda von Führungskonferenzen, Betriebsveranstaltungen, Meetings, etc.

1.2 Verhaltenskodex

1. Beschreibung:

Ein Verhaltenskodex (engl. Code of Conduct) ist eine Sammlung von Verhaltensweisen, die in unterschiedlichsten Umgebungen und Zusammenhängen angewandt werden können bzw. sollen oder die es zu berücksichtigen gilt.

Ein Verhaltenskodex ist eine Selbstverpflichtung, bestimmten Verhaltensmustern zu folgen oder diese zu unterlassen und dafür Sorge zu tragen, dass sich niemand durch Umgehung dieser Muster einen Vorteil oder anderen einen Nachteil verschafft. In einem Verhaltenskodex werden oftmals auch gesetzliche Verpflichtungen (z.B. Vermeidung von Korruption, Vermeidung von Kartellen, Vermeidung von Datenschutzverstößen, etc.) im Überblick adressiert und zusätzlich durch themenspezifische Richtlinien (z.B. Anti-Korruptionsrichtlinie) ergänzt.

Als Bestandteil des CMS beschreibt der Verhaltenskodex – basierend auf Compliance Prinzipien – die Compliance-Kultur eines Unternehmens, fasst deren ethische Grundsätze und Prinzipien für das Handeln aller Beschäftigten zusammen und gibt klare Verhaltensregeln für die praktische Arbeit an die Hand.

2. Vorteile und zu beachtende Rahmenbedingungen:

Vorteile	Zu beachten
• Klares Bekenntnis nach innen, Förderung der Akzeptanz von Compliance • Die Erwartungen des Unternehmens an seine Beschäftigten sind transparent und nachvollziehbar dokumentiert • Positives Image nach Außen (wenn veröffentlicht)	• Verständliche und adressatengerechte Formulierungen • Übersetzung in andere Sprachen (mindestens Englisch) bei international tätigen Unternehmen mit Tochtergesellschaften im Ausland (z.B. Chinesisch, Russisch, etc.) • Kulturelle Unterschiede bei der Gestaltung beachten (z.B. Bilder/Fotos)

3. Umsetzungsstrategie:

Bei der Erarbeitung eines Verhaltenskodex sollten unterschiedliche Fachdisziplinen (z.B. Recht, Compliance, Personal, Datenschutz) mitwirken. Im Umfang sollte es maximal eine Broschüre werden, in einfacher und verständlicher Sprache formuliert und ggf. mit Bildern illustriert. Bei international tätigen Unternehmen ist eine Übersetzung mindestens in die englische Sprache wichtig, ggf. auch in weitere Sprachen.

Sofern vorhanden, sollte (bzw. muss) der Betriebs- oder Personalrat eingebunden werden, damit die Personalvertretung informiert ist und einfacher Akzeptanz bei der Belegschaft erreicht werden kann.

1.3 Transparenz (Dokumentation)

1. Beschreibung:

Transparenz ist ein wesentlicher Grundpfeiler einer funktionierenden Compliance. Der offene Umgang mit Risiken, die Einbettung von Compliance-relevanten Maßnahmen in effiziente und klar strukturierte Prozesse sowie eine zutreffende Dokumentation sind von zentraler Bedeutung. Denn Unternehmen, die im Verborgenen agieren, stehen schnell unter Verdacht, sich nicht an Gesetze zu halten oder zumindest rechtliche Grenzbereiche bewusst über Gebühr zum eigenen Vorteil auszunutzen.

Transparenz schafft sowohl Sicherheit als auch Nachvollziehbarkeit und stärkt das Wertemanagement. Dies führt wiederum zur Akzeptanz unter Mitarbeitern und Stakeholdern. Zudem werden durch Transparenz und Dokumentation Haftungsrisiken erheblich reduziert.

Ein CMS ohne die nötige Transparenz ist daher nicht denkbar.

Wichtige Elemente zur Schaffung einer umfassenden Transparenz sind beispielsweise (diese Elemente sind jedoch nicht ausschließlich Bestandteile der Compliance-Kultur, sondern auch wesentliche Bestandteile des Compliance-Programms und anderer CMS Elemente):

- Organisatorische Transparenz fördernde Maßnahmen (Vier-Augen-Prinzip, Rotationsprinzip, Kontrollmechanismen, Compliance-Ausschüsse, Compliance-Reporting an Vorstand und Aufsichtsrat, Prinzip der Funktionstrennung von vollziehenden, verwaltenden und verbuchenden Tätigkeiten);
- Risikobasierte Einbindung der übergeordneten Unternehmensebenen, ggf. unter Einbeziehung der Compliance-Verantwortlichen (z.B. Genehmigungs- oder Anzeigepflichten im Hospitality-Bereich, Zustimmungserfordernisse bei Risikogeschäften oder Provisionen für externe Berater, Reporting Lines bei Verstößen);
- Dokumentation der Compliance-relevanten Prozesse (z.B. Rechnungsfreigabeprozesse, Beschaffungsprozesse, Business Partner Due Diligence Prüfungen);
- Klare Vertragsgestaltung unter Beschreibung der Leistungsinhalte und Integrity-Prüfungen bei Risikogeschäften (z.B. Beraterverträge im Ausland).

2. Vorteile und zu beachtende Rahmenbedingungen:

Vorteile	Zu beachten
• Rechtssicherheit • Akzeptanz unter Mitarbeitern und Stakeholdern • Haftungsreduktion (u.a. wegen nachvollziehbarer Vorgaben)	• Zusätzlicher Arbeitsaufwand und Kosten

3. Umsetzungsstrategie:

Mit dem Aufbau und der Weiterentwicklung des Compliance-Managementsystems sind die Prozesse im Unternehmen, die Transparenz etablieren und fördern, laufend zu evaluieren und fortzuentwickeln.

1.4 Information/Kommunikation

1. Beschreibung:

Kommunikation ist elementarer Bestandteil für eine effektive Compliance-Arbeit innerhalb einer Organisation. Daher sollte das CMS jedes Unternehmens, unabhängig von seiner Größe und seines Alters, über ein zielgruppenorientiertes, angemessenes Kommunikationssystem (siehe dazu auch Compliance-Kommunikation, Ziffer 6) verfügen.

Durch Compliance-Kommunikation werden Mitarbeiter und Geschäftspartner über für sie relevante unternehmensinterne Regeln, Pflichten, Verantwortlichkeiten, Rollen und Berichtswege der Compliance-Organisation so informiert, dass sie diese verstehen, unterstützen und vor allem einhalten können. Als übergeordnetes Ziel sollen Mitarbeiter und „Dritte“ ein integraler Bestandteil des präventiven CMS werden. Um Compliance-Kommunikation zielgerichtet und effektiv zu gestalten, ist ein Blick auf die unterschiedlichen Zielgruppen innerhalb der Compliance-Organisation wichtig. Denn nicht nur Mitarbeiter prägen das Gelingen einer integralen Compliance-Strategie, auch Führungskräfte, Compliance-Verantwortliche, Geschäftspartner und sogar die Öffentlichkeit sind ausschlaggebend für den Erfolg.

Compliance-Kommunikation muss nicht nur zielgruppengerecht sein, wichtig ist auch, welche Inhalte wie kommuniziert werden. Empfehlenswert ist es, neben ausführlichen Richtlinien z.B. auch zusammenfassende 1- oder 2-seitige Dokumente (sogenannte One-Pager) zur Erfassung der wichtigsten Informationen ergänzend bereitzustellen.

Ausschlaggebend für die Art der Compliance-Kommunikation ist der Umsetzungsgrad des Compliance-Managementsystems basierend auf der Compliance-Strategie. Steht ein Unternehmen ganz am Anfang, sollten erst Risikofelder definiert, bevor Richtlinien und Verantwortlichkeiten formuliert werden. Sobald eine Compliance-Organisation feststeht, können Berichtswege und ein Kommunikations-Konzept erarbeitet werden. In diesem Fall ist die Compliance-Kommunikation maßgeblich dafür verantwortlich, ob das CMS erfolgreich umgesetzt und von allen betroffenen Zielgruppen angenommen wird. Ist ein Unternehmen schon mit Compliance-Richtlinien und -Prozessen ausgestattet, übernimmt die Compliance-Kommunikation eine unterstützende Rolle.

2. Vorteile und zu beachtende Rahmenbedingungen:

Vorteile	Zu beachten
• Definierte und bekannte Wege zur Kommunikation von CMS-relevanten Sachverhalten • Abbau von Hemmnissen durch hohe Transparenz der Verfahren und Regelungen in der Kommunikation	• Intransparente, undefinierte Kommunikation führt zu Unsicherheit – relevante Sachverhalte werden ggf. nicht gemeldet und sollen daher vermieden werden

3. Umsetzungsstrategie:

- Schaffung einer entsprechenden Compliance-Funktion innerhalb der Organisation
- Identifizierung der wichtigsten Zielgruppen für Compliance-Kommunikation
- Inhalte, Maßnahmen und Kanäle der Compliance-Kommunikation festlegen
- Einführung eines CMS
- Implementierung von Maßnahmen
- Verankerung im Unternehmen und kontinuierliche Verbesserung eines bestehenden CMS
z.B. durch definierte und überwachte Kontrollen und Messpunkte

1.5 Null-Toleranz Politik (Verstöße)

1. Beschreibung:

Bestandteil einer gelebten Compliance-Kultur ist eine Null-Toleranz-Politik. Hierunter ist nicht zu verstehen, dass selbst kleinste Verstöße rigoros verfolgt werden.

Null Toleranz bedeutet vielmehr zunächst das klare Bekenntnis der Unternehmensführung, Verstöße gegen Gesetze oder interne Leitlinien nicht zu tolerieren, auch wenn sie aus der Sicht des Mitarbeiters im vermeintlichen „Unternehmensinteresse“ erfolgt sind. Hierzu zählen wirksame und für die Mitarbeiter erkennbare Regelungen und Vorgaben in den Compliance-Richtlinien und die konsequente Verfolgung und Sanktionierung von festgestellten Verstößen.

Konsequente Verfolgung von Verstößen bedeutet, dass jeder Verstoß ohne Ansehen der Person (auch die „Großen“) und des Geschäftsbereiches (z.B. Korruption und Kartell im Vertrieb) untersucht und geprüft und die Entscheidung nachvollziehbar dokumentiert wird. Die Sanktion selber muss jedoch alle Aspekte und Folgen der Tat berücksichtigen und reicht von der Strafanzeige, Beendigung von Geschäftsbeziehungen, fristloser oder fristgerechter Kündigung von Arbeitnehmern, Schadensersatz bei schwerwiegenden Verstößen bis zur bloßen Ermahnung oder auch einem Verzicht auf eine Sanktion bei geringeren Verstößen, wenn beispielsweise der Täter selber durch die Tat oder deren Aufdeckung Nachteile erlitten hat (deliktadäquate Sanktionen).

Ein Hinweis auf diese Sanktionsmöglichkeiten in den einzelnen Compliance-Richtlinien sowie der Compliance-Leitlinie ist empfehlenswert, um die Ernsthaftigkeit der Compliance-Anstrengungen zu unterstreichen.

2. Vorteile und zu beachtende Rahmenbedingungen:

Vorteile	Zu beachten
• Null-Toleranz, das glaubhafte Bekenntnis der Unternehmensleitung ist Basis der Compliance-Kultur • Die kommunizierte Kultur und die Sanktionierung von Verstößen verdeutlicht den Mitarbeitern den Rahmen, in dem sie sich verhalten und mit welchen Sanktionen sie rechnen müssen	• Null-Toleranz ohne Augenmaß kann zu einer Verängstigung und Abschreckung der Mitarbeiter durch übermäßig harte Sanktionen führen. Es besteht die Gefahr, dass Compliance-Verstöße aus Angst und evtl. falsch verstandener Kollegialität vertuscht werden. Dies gilt insbesondere für Unternehmen mit wenig Mitarbeitern und dementsprechend kollegialen Strukturen. • Bei allen Sanktionen ist die evtl. Einbindung der betriebsverfassungsrechtlichen Organe zu berücksichtigen. Die Ausgestaltung der Null-Toleranz-Politik hat auch Auswirkungen auf die Entscheidungen des Aufsichtsrates gegenüber der Unternehmensführung, da er nicht hinter die für alle Mitarbeiter geltenden Regeln zurückfallen kann.

3. Umsetzungsstrategie:

Die Null-Toleranz-Politik sollte in der Compliance-Leitlinie als Bestandteil der Compliance-Kultur niedergelegt und veröffentlicht werden. Zudem ist es denkbar, dass sich in einzelnen Compliance-Richtlinien (z.B. Korruption) klare Aussagen dazu finden. In Unternehmensführung und Aufsichtsrat sollte regelmäßig über festgestellte Verstöße und die getroffenen Entscheidungen kommuniziert werden. Dies sollte mindestens in einem jährlichen Compliance-Bericht erfolgen.

Unternehmensführung und Compliance-Funktion können auch die Belegschaft in der zum Schutz der Betroffenen angemessenen Form über Compliance-Verstöße und deren Handhabung informieren – insbesondere im Rahmen von Compliance-Schulungen eignen sie sich als Beispiele einer gelebten Compliance-Kultur. »

2. Compliance-Ziele

2.1 Compliance-Ziele abgeleitet aus den Unternehmenszielen

1. Beschreibung:

Unter einem CMS sind die eingeführten Grundsätze und Maßnahmen eines Unternehmens zu verstehen, die auf die Sicherstellung eines regelkonformen Verhaltens der gesetzlichen Vertreter und der Mitarbeiter des Unternehmens sowie ggf. von Dritten abzielen. Damit zielen sie auf die Einhaltung bestimmter Regeln und auf die Verhinderung von Verstößen (Definition gemäß IDW PS 980). Vereinfacht gesagt soll das CMS die Geschäftsführer oder Vorstände einer Gesellschaft dabei unterstützen, Gesetzesverstöße systematisch und risikoorientiert zu vermeiden.

Daraus kann auch abgeleitet werden, dass ein CMS die Verwirklichung der im Unternehmen bestehenden Grundwerte durch Einhaltung der rechtlichen Rahmenbedingungen und der internen Verhaltensrichtlinien mit dem Ziel der Durchsetzung einer werteorientierten Unternehmensführung, einer vorbeugenden Risikominimierung und einer Abwehr von Schäden vom Unternehmen, seinen Mitarbeitern und Kunden umfasst.

Durch die Einhaltung der maßgeblichen rechtlichen Rahmenbedingungen wird das Integritätsinteresse des Unternehmens gewahrt. Bei Fehlverhalten drohen rechtliche Konsequenzen, die erhebliche Auswirkungen auf den Ruf und die Geschäftstätigkeit des gesamten Unternehmens haben können.

Grundsätzlich werden Compliance-Ziele auf der Grundlage der allgemeinen Unternehmensziele und der für das Unternehmen bedeutsamen Compliance-Kultur (Werte) festgelegt. Compliance-Ziele umfassen auch die Festlegung der für das Unternehmen mit höchster Priorität zu beachtenden Rechtsgebiete (z.B. Anti-Korruption, Kartellrecht, etc.), siehe Ziffer 2.2.

Ferner können Compliance-Ziele aus firmenspezifischen Grundsätzen (Mission-Statements) abgeleitet werden. Compliance-Ziele stehen somit in einem engen Zusammenhang mit anderen, ggf. bereits in weiteren Managementsystemen (Qualität, Umwelt, Sicherheit) formulierten Zielen.

Zur Erfüllung der oben genannten Anforderungen sollten sich die Compliance-Ziele an den folgenden Kriterien orientieren:

- Compliance-Ziele sollen der Compliance-Kultur entsprechen und das regelkonforme Verhalten des Unternehmens vertreten. So werden die Akzeptanz sowie die Eigenverantwortung der einzelnen Mitarbeiter verstärkt.
- Compliance-Ziele sollen bei vorhandener Kapazität des Unternehmens erreichbar sein und die geltenden Anforderungen für die Geschäftsfelder des Unternehmens berücksichtigen.
- Compliance-Ziele sollen kommuniziert werden und damit die Bereitschaft der Mitarbeiter wecken, die Verantwortung ihres Handelns zu übernehmen.
- Soweit praktikabel sollen Compliance-Ziele messbar sein.
- Compliance-Ziele sollen in regelmäßigen Zeitabständen überwacht werden. Dies kann z.B. auf Grundlage von intern durchgeführten Audits, während der Treffen des Compliance-Ausschusses oder beim jährlichen Managementreview erfolgen.

- Compliance-Ziele sollen in einem eigenständigen Dokument zusammengefasst und z.B. jährlich oder nach Bedarf aktualisiert und/oder revidiert werden. Dies kommt einer besonderen Bedeutung bei wesentlichen Änderungen in dem Unternehmen zu, wie Umstrukturierung des Unternehmens, Erschließung neuer Geschäftsfelder oder Märkte oder Eintreten von Verdachtsfällen.

Für die Erreichung der gesetzten Compliance-Ziele ist bei der Planung die Festlegung von Maßnahmen, Verantwortlichkeiten, Ressourcen sowie Zeitraum umso wichtiger. Grundvoraussetzung für die Wirksamkeit im Verständnis des Unternehmens sollte sein, dass Compliance von den Führungskräften gelebt und in den jeweiligen Zuständigkeitsbereichen umgesetzt wird.

2. Vorteile und zu beachtende Rahmenbedingungen:

Vorteile	Zu beachten
• Compliance Ziele sind die notwendige Voraussetzung für die Etablierung eines risiko-orientierten und systematischen CMS • Compliance Ziele unterliegen einer permanenten Überprüfung und Aktualisierung (lebendes System) • Abgleich mit Zielen aus anderen Managementsystemen • Wirtschaftliche Optimierung des CMS	• Compliance-Ziele müssen interdisziplinär erarbeitet werden

3. Umsetzungsstrategie:

Ableitung von Compliance-Zielen / Schwerpunkte (Beispiele)

Wahrung der Reputation und Schutz des Unternehmens durch

- Verhinderung von Verstößen gegen Kartell- und Antikorruptionsvorschriften,
- Verhinderung von sonstigen „Vermögensstraftaten“ (intern/extern), darunter auch Geldwäsche,
- Verhinderung von Verstößen gegen datenschutzrechtliche Bestimmungen

Die Compliance-Ziele orientieren sich z.B. an der Branche, Internationalität und dem Geschäftsmodell des Unternehmens.

