Empfehlungen für die Ausgestaltung und Beurteilung von Compliance-Management-Systemen

L1

KONSTANZ INSTITUT FÜR CORPORATE GOVERNANCE

KICG CMS-LEITLINIE 1 2014 –

für Unternehmen mit bis zu 250 Mitarbeitern

Empfehlungen für die Ausgestaltung und Beurteilung von Compliance-Management-Systemen

KONSTANZ INSTITUT FÜR CORPORATE GOVERNANCE

L1

KICG CMS-LEITLINIE 1 2014 –
für Unternehmen mit bis zu 250 Mitarbeitern

Impressum

Herausgeber

Konstanz Institut für Corporate Governance (KICG)
der Hochschule Konstanz Technik, Wirtschaft und Gestaltung

Prof. Dr. Stephan Grüninger
Wissenschaftlicher Direktor des KICG

Brauneggerstraße 55
78462 Konstanz
T. +49 [0] 7531 206 251

compliance-pflichten@htwg-konstanz.de
www.kicg.htwg-konstanz.de

Autoren

Stephan Grüninger
Maximilian Jantz
Christine Schweikert
Roland Steinmeyer

Gestaltung

Stefan Klär

Das diesem Dokument zugrundeliegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter dem Förderkennzeichen 17044X11 gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei den Autoren.

GEFÖRDERT VOM

Dieses Dokument kann als Digitalversion unter www.kicg.htwg-konstanz.de bezogen werden. Die vorliegende Publikation einschließlich aller Teile ist urheberrechtlich geschützt und Eigentum des KICG. Alle Rechte, auch der auszugsweisen Vervielfältigung, liegen beim KICG. Verwertungen sind nur unter Angabe der vollständigen Quelle ›KICG CMS-LEITLINIE 1 2014‹ zulässig.

© 2014 Konstanz Institut für Corporate Governance (KICG),
Brauneggerstraße 55, 78462 Konstanz
Stand 04/2014

Rechtliche Hinweise/Haftungsausschluss:

Die in dieser Publikation des Konstanz Institut für Corporate Governance (KICG) dargestellten Inhalte sind lediglich als allgemeine Informationen und Empfehlungen zu verstehen. Sie geben die Auffassung des KICG zum Zeitpunkt der Veröffentlichung wieder und müssen nicht mit den Auffassungen der einzelnen beteiligten Projektpartner übereinstimmen. Obwohl die Informationen und Empfehlungen mit größtmöglicher Sorgfalt erstellt wurden, besteht kein Anspruch auf sachliche Richtigkeit, Vollständigkeit und/oder Aktualität. Insbesondere haben sie weder rechtsverbindlichen Charakter noch stellen sie eine Rechtsberatung dar und können eine individuelle Beratung der Unternehmen bei der Implementierung eines Compliance-Management-Systems durch fachlich qualifizierte Stellen nicht ersetzen. Das KICG übernimmt daher keine Garantie oder Haftung für die Fehlerfreiheit, Genauigkeit, Aktualität, Richtigkeit und Vollständigkeit dieser Informationen.

Die Digitalversion dieses Dokuments enthält sog. ›externe Links‹ (Verknüpfungen zu Webseiten Dritter), auf deren Inhalt wir keinen Einfluss haben und für den wir aus diesem Grund keine Gewähr übernehmen. Für die Inhalte und Richtigkeit der Informationen ist der jeweilige Informationsanbieter der verlinkten Webseite verantwortlich. Als die Verlinkung vorgenommen wurde, waren für uns keine Rechtsverstöße erkennbar. Sollte uns eine Rechtsverletzung bekannt werden, wird der jeweilige Link umgehend von uns entfernt.

Impressum 3

I ***Hinweise zur Benutzung der Leitlinien und begleitenden Dokumente*** 7

1. *Zielsetzung, Intention und Grenzen der Guidance und Leitlinien* 8

2. *Anmerkungen zur Festlegung der vier Unternehmenstypen und Compliance-Komplexitätsstufen* 10

II ***Compliance-Management-Systeme in der Praxis*** 13

1. *Gesetzlicher Rahmen und unternehmerische Pflichten* 14

2. *Wozu ein Leitfaden für die Ausgestaltung und Beurteilung von Compliance-Management-Systemen?* 19

III ***Elemente eines funktionsfähigen Compliance-Management-Systems*** 23

1. *Risikoidentifikation und -bewertung* 27

2. *Compliance-Organisation und Governance-System* 33

3. *Verhaltensgrundsätze und -richtlinien* 43

4. *Geschäftspartnerprüfung* 49

5. *Compliance-Kommunikation & Schulung* 57

6. *Integration in HR-Prozesse* 67

7. *Überwachungs- und Kontrollmaßnahmen* 75

8. *Führung und Unternehmenskultur* 81

IV ***Projektbeteiligte*** 87

Hinweise zur Benutzung der Leitlinien und begleitenden Dokumente

KAPITEL

1. Zielsetzung, Intention und Grenzen der Guidance und Leitlinien

Intention der Guidance und der Leitlinien ist es, den Entscheidungsträgern in Unternehmen (Management und Aufsichtsrat) Hilfestellung und Orientierung für die Entwicklung und Implementierung angemessener Compliance-Maßnahmen sowie für die Beurteilung der Angemessenheit dieser Maßnahmen zu geben. Die Leitlinien für die vier festgelegten Unternehmensgrößenklassen konzentrieren sich darauf, möglichst konkrete Empfehlungen zur Umsetzung von Maßnahmen und Instrumenten zur Implementierung eines Compliance-Management-System (CMS) zu geben, und sind bewusst knapp gehalten. Die ausführlichen Begründungen und weiterführenden Erklärungen zu den einzelnen CMS-Elementen und geeigneten Implementierungsinstrumenten wurden für alle vier Leitlinien in einem gemeinsamen Dokument, der **GUIDANCE**, zusammengefasst. Ergänzt werden die **LEITLINIEN** und die übergeordnete Guidance durch einen **ANNEX** zu den Leitlinien mit spezifischen Anforderungen und Risikotreibern für die Ausgestaltung von CMS.

Die Ausführungen in den Leitlinien sowie der Guidance unterscheiden Maßnahmen und Instrumente, die für die Implementierung eines **angemessenen** und **funktionsfähigen** CMS in der jeweiligen Unternehmensgrößenklasse erforderlich sind, sowie darüber hinaus gehende zusätzliche unterstützende Maßnahmen. *Erforderliche Maßnahmen* sind im Text durch die Verwendung der Begriffe wie ›soll‹ oder ›hat‹ sowie weiterer Begriffe, die einen Aufforderungscharakter ausweisen, gekennzeichnet. *Zusätzliche, unterstützende Maßnahmen*, deren Umsetzung den Unternehmen empfohlen wird, sind an der Verwendung von Begriffen wie ›sollte‹ und ›empfehlenswert‹ zu erkennen. *Freiwillige Maßnahmen*, die im *eigenen Ermessen des Unternehmens* liegen, werden mit ›kann‹ oder ähnlichen Begriffen mit gleichem Bedeutungsgehalt beschrieben. Der Leser möchte beachten, dass mit der Unterscheidung ›Erfordernis – Empfehlung – Ermessen‹ keine juristische Unterscheidung getroffen wird, ob es verpflichtend, ratsam oder völlig frei sei, eine bestimmte Compliance-Maßnahme zu treffen. Vielmehr geht es darum, dem Leser methodisch abgesicherte Plausibilitätsüberlegungen nahe zu bringen. Diesen zu folgen oder nicht, bleibt der unternehmerischen bzw. gutachterlichen Beurteilung anheim gestellt. Die Empfehlungen richten sich an Unternehmen aller Unternehmensgrößen und schließen bewusst keine Unternehmen aufgrund ihrer geringen Unternehmensgröße aus. Gleichwohl ist anzunehmen, dass sich Unternehmen erst ab einer Unternehmensgröße von ca. 50 Mitarbeitern mit dem Thema Compliance befassen und sich systematisch damit auseinandersetzen werden. Dennoch kann es auch für kleinere Unternehmen aufgrund ihrer spezifischen Komplexität (Internationalität, Geschäftsmodell etc.) erforderlich sein, die Empfehlungen der Leitlinien zu beachten.