2.2 Festlegen der relevanten Rechtsgebiete

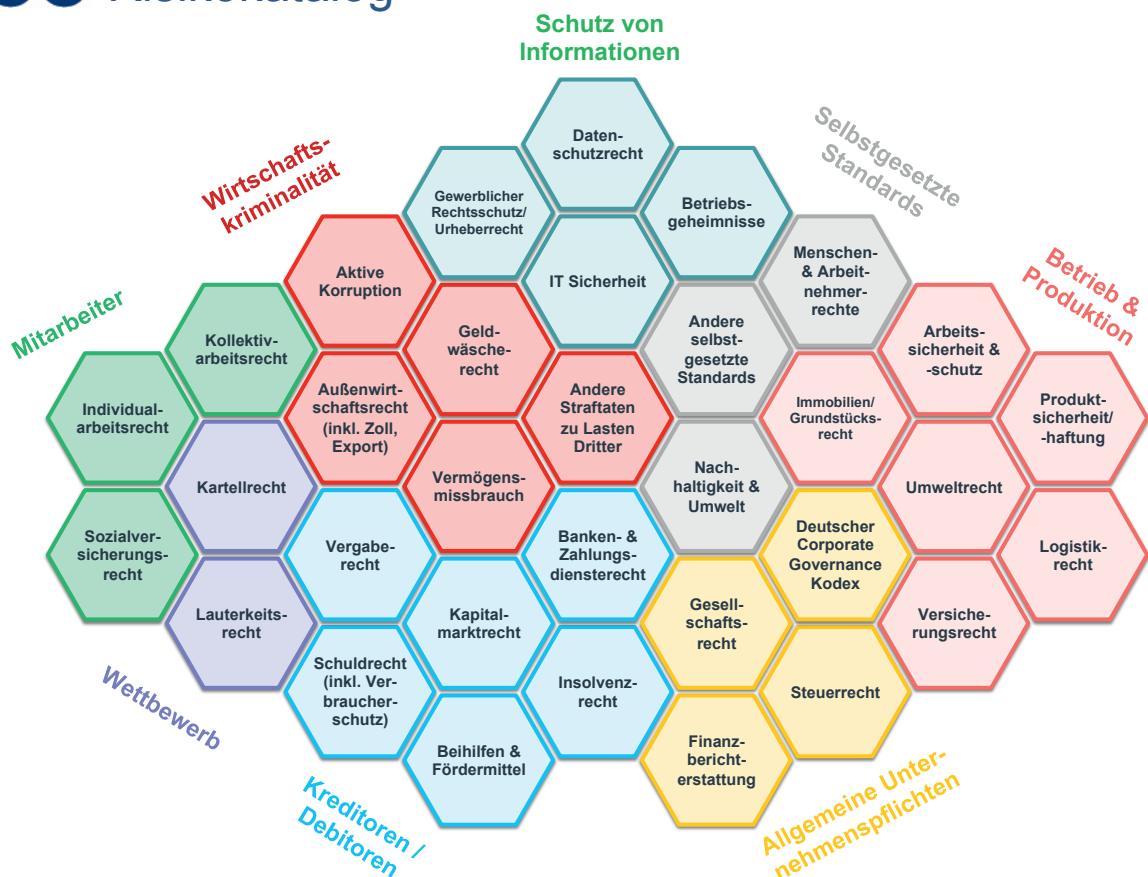
1. Beschreibung:

Zentrales Element eines CMS ist die Festlegung von abgegrenzten Teilbereichen, in denen die Compliance-Regeln gelten sollen und somit die Compliance-Ziele gesetzt werden. In der Regel handelt es sich bei den relevanten Compliance-Bereichen um eine Vielfalt von Rechtsgebieten, für deren Beachtung die Unternehmensführung die Verantwortung trägt.

Schwerpunkte sind die für das Unternehmen risikobehafteten Bereiche, die im Rahmen einer Risikobetrachtung ermittelt wurden. Als zu regelnde Bereiche können in Abhängigkeit der Unternehmensgröße, -tätigkeit sowie der internationalen Aktivitäten z.B. Vertrags-, Vergabe- und Wettbewerbsmanagement, Korruptionsverstöße sowie Zuwendungen, Lobbyismus und Geschäftskontakte definiert und in entsprechenden Richtlinien untersetzt werden.

Im weitesten Sinne hat der DICO Arbeitskreis „Compliance-Risikoanalyse“ insgesamt 33 generische Compliance-Themenfelder aus den Rechtsgebieten identifiziert, aus denen sich für ein Unternehmen relevante rechtliche Bereiche ableiten lassen (siehe Bild).

DICO Risikokatalog



2. Vorteile und zu beachtende Rahmenbedingungen:

Vorteile	Zu beachten
• Schaffung verstärkter Rechtssicherheit für das Unternehmen und die Mitarbeiter • Schutz vor zivil- und strafrechtlicher Haftung und Reputationsschaden • Schrittweiser Auf- und Ausbau des Compliance-Systems • Steigerung der Effizienz und Vermeidung von unnötigem Aufwand	• Compliance-Ziele müssen im Zeitablauf immer wieder auf Aktualität geprüft werden. Ohne die richtigen Compliance-Ziele ist das gesamte CMS ineffizient und ineffektiv.

3. Umsetzungsstrategie:

Festlegung des Geltungsbereiches des CMS (Beispiele), der firmen- und/oder bereichsbezogen gesetzt werden kann.

- Vertrags-, Vergabe- und Wettbewerbsmanagement
- Wirtschaftskriminalität
- Datenschutz und Intellectual Property

Aufstellen von Compliance-Leitlinien (Beispiel)

- Einhaltung der anwendbaren Gesetzen und Vorschriften für die Abwicklung der Geschäftsprozesse
- Transparenz und Kommunikation als der Schlüssel zu Compliance
- Ehrlichkeit und Beachtung der Compliance-Regelungen als Kernelement der Geschäftstätigkeit
- Effektiver Umgang mit Ressourcen und Risiken des Unternehmens
- Verantwortung jedes Mitarbeiters für sein Handeln
- Einhaltung moralisch-ethischer Standards
- Gesetzesverstöße werden nicht toleriert; Mitarbeiter werden nicht für Verluste verantwortlich gemacht, die auf der Einhaltung geltender Gesetze beruhen
- Das Vertrauen von Mitarbeitern und Geschäftspartnern als unverzichtbare Grundlage für nachhaltiges Wachstum »

3. Compliance-Risiken

3.1 Prozess

a. Identifizierung (Workshops/Checklisten/Fragenkatalog, etc.)

1. Beschreibung:

Im ersten Schritt sollen die möglichen Compliance-Risiken identifiziert werden, die einen Einfluss bzw. eine Auswirkung auf die entsprechende Geschäftstätigkeit/Ziele (Compliance-Ziele) des Unternehmens haben können.

Zum Bestandteil der Identifizierung gehören die Bestimmung der relevanten Risikofelder (siehe DICO-Risikokatalog aus dem Arbeitskreis „Compliance-Risikoanalyse“) und deren Detaillierung.

Die Identifizierung stellt die Basis für ein angemessenes und risikoorientiertes Compliance-System dar.

2. Vorteile und zu beachtende Rahmenbedingungen:

Vorteile	Zu beachten
• Risikoanalyse als Voraussetzung für ein maßgeschneidertes System • Angemessene Detaillierungstiefe durch Risikokatalog und inhaltliche Untersetzung. • Verhältnismäßiger Aufwand	• Notwendige Überprüfung auf Aktualität

3. Umsetzungsstrategie:

Z.B. Implementierung von Workshops zur Identifikation der relevanten Risiken unter Nutzung von Risikokatalog (siehe DICO-Risikokatalog aus dem Arbeitskreis „Compliance-Risikoanalyse“). In die Workshops sollen die Fachexperten des Unternehmens, wie z.B. Mitarbeiter Rechtsabteilung, Risikomanagement, interne Revision, Risikomanagement, Fachabteilungen (z.B. Einkauf, Vertrieb usw.) eingebunden werden.

Es sollten interne und externe Informationsquellen herangezogen werden.

Die Ergebnisse der Risikoidentifikation sind nachweisbar zu dokumentieren.

b. Analyse und Bewertung (Brutto/Netto; Bewertungskriterien)

1. Beschreibung:

Analyse: Im zweiten Schritt werden die zuvor identifizierten Compliance-Risikofelder näher untersucht. Hiermit sollen die Compliance-Risiken konkretisiert werden einschließlich einer kurzen Beschreibung des Risikos hinsichtlich seiner möglichen negativen Auswirkungen. Dabei sind die Einflussquellen und Einflussfaktoren hinsichtlich ihrer Wahrscheinlichkeit und Schadenpotenzial darzustellen.

Bewertung: Nach der Beschreibung der möglichen negativen Auswirkung erfolgt nun eine Gewichtung und konkrete Bewertung (Brutto-Bewertung) anhand von monetären und nicht-monetären Kriterien.

Bei der Bewertung wird nach einer Brutto- und Netto-Bewertung unterschieden. Die Risikoanalyse beinhaltet die Brutto-Risiken.

Brutto-Risiko: Risiko ohne Berücksichtigung von Maßnahmen,

Netto-Risiko: Das verbleibende Risiko unter Berücksichtigung von Maßnahmen (Steuerungsmaßnahmen, siehe 3.1 c).

2. Vorteile und zu beachtende Rahmenbedingungen:

Vorteile	Zu beachten
• Kennen der Compliance-Risiken • Fundierte Grundlage für die Priorisierung von Risiken • Ableitung von geeigneten Maßnahmen zur Risikosteuerung	• Auswahl der richtigen Ansprechpartner und stringente Organisation/Agenda

3. Umsetzungsstrategie:

Innerhalb der Workshops der Identifikation ist ebenfalls die Analyse und Bewertung durch die Fachexperten vorzunehmen.

Entwicklung einer einheitlichen Systematik zur Risikobewertung. Hierdurch sollen alle identifizierten Risiken nach einer einheitlichen Methodik bewertet werden.

Zur Veranschaulichung der Bruttonisiken sind diese in Form einer Risikomatrix abzubilden.

Die Ergebnisse der Analyse und Bewertung sind nachweisbar zu dokumentieren.

c. Steuerung (Maßnahmen)/Überwachung/Monitoring (Steuerungsmaßnahmen)

1. Beschreibung:

Ziel ist es, mit geeigneten Maßnahmen die bewerteten Brutto-Risiken mit einer entsprechenden Risiko-Strategie (Vermeiden, Vermindern, Überwälzen, Akzeptieren) zu reduzieren. Voraussetzung hierfür ist eine Festlegung, ab welcher Risikohöhe (Auswirkung des Risikos – qualitativ/quantitativ) Maßnahmen einzuleiten sind.

Die Eignung der Maßnahmen sollte mit einer entsprechenden Prüfung der Wirksamkeit nachgewiesen werden (z.B. das in einer Unterschriftenregelung festgelegte Vier-Augen-Prinzip sollte auf seine Wirksamkeit hin überprüft werden). Die Maßnahmen werden in der DICO-Leitlinie L09 – Compliance Risikoanalyse (CRA) beschrieben.

Geeignete Prüfmethode sind z.B. Prüfungen der internen Revision, Audits, Tests, Begehungen.

2. Vorteile und zu beachtende Rahmenbedingungen:

Vorteile	Zu beachten
• Reduzierung der Risikosituation • Transparenz • Angemessenheit der Maßnahmen	• Wirtschaftlichkeitsprinzip (Nutzen-Kosten-Verhältnis) sollte beachtet werden

3. Umsetzungsstrategie:

Bei der Analyse und Bewertung durch die Fachexperten sind ebenfalls die möglichen Maßnahmen zur Risikobeherrschung (siehe DICO-Leitlinie L09 – Compliance Risikoanalyse (CRA)) abzuleiten.

Die abgeleiteten Maßnahmen, wie auch die Ergebnisse der Überwachung (Prüfungsergebnisse) sind nachweisbar zu dokumentieren.

3.2 Organisation der Risikoanalyse

a. Berichterstattung / Turnus

1. Beschreibung:

Abhängig von der Unternehmensform und -struktur ist die jeweilige gesetzlich geforderte Berichtspflicht zu prüfen.

Weiterhin ist zu prüfen, ob es eine interne Berichtspflicht des Unternehmens an ein mögliches Leitungsgremium/Aufsichtsgremium gibt.

Der Turnus zur Berichterstattung ist unternehmensspezifisch und insbesondere unter Berücksichtigung des Unternehmens- sowie dem Tätigkeitsfeld festzulegen (monatlich/quartalsweise/halbjährlich/jährlich).

2. Vorteile und zu beachtende Rahmenbedingungen:

Vorteile	Zu beachten
• Nachweisbare Dokumentation • Erfüllung der gesetzlichen Forderungen	• Effiziente Abläufe sollten sichergestellt werden

3. Umsetzungsstrategie:

Für die Dokumentation und ggf. Berichterstattung ist folgendes festzulegen:

- der Umfang
- inhaltliche Detaillierungstiefe
- Layout
- Adressatenkreis (Verteiler)

b. IT-Lösung

1. Beschreibung:

Ob eine Softwarelösung für die Dokumentation der Risikoanalyse genutzt wird, ist eine individuelle Unternehmensentscheidung und Abwägung von Nutzen und Kosten. Die Softwarelösung bietet den besten Nachweis der Ergebnisse der Risikoanalyse.

Eine zweite Variante wären Excel und Word. Mit Hilfe von Excel und Word erfolgt zumindest eine temporär verfügbare Dokumentation. Gleichzeitig können mit Hilfe von Excel auch Rechenoperationen programmiert werden, die bei der Bewertung der Brutto-/Nettorisiken sowie der Wirksamkeit der Maßnahmen unterstützen können.

2. Vorteile und zu beachtende Rahmenbedingungen:

Vorteile	Zu beachten
• Revisionssichere Nachweisführung • Transparenz • Effektivität der Arbeitsabläufe, Reduzierung des Pflegeaufwandes	• Kosten für die Softwarebeschaffung, -bereitstellung, -pflege, -wartung und -aktualisierung (keine Einmal-Kosten)

3. Umsetzungsstrategie:

Zuerst ist zu prüfen, welche der zwei Varianten angemessen für das Unternehmen ist. Für die erstmalige Implementierung einer Software-Lösung sollte externe Unterstützung hinzugezogen werden.



4. Compliance-Programm

4.1 Einführung / Vorbereitung eines CMS

a. Compliance-Handbuch

1. Beschreibung:

Das gesamte Compliance-Regelwerk wird als Compliance-Handbuch bezeichnet. Im Compliance-Handbuch werden alle relevanten Elemente des Compliance-Programms beschrieben. Der Code of Conduct (Verhaltenskodex, siehe Ziffer 1.2) und die einzelnen Compliance-Anweisungen können ebenfalls Bestandteile des Compliance-Handbuchs sein.

Das Compliance-Handbuch sollte allen Beschäftigten in einer geeigneten Art und Weise zugänglich sein.

2. Vorteile und zu beachtende Rahmenbedingungen:

Vorteile	Zu beachten
• Alle Compliance-relevanten Regelungen und Informationen befinden sich zentral an einer Stelle	• Unübersichtlichkeit vermeiden

3. Umsetzungsstrategie:

Die Verantwortlichkeit für das Thema Compliance muss festgelegt werden. Dieser Funktion obliegen die vollständige Dokumentation und die Verantwortung für das komplette Regelwerk zu Compliance.

b. Richtlinien und Merkblätter

1. Beschreibung:

Für einzelne, spezielle Compliance-Themen sollte es Regelungen geben, die schnell auffindbar sind. Diese sollten klare, verständliche Anweisungen zum Handeln geben, ggf. können dazu bildliche Darstellungen gewählt werden. Für aktuelle Anlässe (z.B. neue Geschenke-Regelung) können Merkblätter entwickelt und ausgehangen werden. Die Regelungen sollten regelmäßig kommuniziert und geschult werden.

Sie sind Bestandteil des Compliance-Handbuches.

2. Vorteile und zu beachtende Rahmenbedingungen:

Vorteile	Zu beachten
• Klare Anweisung für jeden Beschäftigten	• Verständliche Formulierungen

3. Umsetzungsstrategie:

Es sollten die Compliance-relevanten Sachverhalte definiert werden, für die es einzelne Regelungen geben muss, dabei ist eine Risikobetrachtung durchzuführen (z.B. Anti-Korruptionsrichtlinie und Kartellrechtsrichtlinie)

Für Kartellrecht siehe DICO-Leitlinie L06 „Kartellrechtliche Compliance – Teil 1: Eckpunkte für effektive Compliance-Programme“ und das Arbeitspapier A05 „Beispielhaftes kartellrechtliches Regelwerk (‘‘Dos and Don’ts’’)“.

c. Verhaltenskodex (Code of Conduct)

1. Beschreibung:

Der Verhaltenskodex ist eine Selbstverpflichtung des Unternehmens, in dem die Grundsätze des eigenen Handelns zusammengefasst sind. Dabei wird bei der Festlegung bewusst über die bloße Einhaltung von Gesetzen und Vorschriften hinausgegangen. (siehe auch Ziffer 1.2)

Beim Verhalten im Geschäftsalltag sind die Grundsätze – zum einen als Anspruch an die Beschäftigten selbst, zum anderen als Versprechen nach außen – einzuhalten. Im Kern sind es ganz einfache Dinge: Es werden keine Interessen vermischt, das Unternehmen handelt transparent, das Unternehmensvermögen wird geschützt und die Beschäftigten gehen fair und respektvoll miteinander und mit Externen um.