Die Empfehlungen der vier Leitlinien für die Implementierung eines angemessenen Compliance-Management-Systems sind in einer gemeinsamen **MATRIX** zusammengefasst, die sich in → **KAPITEL IV** der **GUIDANCE** wiederfindet sowie in den verschiedenen Leitlinien bei den acht Elementen eines funktionierenden CMS jeweils in Auszügen abgebildet wird. Die Matrix liefert einen Überblick über wesentliche Instrumente der Implementierung von CMS für Unternehmen der unterschiedlichen Compliance-Komplexitätsstufen und gibt zudem eine Einschätzung hinsichtlich der Notwendigkeit der einzelnen Instrumente für die Sicherstellung der Funktionsfähigkeit des CMS. Die Empfehlungen in den Leitlinien und der Matrix beschreiben damit den Soll-Zustand eines CMS für die unterschiedlichen Unternehmensgrößenklassen, ohne jedoch einen rechtsverbindlichen Charakter aufzuweisen. Nicht Gegenstand dieser Leitlinie ist, im Detail auf die sich aus den unterschiedlichen spezifischen Gesetzen ergebenden Organisations- und Sorgfaltspflichten der Geschäftsleitung einzugehen, sondern vielmehr konkrete Handlungsempfehlungen zu geben, welche organisatorischen Maßnahmen zu erfüllen sind, um Fehlverhalten der Beschäftigten eines Unternehmens im Allgemeinen bestmöglich zu vermeiden.

Die Inhalte dieser Publikation geben die Auffassung des KICG zum Zeitpunkt der Veröffentlichung wieder und müssen nicht mit den Auffassungen der einzelnen beteiligten Projektpartner übereinstimmen.

Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet. Sämtliche Personenbezeichnungen gelten gleichwohl für beiderlei Geschlecht.

2. Anmerkungen zur Festlegung der vier Unternehmenstypen und Compliance-Komplexitätsstufen

Grundlage für die Einordnung eines Unternehmens in die vier Leitlinien bildet die Compliance-Komplexität des Unternehmens. Da jedoch kein Unternehmen dem anderen gleicht, würde sich aus den jeweils unternehmensspezifischen Organisationsstrukturen und Compliance-Risiken eine unendliche Anzahl an Komplexitätsabstufungen und daraus hervorgehender unternehmensspezifischer Kriterienkataloge für die Ausgestaltung eines funktionsfähigen CMS ergeben. Um eine operationalisierbare Anzahl an Leitlinien zu erreichen, wurden verschiedene Annahmen getroffen, auf deren Basis eine Zusammenfassung von Unternehmen in vier spezifischen Unternehmensgrößenklassen erfolgte. Die zugrundeliegenden Annahmen und wissenschaftlichen Begründungen für die Ableitung der vier Unternehmensgrößenklassen sind in den Studien und Forschungspapieren, die im Rahmen des Forschungsprojekts entstanden sind, dargelegt.[01] Das maßgebliche Kriterium für die Einordnung von Unternehmen in eine der vier Leitlinien ist die Unternehmensgröße (gemessen an der Anzahl der Mitarbeiter), da grundsätzlich eine ausstrahlende Wirkung der Unternehmensgröße auf andere Faktoren, die Einfluss auf die Compliance-Komplexität nehmen, angenommen werden kann, d.h. sowohl der Internationalisierungsgrad, das allgemeine Geschäftsrisiko als auch der regulatorische Rahmen werden in aller Regel mit steigender Unternehmensgröße an Komplexität zunehmen.

Zweifellos nehmen aber auch weitere Aspekte wie beispielsweise das Geschäftsmodell, die Kapitalmarktorientierung oder die spezifische Risikoexposition eines Unternehmens wesentlichen Einfluss auf die Ausgestaltung eines CMS. Aus diesem Grund dürfen die in den vier Leitlinien festgelegten Komplexitätsstufen nicht als starre Gruppen angesehen werden, die sich ausschließlich an der Anzahl der Mitarbeiter orientieren. Unter Umständen erfordern bestimmte unternehmensspezifische Faktoren die Erfüllung höherer Anforderungen bezüglich der Ausgestaltung des CMS. Die wesentlichen Faktoren, die zu einer erhöhten Compliance-Komplexität beitragen, sind im → ANNEX zusammengefasst und werden dort jeweils näher erläutert.

01 Die Studien und Forschungspapiere sind zu beziehen über compliance-pflichten@htwg-konstanz.de oder unter http://www.htwg-konstanz.de/KICG-Forschungspapiere.6620.0.html (16.04.2014) abrufbar.

Für die Benutzung der Leitlinien und Umsetzung der Empfehlungen in den Leitlinien kann aus einer erhöhten Compliance-Komplexität folgen, dass ein Unternehmen die Empfehlungen der Leitlinie einer der höheren Unternehmensgrößenklassen beachten sollte, um die Angemessenheit und Funktionsfähigkeit seines CMS sicherzustellen.[02] Die Unternehmen sind daher angehalten, vor ihrer Selbsteinordnung in eine bestimmte Leitlinie anhand der Mitarbeiterzahl zu überprüfen, ob bestimmte unternehmensspezifische Faktoren oder Umstände vorliegen, die eine Einordnung in eine höhere Unternehmensgrößenklasse erfordern. Solche Umstände können beispielsweise erhöhte Compliance-Risiken durch das Geschäftsmodell, die Tätigkeit in Ländern mit erhöhtem Compliance-Risiko, aber auch die Erfüllung bestimmter Anforderungen relevanter Stakeholder (z. B. Kredit-/Geldgeber des Unternehmens, ein wichtiger Kunde des Unternehmens) sein.

Folgende Fragen können für die Selbsteinschätzung der unternehmensspezifischen Compliance-Komplexität und die anschließende Zuordnung des Unternehmens zu einer Leitlinie herangezogen werden:

- Was sind meine Produkte?
- Wo sollen diese Produkte eingesetzt werden?
- In welche Länder werden diese Produkte geliefert?
- Gibt es für mich branchenspezifische Risiken?
- In welchen Ländern sitzen meine Geschäftspartner?
- Kenne ich meine Geschäftspartner? (Was sind deren Produkte? Ist der Geschäftspartner dem privaten oder öffentlichen Sektor zuzuordnen? etc.)
- Über welche Vertriebskanäle vertreibe ich meine Produkte?

Lässt die Beantwortung dieser Fragen auf erhöhte Compliance-Risiken in der Geschäftstätigkeit schließen, ist es ratsam, nicht nur die Empfehlungen der Leitlinie der auf die eigene Mitarbeiterzahl passenden Unternehmensgrößenklasse zu berücksichtigen, sondern die Umsetzung der Empfehlungen einer der höheren Leitlinie zu erwägen. Die Empfehlungen in höheren Leitlinien können darüber hinaus auch als Orientierung herangezogen werden, wenn es beispielsweise darum geht, bestimmte Erwartungen seitens eines Stakeholders oder auch spezifische rechtliche Anforderungen zu erfüllen.

02 Die Anforderungen an die Umsetzung von CMS nehmen von Leitlinie 1 bis zur Leitlinie 4 zu und werden strenger, d.h. umso größer und komplexer ein Unternehmen wird, desto höher werden die Anforderungen an die verschiedenen Implementierungsinstrumente mittels derer die Funktionsfähigkeit des CMS sichergestellt werden soll.

So kann es gerade für kleinere Unternehmen aus strategischen Gründen unter Umständen vorteilhaft sein, das CMS entlang der Empfehlungen aus höheren Leitlinien umzusetzen, um als Lieferant eines großen Unternehmens qualifiziert zu werden und so einen Wettbewerbsvorteil zu erreichen. Unternehmen, deren Mitarbeiterzahl an einer der Größengrenzen angesiedelt ist, wird empfohlen, im Rahmen ihrer Selbsteinordnung besonders kritisch zu prüfen, welche der Leitlinien den eigenen Unternehmensstrukturen und der Compliance-Komplexität eher entspricht.