2. Vorteile und zu beachtende Rahmenbedingungen:

Vorteile	Zu beachten
• Klares Bekenntnis zu Compliance-Werten • Festgeschriebene Regeln für alle Beschäftigten • Die Werte werden dann auch gelebt • Transparenz für die Öffentlichkeit, insbesondere für Geschäftspartner und Kunden • Gibt Sicherheit (Leitplanken)	• Sollte nicht zu bürokratisch wirken • Als Selbstverpflichtung kann ein Nicht-Einhalten nicht rechtlich geahndet werden

3. Umsetzungsstrategie:

- Eine transparente Kommunikation ist die Grundlage für Verständnis und Akzeptanz
- Die Unternehmensführung muss sich klar zu den im Verhaltenskodex festgeschriebenen Werten bekennen.

d. Hinweisgebersystem

1. Beschreibung:

Um Hinweisen auf Korruption und Unregelmäßigkeiten fair und angemessen nachzugehen, richten Unternehmen Hinweisgebersysteme ein. Diese Systeme können es Beschäftigten einerseits und Außenstehenden andererseits ermöglichen, bei Verdachtsfällen auf Verstöße entsprechende Hinweise zentral und ggf. anonym zu melden. Eine Möglichkeit hierfür kann z.B. eine externe Ombudsstelle sein.

Zu Hinweisgebersystemen zählen Telefonhotlines, Ombudsstelle, webbasierte Systeme sowie kombinierte Mechanismen zur sicheren Kommunikation von Missständen und Unregelmäßigkeiten.

Im Hinweisgebersystem ist höchste Vertraulichkeit sicherzustellen. Gleichmaßen sollen die Unternehmen dabei Wert auf Fairness legen – sowohl im Umgang mit Hinweisgebern als auch mit Beschäftigten, die von einem Vorwurf betroffen sind

2. Vorteile und zu beachtende Rahmenbedingungen:

Vorteile	Zu beachten
• Unabhängige Anlaufstelle für Meldungen über Unregelmäßigkeiten • Möglichkeit für Hinweisgeber, die anonym bleiben möchten.	• Ruf des „Anschwärzens“ von Kollegen durch geeignetes System vermeiden • Möglichkeit für Mobbing einschränken • Möglichem schlechten Ruf in Deutschland sollte durch Aufklärung und Kommunikation begegnet werden

3. Umsetzungsstrategie:

Es sollten alle Möglichkeiten für Hinweisgebersysteme geprüft und diese ausgewählt werden, die am meisten Akzeptanz versprechen.

e. Bonus/Malus-Systeme bei der Vergütung

1. Beschreibung:

Eine Bonus/Malus-Regelung bzgl. ausgewählter Compliance-Themen soll mit positiven und negativen Anreizen das gewünschte Verhalten erreichen. Solch ein System wird vorrangig für Führungskräfte in den persönlichen Zielvereinbarungen, teilweise mit monetären Anreizen angewandt und kann dabei unterstützen, dass Führungskräfte ihre Vorbildfunktion in einem Compliance-Managementsystem stärker wahrnehmen.

2. Vorteile und zu beachtende Rahmenbedingungen:

Vorteile	Zu beachten
• Direkter finanzieller Anreiz	• Eine nur auf finanzielle Incentivierung ausgerichtete Compliance sollte vermieden und durch andere Mechanismen ergänzt werden.

3. Umsetzungsstrategie:

Wenn es im Unternehmen bereits ein Bonus/Malus-System gibt, sollte es um die Compliance-Themen ergänzt werden. Wenn nicht, ist zu prüfen, ob ein Bonus/Malus-System tatsächlich einer der ersten Schritte bei der Einführung eines CMS sein sollte.

f. Business Partner Screening

1. Beschreibung:

Rechtsverletzungen, die ein Geschäftspartner begeht, können dem eigenen Unternehmen erheblich schaden. Mit den Mitteln der Geschäftspartner-Compliance können Bonitäts- oder Qualitätsrisiken bei Lieferanten und Kunden überwacht und nachgehalten werden.

Die Ausgestaltung wird immer unterschiedlich und unternehmensspezifisch sein und in Abhängigkeit zum Risikoprofil und der Unternehmensstruktur stehen. Die möglichen Risiken aus dem Kontakt mit dem Geschäftspartner müssen erkannt und angemessene Maßnahmen abgeleitet werden. Zunächst sind die konkreten Pflichten für das Unternehmen und mögliche Risiken einer Pflichtverletzung zu prüfen. Pflichten zum Geschäftspartnerscreening können sich auch aus gesetzlichen Vorgaben ergeben. Schließlich muss festgelegt werden, unter welchen Voraussetzungen Prüfungen mit welchen Inhalten durchgeführt werden. Das kann auch eine Abstufung der Geschäftspartner nach verschiedenen Kriterien (z.B. Branche und Art der Geschäftstätigkeit, durchschnittliche Auftragshöhe, Häufigkeit der Beauftragung usw.) bedeuten.

Für das Geschäftspartnerscreening stehen unterschiedliche Anbieter zur Verfügung, die öffentlich verfügbare Daten nach ausgewählten Kriterien zur Verfügung stellen. So können z.B. gesellschaftsrechtliche Verhältnisse, die Vermögens-, Finanz- und Ertragslage, Presserecherchen, PEP-Listen, Sanktionslisten, etc. offengelegt werden.

2. Vorteile und zu beachtende Rahmenbedingungen:

Vorteile	Zu beachten
• Vermeidung von Reputationsschäden und Haftungsfällen • Förderung des Geschäftserfolges • Identifikation von Bonitäts- und Qualitätsrisiken bei Lieferanten und Kunden • Vermeidung von Rechtsverstößen	• Einführungsaufwand sowohl personell als auch monetär • Kosten für evtl. eingesetzte Datenbanken

3. Umsetzungsstrategie:

In einem Konzept sollte festgelegt werden, unter welchen Umständen welche Geschäftspartner in welchem Umfang einer Prüfung unterzogen werden.

Es sollte auch entschieden werden, ob und in welchem Umfang Datenbanken zur Prüfung eingesetzt werden oder ob solche Lösungen ausgelagert werden. In diesem Zusammenhang sind auch die Datenbank(en) oder Outsourcingpartner auszuwählen, die für das Unternehmen am geeignetsten sind.

Es können die DICO-Leitlinien genutzt werden:

- L01 „Geschäftspartner-Compliance“
- L08 „Sanktionslisten-Screening in der Unternehmenspraxis“

4.2 Implementierung eines CMS

a. „Mission Statement“ der Unternehmensführung (Compliance-Bekenntnis)

1. Beschreibung:

Das Mission Statement ist ein formales Bekenntnis der Unternehmensführung zur Einhaltung aller Gesetze, Verordnungen und ethischen Grundsätzen sowie von unternehmensinternen Regelungen.

Ein Bekenntnis der Unternehmensführung zur Rechtstreue prägt wesentlich die Compliance-Kultur. Daher sollte der Wortlaut zur nachhaltigen Akzeptanz des Mission Statements glaubwürdig und realistisch gewählt werden.

Ein Mission Statement dient der internen und externen Kommunikation. Da es den sogenannten „Tone at the top“ respektive „Tone from the Top“ signalisiert, ist ein unmissverständliches Bekenntnis der Unternehmensführung zu Compliance unabkömmlich. (siehe auch Ziffer 1.1)

Mit der Betonung, dass Compliance ein ernsthaftes Anliegen der Unternehmensführung ist, sind alle Beteiligten – Mitarbeiter, Lieferanten, Dienstleister und Kunden – aufgefordert, sich aufrichtig mit Compliance und den Konsequenzen bei Verstößen auseinanderzusetzen.

2. Vorteile und zu beachtende Rahmenbedingungen:

Vorteile	Zu beachten
• Basis einer erfolgreichen Compliance-Kultur • Bekenntnis der Unternehmensleitung zu Compliance • Identifikation der Beschäftigten • Positives Signal in der Verbesserung der Außenwirkung	• Wirkungslos, solange die Unternehmensleitung dem Mission Statement nicht folgt und geschlossen dahinter steht • Gefahr der Unglaubwürdigkeit bei Überziehung

3. Umsetzungsstrategie:

- Formulierung des Mission Statements (glaubwürdig, realistisch, verständlich)
- Kommunikation des Mission Statements an alle Unternehmensbeteiligte; Kommunikationsformen: Intranet, Broschüren, Plakate, etc.
- Mission Statement bei sämtlichen Compliance-Programmen, wie z.B. Schulungsmaßnahmen, voranstellen

b. Betriebsvereinbarung Aufnahme in den Arbeitsvertrag/Direktionsrecht

1. Beschreibung:

Betriebsvereinbarungen ermöglichen eine vereinfachte Implementierung von Compliance-Richtlinien und -Vorgaben, da diesen dann nicht individualvertraglich zugestimmt werden muss. Dennoch bietet es sich an, in sensiblen Geschäftsbereichen wie etwa dem Einkauf oder Vertrieb Compliance-Klauseln auch arbeitsvertraglich aufzunehmen. Auch regelmäßige (jährliche) Erklärungen dieser Mitarbeiter sowie von Leitungspersonen, dass die entsprechenden Verhaltensvorgaben eingehalten wurden, sind zu empfehlen.

Der Compliance-Beauftragte nimmt Aufgaben wahr, die originär die Unternehmensführung treffen. Um seine Aufgaben erfüllen zu können, muss er mit entsprechenden Ressourcen ausgestattet sein. Gleichzeitig sind aber auch Weisungs- und Direktionsrechte möglicher Gegenstand der Delegation. Dadurch steigen einerseits die Befugnisse, gleichzeitig aber auch die Verantwortung. Letztendlich schuldet der Compliance-Beauftragte die Pflichten, die er tatsächlich übernommen hat. Daher bietet sich die Dokumentation der übernommenen Pflichten ebenfalls im Rahmen des Arbeitsvertrages an. Dem Compliance-Beauftragten sollte daran gelegen sein, die Aufgaben präzise zu beschreiben und zugleich auch zu begrenzen.

2. Vorteile und zu beachtende Rahmenbedingungen:

Vorteile	Zu beachten
• Direktionsrechte senken die Verantwortlichkeit der Geschäftsleitung • Betriebsvereinbarungen vereinfachen die Implementierung einer adäquaten Richtlinienlandschaft (einmalig und nicht fortlaufend) • Arbeitsvertragliche Regelungen und jährliche Abfragen erhöhen die Sensibilität • Arbeitsvertragliche Regelungen über die Rechte und Pflichten des Compliance-Beauftragten ersetzen unklare und nicht dokumentierte verbale Übereinkommen.	• Direktionsrechte erhöhen die Verantwortung des Compliance-Beauftragten • Aufwand durch regelmäßige Compliance-Erklärungen • Betriebsvereinbarung wird weniger stark wahrgenommen als Individualvereinbarung

3. Umsetzungsstrategie:

- Erstellung von zustimmungspflichtigen Richtlinien in Abstimmung mit Betriebsrat; Betriebsvereinbarung eingehen
- Identifikation von Mitarbeitern, für die Compliance-Klauseln und Compliance-Erklärungen relevant sind; Erstellung und Implementierung entsprechender Klauseln und Erklärungen
- Bestimmung der Rechte (ggf. auch Direktionsrechte) und Pflichten des Compliance-Beauftragten. Aufnahme der Vereinbarung in den Arbeitsvertrag

c. Trainings und Schulung aller Mitarbeiter

1. Beschreibung:

Trainings und Schulungen dienen dazu, das Compliance-Bewusstsein für unternehmensspezifische Risiken bei allen Mitarbeitern zu schärfen. Daneben soll das Unverständnis für Regelungen abgebaut werden, indem unvermeidbare Regulierungen in den Unternehmensalltag übersetzt werden, so dass die betroffenen Mitarbeiter den Hintergrund und die Auswirkungen nachvollziehen können.

Die Schulung der Mitarbeiter sollte bedarfsgerecht erfolgen. Dazu sind möglichst homogene und überschaubare Gruppen mit jeweils unterschiedlichem Schulungsbedarf zu bilden. Dies können z.B. Schulungen in Exportkontrolle und Kartellrecht für die Verkaufsabteilungen sein, Anti-Korruptionsschulungen für Außendienstler, Mitarbeiter, die für technische Abnahmen verantwortlich sind und Einkäufer in ausgewählten Bereichen sowie allgemeine Schulungen zur Betrugsprävention für ausgewählte Mitarbeiter im Rechnungswesen. Es empfiehlt sich, mit der Schulung der Unternehmensführung gefolgt von den Mitarbeitern, die den größten Compliance-Risiken ausgesetzt sind, zu beginnen.

Aufgrund der verschiedenen Schulungsbedarfe können unterschiedliche Schulungsschwerpunkte gesetzt werden. Am Beispiel Kartellrecht verdeutlicht gilt hier, dass das Ziel der Kartellrechtsschulung nicht sein sollte, alle Feinheiten des Kartellrechts zu unterrichten, sondern vielmehr ein Problembewusstsein bei den Mitarbeitern zu schaffen, damit diese kartellrechtliche Risiken erkennen und im Bedarfsfall auch Rat einfordern können.

Zu Beginn der Schulungen sollte eine persönliche Betroffenheit der Mitarbeiter hergestellt werden, indem die Konsequenzen bei nicht integrem Verhalten sowohl für das Unternehmen als auch für den einzelnen Mitarbeiter verdeutlicht werden.

Grundsätzlich können zwei Arten von Schulungen unterschieden werden: Präsenzs Schulungen und E-Learning Programme.

Der Vorteil von Präsenzs Schulungen liegt in dem direkten Dialog zwischen Trainer und Teilnehmern. Bei dieser Schulungsmethode hilft eine offene Atmosphäre in einer nicht zu großen Schulungsgruppe, um diese zu Gesprächen und Fragen zu ermutigen. Teilnehmer können Einzelfragen stellen, auf deren Bedürfnisse der Trainer direkt eingehen kann. Der Trainer hingegen erhält aufgrund vieler Hinweise über gängige Geschäftspraktiken oder Vorfälle aus der Vergangenheit einen guten Überblick über bestehende Compliance-Risiken.

Präsenzs Schulung sollten durch Compliance-Beauftragte, Mitarbeiter der Rechts- bzw. Fachabteilung oder externe Anbieter durchgeführt werden. Als Ansprechpartner sollte jedoch immer der Compliance-Beauftragte zur Verfügung stehen. Auch sollte der Compliance-Beauftragte, sofern andere die Schulungsunterlagen erstellen, diese vor Verwendung in jedem Fall durchsehen, ggf. ändern und freigeben.

E-Learning Programme bieten den Vorteil, dass leicht eine breite Fläche an Mitarbeitern erreicht werden kann. Die Vielzahl an Mitarbeitern unterschiedlicher Fachbereiche führt jedoch häufig dazu, dass diese Schulungsmethode vorwiegend dazu dient, einen groben Überblick über Compliance-bezogene Risiken zu verschaffen anstatt auf (fach-)spezifische Fragestellungen einzugehen. Werden E-Learning Programme dennoch fachspezifisch eingesetzt, empfehlen sie sich insbesondere für Auffrischungsschulungen, bei denen der persönliche Kontakt bereits in den ersten Schulungen hergestellt werden konnte.

Die Gestaltung der Schulung kann in Abhängigkeit der Unternehmen und Schulungsinhalte stark variieren. So kann der Einstieg in die Schulung beispielsweise durch ein Quiz oder Compliance-Spiel erfolgen, in dem der Kenntnisstand der Teilnehmer abgefragt wird. Alternativ können Fallstudien oder (kurze) Videosequenzen zur Auflockerung eingebaut werden. Wichtig ist, die für den Teilnehmerkreis vertraute Sprache zu treffen, ausreichend Beispiele aus den jeweiligen Bereichen zu nennen und genügend Raum für Fragen zu lassen.

Die Wiederholung der Schulung in regelmäßigen Abständen ist essentiell. Ein Schulungsturnus von zwei bis drei Jahren ist empfehlenswert. Bei Bereichswechseln, Neueintritten und rechtlichen Änderungen sind bedarfsorientiert adhoc-Schulungen für die Zielgruppe durchzuführen. Mitarbeiter, die in risikobehafteten Tätigkeitsfeldern arbeiten bzw. als Vorbild fungieren, sollten regelmäßig Präsenzs Schulungen erhalten.

2. Vorteile und zu beachtende Rahmenbedingungen:

Vorteile	Zu beachten
• Fragen der Mitarbeiter können beantwortet werden • Stärkung der Compliance-Wahrnehmung • Schaffung eines einheitlichen Compliance-Verständnisses. Abbau von Unklarheiten in Bezug auf Regulierungen und Compliance-Risiken	• Schulungen sollten dem Unternehmenstyp gerecht werden, z.B. bei einem hohen Anteil gewerblich Beschäftigter eine zielgruppenspezifische Sprache verwenden • Zeit und Kosten sollten gemessen am Schulungsziel festgelegt werden

3. Umsetzungsstrategie:

- Teilnehmer-/Schulungsgruppen bilden
- Form der Trainings und Schulungen festlegen
- Bei Präsenzs Schulungen: Bestimmung des Trainers
- Bei E-Learning Programmen: Auswahl des Programms
- Gestaltung der Schulungsinhalte: Quiz, Fallstudien, etc.
- Teilnahmebestätigung durch Mitarbeiter unterzeichnen lassen oder online registrieren
- Turnus der Schulungen festlegen und regelmäßige Wiederholung
- siehe DICO-Leitlinie 05 „Zielgruppenorientiertes Schulungskonzept“

d. Training der Compliance-Verantwortlichen

1. Beschreibung:

Es gilt nicht nur die Mitarbeiter zu Compliance-relevanten Fragestellungen zu schulen. Gleichzeitig müssen sich auch die Compliance-Verantwortlichen stetig weiterbilden und aktuelle Entwicklungen im Auge behalten (dynamische Themen). Hierzu eignet sich neben aktueller Literatur insbesondere ein Engagement in Verbänden wie DICO. Diese fördern den Austausch über Erfahrungen zwischen Experten. Gleichzeitig wird Informationsmaterial angeboten, wozu Leitlinien, Arbeitspapiere und weitere Arbeitsergebnisse gehören. Außerdem werden unterschiedliche Themenfelder in spezifischen Arbeitskreisen beleuchtet.

Eine Weiterbildung ist auch im Rahmen von Veranstaltungen möglich. Insbesondere Kanzleien führen (in der Regel kostenfreie) Workshops zu aktuellen Themen durch.

Es besteht auch die Möglichkeit einer Zertifizierung des Compliance-Managementsystems (z.B. durch Zertifizierungs- oder WP-Gesellschaften).

Wichtig ist indes ebenfalls die Weiterbildung über unternehmensspezifische Sachverhalte. Der Compliance-Verantwortliche muss das Unternehmen, die Organisation, die Geschäftsprozesse und Risiken kennen. Hierfür bietet sich der Austausch mit Kollegen an, bei denen auch Compliance-relevante Fragestellungen adressiert werden können.

2. Vorteile und zu beachtende Rahmenbedingungen:

Vorteile	Zu beachten
• Compliance-Verantwortlicher erkennt aktuelle Entwicklungen rechtzeitig und kann diese antizipieren • Ermöglicht das Adressieren von Problemstellungen • Netzwerken und Erfahrungsaustausch mit anderen Experten, die den gleichen Herausforderungen gegenüberstehen oder -standen • Gemeinsame Lösungsentwicklung mit Kollegen/Best Practice • Information über das Unternehmen und dessen Schwachstellen	• Zeitaufwand und Reisekosten für den Erfahrungsaustausch planen • Kosten für eine Zertifizierung (einschließlich des eigenen Zeitanteils der Mitarbeiter für die Vorbereitung und im Rahmen der Durchführung), falls diese vom Unternehmen gewünscht ist • Enge Einbindung in das Tagesgeschäft erlaubt nur ein eingeschränktes Engagement

3. Umsetzungsstrategie:

- Gespräche mit Führungskräften
- Ständiger Informationsaustausch mit Kollegen („Open Door“)
- Identifikation der Risiken durch Risikoanalyse/Anknüpfungspunkt für Diskussionen
- aktuelle Literatur/Zeitschriften
- Engagement in Verbänden (DICO)
- Teilnahme an entsprechenden Veranstaltungen.

e. Compliance-Modul für neue Mitarbeiter

1. Beschreibung:

Beim Compliance-Modul handelt es sich um Maßnahmen die ergriffen werden, um neue Mitarbeiter an das Thema heranzuführen. Hierzu kann ihnen zunächst ein Handbuch zur Verfügung gestellt werden, dem alle relevanten Richtlinien und Verhaltensweisen zu entnehmen sind. Wichtig erscheint, dass diese Vorgaben nicht nur übergeben, sondern gleichfalls erläutert werden. Hierzu bieten sich sowohl Einzelgespräche, Workshops oder Schulungen an, die durch die Compliance-Beauftragten geleitet werden und sich insbesondere an praktisch relevanten Fallbeispielen orientieren. Dadurch werden Organisation, Verantwortlichkeiten und Ansprechpartner vorgestellt.

2. Vorteile und zu beachtende Rahmenbedingungen:

Vorteile	Zu beachten
• Stellenwert von Compliance wird unmittelbar verdeutlicht • Wertevermittlung • Diskussionsmöglichkeiten; Austausch über bisherige Erfahrungen • Hohe Sensibilisierungsmöglichkeit • Diskussionsmöglichkeiten • Direkter Austausch mit Compliance-Verantwortlichen	• Organisations- und Zeitaufwand für Vorbereitung des Handbuchs und die Gespräche

3. Umsetzungsstrategie:

- Handbuch/Material zusammenstellen
- Adressaten identifizieren
- Zeitrahmen/Dauer festlegen (Stunden/ganztägig)
- Termin finden/koordinieren
- Veranstaltungsort festlegen
- Präsentationsunterlagen erstellen

4.3 Pflege / Kontinuierliche Weiterentwicklung / Verbesserung

a. Analyse tatsächlicher Compliance-Vorfälle im Unternehmen

1. Beschreibung:

Hinweise auf doloses Verhalten können auf unterschiedliche Weise bei Unternehmen und insbesondere bei Compliance-Verantwortlichen eingehen. Dies muss nicht zwangsläufig durch eigene Mitarbeiter erfolgen. Auch unternehmensexterne Dritte können Informationen über Compliance-relevante Sachverhalte haben. Umso wichtiger ist es, dass auch ihnen die Möglichkeit zur Meldung offensteht.

Sobald Hinweise im Unternehmen eingehen, muss hierauf reagiert werden. Alternativ können und sollten Unternehmen auch proaktiv nach Hinweisen suchen. Dazu bieten sich Gespräche und systematische Datenanalysen an. Sollten sich aus den vorgenannten Maßnahmen Verdachtsfälle ergeben, muss diesen im Detail nachgegangen werden.

Sofern sich der Verdacht erhärtet, also tatsächlich ein Compliance-Fall vorliegt, müssen entsprechende Maßnahmen ergriffen werden. Um sicherzustellen, ob ein Verdacht tatsächlich zutrifft, müssen ausgewählte Prüfungshandlungen vorgenommen werden, z.B. Gespräche mit ausgewählten Mitarbeitern, analytische Auswertung von Buchhaltungsdaten, ggf. Hintergrundrecherchen in öffentlich verfügbaren Quellen, risikoorientierte Durchsicht von Daten auf den Computern ausgewählter Personen (z.B. E-Mails) mit Spezialsoftware sofern (datenschutz)rechtlich erlaubt sowie die detaillierte Durchsicht ausgewählter Unterlagen und Daten. Die Prüfungshandlungen führen dann in der Regel zu einer klaren Sachverhaltslage oder zumindest einem deutlich klareren Bild. Die Beteiligungsrechte des Betriebsrates bei der Prüfung sind ebenfalls zu wahren. Bei konfrontativen Interviews mit Beschuldigten sollte vorher fachkundiger Rat eingeholt werden.

Weiter ist sorgfältig abzuwägen, wie mit dem Mitarbeiter umgegangen werden soll. Räumt der Mitarbeiter das Fehlverhalten ein oder bestehen daran keine Zweifel, müssen darauf auch angemessene Reaktionen erfolgen. Dies umfasst zunächst die Verbesserung der Prozesse, damit ähnliches Fehlverhalten mit hinreichender Wahrscheinlichkeit ausgeschlossen werden kann. Weiter bedarf es auch einer deliktadäquaten Sanktion des Mitarbeiters, die auch sichtbar sein sollte, um abschreckende Wirkung entfalten zu können.

Im Ergebnis trägt all dies auch zur Verbesserung des CMS bei.

2. Vorteile und zu beachtende Rahmenbedingungen:

Vorteile	Zu beachten
• Zuwiderhandlungen werden rechtzeitig erkannt. Behördlichen Durchsuchungen kann dadurch zuvorgekommen oder diese vermieden werden. • Das Unternehmen behält die Kontrolle über die Verfahrensweise. • Künftigem Fehlverhalten wird entgegengewirkt. • Abschreckende Wirkung durch Sanktion der Mitarbeiter.	• Die proaktive Suche nach Compliance-Fällen bedarf zusätzlicher Ressourcen und ggf. auch externer Unterstützung. • Die datenschutzrechtliche Zulässigkeit computerforensischer Maßnahmen sollte vom Datenschutzbeauftragten geprüft werden • Bei Verhören ist Vorsicht geboten. Dies macht Rechtsbeistand erforderlich. • Art und Umfang der Prüfung sollten sorgfältig geplant werden.

3. Umsetzungsstrategie:

- Eingehenden Hinweisen muss nachgegangen werden, falls diese glaubwürdig sind. Zusätzlich sollte auch nach Hinweisen proaktiv gesucht werden.
- Erhärtet sich der Verdachtsfall sind ausgewählte Prüfungshandlungen erforderlich, die auch Interviews, Hintergrundrecherchen und computerforensische Maßnahmen enthalten können. Hierzu sollte Rechtsbeistand eingeholt werden.
- Bestehen an der Zuwiderhandlung keine Zweifel sind Maßnahmen zu implementieren, um derartige Sachverhalte künftig zu vermeiden. Außerdem muss der Mitarbeiter deliktadäquat sanktioniert werden.

b. Austausch mit anderen Compliance-Verantwortlichen

1. Beschreibung:

Compliance ist ein äußerst dynamisches Thema. Umso wichtiger ist es, immer über die aktuellen Entwicklungen und Trends informiert zu bleiben, um auf dieser Grundlage gegebenenfalls auch neue Risikofelder zu identifizieren.

Hierzu bieten sich neben Weiterbildungsmaßnahmen insbesondere Gespräche mit anderen Compliance-Verantwortlichen an. Das DICO bietet hierzu eine entsprechende Plattform.

Besonders hilfreich kann der Austausch mit Compliance-Verantwortlichen der gleichen Branche sein. Diese sind regelmäßig den gleichen Risiken ausgesetzt. Der Austausch mit diesen ist allerdings möglicherweise mit kartellrechtlichen Risiken verbunden. Daher sollte bei solchen Gesprächen auch ein Monitor zugegen sein, der die Kartellrechtskonformität des Informationsaustausches gewährleistet. Solche branchenweiten Compliance-Gespräche können in erheblichem Maße zu einem „Level Playing Field“ beitragen und damit erheblichen Mehrwert schaffen. Im Ergebnis können sie in einem Integritätspakt münden.

2. Vorteile und zu beachtende Rahmenbedingungen:

Vorteile	Zu beachten
• Der Austausch mit Kollegen schafft Ansprechpartner mit ggf. ähnlichen Herausforderungen. • Erfahrungen können ausgetauscht werden. • Sofern Compliance-Verantwortliche der gleichen Branche kooperieren, kann ein Branchenstandard gesetzt werden.	• Ggf. sind kartellrechtliche Risiken zu berücksichtigen. • Zeit für Engagement erforderlich.

3. Umsetzungsstrategie:

- Proaktiver Austausch mit Kollegen
- Mitgliedschaft beim DICO
- Teilnahme an relevanten Veranstaltungen

c. Mitarbeiterbefragungen**1. Beschreibung:**

Mitarbeiter sind eine wichtige Erkenntnisquelle für die Verbesserung eines CMS. Ihnen kann Fehlverhalten nicht nur bekannt sein, häufig kennen sie auch Schwachstellen bei den internen Kontrollen, die der Prävention dienen. Diese Schwachstellen können dann identifiziert und behoben werden. Hierfür ist allerdings eine Partnerschaft zwischen der Compliance-Abteilung und den jeweiligen Fachbereichen erforderlich. Das dafür erforderliche Vertrauen kann nicht erzwungen werden.

Mitarbeiter können auch zu ihrer Zufriedenheit mit der Compliance-Arbeit im Unternehmen befragt werden (Evaluation). Dies ermöglicht die Identifikation von Handlungsfeldern. Die Effektivität der Compliance-Arbeit wird dadurch erhöht. Diese Maßnahme steigert zudem die Akzeptanz durch die Mitarbeiter.

2. Vorteile und zu beachtende Rahmenbedingungen:

Vorteile	Zu beachten
• Identifikation von Compliance-Fällen • Identifikation von Schwachstellen • Identifikation von Handlungsfeldern durch Evaluation • Evaluation erfordert eine kritische Selbstreflektion der Compliance-Abteilung • Evaluation kann die Effektivität der Compliance-Arbeit erhöhen	• Über Schwachstellen und Fehlverhalten wird nur berichtet, wenn ausreichendes Vertrauen zwischen den Fachbereichen und der Compliance-Abteilung besteht. Dieses muss langwierig aufgebaut werden.

3. Umsetzungsstrategie:

- Compliance-Abteilung etablieren, Vertrauen aufbauen „Walk the Talk“
- Mitarbeiter befragen, um Risiken, Fehlverhalten und Kontrolldefizite zu identifizieren
- Compliance-Arbeit evaluieren lassen
- Maßnahmen ableiten

d. Stichprobenartige Prüfungen der Wirksamkeit von Kontrollen

1. Beschreibung:

Stichprobenartige Prüfungen der Wirksamkeit von Kontrollen können für die Weiterentwicklung und Verbesserung des CMS genutzt werden. Wenn diese Prüfungen Defizite bei bestehenden Prozessen und Kontrollen ergeben, weil diese nicht eingehalten werden, kann das als Erkenntnisquelle für Optimierungen genutzt werden. Schwachstellen werden identifiziert und behoben. Sie leisten einen Beitrag zur Prävention.

Außerdem erhöhen stichprobenartige Prüfungen die Entdeckungswahrscheinlichkeit. Damit wird eine abschreckende Wirkung erzielt, weil Mitarbeiter jederzeit mit der Erkennung von Fehlverhalten rechnen müssen.

2. Vorteile und zu beachtende Rahmenbedingungen:

Vorteile	Zu beachten
• Prozess- und Kontrollschwächen werden identifiziert und behoben. • Prüfungen der Wirksamkeit von Kontrollen erhöhen Entdeckungswahrscheinlichkeit und entfalten präventiven Charakter.	• Kontrolltests können den Eindruck einer „Unternehmenspolizei“ erwecken. • Vertrauen droht verloren zu gehen, wenn die Kontrolltests falsch angegangen werden. • Es sollten die richtigen Schlüsselkontrollen ausgewählt werden.

3. Umsetzungsstrategie:

- Risikobereiche identifizieren
- Kontrollziele festlegen und Kontrollmaßnahmen ableiten
- Prüfungsergebnisse nutzen, um Schwachstellen zu identifizieren und optimieren

e. Dokumentation

1. Beschreibung:

Auch wenn Dokumentation häufig als bürokratisches Ärgernis angesehen wird – für die Compliance-Arbeit ist sie von großer Bedeutung. Unternehmen müssen in der Lage sein, selbst Sachverhalte die mehrere Jahre zurück liegen zu rechtfertigen. Dies gelingt nur mit entsprechenden Dokumentationsanforderungen.

Prozesse und Kontrollen zur Prävention von beispielsweise indirekter Korruption (Bestechung durch Berater, Vertreter oder andere Drittparteien) müssen dokumentiert sein, damit sie haftungsbefreiende oder -mindernde Wirkung entfalten können. Wird ein Geschäftspartner geprüft, diese Prüfung allerdings nicht dokumentiert, dann nützt dies wenig. Dokumentation ist daher auch für die Exkulpation der Mitarbeiter und Organe erforderlich.

Dementsprechend sind auch die Maßnahmen zur Pflege, kontinuierlichen Weiterentwicklung und Verbesserung des CMS zu dokumentieren.

Bei aller Relevanz ist dennoch darauf zu achten, dass die Dokumentation zwar das Erforderliche erfasst. Eine Aufbürdung unnötiger Dokumentationspflichten hingegen ist unbedingt zu vermeiden.

2. Vorteile und zu beachtende Rahmenbedingungen:

Vorteile	Zu beachten
• Transparenz • Nachweisbarkeit • Exkulpation	• Aufwand • wird ggf. als lästig wahrgenommen

3. Umsetzungsstrategie:

- Prozessschritte identifizieren, deren Dokumentation erforderlich ist
- Dokumentationspflichten auferlegen
- Einhaltung der Dokumentationspflichten durch stichprobenartige Kontrollen (risikobasierter Ansatz) überprüfen
- Erforderlichkeit der Dokumentation an beteiligte Mitarbeiter begründen »

5. Compliance-Organisation

5.1 Strukturell

a. Kombination und Abgrenzung mit anderen Governance-Funktionen (allgemein)

1. Beschreibung:

Ausgangspunkt der organisatorischen Überlegungen ist die grundsätzliche Möglichkeit der Zusammenfassung von Compliance mit anderen Governance-Funktionen. Als solche werden hier nicht nur die in der Finanzindustrie notwendigen Schlüsselfunktionen wie Interne Revision, Compliance, Risikomanagement (bei Versicherungen auch die mathematische Funktion) betrachtet, sondern auch weitere teils von den Unternehmen definierte Funktionen wie z.B. Recht.

Grundsätzlich gilt für die Governance-Funktionen das „Three-Lines-of-Defence“-Konzept. Danach ist die erste Verteidigungslinie in den Fachbereichen angesiedelt, in der zweiten Linie sind Risikomanagement und Compliance sowie das interne Kontrollsystem vorhanden. Die dritte Verteidigungslinie umfasst die interne Revision mit der Aufgabe, sowohl die Fachbereiche als auch die Funktionsfähigkeit der zweiten Verteidigungslinie zu überprüfen. Alle Governance-Funktionen sind verpflichtet, zu prüfen, ob die anderen Funktionen grundsätzlich von Kapazität, Fähigkeiten und Stellung im Unternehmen in der Lage sind, ihre Aufgaben sachgerecht wahrzunehmen. Die Interne Revision hat zudem die anderen Governance-Funktionen wie alle anderen Funktionen im Unternehmen regelmäßig zu prüfen.

Um Interessenskonflikte zu vermeiden, bietet es sich an, die Funktionen unabhängig zu gestalten und angemessen zu trennen.

Je größer ein Unternehmen ist, desto eher sollte eine Kombination der Funktionen vermieden werden, um die Unabhängigkeit sicherzustellen.

Je kleiner die Unternehmen sind, desto eher können die Funktionen – insbesondere im Mittelstand – gekoppelt werden, bis zur personenidentischen Wahrnehmung durch eine natürliche Person. Bei kleineren Unternehmen dominieren daher tendenziell nachgelagerte Kontrollen. Insoweit gilt das Proportionalitäts-(Angemessenheits-) Prinzip. In solchen Fällen, muss sich die Unternehmensführung der besonderen Risiken bewusst sein und eine solche Lösung erst unter sorgfältiger Abwägung der Risiken treffen. In Betracht kommt beispielsweise stattdessen auch ein externes Outsourcing aller oder einzelner Governance-Funktionen. Die Letztverantwortung hat jedoch immer die Unternehmensführung des auslagernden Unternehmens; die hierzu notwendigen qualitativen und quantitativen Ressourcen müssen vorgehalten werden.

2. Vorteile und zu beachtende Rahmenbedingungen:

Vorteile	Zu beachten
• Eine enge Verzahnung von Compliance mit anderen Governance-Funktionen kann die Effizienz erheblich erhöhen und Redundanzen vermeiden.	• Aufwand für ein optimiertes Konzept. Mögliche Befindlichkeiten der Stelleninhaber.