Darüber hinaus ist bei der Benutzung der Leitlinien generell zu beachten, dass die Empfehlungen in den Leitlinien und der Matrix nur zur Orientierung im Rahmen der Erstplanung eines CMS herangezogen werden dürfen bzw. nur dann zur Orientierung für ein bereits implementiertes CMS dienen können, solange dem Unternehmen keine schwerwiegenden Compliance-Verstöße oder schwerwiegende Lücken und Mängel am CMS bekannt geworden sind. Im Falle des Vorliegens schwerwiegender Compliance-Verstöße hat die Geschäftsleitung gesteigerte Obliegenheiten sowie höhere Anforderungen an die Umsetzung von Compliance im Unternehmen zu erfüllen, so dass die Compliance-Verstöße und/oder Mängel am CMS unverzüglich umfassend aufgeklärt und durch die Umsetzung entsprechender Maßnahmen umgehend beseitigt werden. Dies kann – entgegen den allgemeinen Empfehlungen in den Leitlinien – weitaus umfassendere Maßnahmen erforderlich machen (vgl. hierzu insbesondere → ABSCHNITT I.6 ›COMPLIANCE-REMEDIATION NACH ENTDECKTEM SYSTEMATISCHEM FEHLVERHALTEN‹ im ANNEX).

Compliance-Management-Systeme in der Praxis

KAPITEL II

1. Gesetzlicher Rahmen und unternehmerische Pflichten

Die Einhaltung von Gesetzen und Normen ist nicht beliebig, sondern muss von jedem Unternehmen bei der Ausübung der geschäftlichen Tätigkeit gewährleistet werden. Gesetzesverstöße, Fehlverhalten gegen sonstige Normen und Standards sowie ethisch fragwürdige Handlungen seitens der Geschäftsleitung oder der Mitarbeiter bergen erhebliche Risiken, sowohl für die Geschäftsleitung, für die Beschäftigten als auch das Unternehmen selbst.

Das Gesetz adressiert an verschiedenen Stellen Anforderungen zu den Organisations- und Sorgfaltspflichten der Geschäftsleitung, die sich aus der Ausübung der Geschäftsführungstätigkeit der Geschäftsleitung ergeben. Dabei lassen sich entsprechende Organisationspflichten insbesondere aus folgenden Normen ableiten, die in den nachfolgenden Abschnitten genauer beschrieben werden:

- Strafrechtliche bzw. ordnungswidrigkeitsrechtliche Normen
- Gesellschaftsrechtliche Normen
- Spezialgesetzliche Normen
- Internationale Normen

Ordnungswidrigkeitsrechtlicher Rahmen

Das Ordnungswidrigkeitengesetz (OWiG) enthält insbesondere in den §§9, 30 und 130 OWiG konkrete Anforderungen an das Unternehmen sowie die Geschäftsleitung zu den Organisations- und Aufsichtspflichten.

Am 30.06.2013 ist die 8. Novelle des Gesetzes gegen Wettbewerbsbeschränkungen in Kraft getreten[03], das insbesondere wichtige Änderungen zur Unternehmensgeldbuße im Ordnungswidrigkeitenrecht mit sich bringt. Bislang sah §30 OWiG vor, dass gegen das Unternehmen eine Geldbuße von bis zu 1 Mio. Euro festgesetzt werden kann, wenn eine Person als vertretungsberechtigtes Organ bzw. Organmitglied oder bestimmte Personen in leitender Stellung (§9 OWiG) eines Unternehmens eine Straftat oder Ordnungswidrigkeit begehen, durch die Pflichten des Unternehmens verletzt wurden oder - wenn das Unternehmen bereichert wurde oder bereichert werden sollte. Durch die Gesetzesänderung wurde die Höhe des Bußgelds verzehnfacht und beträgt nunmehr statt wie bisher 1 Mio. Euro künftig 10 Mio. Euro bei vorsätzlichen und 5 Mio. Euro bei fahrlässigen Straftaten oder Ordnungswidrigkeiten. Eine Überschreitung dieses Höchstmaßes ist nach §§30 Abs. 3, 17 Abs. 4 OWiG weiterhin im Wege der sogenannten Abschöpfung des wirtschaftlichen Vorteils, den das Unternehmen durch die Straftat oder Ordnungswidrigkeit erlangt hat, möglich. Auf diesem Wege wurden in der Vergangenheit bereits Geldbußen in Höhe von mehrstelligen Millionenbeträgen gegen verschiedene deutsche Unternehmen verhängt.

Eine weitere wesentliche Änderung erfährt §30 OWiG in seinem neu eingefügten Absatz 2a, der nunmehr die Verhängung einer Unternehmensgeldbuße auch gegenüber Rechtsnachfolgern eines Unternehmens zulässt. Dies kann beispielsweise in den Fällen der Verschmelzung oder Aufspaltung des Unternehmens erfolgen. Für Unternehmen wird diese Neuerung daher insbesondere im Bereich von Unternehmenszusammenschlüssen (Mergers & Acquisitions) an Bedeutung gewinnen und eine gründliche Überprüfung des Zielunternehmens auf mögliche Compliance-Verstöße in der Vergangenheit aus Risikogesichtspunkten unumgänglich machen.

Neben der Unternehmensgeldbuße droht auch dem Inhaber eines Betriebes oder Unternehmens selbst eine Geldbuße (§130 OWiG), wenn er »*Aufsichtsmaßnahmen unterlässt, die erforderlich sind, um in dem Betrieb oder Unternehmen Zuwiderhandlungen gegen Pflichten zu verhindern, die den Inhaber treffen und deren Verletzung mit Strafe oder Geldbuße bedroht ist, und wenn eine solche Zuwiderhandlung begangen wird, die durch gehörige Aufsicht verhindert oder wesentlich erschwert worden wäre. Zu den erforderlichen Aufsichtsmaßnahmen gehören auch die Bestellung, sorgfältige Auswahl und Überwachung von Aufsichtspersonen.*« Die konkreten, zu erfüllenden Aufsichtsmaßnahmen werden in §130 OWiG zwar nicht näher bestimmt, doch haben Rechtsprechung und Literatur hieraus insbesondere folgende Pflichten des Betriebsinhabers abgeleitet[04]:

[03] Achtes Gesetz zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen v. 26.06.2013 BGBl. I S. 1738 (Nr. 32), abrufbar unter: http://www.bgbl.de/Xaver/text.xav?bk=Bundesanzeiger_BGBl&start=%2F%2F*[%40attr_id%3D%27bgbl113s1737.pdf%27]&wc=1&skin=WC#__Bundesanzeiger_BGBl__%2F%2F*[%40attr_id%3D%27bgbl113s1738.pdf%27]__1395136949617 (16.04.2014)

[04] Vgl. Rogall in, Karlsruher Kommentar zum OWiG, 3. Auflage 2006, §130, Rn. 40, BayObLG, Beschluss vom 10.08.2001 - 3 ObOWi 51/2001, in NJW 2002, 766 (zur Pflicht zur Überwachung von bestellten Aufsichtspersonen); OLG Düsseldorf: Beschluss vom 12.11.1998 - 2 Ss (OWi) 385/98-112/98 III, in NStZ-RR 1999, 151 (zur Pflicht zur Vermeidung von Kompetenzüberschneidungen)

1. Sorgfältige Auswahl von Mitarbeitern

2. Sachgerechte Organisation und Aufgabenverteilung

3. Aufklärung und Instruierung der Mitarbeiter über ihre Aufgaben und Pflichten

4. Überwachung und Kontrolle der Mitarbeiter

5. Einschreiten gegen Verstöße

Gesellschaftsrechtlicher Rahmen

Für die Organe von Kapitalgesellschaften wie der GmbH oder der Aktiengesellschaft (z.B. GmbH-Geschäftsführer, Vorstand, Aufsichtsrat) werden in den §§43 GmbHG, 93, 116 AktG generalklauselartig unternehmerische Verhaltenspflichten umschrieben. Aufgrund ihrer besonderen Pflichtenstellung zur Gesellschaft haben diese bei der Geschäftsführung die erforderliche *Sorgfalt* anzuwenden und sind dem Wohl des Unternehmens verpflichtet. Verletzt ein Organ schuldhaft seine aus dem Gesellschaftsrecht resultierenden (Sorgfalts-)Pflichten, so kann es zivilrechtlich zur Rechenschaft gezogen werden und der Gesellschaft gegenüber für den Ersatz des daraus entstehenden Schadens persönlich haften (§§43 GmbHG, 93, 116 AktG).