3. Umsetzungsstrategie:

- Prozessschritte identifizieren, deren Dokumentation erforderlich ist
- Dokumentationspflichten auferlegen
- Einhaltung der Dokumentationspflichten durch stichprobenartige Kontrollen (risikobasierter Ansatz) überprüfen
- Erforderlichkeit der Dokumentation an beteiligte Mitarbeiter begründen

b. Compliance-Management – Risikomanagement**1. Beschreibung:**

Compliance und Risikomanagement sind unabhängige Funktionen.

Compliance bewertet die Compliance-Risiken, zu denen je nach Unternehmen auch allgemeine Reputationsrisiken gerechnet werden können, unter eher qualitativen Aspekten wie Strafen / Bußgelder z.B. bei Geldwäsche oder Kartellverstößen, Haftung der Verantwortlichen und Nichtigkeit von Verträgen. Risikomanagement als Funktion ist hingegen für das Management sämtlicher Risiken einschließlich deren Quantifizierung zuständig.

Es gibt jedoch einige Gemeinsamkeiten der Risikomanagement- und Compliance-Funktion, z.B. die Aufgaben der Risikoidentifikation, -vermeidung und -kontrolle, wenngleich diese Funktion bei Compliance naturgemäß enger zugeschnitten ist. Solche Gemeinsamkeiten erleichtern eine Zusammenfassung der Funktionen unter einheitlicher Leitung.

Eine Zusammenarbeit zwischen beiden Funktionen, auch wenn sie nicht unter einheitlicher Leitung stehen, ist jedoch erforderlich, um eine einheitliche Sicht auf die Gesamtrisikosituation des Unternehmens zu erhalten und eine methodische Verzahnung der Funktionen sicherzustellen.

2. Vorteile und zu beachtende Rahmenbedingungen:

Vorteile	Zu beachten
Vorteile einer Zusammenlegung/einheitliche Leitung: • Synergieeffekte • einheitliche Sicht auf die Risikosituation (Integrated Governance)	• Keine vollständige Unabhängigkeit • Gefahr der Vermischung der unterschiedlichen Aspekte • Risiko des Vorrangs der quantitativen Risikoaspekt über qualitative Complianceaspekte • Generell: Eine „Warn-„ Funktion weniger

3. Umsetzungsstrategie:

Sorgfältige Analyse der Vor- und Nachteile vor einer Entscheidung. Die Entscheidung muss sorgfältig dokumentiert werden. Generell sollte im Zweifel eine Kombination unterbleiben.

c. Compliance-Management – Interne Revision

1. Beschreibung:

Grundsätzlich haben Compliance und Interne Revision unterschiedliche Zielrichtungen, die Interne Revision hat zudem die Compliance-Funktion auf Angemessenheit und Wirksamkeit zu prüfen. Werden daher Compliance und interne Revision unter einheitlicher Leitung oder auch Personenidentität bei Mitarbeitern zusammengefasst, muss durch organisatorische Maßnahmen die Unabhängigkeit insbesondere der Internen Revision auf der 3. Verteidigungslinie sichergestellt werden (z.B. indem die Revision der Compliance-Funktion ausgelagert wird). Soweit es die Größe des Unternehmens zulässt, sollte diese Kombination vermieden werden.

Zwischen Compliance und interner Revision sind eine enge Zusammenarbeit und insbesondere eine Abstimmung der jährlichen Aktivitäten Pläne notwendig.

2. Vorteile und zu beachtende Rahmenbedingungen:

Vorteile	Zu beachten
Vorteile einer Zusammenlegung: • Synergieeffekte • einheitliche Sichtweise	• Die Nachteile und Risiken sind bei der Internen Revision am größten, weil die Revision die anderen Governance-Funktionen ihrerseits zu prüfen hat, und jede Kombination ein Risiko für ihre Unabhängigkeit darstellt.

3. Umsetzungsstrategie:

Die Kombination ist grundsätzlich zu vermeiden und bedarf ggf. einer besonders sorgfältigen Begründung und der Implementierung von Sicherungsmaßnahmen.

d. Compliance-Management – Rechtsabteilung

1. Beschreibung:

Recht wird üblicherweise nicht zu den Governance-Funktionen gerechnet, doch bestehen Überschneidungen mit der Compliance-Funktion, da beide für das rechtliche Agieren des Unternehmens verantwortlich sind.

Compliance ist dabei eher präventiv, systematisch beratend, aber auch kontrollierend tätig; Compliance muss interessenkonfliktfreie Strukturen und die Rahmenbedingungen zum Ausschluss von Rechtsverstößen schaffen. Recht arbeitet eher operativ und fallbezogen. Recht nimmt eher die Vertretung nach Außen wahr, Compliance hingegen die interne Überwachung.

Auf Grund der Sachnähe ist daher eine Koppelung und enge Zusammenarbeit der Funktionen möglich und evtl. auch zweckmäßig. Compliance kann bspw. für die Beurteilung komplexer Rechtsfragen auf Recht zurückgreifen.

Sichergestellt werden sollte auch hier die organisatorische und fachliche Unabhängigkeit, daher muss Compliance z.B. einen von der Rechtsabteilung erteilten Rechtsrat zumindest auf juristische Plausibilität überprüfen, ferner müssen Interessenkonflikte vermieden werden: Recht hat eher das Management im täglichen Geschäft zu unterstützen (und wird insoweit teilweise auch der 1. Verteidigungslinie zugerechnet), während Compliance für das rechtmäßige Verhalten generell verantwortlich ist. Die hieraus im Einzelfall entstehenden Interessenkonflikte müssen vermieden werden.

2. Vorteile und zu beachtende Rahmenbedingungen:

Vorteile	Zu beachten
• Synergieeffekte, einheitliche Sichtweise auf die Themen	• Ist Compliance Recht untergeordnet oder vollständig integriert, besteht das Risiko, dass sich die im Regelfall businessnähere Rechtsfunktion durchsetzt und die Compliance-Aspekte nicht ausreichend berücksichtigt werden.

3. Umsetzungsstrategie:

- Vermeidung von Interessenkonflikten durch Aufgabenverteilung
- Pflicht, bei unterschiedlichen Einschätzungen von Recht und Compliance die nächste Verantwortungsebene zu involvieren
- Unmittelbares Recht der Compliance-Funktion, eine Vorstandsentscheidung herbeizuführen

e. Compliance-Management – Internes Kontrollsystem (IKS)

1. Beschreibung:

Die genannten Grundsätze gelten auch für die Kombination mit weiteren unternehmensindividuellen Governance – und Kontrollfunktionen bzw. Systemen, wie Controlling, IKS, Datenschutz, Geldwäsche, soweit diese nicht bereits Bestandteile von Compliance oder Risikomanagement sind.

Das IKS stellt die Summe aller Methoden, Strukturen und Maßnahmen innerhalb eines Unternehmens dar, die das Vermögen und die Wirtschaftlichkeit aller Geschäftsvorfälle sichern sowie die zugehörigen Abläufe ordnungsgemäß erfassen und nachvollziehbar machen. Es beinhaltet zumindest Verwaltungs- und Rechnungslegungsverfahren, einen internen Kontrollrahmen, angemessene Melderegungen auf allen Unternehmensebenen und eine Compliance-Funktion als Funktion zur Überwachung der Einhaltung der an das Unternehmen gestellten Anforderungen. Die einzelnen Elemente sind in den COSO – Standards definiert (<https://www.coso.org/>). Ein wesentliches Prinzip ist hierbei die Funktionstrennung, die sicherstellen soll, dass insbesondere risikoschaffende und risikokontrollierende Funktionen getrennt verantwortet werden.

Bei dem IKS handelt es sich nicht um eine Funktion des Unternehmens, sondern ein System – ähnlich wie das Compliance-Managementsystem (CMS) nicht identisch ist mit der Compliance-Funktion. IKS relevant sind jedoch insbesondere die Governance-Funktionen Interne Revision, Risikomanagement, Datenschutzbeauftragter, Geldwäschebeauftragter. Die Compliance-Funktion hat hierbei die Einhaltung der rechtlichen und unternehmensinternen Regeln sicherzustellen, und beispielsweise das Vorhandensein von Richtlinien, Leitlinien Geschäftsanweisungen sicherzustellen und deren Einhaltung zu prüfen. Diese Richtlinien können jedoch auch durch andere Unternehmensbereiche wie z.B. Risikomanagement und Betriebsorganisation erlassen werden.

Compliance ist daher ein notwendiger Bestandteil des Internen Kontrollsystems, ohne diesem aber als Funktion organisatorisch oder hierarchisch untergeordnet zu sein. Umgekehrt sind Teile des Internen Kontrollsystems auch compliance-relevant, da es sich um Maßnahmen handelt um Verstöße gegen interne Richtlinien und gesetzliche Vorgaben zu verhindern.

2. Vorteile und zu beachtende Rahmenbedingungen:

Vorteile und zu beachtende Rahmenbedingungen der anderen Kombinationen gelten hier sinngemäß.

3. Umsetzungsstrategie:

Das Unternehmen muss sein eigenes, auf die jeweiligen Gegebenheiten abstellendes IKS entwickeln und dabei auch die Rolle der Compliance-Funktion definieren.

f. Compliance-Management als eigenständiger Bereich

1. Beschreibung:

Compliance-Funktionen können einen eigenständigen Bereich darstellen oder in anderen Unternehmensbereichen angesiedelt sein.

Wenn sich Unternehmen gegen einen eigenständigen Compliance-Bereich entscheiden, werden stattdessen Compliance-Funktionen häufig in „Compliance-verwandten“ Abteilungen geschaffen, wie etwa in der Rechtsabteilung, dem Controlling, der Revision oder im Risikomanagement (zur Bewertung einer solchen Vorgehensweise siehe weiter oben).

Auch in Unternehmen mit eigenständiger Compliance-Abteilung werden flankierende Compliance-Verantwortlichkeiten häufig auch in anderen Bereichen geschaffen. Dies gilt insbesondere für operative Einheiten, die häufig mit der Umsetzung der Compliance-Maßnahmen betraut sind.

2. Vorteile und zu beachtende Rahmenbedingungen:

Vorteile	Zu beachten
• Unabhängigkeit von anderen Unternehmensbereichen • Größerer Fokus einzelner Mitarbeiter auf das Thema Compliance	• In kleinen und mittleren Unternehmen kann die Schaffung einer eigenständigen Compliance-Funktion mit hohen Kosten verbunden sein. Daher neigen vor allem kleinere Unternehmen dazu, zu Beginn andere, bestehende Funktionen (z.B. Rechtsabteilung) mit der Wahrnehmung der Compliance-Aufgaben zu betrauen.

3. Umsetzungsstrategie:

Es müssen unternehmensspezifische, praktikable und akzeptierbare Organisationsmodelle festgelegt werden.

g. Compliance intern/extern (In-house/Outsourcing)

1. Beschreibung:

Compliance ist eine originäre Aufgabe der Unternehmensführung. Die Unternehmensführung kann und sollte ihre Compliance-Aufgabe auf untergeordnete Unternehmensebenen delegieren. Das Organ wird hierdurch nicht von seiner Compliance-Verantwortung frei; es ist weiterhin verpflichtet, die Compliance-Verantwortlichen sorgfältig auszuwählen, angemessen anzuweisen und regelmäßig zu überwachen. Die Delegation erfolgt entweder auf Compliance-Verantwortliche in eigenständigen Compliance-Abteilungen und/oder auf Compliance-Beauftragte, die in anderen Abteilungen tätig sind (Rechtsabteilung, Revision, Risikomanagement etc.).

Die Einbindung von externen Compliance-Beratern zur fallweisen Unterstützung der Compliance-Tätigkeit im Unternehmen ist üblich und in bestimmten Konstellationen auch geboten (z.B. bei mangelnder fachlicher Expertise oder fehlender personeller Ressourcen); insbesondere bei internen Ermittlungen oder wichtigen Compliance-relevanten Geschäftsentscheidungen werden häufig Externe eingeschaltet.

Hiervon abzugrenzen ist der Einsatz externer Compliance-Beauftragter. Im Gegensatz zu internen Compliance-Beauftragten sind externe Compliance-Beauftragte keine Mitarbeiter des Unternehmens, sondern externe Berater. Externe Compliance-Beauftragte sind eher selten, aber auch diese Dienstleistung wird von manchen Beratungsfirmen angeboten. In Betracht kommen hierfür allenfalls kleinere Unternehmen, wobei es dabei mangels direkter Integration im Unternehmen zu Informationsdefiziten kommen kann.

2. Vorteile und zu beachtende Rahmenbedingungen:

Vorteile	Zu beachten
• Unabhängigkeit von anderen Unternehmensbereichen • Größerer Fokus einzelner Mitarbeiter auf das Thema Compliance	• In kleinen und mittleren Unternehmen kann die Schaffung einer eigenständigen Compliance-Funktion mit hohen Kosten verbunden sein. Daher neigen vor allem kleinere Unternehmen dazu, zu Beginn andere, bestehende Funktionen (z.B. Rechtsabteilung) mit der Wahrnehmung der Compliance-Aufgaben zu betrauen.

3. Umsetzungsstrategie:

Die Aufgabenverteilung zwischen internen Compliance-Funktionen und externem Compliance-Rat ist je nach Ressourcen, Budget und Unternehmensstruktur individuell zu bestimmen.

h. Compliance-Management – Zentrale Strukturen

1. Beschreibung:

Die Organisationsform der Compliance-Funktion ist nicht vorgegeben, auch nicht in regulierten Industrien, in denen detaillierte Regulierungen herrschen. Die Unternehmen können daher selbst entscheiden, ob sie eine zentrale oder eine dezentrale, eine eigenständige oder eine integrierte Compliance-Organisation wählen oder Mischformen derselben.

Im Sinne einer guten Corporate Governance sollte jedoch die Gesamtverantwortung für die Compliance-Funktion im jeweiligen Unternehmen bei nur einer natürlichen Person liegen (Chief Compliance Officer).

In einer zentralen Struktur ist die Compliance-Abteilung für sämtliche Compliance-Angelegenheiten des Unternehmens zuständig, entsprechend in einer Unternehmensgruppe auch auf der Basis von Dienstleistungsverträgen für die Tochtergesellschaften.

2. Vorteile und zu beachtende Rahmenbedingungen:

Vorteile	Zu beachten
• Zentrale Compliance-Funktionen haben den Vorteil, dass das Know-How gebündelt ist und mehr Kompetenzen vorgehalten werden können. • Bei Zentralisierung besteht oft eine höhere Durchschlagskraft. • Compliance hat einen einheitlichen Blick auf die Risiken sämtlicher Unternehmensteile und hat eine Nähe zur Gesamtleitung des Unternehmens.	• Nachteil (ausschließlich) zentraler Compliance-Funktionen ist die Ferne vom Business, kritische Entwicklungen werden möglicherweise zu spät aufgegriffen. • Ferner besteht das Risiko fehlender Akzeptanz in den Businessbereichen („Elfenbeinturm“). • Daher bietet es sich an, Compliance-Mitarbeiter in den Tochtergesellschaften zu integrieren, die im Sinne einer funktionalen Organisation der zentralen Compliance-Abteilung unterstellt sind.

3. Umsetzungsstrategie:

Kleine Einheiten können sich mit einer zentralen Compliance-Funktion begnügen. In größeren Unternehmen sollten zentrale und dezentrale Elemente miteinander gekoppelt werden.

i. Compliance-Management – Dezentrale Strukturen

1. Beschreibung:

Dezentrale Compliance-Abteilung

In dezentralen Strukturen sind die Verantwortlichkeiten verschiedenen Bereichen zugeordnet, entweder nach Organisationsstrukturen (Unternehmen) oder Themenbereichen. Im Regelfall wird die Funktion dort durch einen eigenen dezentralen Compliance Officer (CO) wahrgenommen. Eine Berichtslinie an einen (zentralen) Chief Compliance Officer (CCO) – soweit existent – ist dringend zu empfehlen.

Neben dezentralen Funktionen mit eigenem Compliance-Officer kann die Compliance-Funktion durch weitere dezentrale Elemente ergänzt werden.

Compliance-Beauftragte

Sie haben die Aufgabe, Ansprechpartner für Compliance Themen als Schnittstelle im eigenen Bereich zu sein und die Compliance-Themen in dem eigenen Bereich bewusst zu machen und zu fördern. Sie sind anders als Compliance Officer nicht Bestandteil der Compliance-Funktion/Abteilung, sollten jedoch eine Berichtsmöglichkeit an den jeweiligen CCO/CO haben.

Compliance-Beiräte

Gute Praxis ist es – zumindest in größeren Unternehmen – Compliance-Beiräte oder Ausschüsse zu bilden. Ihre Aufgabe ist es, im Gesamtunternehmen den Blick für Compliance zu schärfen und auch die übergreifende Compliance-Situation im Unternehmen besser analysieren zu können. Wesentliche Compliance-Themen können dort diskutiert und ggf. auch entschieden werden, die Letztverantwortung muss jedoch beim CCO verbleiben.

Mischformen

Insbesondere in Unternehmensgruppen haben die einzelnen Unternehmen oft eigene Compliance-Abteilungen. Hier sind die Zuständigkeiten und Verantwortlichkeiten der dezentralen Abteilungen im Verhältnis zur zentralen Abteilung genau zu definieren.

2. Vorteile und zu beachtende Rahmenbedingungen:

Vorteile	Zu beachten
• Eine Stärkung dezentraler Elemente führt zu einer größeren Nähe zum Business, d.h. Compliance kennt die Strategien, ist vor Ort, kennt die besonders problematischen Geschäftsvorfälle. • Insbesondere im Vertrieb ist örtliche Nähe der Compliance-Funktion zur effektiveren Überwachung von Vorteil.	• Dezentrale Compliance-Funktionen sind meist personell schwächer ausgestattet. • Sie sind weniger schlagkräftig und durch die Nähe zum Geschäftsbereich besteht das Risiko, dass sie zu stark die Fachbereichsinteressen wahrnehmen.