Als zentrales Element der Sorgfaltspflicht wird die Legalitätspflicht angesehen, die besagt, dass die Geschäftsleitung die Verantwortung trägt, dass sich Führungskräfte und Mitarbeiter sowie die Organmitglieder und Mitarbeiter von Tochterunternehmen im Rahmen der dienstlichen Tätigkeit an die einschlägigen Gesetze halten.

Der Gesetzgeber berücksichtigt zwar, dass eine unternehmerische Tätigkeit zwangsläufig auch die Eingehung von Risiken miteinschließt und ohne Eingehen von Risiken nahezu undenkbar ist. Daher wurde in §93 Abs. 1 Satz 2 AktG die Business Judgement Rule für den Vorstand der Aktiengesellschaft verankert, wo es heißt: »*Eine Pflichtverletzung liegt nicht vor, wenn das Vorstandsmitglied bei einer unternehmerischen Entscheidung vernünftigerweise annehmen durfte, auf der Grundlage angemessener Information zum Wohle der Gesellschaft zu handeln*«.

Die Business Judgment Rule, die gleichermaßen für Aufsichtsratsmitglieder (§§116, 93 AktG) sowie GmbH-Geschäftsführer Anwendung findet, sichert den Organen von Kapitalgesellschaften somit den unternehmerischen Entscheidungsspielraum. Allerdings steht der Geschäftsleitung bezüglich ihrer Pflicht zur Einhaltung der Gesetze im Rahmen der Unternehmensführung (Legalitätsprinzip) kein Ermessenspielraum zu. Die Frage danach, ›ob‹ das Unternehmen organisatorische Maßnahmen zur Sicherstellung von Compliance zu treffen hat, steht der Geschäftsleitung somit nicht zur Disposition. Ein Entscheidungs- und Ermessensspielraum steht der Geschäftsleitung lediglich zu der Frage zu, ›welche Art‹ von Organisation das Unternehmen benötigt und welche Umsetzungsmaßnahmen unter Risikobegrenzungsgesichtspunkten zweckmäßig sind. Eine weitere Einschränkung erfährt die Business Judgement Rule durch gesellschaftsrechtliche Vorschriften (§§93 Abs. 2 S. 2, 116 AktG), wonach den Organmitgliedern in einem Schadensersatzprozess die Beweislast auferlegt wird mit der Folge, dass einer Haftung nur der entgeht, wer darlegen kann, dass er gewissenhaft und sorgfältig gehandelt hat. Somit besteht für die Organe von Kapitalgesellschaften trotz der Business Judgement Rule weiterhin ein nicht unerhebliches Haftungsrisiko.

Spezialgesetzlicher Rahmen

Organisationspflichten ergeben sich aus unterschiedlichen spezialgesetzlichen Vorschriften. So ist beispielsweise nach dem Allgemeinen Gleichbehandlungsgesetz (AGG) jeder Arbeitgeber verpflichtet, im Betrieb eine *Beschwerdestelle* einzurichten, an die sich die Mitarbeiter wenden können, wenn sie sich ›im Zusammenhang mit dem Beschäftigungsverhältnis‹ benachteiligt fühlen. Ferner gibt es für Unternehmen unter bestimmten Voraussetzungen die Pflicht, bestimmte Beauftragte im Unternehmen zu benennen, die für die Durchführung und Beachtung von Vorschriften verantwortlich sind, die der Gesetzgeber als besonders wichtig ansieht. Zu nennen sind beispielsweise der Ausfuhrverantwortliche im Bereich der Exportkontrolle, der Datenschutzbeauftragte, sowie der Umweltschutzbeauftragte.[05]

Auch im Geldwäschegesetz (GWG) finden sich gewisse spezifische Sorgfaltspflichten sowie organisatorische Pflichten, die in bestimmten, im Gesetz näher genannten Fällen von Unternehmen zu erfüllen sind und daher im Rahmen der Umsetzung von CMS von Bedeutung sein können. Das GWG unterscheidet dabei zwischen allgemeinen (§3 GWG), vereinfachten (§5 GWG) sowie verstärkten (§6 GWG) Sorgfaltspflichten und legt in §9 GWG[06] bestimmte zu erfüllende Organisationspflichten fest. Unternehmen haben zu beachten, dass in den Anwendungsbereich des GWG nicht nur Unternehmen aus dem Finanzsektor fallen, sondern u.a. auch Unternehmen, die gewerblich

05 Eine Auflistung verschiedener gesetzlicher Normen, wonach ein Unternehmen bei Vorliegen bestimmter Voraussetzungen besondere Beauftragte zu bestellen hat, findet sich am Ende des **ANNEX** in → **KAPITEL II.**

06 Nach §9 GWG sind u.a. angemessene geschäfts- und kundenbezogene Sicherungssysteme zur Verhinderung der Geldwäsche und der Terrorismusfinanzierung zu entwickeln und zu aktualisieren.

mit Gütern handeln und es daher Fallkonstellationen geben kann, in denen auch sie die allgemeinen sowie verstärkten Sorgfaltspflichten zu erfüllen haben.

Internationaler Rahmen

Ist das Unternehmen international tätig, so wird es mit Gesetzen (wie z.B. dem UK Bribery Act und dem US-amerikanischen Sarbanes Oxley Act) konfrontiert, die extraterritoriale Wirkung haben können und damit Auswirkungen auf die Organisationspflichten des Unternehmens entfalten.[07]

Sonstige Risiken aufgrund von Rechtsverstößen

Neben den zuvor dargelegten straf- und haftungsrechtlichen Folgen drohen dem Unternehmen auch weitere negative wirtschaftliche Folgen im Falle von Rechtsverstößen. So laufen Unternehmen beispielsweise im Falle von Korruption Gefahr, von öffentlichen Aufträgen ausgeschlossen und in entsprechenden Korruptionsregistern[08] gelistet zu werden.

Und schließlich kann der mit Fehlverhalten sowie mit rechtlich zulässigen jedoch ethisch fraglichen Geschäftspraktiken einhergehende Reputationsverlust sich nachhaltig negativ auf die Unternehmensmarke und damit auf den Unternehmenswert und -gewinn auswirken.

07 Im ANNEX wird unter → ABSCHNITT I.2 ›INTERNATIONALISIERUNGSGRAD‹ auf verschiedene internationale Normen näher eingegangen.

08 Korruptionsregister werden u.a. von den Bundesländern Bremen, Berlin, Hamburg und Nordrhein-Westfalen geführt.

2. Wozu ein Leitfaden für die Ausgestaltung und Beurteilung von Compliance-Management-Systemen?

Die Geschäftstätigkeit von Unternehmen ist permanent bedroht durch vielfältige Risiken, insbesondere Reputations- und Compliance-Risiken. Unternehmen müssen darum Vorkehrungen treffen, die dazu geeignet sind, diese Risiken zu identifizieren und sie bestmöglich zu mildern oder ganz zu vermeiden. Die Vermeidung sich aus der Geschäftstätigkeit potenziell ergebender Risiken sowie die Sicherstellung der Einhaltung von gesetzlichen und regulatorischen Anforderungen, internen Regelungen und Verhaltensstandards ist Leitungsaufgabe der Unternehmensführung und kann aus rechtlicher Sicht den Organisations- und Aufsichtspflichten der Geschäftsleitung zugeordnet werden (vgl. → ABSCHNITT II.1).