3. Umsetzungsstrategie:

Kleine Einheiten können sich mit einer zentralen Compliance-Funktion begnügen. In größeren Unternehmen sollten zentrale und dezentrale Elemente miteinander gekoppelt werden.

j. Compliance-Management – Vorstandsressort

1. Beschreibung:

Compliance gehört im Rahmen der Legalitätspflicht zur Aufgabe eines jeden Organmitglieds unabhängig von der jeweiligen Ressortzuständigkeit. Compliance ist Gesamtaufgabe der Unternehmensführung. In der Praxis ist die Delegation von Compliance auf untergeordnete Unternehmensebenen üblich und auch zu empfehlen. Letztlich verbleibt aber auch dann die Gesamtverantwortung bei den Organmitgliedern.

Um die Arbeit der Unternehmensführung effizienter zu machen, hat sich die Zuweisung einzelner Ressorts an einzelne Organmitglieder (zumindest bei größeren Unternehmen) durchgesetzt. Dies bietet sich auch für die Zuständigkeit „Compliance“ an. Die Compliance-Aufgaben sind dann bei einer Person konzentriert. Dennoch sind die anderen Organmitglieder weiterhin verpflichtet, für die nötige Compliance im Unternehmen zu sorgen. Sie werden also nicht gänzlich ihrer Compliance-Verantwortung enthoben. Die klare Aufgabenzuteilung an eine Person führt in der Regel dazu, dass Compliance-Themen fokussiert und effektiver angegangen werden können. Außerdem gibt es einen klaren Ansprechpartner auf höchster Unternehmensebene.

2. Vorteile und zu beachtende Rahmenbedingungen:

Vorteile	Zu beachten
• Klare Zuständigkeiten, eindeutiger Ansprechpartner auf Ebene der Unternehmensführung • Effektives Management der Compliance im Unternehmen • Themen landen „ganz oben“ und werden so häufiger Gegenstand von Board Meetings	• Bei kleinen und mittleren Unternehmen ist ein funktionsgetrenntes Vorstands- oder Geschäftsführungsressort mit der Zuständigkeit Compliance aus wirtschaftlichen Gründen nur selten praktikabel.

3. Umsetzungsstrategie:

Kleine Einheiten können sich mit einer zentralen Compliancefunktion begnügen. In größeren Unternehmen sollten zentrale und dezentrale Elemente miteinander gekoppelt werden.

k. Compliance-Management – Konzern

1. Beschreibung:

Der Konzernvorstand ist dazu verpflichtet, geeignete Compliance-Maßnahmen für den gesamten Konzern zu schaffen. Dabei ist darauf zu achten, dass die Compliance-Struktur auch mit der gesellschaftsrechtlichen Struktur im Einklang steht.

Die Ausgestaltung des CMS im Konzern liegt im Ermessen des Konzernvorstands. Unterschieden werden kann zwischen der Schaffung von divisionalen, regionalen und funktionalen Compliance-Funktionen. Die Berichtslinie sollte immer direkt bis zum Konzernvorstand reichen.

Die Verantwortung zur Umsetzung der Compliance-Verantwortung liegt dabei auch bei der Unternehmensführung der einzelnen Konzerngesellschaften.

Compliance im Konzern stellt Unternehmen vor viele organisatorische Herausforderungen. Insbesondere bei Matrix-Strukturen und historisch gewachsenen Besonderheiten in der Konzernstruktur können sich diverse Fragestellungen ergeben.

2. Vorteile und zu beachtende Rahmenbedingungen:

Vor- und Nachteile der anderen Kombinationen gelten hier sinngemäß.

Vorteile	Zu beachten
Einheitliche Compliance-Vorgaben für den gesamten Konzern	Schwierigkeiten bei der Umsetzung im oft „organisch“ gewachsenen Konzerngefüge

3. Umsetzungsstrategie:

Individuelle Ausgestaltung liegt im Ermessen der Geschäftsführung bzw. des Konzernvorstands und ist abhängig von Größe, Tätigkeitsfeld, Auslandsbezug und regulatorischen Vorgaben des Unternehmens.

I. Compliance-Management – Compliance-Gremien

1. Beschreibung:

Compliance-Gremien unterstützen die Unternehmensführung bei der Erfüllung ihrer Compliance-Aufgaben. Sie dienen als Schnittstelle zwischen den Compliance-relevanten Bereichen im Unternehmen (Recht, Finanz- und Rechnungswesen, Risikomanagement, Revision, Datenschutzbeauftragter etc.).

Regelmäßige Sitzungen des Gremiums stellen sicher, dass Informationen aus einzelnen Abteilungen, die auch Implikationen für andere Bereiche aufweisen, frühzeitig bei den anderen Compliance-Verantwortlichen im Unternehmen landen. Außerdem erfordert die Aufarbeitung Compliance-relevanter Sachverhalte oftmals einen interdisziplinären Austausch (z.B. Datenschutz und Arbeitsrecht, Revisionsmethoden, etc.)

Die Einrichtung eines Compliance-Gremiums institutionalisiert den Austausch zu Compliance-Themen und sorgt für ein regelmäßiges Reporting an die Unternehmensführung.

Compliance-Gremien sind insbesondere dort zu empfehlen, wo die Compliance-Abteilung nur ein beschränktes Tätigkeitsfeld hat (z.B. „nur“ Anti-Korruption-Compliance und Kartellrechts-Compliance) bzw. einzelne Compliance-Kompetenzen auf ganz unterschiedliche Bereiche im Unternehmen verteilt sind.

2. Vorteile und zu beachtende Rahmenbedingungen:

Vorteile	Zu beachten
• Effektiver Informationsaustausch zwischen Compliance-relevanten Bereichen • Institutionalisierung von regelmäßigem Compliance-Reporting an Vorstand	• Zeitlich nicht immer unmittelbar handlungsfähig; Compliance-Gremien können deshalb – zumindest in größeren Unternehmen – nicht immer eine Compliance Abteilung ersetzen. Die Verfügbarkeit der Mitglieder des Compliance-Gremiums kann auch durch Telefon- oder Videokonferenzen erleichtert werden.

3. Umsetzungsstrategie:

Identifizierung der verschiedenen Compliance-Funktionen im Unternehmen und Festlegung einer sinnvollen Sitzungspraxis.

5.2 Ressourcen

Ein wirksames Compliance Management System benötigt Zugriff auf Ressourcen.

1. Beschreibung:

a) Personelle Ressourcen

Grundsatz: Es gibt kein „one-fits-all“. Je größer und komplexer das Unternehmen, umso größer ist tendenziell die Compliance-Organisation, d.h. abhängig von Risikoexposition, Branche, Größe, Struktur und Internationalität des Unternehmens.

Möglichkeiten:

- Zentrale Mitarbeiter versus dezentrale Funktionen
- Eigenständige Compliance-Organisation
- Compliance-Beauftragte (ggf. auch Teilzeit) aus anderen Bereichen (Legal, HR, Finance etc.)
- Compliance-Gremien
- Outsourcing bestimmter Aufgaben an Externe

b) Finanzielle Ressourcen

Das finanzielle Budget ist festzulegen und muss regelmäßig auf Angemessenheit überprüft werden. Dazu gehören neben den Personalkosten für die Compliance-Mitarbeiter Kosten für

- Compliance-Audits (Kosten durch Externe oder Mitarbeiter anderer Abteilungen, z.B. Revision)
- Beratungskosten für unterschiedliche Themen, z.B. Rechtsberatung, Zertifizierung des CMS, etc.
- Aus- und Weiterbildungskosten für Compliance-Mitarbeiter
- Sachkosten für die Compliance-Abteilung, Reisekosten für Compliance-Mitarbeiter (z.B. für Schulungen im Ausland), Kosten für ein Hinweisgebersystem (z.B. für eine externe Ombudsstelle)

c) IT-Ressourcen

Zur Sicherstellung einer effektiven Compliance-Funktion werden ggf. Softwarelösungen benötigt. Dabei kann es sich um folgende Lösungen handeln:

- Elektronisches Hinweisgebersystem
- Compliance-Datenbanken zur Durchführung von Hintergrundrecherchen und mit einer möglichen Schnittstelle zu Buchhaltungssystemen
- Tools für Prozess- und Datenanalysen
- Tools zur Auswertung unstrukturierter Daten, z.B. E-Mail Reviews

2. Vorteile und zu beachtende Rahmenbedingungen:

Vorteile	Zu beachten
Die Bereitstellung von notwendigen Ressourcen: • trägt zur Erfüllung der Legalitätspflicht der Unternehmensführung/ (Delegation von Compliance) bei • ist ein nachhaltiger Wettbewerbsvorteil • schützt vor Compliance-Verstößen/Haftung/Strafen/Kosten • ist Teil der Unternehmenskultur • ermöglicht ein effektiven Compliance-Management	• Die Bereitstellung von Ressourcen kann zur Fehleinschätzung („Enthftung“) verleiten • Fehleinschätzung Ist/Soll • Fehlkalkulationen, Ineffizienzen

3. Umsetzungsstrategie:

- Risikoanalyse (Branche, Produkt, Unternehmen)
- Vergleich Ist/Soll-Zustand
- Implementierung der für das Unternehmen passenden Lösung

5.3 Anforderungsprofil

Sowohl die Führungskräfte als auch Mitarbeiter in Compliance-Bereichen sollten sowohl über fachliche als auch überfachliche Kompetenzen verfügen.

1. Beschreibung:

Fachliche Kompetenzen

- Wirtschaftliche und rechtliche Kenntnisse, nicht zwingend Volljurist
- Hilfreich kann Kenntnis über das Unternehmen/das Geschäftsmodell sein
- Praxiserfahrung des Chief Compliance Officers
- Prozessverständnis
- Branchenkenntnisse
- Kenntnisse anderer Governance-Systeme (Risikomanagement, IKS, etc.)

Überfachliche Kompetenzen/Soft Skills

- Kommunikationsfähigkeit
- Durchsetzungsfähigkeit
- Empathie
- Emotionale Stabilität
- Analytisches und strategisches Denkvermögen
- Gewissenhaftigkeit
- Offenheit für Neues

2. Vorteile und zu beachtende Rahmenbedingungen:

Vorteile	Zu beachten
• Eine Berücksichtigung möglichst vieler Faktoren führt zur bestmöglichen Besetzung	• Es ist selten möglich alle Kompetenzen in einer Person zu vereinen. Daher sollte ein Compliance-Team bzw. -Gremium diese Voraussetzungen als Gruppe erfüllen (z.B. Juristen und Betriebswirte).

3. Umsetzungsstrategie:

- Anforderungsprofil auf das Unternehmen anpassen
- Vertrauensposition beachten
- Abgleich Intern vs. Extern »

6. Compliance-Kommunikation

6.1 Einführung/Fortentwicklung eines CMS

a. Give-Aways

1. Beschreibung:

- Kostengünstige Artikel (bis ca. 5 Euro) werden mit Compliance-Themen bedruckt
- Beispiele sind: Stifte, Kompass, Tischaufsteller, Kalender, Taschenlampen, Tassen, Weihnachtskarten.

2. Vorteile und zu beachtende Rahmenbedingungen:

Vorteile	Zu beachten
• Andere Darbietungsform erhöht Aufmerksamkeit • Nützliche Gegenstände erinnern permanent an Compliance • Hoher Wiedererkennungswert	• Passt nicht in jede Firmenkultur • In Krisen sollte ein möglicher Eindruck einer „unnützen“ Ausgabe bedacht werden • Schlechte Give-Aways können mehr schaden als nutzen

3. Umsetzungsstrategie:

Verteilung im Rahmen von Schulungen, Gesprächen oder als Gewinn bei einer Compliance-Aktion.

b. Spiele

1. Beschreibung:

- Ein Spiel im Zusammenhang mit Compliance beinhaltet Compliance-relevante Fragen oder Fälle, die in spielerischer Form beantwortet werden
- Beispiele können hier ein Roulettespiel, ein Glücksrad oder ein Brettspiel mit zu lösenden Fällen sein

2. Vorteile und zu beachtende Rahmenbedingungen:

Vorteile	Zu beachten
• Positive Assoziationen • Interessante Darbietungsform • „Spieltrieb“ kann andere Zielgruppen erreichen • Je nach Spiel einfache Herstellung, z.B. bei Roulette	• Passt nicht in jede Firmenkultur • Erstellung von Fällen und Lösungen kann aufwendig sein

3. Umsetzungsstrategie:

- Einkauf fertiger Produkte oder eigene Erstellung
- Einsatz statt Vorträgen oder als Ergänzung auf internen Compliance-Veranstaltungen
- Ggf. mit Train-the-trainer Methode auch in Fachabteilungen selbständig einsetzbar

c. Compliance-Tage unter Einbindung weltweiter Niederlassungen

1. Beschreibung:

- Compliance-Veranstaltung mit physischem Treffen unter Teilnahme von Mitarbeitern verschiedener Standorte
- Ziel der Vermittlung von Compliance-Kultur, -Richtlinien und -Anforderungen sowie Sensibilisierung der Mitarbeiter
- Teilnahme der Unternehmensführung, um dem Thema Nachdruck zu verleihen
- Regelmäßige Wiederholung
- Verschiedene Inhalte und Formate möglich, z.B.
 - o Vorstellung des Compliance-Systems der Unternehmensgruppe oder besonders wichtiger Richtlinien
 - o Bearbeitung von Case Studies z.B.
- zum Umgang mit Risikosituationen
- zum Umgang mit Verdachtsfällen
- zu Fällen aus der Vergangenheit
 - o Workshops zur Identifikation von Risikobereichen
 - o Diskussions- und Fragerunden

2. Vorteile und zu beachtende Rahmenbedingungen:

Vorteile	Zu beachten
• Interaktion, aktive Einbindung der Mitarbeiter möglich • Flexible inhaltliche Gestaltung aufgrund persönlichen Kontakts • Erhöhter Lerneffekt durch Fokussierung, direkte Ansprache und Möglichkeit der Interaktion • Hoher Praxisbezug darstellbar • Möglichkeit jurisdiktions- und abteilungsübergreifende Compliance-Aspekte abzudecken; dadurch Sensibilisierung auch für Themen, die nicht unmittelbar die „eigene“ Jurisdiktion oder Abteilung betreffen • Ermöglicht Networking unter den Mitarbeitern • Wiederholungseffekt durch Schulungscharakter	• Hohe Kostenbelastung (ggf. regionale Meetings) • Hohe zeitliche Belastung • Logistik für Planung und Durchführung • Ggf. Sprachbarrieren • Gefahr der Verletzung z.B. datenschutzrechtlicher Bestimmungen bei offenen Fragerunden abteilungs- und/oder länderübergreifend • Gefahr eines „one fits all“-Ansatzes

3. Umsetzungsstrategie:

- Durch gezielte Planung und Gestaltung ist eine Begrenzung des Aufwands möglich:
 - o Kombination mit ohnehin stattfindenden Veranstaltungen wie Sales- und Management Meetings oder Veranstaltungen für neue Mitarbeiter
 - o Fokussierung auf besonders relevante Zielgruppen (z.B. Vertrieb, Einkauf)
 - o Regionale Veranstaltungen zur Verringerung von Reisekosten und -zeiten
- Durchführung durch eigene Mitarbeiter vs. Externe
- Erfolgskontrolle und Evaluierung wichtig
- Wiederholung in regelmäßigen Abständen unter Einbeziehung der Evaluierungsergebnisse
- Anschlussmaßnahmen, die an Compliance-Tage anknüpfen, aber keine Präsenz erfordern (z.B. Follow-up Video-Konferenzen; Austausch unter Teilnehmern; Zurverfügungstellung der Materialien über Intranet).

d. Compliance als Block der Einführungsveranstaltung für neue Mitarbeiter

1. Beschreibung:

- Vermittlung durch den Compliance-Beauftragten was Compliance ist, was Compliance für das Unternehmen bedeutet und wie Compliance im Unternehmen umgesetzt wird.
- Vermittlung von Regeln und Prozessen und wie bei (eventuellen) Verstößen zu reagieren ist.
- Diskussion und Fragerunde.

2. Vorteile und zu beachtende Rahmenbedingungen:

Vorteile	Zu beachten
• Neue Mitarbeiter werden bzgl. des Themas Compliance direkt „mitgenommen“ (Auslösen eines WIR-Gefühls) und lernen „ihren“ Ansprechpartner in Sachen Compliance gleich zu Beginn kennen • Eigener Block in der Einführungsveranstaltung zeigt Stellenwert des Themas im Unternehmen. • Interaktive Gestaltung ermöglicht Diskussion und Bewusstseinschärfung von Anfang an.	• Gefahr, dass Thema unter all den anderen Themenblöcken „untergeht“. Deshalb unbedingt bei der Vermittlung einen emotionalen, kreativen und verständlichen Ansatz wählen und Wiederholung in Compliance-Schulungen, -Trainings oder -Workshops

3. Umsetzungsstrategie:

- Fester Bestandteil als Block der Einführungsveranstaltung für neue Mitarbeiter.
- Emotionale, kreative Vermittlung des Themas Compliance auch in Verbindung mit den Werten des Unternehmens (Auslösen eines WIR-Gefühls), z.B. Videobotschaft der Unternehmensführung, kleines Rollenspiel, etc.

e. Interne Veröffentlichungsmöglichkeiten

1. Beschreibung:

- Intranet mit Compliance-Basisinformationen, aktuellen Entwicklungen, Frage- und Hinweismöglichkeiten, ständige Erweiterung und Aktualisierung
- Mitarbeiterzeitung mit einem oder regelmäßigen Artikeln zu Compliance im Unternehmen
- Aushänge

2. Vorteile und zu beachtende Rahmenbedingungen:

Vorteile	Zu beachten
• Nutzung bereits vorhandener Prozesse und Medien ermöglicht Kostenvorteile • Schnelle Erstellung für Artikel und Aushänge möglich • Zugriff von (internationalen) Mitarbeitern auf relevante Informationen • Hohe Aktualität	• Intranetauftritt ist pflegeintensiv • Aushänge werden schnell übersehen und gelten oftmals als veraltetes Medium

3. Umsetzungsstrategie:

- Permanente Bereitstellung von Compliance-Informationen
- Nutzung von Synergien mit bestehenden Medien

f. Poster/Kampagnen/Comics

1. Beschreibung:

- Ein oder mehrere Poster, die im Zusammenhang mit der Tätigkeit der Firma stehen, werden mit Compliance-Aussagen verknüpft
- Je nach Branche können erlaubte oder verbotene Handlungen der Mitarbeiter auch in einfacher Bildsprache, z.B. als Comic dargestellt werden

2. Vorteile und zu beachtende Rahmenbedingungen:

Vorteile	Zu beachten
• Überschaubare Produktionskosten • Erregt Aufmerksamkeit • Bleibt eher im Gedächtnis als reiner Text • Positive Verknüpfung möglich (vergleichbar mit Werbung)	• Passt nicht in jede Firmenkultur • Bildsprache stellt Sachverhalte stark vereinfacht dar (keine Detailtiefe möglich) • Unterschiedliches kulturelles Verständnis von Bildern

3. Umsetzungsstrategie:

- Produktionsqualität je nach Budget möglich
- Einfache Verbreitung durch Aushänge/Ausdrucke
- Verwendung bei Schulungen, Einführungsveranstaltung für neue Mitarbeiter, etc.

g. Videobotschaft der Unternehmensführung

1. Beschreibung:

- Unternehmensführung vermittelt in einer Videobotschaft in einer einfachen und verständlichen Sprache was Compliance ist, was Compliance für das Unternehmen bedeutet und wie Compliance im Unternehmen umgesetzt wird.
- Videobotschaft kann zu unterschiedlichen Anlässen gezeigt werden (z.B. Internet, Intranet, Schulungen, etc.).

2. Vorteile und zu beachtende Rahmenbedingungen:

Vorteile	Zu beachten
• Direkte Ansprache der Mitarbeiter • Ggf. über das Internet auch direkte Ansprache von Besuchern der Internetseite (d.h. (potentielle) Kunden, künftige Mitarbeitern, etc.) • Durch die Vermittlung seitens der Unternehmensführung bekommt das Thema entsprechendes Gewicht („Tone from the Top“) • Kann zu unterschiedlichen Anlässen eingesetzt werden	• Einseitig, nicht interaktiv • Einzelne Mitarbeiter (z.B. Produktion) werden möglicherweise nicht erreicht • Produktionskosten für die Erstellung

3. Umsetzungsstrategie:

- Qualitativ hochwertige Produktion der Videobotschaft
- Einstellen der Videobotschaft in das Intranet oder Internet zum Zeitpunkt der Einführung eines Compliance-Managementsystems
- Abspielen der Videobotschaft als Kick-Off bei Schulungen, Einführungsveranstaltung für neue Mitarbeiter, etc.

h. Workshops

1. Beschreibung:

Workshops sind Veranstaltungen, in denen kleinere Gruppen mit begrenzter Zeitdauer intensiv an einem Thema arbeiten. Ein Kennzeichen ist dabei die kooperative und moderierte Arbeitsweise an einem gemeinsamen Ziel. Workshops können gesondert zum Thema durchgeführt oder in bereits bestehende Veranstaltungen eingebunden werden, hierbei kann aber ggf. die Bedeutung des Themas untergehen.

Es können entsprechend der Unternehmensgröße und -organisation zentrale wie auch dezentrale Workshops organisiert werden.

Sie sollten durch den Compliance-Beauftragten durchgeführt werden, damit dem Thema ein „Gesicht“ gegeben wird.

Unternehmensspezifika müssen berücksichtigt werden.

2. Vorteile und zu beachtende Rahmenbedingungen:

Vorteile	Zu beachten
• Direkte Kommunikation mit der gewünschten Zielgruppe • Direkter Austausch mit dem Compliance-Verantwortlichen möglich • Hohe Sensibilisierungsmöglichkeit • Diskussionsmöglichkeiten • Feedback • Anregungen können direkt aufgenommen werden	• Ggf. werden nicht alle Mitarbeiter beteiligt • Organisations- und Zeitaufwand • Verfügbarkeit der Teilnehmer

3. Umsetzungsstrategie:

- Teilnehmerkreis definieren
- Zeitrahmen/Dauer festlegen (Stunden/ganztägig)
- Termin finden/koordinieren
- Veranstaltungsort festlegen
- Externe Unterstützung prüfen
- Präsentationsunterlagen erstellen

i. Compliance-App für Führungskräfte

1. Beschreibung:

- App zur Nutzung auf mobilen Endgeräten aller Führungskräfte mit den wichtigsten Informationen zu Compliance in kompakter Form
- Wissensbasis, Updates und Anwendungsfälle mit schnellem Zugriff
- Ziele: einfache Kommunikation mit allen betroffenen Mitarbeitern, ggf. auf einem als modern empfundenen Weg, schnelle Hilfe bei konkreten Fragen.

2. Vorteile und zu beachtende Rahmenbedingungen:

Vorteile	Zu beachten
• Durch Einbindung in alle mobilen Firmenendgeräte hoher Durchdringungsgrad • Einfacher Zugang zu den Themen und Problemen für die Mitarbeiter • Hinweis auf die App über internen Emailverteiler möglich • Updates können schnell an den relevanten Kreis verteilt werden • Bei Einbindung von Hotlines und Kontaktdaten schneller und niedrigschwelliger Kontakt zu den Compliance-Stellen des Unternehmens • Einbinden von Podcasts oder Spielen zur Steigerung der Attraktivität möglich • Rückmeldung durch Mitarbeiter über Bewertung der App	• Kosten für Entwicklung und Anpassung an die individuellen Bedürfnisse des Unternehmens • Regelmäßige Updates erforderlich, um das Interesse an der App zu erhalten • Userführung muss einfach und intuitiv gestaltet werden • User müssen ggf. geschult werden • Gefahr der übermäßigen Vereinfachung von Inhalten

3. Umsetzungsstrategie:

- Definition des relevanten Inhalts, zum Beispiel:
 - o Code of Conduct des Unternehmens/Grundsätze der Unternehmensführung
 - o Wissen zu Compliance, Wettbewerbs- und Kartellrecht, Personalführung und Umgang mit Zulieferern
 - o Konkrete Verhaltenstipps in typischen Situationen wie Gastgeschenke, Essenseinladungen, Korruption, Insiderinformationen
 - o Hinweise auf entscheidungsbefugte Stellen im Unternehmen, Hotlines oder Stellen, die bei konkreten Fragen Hilfestellung geben können
- Entwickeln einer möglichst einfachen und intuitiven Struktur:
 - o Einschalten eines externen Anbieters
 - o Rückgriff auf eigene IT-Abteilung
 - o Rückmeldung durch die Mitarbeiter ermöglichen, zum Beispiel über ein Bewertungssystem mit Sternen o.ä.

- Verteilung der App an die Mitarbeiter:
 - o Testläufe mit engerem Mitarbeiterkreis, um Probleme im Umgang mit der App frühzeitig zu erkennen
 - o Identifikation des relevanten Personenkreises
 - o Push-Service bei firmeneigenen Endgeräten
 - o Hinweis auf Downloadmöglichkeiten per Email an den relevanten Personenkreis
 - o Bereitstellen in firmeneigenen Appstores
 - o Vorinstallation auf neu ausgegebenen Firmengeräten
- Inhaltliche Verknappung und Aktualität müssen vereinbart werden; einfache Bedienung ermöglicht raschen Zugriff auf relevantes Wissen.

6.2 Meldewege für Compliance-Verdachtsfälle

a. Vorgesetzter/Inhaber

1. Beschreibung:

Grundsätzlich sollten Verstöße bzw. Verdachtsfälle gegen gesetzliche oder unternehmensinterne Regelungen dem direkten Vorgesetzten bzw. Ansprechpartner mitgeteilt und möglichst auf dem normalen Dienstweg erledigt werden. Falls ein Compliance-Beauftragter benannt ist, sollte dieser informiert und einbezogen werden.

Wenn sich der Verdachtsfall gegen den eigenen Vorgesetzten und sein Handeln bezieht, sollten andere Meldewege benutzt werden z. B. CCO, Ombudsstelle, Unternehmensführung.

Bei einem Verdacht gegen die Unternehmensführung meldet der CCO direkt an den AR bzw. Gesellschafter, um Interessenkonflikte zu vermeiden.

Die Meldewege müssen klar definiert und beschrieben sein.

2. Vorteile und zu beachtende Rahmenbedingungen:

Vorteile	Zu beachten
• Die Personen kennen sich und ihr Umfeld • Es kann kurzfristig gemeldet und reagiert werden. • Der Sachverhalt kann kurz und schnell beschrieben werden, da das Arbeitsumfeld bekannt ist.	• Der Vorgesetzte als Ansprechpartner ist gleichzeitig fachlich und disziplinarisch verantwortlich. • Es ist keine Neutralität des Vorgesetzten als Ansprechpartner vorhanden • Der Vorgesetzte befindet sich als Ansprechpartner ggf. in einem Interessenskonflikt zwischen dem Inhalt der Meldung und eigenem Handeln. Daher ist als Alternative immer ein Compliance-Mitarbeiter und/oder ein externer Ombudsmann empfehlenswert.

3. Umsetzungsstrategie:

- Sensibilisierung der Führungskräfte und Compliance-Ansprechpartner
- Klar beschriebene und dokumentierte Prozesse zum Umgang mit Meldungen, insbesondere die Vertraulichkeit

b. Interner Compliance-Beauftragter (CCO)

1. Beschreibung:

Wenn ein Hinweisgeber bei Compliance-Verdachtsfällen davon ausgeht, dass eine Erledigung auf dem normalen Dienstweg nicht sichergestellt ist, kann ihm der Compliance-Beauftragte als prozessunabhängiger Ansprechpartner zur Verfügung stehen. Die internen Ermittlungen werden direkt vom Compliance-Beauftragten durchgeführt, bei externen Ermittlungen ist er der Ansprechpartner für die Staatsanwaltschaft.

Den Mitarbeitern können z.B. folgende Meldewege angeboten werden:

- persönlich
- telefonisch
- per E-Mail (ggf. anonymisiert)
- schriftlich

2. Vorteile und zu beachtende Rahmenbedingungen:

Vorteile	Zu beachten
• Mitarbeiter aus dem Unternehmen haben ggf. mehr Vertrauen zu internen Meldewege als zu externen • Bessere Untersuchungsmöglichkeit als z.B. bei ausschließlicher Benennung einer externen Ombudsstelle • Kürzere Wege, schnellere Ergebnisse als z.B. bei ausschließliche Einbindung einer externen Ombudsstelle • Verdachtsmeldung über eigene Führungskräfte können neutral abgegeben werden	• Ggf. fehlende Akzeptanz des CCO • Ggf. fehlender Bekanntheitsgrad des CCO • Ggf. eingeschränkte Möglichkeiten eines Hinweisgeberschutzes • Ggf. mangelnde Erfahrung bzgl. der Einschätzung der Validität von Hinweisen

3. Umsetzungsstrategie:

- Bekanntmachung des CCO und der entsprechenden Meldewege
- gelebte Unterstützung des CCO durch Unternehmensführung
- Anonyme Meldewege anbieten

c. Externe Ombudsstelle

1. Beschreibung:

Eine Ombudsstelle erfüllt im eigentlichen Sinne die Aufgabe einer unparteiischen Schiedsperson, an die sich Mitarbeiter mit Compliance-relevanten Sachverhalten und Verdachtsfällen wenden können.

Im Zusammenhang mit Compliance-Verstößen haben viele Unternehmen eine externe Ombudsstelle (i.d.R. auf Wirtschaftskriminalität spezialisierte Rechtsanwälte) eingerichtet und diese in ein Hinweisgebersystem (Whistleblowing) eingebettet. Die Ombudsstelle kann Mitarbeitern eines Unternehmens sowie Externen als Anlaufstelle zur vertraulichen, anonymen Meldung von Hinweisen auf etwaige Verstöße gegen Gesetze, interne Richtlinien des Unternehmens etc. dienen. Die Ombudsstelle unterliegt der berufsrechtlichen Verschwiegenheitspflicht, wodurch die Identität des Hinweisgebers grundsätzlich nicht preisgegeben wird.

2. Vorteile und zu beachtende Rahmenbedingungen:

Vorteile	Zu beachten
• Hemmschwelle für Mitarbeiter, etwas zu melden, wird genommen, - o da sie extern ist - o die Anonymität gewahrt bleibt - o und die Ombudsstelle der berufsrechtlichen Verschwiegenheitspflicht unterliegt.	• Ggf. zusätzliche Kosten • Interne Ermittlungen sind für eine externe Stelle schwieriger, allerdings kann diese durch gute Anbindung an die Compliance-Abteilung sehr effektiv arbeiten • Hinweisgeberschutz durch Rechtsprechung etwas eingeschränkt

3. Umsetzungsstrategie:

- Bekanntgabe der Ombudsstelle und der entsprechenden Meldewege
- Vertraulichkeit vermitteln und leben
- Extern einrichten – entsprechende auf Wirtschaftskriminalität spezialisierte Rechtsanwälte oder Wirtschaftsprüfer

d. Aufsichtsgremium

1. Beschreibung:

Die Unternehmensführung muss dem Aufsichtsgremium in regelmäßigen Abständen Compliance-Vorfälle bzw. Verdachtsfälle mitteilen. Besteht das Risiko eines erheblichen Compliance-Vorfalles, sollte eine Ad-Hoc-Mitteilung an das Aufsichtsgremium erfolgen.

Im Regelfall ist eine schriftliche Berichterstattung vorgesehen, die jedoch dann nicht gilt, wenn eine Information in Textform kurzfristig nicht möglich ist und dringender Handlungsbedarf besteht.

Darüber hinaus ist auch von dritter Seite eine Informationsweitergabe an das Aufsichtsgremium vorgesehen: Das Aufsichtsgremium erhält bspw. den Bericht über die Jahresabschlussprüfung oder Revisionsberichte, in denen Compliance-relevante Informationen enthalten sein können.

Ferner sollte das Aufsichtsgremium in bestimmten Konstellationen direkt von dem Compliance Officer oder einem anderem Mitarbeiter des Unternehmens informiert werden. Dies ist insbesondere dann der Fall, wenn ein Mitglied der Unternehmensführung selbst betroffen ist oder aufgrund von Diskrepanzen bei der Beurteilung ein zusätzliches direktes Reporting an den Aufsichtsrat angezeigt ist. Mindestens müssen die Aufsichtsratsmitglieder, die Informationen erhalten, diese an den Aufsichtsratsvorsitzenden und an den Prüfungsausschuss weitergeben.

2. Vorteile und zu beachtende Rahmenbedingungen:

Vorteile	Zu beachten
• Neutralität der Ansprechpartner im Aufsichtsgremium ist gegeben und es besteht kein Interessenkonflikt. • Mit Unternehmensführung als (grundsätzlichen) Informationsträger ist Zuständigkeit klar definiert. • Auch wenn z.B. die Unternehmensführung selbst betroffen ist, ist ein Informationserhalt seitens des Aufsichtsgremiums sicher gestellt. • Aufsichtsrat kann jederzeit seinen Pflichten gerecht werden.	• U. U. erreichen Compliance-Vorfälle bzw. Verdachtsfälle zeitverzögert das Aufsichtsgremium, da im Regelfall zuvor die Unternehmensführung durch Dritte Kenntnis erlangen muss. • Politische Eskalationen sind möglich, wenn die Unternehmensführung sich nicht eingebunden fühlt (und nicht betroffen ist). Dies kann aber durch klare Festlegung der Kommunikationswege verhindert werden. • Der Aufsichtsrat ist entfernt vom operativen Geschäft und hat möglicherweise Probleme, die Sachverhalte und deren Tragweite einzuschätzen. Er kann sich aber dazu einer (externen) Unterstützung bedienen.

3. Umsetzungsstrategie:

- Klare Kommunikation der Pflichten zur Informationsweitergabe.
- Evtl.: Erarbeitung einer „Informationsordnung“, die sich an den gesetzlichen Vorgaben orientiert.
- Unterstützung des Aufsichtsrates bei der Beurteilung der Compliance-Fälle.

e. Interne Revision

1. Beschreibung:

Die Interne Revision erbringt unabhängige und objektive Prüfungs- und Beratungsdienstleistungen, die darauf ausgerichtet sind, Mehrwerte zu schaffen und Geschäftsprozesse zu verbessern. Sie unterstützt die Organisation bei der Erreichung ihrer Ziele, indem sie mit einem systematischen und zielgerichteten Ansatz, die Effektivität des Risikomanagements, der Kontrollen und der Führungs- und Überwachungsprozesse bewertet und diese verbessern hilft.

Auftraggeber der Internen Revision ist die Unternehmensführung.

Die Interne Revision sollte, wenn sie von einem Compliance-Verdachtsfall erfährt, den Compliance-Beauftragten informieren und sich mit ihm entsprechend abstimmen, wer die Ermittlungen in dem Fall übernimmt. Sie kann allerdings auf Vorschlag des CCO durch die Unternehmensführung mit der Ermittlung beauftragt werden oder diese in Teilen unterstützen

2. Vorteile und zu beachtende Rahmenbedingungen:

Vorteile	Zu beachten
• Stabstelle im Unternehmen, nicht operativ tätig, daher relativ unabhängig • Interne Ermittlungen leichter als für Externen, da die Interne Revision das Unternehmen und seine Abläufe kennt	• Interne Revision hat eventuell nicht das notwendige Know-how, um umfassende Ermittlungen alleine durchzuführen • u. U. zu geringe Objektivität, da Teil des Unternehmens

3. Umsetzungsstrategie:

- Es sollte klar geregelt werden, wie der Meldeweg aussieht, wenn Hinweise bei der Internen Revision eingehen
- Es sollte keinesfalls die Interne Revision ohne Rücksprache mit dem Compliance-Beauftragten prüfen

6.3 Berichtswege

a. Berichtswege für Compliance-Beauftragte

1. Beschreibung:

- Definition der zu berichtenden Ereignisse (wichtig ist eine klare Definition, z.B. nur strafrechtlich relevante Vorgänge oder auch Verstoß gegen internes Regelwerk? Nur wenn, es aus dem Unternehmen heraus begangene Taten betrifft oder auch seitens Mitarbeitern gegen das Unternehmen begangene Taten?)
- Verpflichtung von Tochtergesellschaften die definierten Vorfälle an den Compliance-Beauftragten zu berichten, indem sie durch Beschluss der jeweiligen Unternehmensführung einen Verantwortlichen benennen
- Definition, wann, wie oft und an wen die Compliance Vorfälle seitens des Compliance-Beauftragten zu berichten sind. Z.B. bei Vorfällen größerer Bedeutung an die Unternehmensführung sofort, sonst z.B. als Teil des Quartalsberichtes an Unternehmensführung und (soweit vorhanden) Aufsichtsrat. Ggf. auch Report an die Muttergesellschaft.
- Zusätzliche Ad-Hoc-Berichtspflicht der Tochtergesellschaften an HR und Compliance-Beauftragten bei Verdacht von Straftaten seitens Mitarbeitern, um die Einhaltung evtl. Kündigungsfristen sicher zu stellen.
- Teile des Jahresberichts mit Gründen, aus denen Mitarbeiter gekündigt wurden (anonymisiert) in das Intranet stellen. Beispielsweise um deutlich zu machen, was zur Kündigung führt.