In der Unternehmenspraxis hat sich die Einführung von Compliance-Management-Systemen (CMS) als geeignete Maßnahme erwiesen, um die vom Gesetzgeber an die Geschäftsleitung gestellten Organisations- und Aufsichtspflichten zu erfüllen und eine redliche und regelgetreue Geschäftsführung sicherzustellen. Zielsetzung von CMS ist es, die Einhaltung von Gesetzen, internen Regeln, Standards und Normen im Unternehmen sicherzustellen sowie Fehlverhalten der Unternehmensangehörigen durch geeignete Management-Maßnahmen vorzubeugen. Der Nachweis eines angemessenen und funktionsfähigen CMS kann sich im Schadensfall auf Ansprüche gegenüber dem Unternehmen, seiner Organe und Mitarbeiter haftungsmildernd oder -vermeidend auswirken. Glaubwürdiges Compliance Management wirkt sich zudem positiv auf die Reputation des Unternehmens aus und trägt so zur Stabilisierung bestehender und potenzieller Kooperationsbeziehungen bei.

Die zentrale Frage bei der Einführung von CMS im Unternehmen ist die Frage danach, wie das CMS bzw. die einzelnen Maßnahmen auszugestalten sind, damit das CMS für das jeweilige Unternehmen angemessen (Organisationskomplexität/allgemeines Geschäftsrisiko/regulatorischer Rahmen vs. aufgewendete Ressourcen) und funktionsfähig (hinsichtlich der Vermeidung von Fehlverhalten im Unternehmen) sein kann. Die Frage der Wirksamkeit eines CMS beschäftigt nicht nur die Unternehmen selbst (Vorstand, Geschäftsführer, Aufsichtsrat), sondern auch deren Abschlussprüfer und andere Prüfer, die das CMS eines Unternehmens prüfen und hinsichtlich seiner Funktionsfähigkeit

beurteilen. Ebenso befassen sich Staatsanwälte und Richter mit der Frage der Angemessenheit, wenn sie im Rahmen von Verfahren über vorgefallene Straftaten in einem Unternehmen darüber entscheiden müssen, ob und ggf. inwieweit zusätzlich zu einer etwaigen Straftat eines oder mehrerer Täter ein Organisationsverschulden des Managements vorliegt, wenn dieses seinen Aufsichts- und Sorgfaltspflichten (Organisationspflichten) nicht (in ausreichendem Maß) nachgekommen ist.

In der Umsetzung von CMS im Unternehmen sind die Leitungsgremien nicht auf sich allein gestellt. Zahlreiche Standards und Rahmenwerke beschäftigen sich mit der Ausgestaltung und Implementierung von CMS und geben Empfehlungen hinsichtlich wesentlicher Elemente funktionsfähiger CMS. Zu diesen Standards gehören insbesondere die COSO-Rahmenwerke[09], der Australian Standard™ AS 3806-2006 (Compliance programs)[10], die US Sentencing Guidelines for Organizations[11], das Red Book der Open Compliance and Ethics Group (OCEG)[12], die Guidance zum UK Bribery Act[13], in Deutschland der Prüfungsstandard 980 ›Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen‹ des Instituts der Wirtschaftsprüfer (IDW)[14] und der ComplianceProgramMonitor[ZfW] des Zentrums für Wirtschaftsethik[15] sowie themenspezifische Referenzwerke wie die ICC Rules of Conduct[16] oder die Business Principles for Countering Bribery[17] im Bereich der Korruptionsprävention. Diese generischen Standards stellen für Unternehmen, Prüfer und Behörden eine wichtige und wesentliche Informationsquelle

09 Zu beziehen über http://www.coso.org (16.04.2014)

10 Zu beziehen über http://www.saiglobal.com/ (16.04.2014)

11 Zu beziehen über http://www.ussc.gov/Guidelines/Organizational_Guidelines/index.cfm (16.04.2014)

12 Zu beziehen über http://www.oceg.org/resources/grc-capability-model-red-book/ (16.04.2014)

13 Zu beziehen über https://www.gov.uk/government/publications/bribery-act-2010-guidance (16.04.2014)

14 Zu beziehen über https://www.idw.de (16.04.2014)

15 Zu beziehen über http://www.dnwe.de/complianceprogrammonitor.html (16.04.2014)

16 Zu beziehen über http://www.iccwbo.org/advocacy-codes-and-rules/document-centre/ (16.04.2014)

17 Zu beziehen über http://www.transparency.org/whatwedo/tools/business_principles_for_countering_bribery (16.04.2014)

für die Entwicklung von CMS sowie deren Prüfung auf Funktionsfähigkeit dar. Jedoch fehlt es ihnen an konkreten, detaillierteren inhaltlichen Empfehlungen für die Ausgestaltung angemessener Compliance-Maßnahmen in unterschiedlichen Unternehmenstypen.

Zielsetzung dieser Leitlinie ist es, die Anforderungen an die Ausgestaltung von CMS weiter zu konkretisieren, indem die bislang eher generischen Anforderungen von Compliance-Maßnahmen auf die Gegebenheiten und Möglichkeiten zur Ausgestaltung in verschiedenen Unternehmenstypen heruntergebrochen und näher bestimmt werden. Die exakteren Empfehlungen in dieser Leitlinie sollen Unternehmen sowie beratende Dienstleister darin unterstützen, im Rahmen eines angemessenen CMS geeignete Prozesse, Maßnahmen und Instrumente zur Erfüllung der Organisations- und Aufsichtspflichten zu entwickeln. Zudem sollen die Ausführungen in dieser Leitlinie einen weiteren Beitrag zur Diskussion der Angemessenheit von CMS leisten mit dem Ziel, für Unternehmen ein möglichst hohes Maß der Konkretisierung und Verbindlichkeit von Standards hinsichtlich der Erfüllung von Organisations- und Aufsichtspflichten und damit eine erhebliche Steigerung der Rechtssicherheit zu erreichen (vgl. → ABBILDUNG 01).

Hierzu legt die Leitlinie im Folgenden dar, welche Elemente ein funktionsfähiges CMS beinhalten muss und warum es wichtig ist, die verschiedenen Elemente im Unternehmen zu implementieren. Darüber hinaus wird für jedes CMS-Element im Einzelnen aufgezeigt, welche Maßnahmen in Unternehmen mit bis ca. 250 Mitarbeitern angemessen und dazu geeignet sind, die Organisations- und Aufsichtspflichten zu erfüllen und Fehlverhalten zu vermeiden, sowie welche Aspekte bei der Ausgestaltung der Maßnahmen ggf. zu beachten sind.

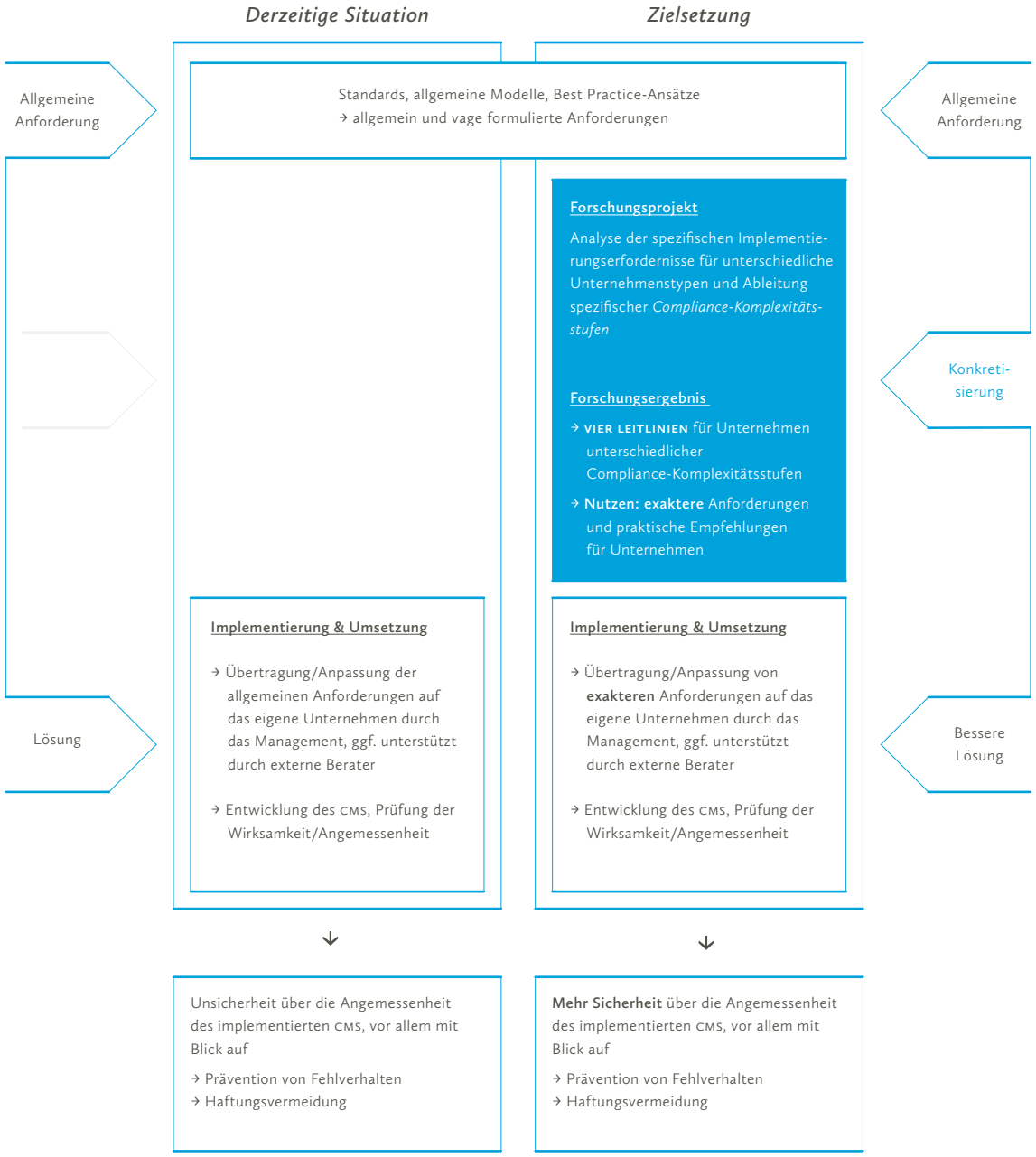

Abbildung 01 / Einordnung des Forschungsansatzes

Elemente eines funktionsfähigen Compliance-Management-Systems

KAPITEL

Die Empfehlungen zur Ausgestaltung angemessener Compliance-Management-Systeme für Unternehmen verschiedener Größenklassen basieren auf den Erkenntnissen und Hinweisen zahlreicher, bereits vorhandener Standards und Leitfäden im Bereich Compliance und Integrity Management. Ausgehend von den Empfehlungen dieser Rahmenwerke sowie von Gesetzen und Rechtsprechung zu den Organisations- und Aufsichtspflichten von Unternehmen will die vorliegende Leitlinie mit den Hinweisen und Empfehlungen einen Beitrag zur weiteren Konkretisierung von Anforderungen an die Ausgestaltung angemessener CMS leisten: Aus den eher allgemein formulierten und an alle Unternehmenstypen gleichermaßen gerichteten Empfehlungen der anerkannten Rahmenwerke zu Compliance und Integrity Management werden für Unternehmen unterschiedlicher Größenklassen spezifischere Anforderungen für die Angemessenheit eines CMS abgeleitet und konkretere Hinweise zur Ausgestaltung funktionsfähiger CMS-Maßnahmen für Unternehmen der jeweiligen Größenklasse gegeben.

In der vorliegenden Leitlinie finden Unternehmen mit einer Unternehmensgröße von bis zu ca. 250 Mitarbeitern Orientierung und Hilfestellung, welche Führungs- und Steuerungsinstrumente, Maßnahmen und Prozesse geeignet und notwendig sind, um ein der Unternehmens- und Compliance-Komplexität angemessenes und funktionsfähiges CMS zu installieren und umzusetzen. Neben der Sicherstellung einer integren Geschäftsführung und der Vermeidung von Fehlverhalten im Unternehmen stellt die Implementierung eines angemessenen CMS für die Geschäftsleitung ein wirksames Instrument zur Erfüllung ihrer mit der Führung eines Unternehmens verbundenen Organisations- und Aufsichtspflichten dar.

Damit ein CMS in der Lage ist, die drei ihm zugewiesenen Funktionen der Prävention, Aufdeckung und Reaktion auf Fehlverhalten zu erfüllen, muss es die folgenden Elemente umfassen:

- Risikoidentifikation und -bewertung
- Compliance-Organisation und Governance-System
- Verhaltensgrundsätze und -richtlinien
- Geschäftspartnerprüfung
- Compliance-Kommunikation & Schulung
- Integration in HR-Prozesse
- Überwachungs- und Kontrollmaßnahmen
- Führung und Unternehmenskultur

Die Festlegung dieser Elemente basiert auf den Anforderungen relevanter anerkannter, einschlägiger Standards im Bereich Compliance und Integrity Management. Für Unternehmen der vorliegenden Leitlinie (mit bis 250 Mitarbeitern) heißt dies nicht, dass sie bei der Umsetzung von Compliance und Integrity Management denselben Aufwand betreiben müssen, wie multinationale, große Unternehmen – dies ist ihnen schon allein aufgrund ihrer Ressourcenausstattung nicht zumutbar. Gleichwohl müssen sich auch Unternehmen dieser Leitlinie mit dem Thema Compliance und Integrity Management befassen und geeignete Maßnahmen umsetzen, um ihren Organisations- und Aufsichtspflichten gerecht zu werden. Die vorliegende Leitlinie zeigt für die acht wesentlichen Elemente eines CMS auf, welche Zielsetzungen jeweils mit den einzelnen Elementen verfolgt werden und welche Maßnahmen für Unternehmen mit einer Unternehmensgröße bis ca. 250 Mitarbeitern geeignet sind, um diese Ziele erreichen zu können.

Risikoidentifikation und -bewertung

1

CMS-ELEMENT

Vielfältige Risiken bedrohen die Geschäftstätigkeit von Unternehmen und können (langfristig) eine Gefahr für die Unternehmensexistenz darstellen. Um den Fortbestand des Unternehmens zu sichern und das Unternehmen wirksam vor Risiken zu schützen, müssen Unternehmen ihre Risiken kennen und entsprechende Maßnahmen zu ihrer Vermeidung bzw. Reduzierung implementieren. Im Fokus des Compliance Managements steht die Vermeidung von Compliance- und Integrity-Risiken (im Weiteren als Compliance-Risiken bezeichnet), d.h. von Risiken aus Fehlverhalten von Topmanagement, Führungskräften und Mitarbeitern. Compliance-Risiken ergeben sich aus der Nichteinhaltung und Missachtung von Gesetzen, internen Regelungen, Werten und Normen im Unternehmen und sind aufgrund ihrer erheblichen negativen Auswirkungen für das Unternehmen (ökonomisch, rechtlich und bezüglich der Reputation) besonders kritisch.

Um ein funktionsfähiges und angemessenes CMS entwickeln und entsprechende Maßnahmen implementieren zu können, muss das Unternehmen zunächst seine Compliance-Risiken kennen. Die Risikoidentifikation und -bewertung dient dann dem möglichst sinnvollen und effizienten Einsatz der zur Verfügung stehenden Ressourcen (finanziell und personell) zur bestmöglichen Risikovermeidung und -reduzierung – wohlwissend dass ein CMS es nicht leisten kann, Fehlverhalten von vornherein vollständig auszuschließen.