Zusätzlich:

- Compliance Vorfälle werden in einem Compliance Gremium (z.B. Steuerungskreis Compliance) berichtet und analysiert um eventuelle Handlungsfelder zu eruieren. Ideal ist, wenn in diesem Kreis auch die Unternehmensführung vertreten ist.
- Evtl. Kommunikation außerhalb des Unternehmens im Rahmen von CSR Bericht

2. Vorteile und zu beachtende Rahmenbedingungen:

Vorteile	Zu beachten
• Unternehmensinterne Transparenz ermöglicht Trends und Handlungsfelder festzustellen. Kommunikation hierüber (anonymisiert) lässt auch Manager Risikobereiche erkennen.	• Adressatengerechte Kommunikation

3. Umsetzungsstrategie:

Es müssen unternehmensspezifische, praktikable und akzeptierbare Berichtswege festgelegt werden.

b. Wiederholende Sensibilisierung auf Basis von Compliance-Vorfällen

1. Beschreibung:

- Nutzung von tatsächlichen Compliance-Vorfällen im Rahmen der Compliance-Kommunikation zur Sensibilisierung von Mitarbeitern
- Grundsätzlich im Rahmen jeglicher Compliance-Kommunikation im Unternehmen möglich. Aufgrund des sensiblen Gegenstandes empfehlen sich aber fokussierte Maßnahmen mit begrenztem Teilnehmerkreis wie
 - o Schulungen, Präsentationen
 - o Workshops, Compliance-Tage
 - o Einführungsveranstaltungen für neue Mitarbeiter

2. Vorteile und zu beachtende Rahmenbedingungen:

Vorteile	Zu beachten
• Hoher Praxisbezug • Große Anschaulichkeit (besser als bei abstrakten Beispielen) • Macht akute Compliance-Risiken des Unternehmens besonders deutlich • Fokussierung auf Arten von Compliance-Vorfällen, die das eigene Unternehmen tatsächlich betreffen • Erkenntnisse für Teilnehmer leicht auf die eigenen Tätigkeitsfelder übertragbar • Konsequenzen von Compliance-Vorfällen und deren nachteilige Auswirkungen auf das Unternehmen können besonders deutlich vermittelt werden • Geringer zusätzlicher Aufwand	• Gefahr der Ausgrenzung und Demotivation der betroffenen Unternehmensbereiche, daher geschickte Kommunikation • Kann Abwehrhaltung bei betroffenen und anderen Mitarbeitern erzeugen • Materialien dürfen keine Rückschlüsse auf beteiligte Personen enthalten • Gefahr der Wahrnehmung als rückwärts-gewandtes Shaming statt als Maßnahme, die Compliance-gemäßes Verhalten in der Zukunft fördert. • Mögliche negative Auswirkungen auf internes und externes Unternehmensimage. Möglicherweise wenige Fälle, die sich tatsächlich eignen

3. Umsetzungsstrategie:

- Voraussetzungen für in Frage kommende Compliance-Fälle:
 - o Öffentlich bekannt oder Darstellung so möglich, dass Bekanntwerden unschädlich wäre
 - o Vollständig aufgearbeitet
 - o Keine laufenden Verfahren mehr
 - o Keine Gefahr der Geltendmachung von Ansprüchen durch Dritte
- In Frage kommen Compliance-Vorfälle:
 - o in der eigenen Organisation
 - o außerhalb der eigenen Organisation auf Basis von öffentlich verfügbaren Informationen

- Inhalt:
 - o Zugrundeliegender Sachverhalt (aufbereitet und anonymisiert)
 - o Verdeutlichung, worin genau zu missbilligendes Verhalten liegt
 - o Darstellung der negativen Konsequenzen für das Unternehmen und die Beteiligten
 - o Verdeutlichung wie in der Praxis die Gefahr ähnlicher Verstöße vermieden werden kann (Red Flags) und was die richtige Verhaltensweise gewesen wäre
 - o Umgang mit Verdachtsfällen
- Konsistenz mit übriger Compliance-Kommunikation wichtig, um gewünschte Wirkung zu erzeugen; es muss deutlich werden, dass dieses Verhalten nicht geduldet wird und im Widerspruch zur Compliance-Kultur des Unternehmens steht. »

7. Compliance-Überwachung

7.1 Implementierung IKS

1. Beschreibung:

Das Interne Kontrollsystem (IKS) umfasst die Gesamtheit aller Regelungen, Prozesse sowie technischen, organisatorischen und personellen Maßnahmen zur Steuerung von Risiken in Bezug auf die Erreichung der Ziele und den Schutz der Vermögenswerte einer Organisation.

Es berücksichtigt damit alle wesentlichen Geschäftsprozesse, die für Leistungsfähigkeit und Effizienz des Unternehmens von Bedeutung sind. Ein IKS soll sicherstellen, dass die einzelnen Prozesse reibungslos funktionieren und wesentliche Fehler im Prozessablauf vermieden bzw. erkannt und korrigiert werden. Zudem stellt ein effizientes und transparentes Internes Kontrollsystem die Ordnungsmäßigkeit der Geschäftsprozesse sicher und beugt Haftungsrisiken durch eine stringente Kontrollstruktur vor.

Die Qualität des Internen Kontrollsystems basiert auf den Faktoren:

- Analyse des internen Unternehmensumfelds
- Durchführung einer Risikoanalyse ausgehend von den Geschäftsprozessen
- Formulierung von Risiken und Kontrollzielen je Geschäftsprozess
- Erhebung der implementierten Steuerungs- und Kontrollmaßnahmen und deren Zuordnung zu den Kontrollzielen
- Bewertung der Kontrolllücken und Restrisiken und ggf. Definition und Einführung von zusätzlichen Kontrollmaßnahmen
- Information und Kommunikation des Kontrollsystems sowie der Vorgaben zur Dokumentation der Kontrolldurchführung
- permanenten Systemüberwachung und regelmäßige Optimierung des IKS z.B. bei Veränderungen des Umfelds oder dem Auftreten neuer Anforderungen

Das IKS ist entsprechend den Bedürfnissen und Zielen der Organisation auszurichten und die hieraus abzuleitenden Inhalte und Maßnahmen sind adäquat und effizient zu gestalten.

Zur effizienten Gestaltung des IKS empfiehlt es sich

- Kontrollen zu priorisieren und Schlüsselkontrollen (Key Controls) zu definieren
- Kontrollen zu erheben, die in den etablierten Geschäftsprozessen bereits genutzt werden
- möglichst auf bereits vorhandene Dokumentation zur Kontrolldurchführung zurückzugreifen- Kontrollen weitestgehend zu automatisieren (z.B. elektronische Freigaben, E-Mail Benachrichtigung im Fehlerfall)

Im Rahmen der Risikoanalyse werden die relevanten Risiken identifiziert, beurteilt und die Maßnahmen zu deren Vermeidung oder Reduzierung festgelegt. Zudem verlangen die „Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elek-

tronischer Form sowie zum Datenzugriff“ (GoBD) bei der Implementierung und insbesondere dem „Betrieb“ eines IKS eine umfassende und korrekte Dokumentation des Internen Kontrollsystems, die von einem Sachverständigen Dritten hinsichtlich ihrer formellen und sachlichen Richtigkeit überprüfbar sein muss. Diese sollte insbesondere die Beschreibung des Verfahrens, der Fehlerrisiken und der vermeidenden oder entdeckenden Kontrollen sowie der Nachweisdokumentation umfassen.

2. Vorteile und zu beachtende Rahmenbedingungen:

Vorteile	Zu beachten
• Beugt Haftungsrisiken vor • Erhöht die Prozesssicherheit und vermeidet Fehler • Schafft Transparenz durch wirksame Kontrollen. • Steigert Effektivität und Effizienz von Prozessen und Reduziert Fehlerquellen	• Vorhandenes IKS für Compliance nutzen (dadurch reduzierter Aufwand), um Fehlverhalten zu verhindern • Zusätzliche Dokumentationen müssen ggf. gepflegt und fortgeschrieben werden.

3. Umsetzungsstrategie:

- Klare Definition der Verantwortlichkeit für das IKS im Unternehmen (meist Stabstelle) und Schnittstelle zu Compliance
- Einbindung aller Verantwortlichen – Prozess- und Kontrollverantwortliche
- Definition der Unternehmensziele
- Berücksichtigung der Anforderungen aller Interessensvertreter (Kunden, Mitarbeiter, Gesetzgeber etc.) an das IKS
- Durchführung einer Risikoanalyse zur Identifizierung, Beurteilung und Vermeidung relevanter Risiken
- Definition und Priorisierung von Maßnahmen und Kontrollen, ggf. Anpassung von Prozessen
- Dokumentation des IKS, verzugsweise in einer Risiko-Kontroll-Matrix (RKM)
- Kontinuierliche Überwachung/Optimierung z.B. durch jährliche Rücksprache mit den Kontroll- und Prozessverantwortlichen

7.2 Interne Compliance-Audits

1. Beschreibung:

Regelmäßig sollte die Umsetzung der Compliance-Organisation, ihre Ordnungsmäßigkeit sowie ihre Wirksamkeit in der betrieblichen Praxis in den Abteilungen und an einzelnen Standorten durch Compliance-Audits geprüft werden. Im Rahmen der Compliance-Audits wird geprüft, ob die Unternehmensbereiche konform agieren und die dabei geltenden Regelungen einhalten. In einem Compliance Audit werden dabei spezielle Compliance-Themen danach geprüft, wie die Compliance-Organisation in einzelnen Abteilungen oder bei den operativen Prozessen umgesetzt ist. Mit Hilfe regelmäßiger interner Compliance-Audits soll u. a. das Ziel erreicht werden, Compliance-Risiken früh zu erkennen und Compliance-Verstöße aufzudecken. Deshalb können solche Compliance-Audits auch eine präventive Wirkung entfalten, weil sie auf potenzielle Täter abschreckend wirken. Schließlich kann ein Compliance-Audit auch zur Integration neuer Geschäftseinheiten beitragen.

So könnte es zu den Aufgaben der Internen Revision gehören, die Wirksamkeit des Compliance Managements in den operativen Geschäftsbereichen zu überprüfen. Hierzu ist es hilfreich, den Compliance-Auditplan mit dem Prüfungsplan der Internen Revision abzustimmen.

2. Vorteile und zu beachtende Rahmenbedingungen:

Vorteile	Zu beachten
• Identifikation von Red Flags in Geschäftsvorfällen • Schadensprävention bzw. -früherkennung Schafft Transparenz der Geschäftsabläufe; erfüllt damit Informationsfunktion	• Ggf. Follow-up im Rahmen einer Investigation und/oder Systemverbesserung notwendig • Zusätzliche Ressourcen oder Outsourcing

3. Umsetzungsstrategie:

Vorab ist zu prüfen, ob entsprechende Fachkompetenzen zur Durchführung interner Compliance-Audits vorhanden sind. Weiter ist zu entscheiden, welcher Bereich (z.B. Interne Revision) diese Compliance-Audits durchführt.

7.3 Externe Compliance-Managementsystem-Audits

1. Beschreibung:

Externe Compliance-Managementsystem-Audits haben häufig das Ziel, die Einhaltung von Compliance- & Aufsichtsregelungen zu begutachten, meist auf Basis des Standards zur Prüfung von Compliance-Management-Systemen (z.B. IDW PS 980). Naturgemäß beschränkt sich dieser Standard auf generelle Aussagen zu den Grundelementen eines CMS und dessen Prüfung – in der Regel durch unabhängige Sachverständige. Jedoch kann die Überprüfung der Angemessenheit und Wirksamkeit des Compliance-Managementsystems in den operativen Geschäftsbereichen auch von der Internen Revision durchgeführt werden.

Das Ziel ist, Schwachstellen im Compliance-Managementsystem zu erkennen und zu beheben sowie die Einhaltung der Compliance-Vorgaben zu überprüfen. Hat das Compliance-Management-System-Audit beispielsweise einen Schwerpunkt im Teilbereich Antikorruption, bezieht sich die Prüfung aller Grundelemente auf dieses Thema. Im Rahmen dieses Audits wird die Umsetzung von relevanten Aufgaben und Maßnahmen hinterfragt und analysiert und Optimierungspotenziale aufgezeigt.

2. Vorteile und zu beachtende Rahmenbedingungen:

Vorteile	Zu beachten
• Unabhängige Prüfung der Angemessenheit des CMS; Identifikation von Verbesserungspotential • Informationen darüber, ob das CMS gelebt wird • Schafft Transparenz der Geschäftsabläufe; erfüllt damit eine Informationsfunktion	• Die Prüfung sollte wiederkehrend stattfinden (z.B. jährliche Follow-ups), um die Umsetzung der Maßnahmen zu prüfen und Veränderungen zu beachten

3. Umsetzungsstrategie:

Externe Compliance-Managementsystem-Audits können jederzeit beauftragt werden. Voraussetzung ist aber ein bereits eingeführtes Compliance-Managementsystem, gegen das anhand des o.g. Standards der Umsetzungsgrad geprüft wird. Somit erhält man nach erfolgter Etablierung, ein unabhängiges Bild und Hinweise für Verbesserungspotenziale.

7.4 Prüfungen der Internen Revision

1. Beschreibung:

Die Interne Revision erbringt unabhängige und objektive Prüfungs- und Beratungsdienstleistungen, welche darauf ausgerichtet sind, Mehrwerte zu schaffen und die Geschäftsprozesse zu verbessern. Sie unterstützt die Organisation bei der Erreichung ihrer Ziele, indem sie mit einem systematischen und zielgerichteten Ansatz die Effektivität des Risikomanagements, der Kontrollen und der Führungs- und Überwachungsprozesse bewertet und diese verbessern hilft. (Quelle: Internationale Standards für die berufliche Praxis der Internen Revision). Damit hilft die Interne Revision auch dabei Handlungsbedarf aufzuzeigen und eine Informationsgrundlage für Entscheidungen und erforderliche Anpassungen zu liefern.

Die Interne Revision ist ein wesentlicher Baustein des prozessunabhängigen internen Überwachungssystems eines Unternehmens. Die prozessintegrierten Überwachungsmaßnahmen sind von der Internen Revision zu prüfen. Außerdem prüft die interne Revision das Compliance-Management System. Zwischen der Compliance-Abteilung und der Internen Revision besteht im Rahmen der Prüfungsplanung und bei dem Austausch der Prüfungsergebnisse eine enge Kommunikation

2. Vorteile und zu beachtende Rahmenbedingungen:

Vorteile	Zu beachten
• Interne Revision kann Schwachstellen im CMS aufdecken • Interne Revision profitiert von der Erhebung der Compliance-Risiken im Rahmen der Planung • Interne Revision vermittelt der Compliance-Abteilung kritische Prüfungsergebnisse zur Nachschulung der Mitarbeiter, als Grundlage für eine Investigation. Etc. • Unabhängige Prüfung von Geschäftsabläufen; Identifikation von Verbesserungspotential • Schafft Transparenz der Geschäftsabläufe; erfüllt damit Informationsfunktion	• Regelmäßiger Austausch muss vorgesehen und geregelt werden

3. Umsetzungsstrategie:

- Festlegung der entsprechenden Zuständigkeiten mit direkter Anbindung an die Unternehmensführung
- Gewährleistung der Unabhängigkeit, Ausstattung mit Weisungsbefugnissen und Ressourcen zur Durchführung der Prüfungs- und Beratungsdienstleistungen
- Identifikation von Revisionsfeldern (risikobasierter Ansatz)
- Erstellung eines Prüfungsplans
- Durchführung der Prüfungen (Planung; Durchführung Soll-Ist-Vergleich; Empfehlung; Überwachung Umsetzung)

Über DICO:

DICO – Deutsches Institut für Compliance e.V. wurde im November 2012 in Berlin auf Betreiben führender Compliance-Praktiker und -Experten gegründet und hat als gemeinnütziger Verein Mitglieder aus allen Branchen in Deutschland, darunter namhafte DAX-Unternehmen, Wirtschaftsprüfungs- und Beratungsgesellschaften, sowie aus der Wissenschaft. DICO versteht sich als unabhängiges interdisziplinäres Netzwerk für den Austausch zwischen Wirtschaft, Wissenschaft, Politik und Verwaltung und sieht sich als zentrales Forum für die konsequente und praxisbezogene Förderung und Weiterentwicklung von Compliance in Deutschland.

DICO fördert Compliance in Deutschland, definiert in diesem Bereich Mindeststandards, begleitet Gesetzgebungsvorhaben und unterstützt zugleich die praktische Compliance-Arbeit in privaten und öffentlichen Unternehmen, fördert Aus- und Weiterbildung und entwickelt Qualitäts- sowie Verfahrensstandards.



DICO – Deutsches Institut für Compliance

Chausseestraße 13

D-10115 Berlin

info@dico-ev.de

www.dico-ev.de