Zielsetzungen des CMS-Elements
Risikobeurteilung und Risikoorientierung

- ✓ Vermeidung und Minimierung von ökonomischen, rechtlichen und Reputationsschäden
- ✓ Sicherung der Unternehmensexistenz
- ✓ Frühwarnsystem
- ✓ Sensibilisierung und Aufmerksamkeit für Gefahren und Chancen aus der Geschäftstätigkeit schaffen
- ✓ Effiziente und sinnvolle Ressourcenverwendung (personell, finanziell)
- ✓ Fokussierung auf die ›richtigen‹ Compliance-/Integrity-Risiken

INSTRUMENTE Für Unternehmen mit einer Mitarbeiteranzahl von	LEITLINIE 1 bis 250	LEITLINIE 2 250 – 3.000	LEITLINIE 3 3.000 – 20.000	LEITLINIE 4 mehr als 20.000
Durchführung einer Analyse und Bewertung der Compliance-Risiken	**erwartet**	**erwartet**	**erwartet**	**erwartet**
Risikoidentifikation und -bewertung erfolgt zentral Möglichkeiten der Umsetzung: – durch Unternehmensleitung allein – durch Unternehmensleitung unter Einbindung der Führungskräfte/Leiter der Fachabteilungen/ Geschäftseinheiten – Delegation z.B. an Compliance-Beauftragten möglich	erwartet	erwartet	erwartet	erwartet
Zusätzlich zur zentralen Risikoidentifikation und -bewertung erfolgt eine dezentrale Risikoidentifikation und -bewertung in den Geschäftseinheiten, die zentral zusammengeführt wird	im Ermessen	empfohlen	erwartet	erwartet
Einrichtung eines Risk-Committee/Risiko-Ausschusses (bestehend aus den Leitern der verschiedenen Fachabteilungen wie Recht, IR, Einkauf, Vertrieb etc.)	im Ermessen	im Ermessen	empfohlen	erwartet
Herausgabe einheitlicher Vorgaben und Anforderungen an die Durchführung der Compliance-Risikoidentifikation und -bewertung an die einzelnen Geschäftseinheiten und Abteilungen durch die Compliance-Abteilung	im Ermessen	empfohlen	empfohlen	erwartet
Compliance-Risikosteuerung	**erwartet**	**erwartet**	**erwartet**	**erwartet**
Fortlaufende Analyse des Risikoumfeldes bezüglich Veränderungen (z.B. Unternehmenszukauf, Eintritt in neue Märkte) durch die Unternehmensleitung	erwartet	erwartet	erwartet	erwartet
Systematische Gesamtprüfung der Compliance-/ Integrity-Risiken (*jährlich*)	im Ermessen	im Ermessen	empfohlen	erwartet
Systematische Gesamtprüfung der Compliance-/ Integrity-Risiken (*alle drei Jahre*)	empfohlen	empfohlen	erwartet	erwartet
Regelmäßiges Risikoreporting der dezentralen Geschäftseinheiten (*jährlich*)	im Ermessen	empfohlen	erwartet	erwartet

Empfehlungen und Hinweise für die Umsetzung

Risikoidentifikation

- ✓ Die Verantwortung für die Compliance-Risikoidentifikation und -bewertung sowie für die Ableitung entsprechender Maßnahmen zur Steuerung von Compliance-Risiken liegt bei der Geschäftsleitung.

  Identifikation der Compliance-/ Integrity-Risiken

- ✓ Zunächst muss die Geschäftsleitung bzw. müssen die entsprechenden Verantwortlichen sich einen Überblick über die wesentlichen Compliance-Risiken des Unternehmens verschaffen.

- ✓ Die Risikoidentifikation und -bewertung erfolgt zentral. Sie wird durch die Geschäftsleitung initiiert und kann von ihr selbst durchgeführt werden. Es ist auch denkbar, die Risikoidentifikation zu delegieren. Dabei kommen jedoch nur Personen in Betracht, die aufgrund ihrer Position im Unternehmen über eine/n entsprechende/n Kenntnis und Überblick über das Unternehmen verfügen.

  Zentrale Risiko-identifikation und -bewertung

- ✓ Im Rahmen von Workshops oder mehreren Arbeitssitzungen, die durch die Geschäftsleitung moderiert und geleitet werden, können weitere Mitarbeiter in Schlüsselfunktionen oder Führungskräfte, die über Kenntnis des Geschäfts und der Prozesse verfügen, in die Risikoidentifikation miteinbezogen werden. So kann sich die Geschäftsleitung schnell und effektiv ein umfassendes Bild vom Risikoprofil des Unternehmens verschaffen.

- ✓ Ggf. können weitere Methoden und Quellen für die Risikoidentifikation herangezogen werden:
  - Kreativtechniken wie Brainstorming, Mindmapping
  - Ggf. Erkenntnisse aus früheren Compliance-Fällen
  - Expertenbefragungen (z.B. Verbände, Handelskammern, Berater)
  - Studien und Umfragen aus den Bereichen Compliance Management und Compliance-Risiken (z.B. Corruption Perceptions Index (CPI) der Antikorruptionsorganisation Transparency International für Länderrisiken, Studien von Beratungs- und Wirtschaftsprüfungsunternehmen)

- ✓ Aufgrund des Schadensausmaßes und möglichen negativen Auswirkungen auf die Reputation des Unternehmens stehen insbesondere die folgenden Compliance-Risiken im Fokus:
  - Korruption
  - Vermögensschädigung des Unternehmens, wie z.B. Untreue, Betrug, Diebstahl
  - Kartellabsprachen, wie z.B. Preisabsprachen, Aufteilung von Märkten/Gebietsabsprachen, Absprachen über Produktions- bzw. Verkaufsbeschränkungen

  Darüber hinaus können jeweils unternehmens- bzw. branchenspezifische Risiken hinzukommen.

- ✓ Die Risikoidentifikation ist kein einmaliger Prozess, sondern muss fortlaufend und kontinuierlich durchgeführt werden, um auf mögliche Änderungen im Risikoumfeld des Unternehmens frühestmöglich reagieren zu können.

  Fortlaufende Analyse des Risikoumfeldes

Risikobewertung

- ✓ Bei der Bewertung der Compliance-Risiken ist zwischen Bruttorisiko (ohne die Auswirkungen bereits getroffener Gegenmaßnahmen) und Nettorisiko (verbleibendes Restrisiko unter Einbezug getroffener Gegenmaßnahmen) zu unterscheiden.

  Bewertung der Compliance-/ Integrity-Risiken

- ✓ Geeignete Kriterien und Methoden für die Risikobewertung (Auswahl):
  - Potenzielles Schadensausmaß (finanziell, rechtlich, Reputation)
  - Eintrittsmöglichkeit bzw. potenzielle Realisierbarkeit des Risikos
  - Risiko-Ratings aus öffentlich zugänglichen, verlässlichen Checklisten, Studien und Erhebungen (z.B. CPI, Bribe Payer's Index, COFACE)

- ✓ Wichtig ist eine ehrliche und ungeschönte Einschätzung der Risiken.

Risikosteuerung

- ✓ Einleitung entsprechender Maßnahmen (risiko- und bedarfsorientiert) zur Vermeidung und Reduzierung der identifizierten Compliance-/Integrity-Risiken wie in den einzelnen CMS-Elementen im Folgenden beschrieben.
- ✓ Fortlaufende Analyse des Risikoumfeldes durch die Geschäftsleitung, so dass Veränderungen und potenzielle/neue Risiken möglichst frühzeitig erkannt und das CMS entsprechend angepasst sowie ggf. zusätzliche Compliance-Maßnahmen eingeleitet werden können.

  — Fortlaufende Analyse des Risikoumfeldes
- ✓ Neben der fortlaufenden Analyse bezüglich Veränderungen im Risikoumfeld empfiehlt sich, alle drei Jahre eine systematische Gesamtprüfung der Compliance- und Integrity-Risiken durchzuführen.

  — Systematische Gesamtprüfung der Compliance-/Integrity-Risiken

Compliance-Organisation und Governance-System

CMS-ELEMENT **2**

Nachdem das Unternehmen seine spezifischen Compliance-Risiken identifiziert hat, gilt es, im Unternehmen die entsprechende ›Organisation von Compliance‹ zu schaffen, um Rechtsverstöße, seien sie vorsätzlich oder unbeabsichtigt begangen, in diesen Risikobereichen bestmöglich zu vermeiden.

Über eine Compliance-Organisation kommt die Geschäftsleitung ihren gesellschaftsrechtlichen Sorgfalts- und Organisationspflichten nach. Diese umfassen insbesondere die Sicherstellung der sogenannten Legalitätspflicht, die besagt, dass jedes einzelne Mitglied der Geschäftsleitung geltendes Recht zu beachten sowie dafür Sorge zu tragen hat, dass auch das Verhalten aller Beschäftigten im Rahmen der dienstlichen Tätigkeit den gesetzlichen sowie internen, unternehmensspezifischen Regelungen, Normen etc. entspricht. Wie im Einzelnen die Organisation von Compliance zu erfolgen hat, wird seitens der deutschen Gesetze bislang für Wirtschaftsunternehmen nicht näher konkretisiert, sondern liegt vielmehr im Ermessen der Geschäftsleitung.

Mit der Schaffung von Organisationsmaßnahmen sorgt die Geschäftsleitung für Strukturen, die der Vermeidung von Fehlverhalten im Unternehmen dienen und das Schadensrisiko für das Unternehmen und die Geschäftsleitung verringern. Damit kommt sie letztendlich einer verantwortungsvollen Unternehmensführung (Good Corporate Governance) nach.

Zielsetzungen des CMS-Elements
Compliance-Organisation und Governance-System

- ☑ Erfüllung der gesellschaftsrechtlichen Sorgfalts- und Organisationspflichten (insbesondere des Legalitätsprinzips)
- ☑ Risikominimierung durch Implementierung von organisatorischen Compliance-Maßnahmen
- ☑ Entlastung der Geschäftsleitung durch Delegation von Compliance-Aufgaben und -Pflichten
- ☑ Sicherstellung, dass die Geschäftsleitung ihrer Primärverantwortung von Compliance nachkommen kann durch Einrichtung eines Berichtswesens
- ☑ Wahrnehmung von gesetzlichen und vertraglich festgelegten Kontroll- und Beratungsaufgaben (Aufsichtsrat/Beirat)

INSTRUMENTE Für Unternehmen mit einer Mitarbeiteranzahl von	LEITLINIE 1 bis 250	LEITLINIE 2 250 – 3.000	LEITLINIE 3 3.000 – 20.000	LEITLINIE 4 mehr als 20.000
Angemessene Ressourcenausstattung der Compliance-Organisation	**erwartet**	**erwartet**	**erwartet**	**erwartet**
Bestellung eines Compliance-Beauftragten (sog. Compliance Officer/Chief Compliance Officer), der mindestens 50% seiner Arbeitszeit für die Compliance-Aufgaben aufbringt	im Ermessen	empfohlen	erwartet	erwartet
Zurverfügungstellung ausreichender personeller Ressourcen zur Erfüllung der Compliance-Aufgaben (mindestens 1 Vollzeitäquivalent (VZÄ) pro 2.000 Mitarbeiter) mit klarer Festlegung der Rollen und Verantwortlichkeiten	erwartet	erwartet	erwartet	erwartet
Compliance-Governance und operative Umsetzung von Compliance	**erwartet**	**erwartet**	**erwartet**	**erwartet**
Unternehmensleitung nimmt Compliance-Aufgaben operativ wahr (Unternehmensleitung übernimmt die Compliance-Funktion)	alternativ	alternativ	nicht geeignet	nicht geeignet
Delegation der Compliance-Funktion an geeignete zentrale Stelle (z.B. Recht, Revision, HR, Unternehmensbeauftragte)	alternativ	alternativ	alternativ	nicht geeignet
Delegation an zentrale eigenständige Compliance-Abteilung	im Ermessen	im Ermessen	alternativ	erwartet
Übertragung und Zuordnung der Verantwortlichkeit von Compliance an ein Mitglied der Unternehmensleitung (Vorstand, Geschäftsführer) im Wege der Ressortverteilung	im Ermessen	im Ermessen	empfohlen	erwartet
Hierarchische Einordnung des Compliance-Beauftragten: *mindestens 3. Ebene*	alternativ	alternativ	nicht geeignet	nicht geeignet
Hierarchische Einordnung des Compliance-Beauftragten: *mindestens 2. Ebene* (direkte Berichterstattung an die Unternehmensleitung)	alternativ	alternativ	erwartet	erwartet

INSTRUMENTE Für Unternehmen mit einer Mitarbeiteranzahl von	LEITLINIE 1 bis 250	LEITLINIE 2 250 – 3.000	LEITLINIE 3 3.000 – 20.000	LEITLINIE 4 mehr als 20.000
	↓	↓	↓	↓
Benennung dezentraler Compliance-Beauftragter in den Geschäftseinheiten, Landesgesellschaften etc.	im Ermessen	empfohlen	erwartet	erwartet
Einsetzung eines Compliance-Committees	im Ermessen	im Ermessen	empfohlen	erwartet
Einrichtung eines Berichtswesens zu Compliance	**erwartet**	**erwartet**	**erwartet**	**erwartet**
Berichterstattung des Compliance-Beauftragten an Unternehmensleitung z.B. im Rahmen von Jours Fixes sowie ad-hoc (anlassbezogen)	erwartet	erwartet	erwartet	erwartet
Schriftliche Compliance-Berichterstattung des Compliance-Beauftragten an die Unternehmensleitung (*mindestens jährlich*)	im Ermessen	empfohlen	erwartet	erwartet
Schriftliche Compliance-Berichterstattung durch die Unternehmensleitung an den Aufsichtsrat/Beirat (*mindestens jährlich*) sowie anlassbezogene (ad-hoc) Compliance-Berichterstattung der Unternehmensleitung an den Aufsichtsrat/Beirat	erwartet	erwartet	erwartet	erwartet
Schaffung einer Berichtsmöglichkeit des Compliance-Beauftragten an den Aufsichtsrat/Beirat (*dotted line*)	im Ermessen	im Ermessen	empfohlen	erwartet
Schriftliche Compliance-Berichterstattung durch den Compliance-Beauftragten an den Aufsichtsrat/Beirat (*jährlich*)	im Ermessen	im Ermessen	empfohlen	erwartet

	↓	↓	↓	↓
Spezielle Governance-Strukturen bezüglich des Aufsichtsrats/Beirats	**im Ermessen**	**empfohlen**	**erwartet**	**erwartet**
Einrichtung eines Ausschusses, der sich mit Compliance beschäftigt (z.B. Prüfungsausschusses/Audit Committee)	im Ermessen	im Ermessen	im Ermessen	empfohlen
Aufsichtsrat hat die Pflicht, die Inhalte für die Compliance-Berichterstattung festzulegen, einschließlich der Berichterstattung über Fälle von Non-Compliance	im Ermessen	im Ermessen	erwartet	erwartet
Feststellung der Effektivität des CMS (z.B. durch Berichterstattung über interne/externe Prüfungsmaßnahmen)	im Ermessen	empfohlen	erwartet	erwartet

Empfehlungen und Hinweise für die Umsetzung

Compliance-Governance und operative Umsetzung von Compliance

- ✓ Die Primärverantwortung für Compliance liegt bei der Geschäftsleitung

  Primärverantwortung für Compliance

- ✓ Die Compliance-Funktion, d.h. die Erfüllung der Compliance-Aufgaben, kann von der Geschäftsleitung selbst wahrgenommen werden

  Wahrnehmung der Compliance-Funktion durch Geschäftsleitung

- ✓ Besteht die Geschäftsleitung aus mehreren Personen, so sind klare Zuständigkeiten festzulegen. Dabei kann die Verantwortung für Compliance im Wege der Geschäftsverteilung einem Mitglied der Geschäftsleitung übertragen werden.

  Übertragung der Compliance-Verantwortung im Wege der Geschäftsverteilung

- ✓ Um das operative Geschäft zu erleichtern und die Geschäftsleitung zu entlasten, können[18]
  - die Compliance-Funktion (*nicht aber die Verantwortung für Compliance!*) von der Geschäftsleitung an eine nachgeordnete Person delegiert werden

    oder
  - einzelne Compliance-Aufgaben an nachgeordnete Personen delegiert werden

    Delegation von Compliance an nachgeordnete Ebenen

- ✓ Erfolgt die Delegation der Compliance-Funktion an eine nachgeordnete Person/Stelle, so muss diese Person unabhängig und mit weitreichenden Kompetenzen ausgestattet sein und daher auf einer entsprechenden Hierarchiestufe im Unternehmen angesiedelt sein (*mindestens 3. Führungsebene*)

- ✓ Im Rahmen der Delegation von Compliance ist weiterhin zu beachten:
  - Es hat eine sorgfältige Auswahl der mit Compliance-Aufgaben betrauten Person(en), insbesondere bezüglich der persönlichen Eignung und Zuverlässigkeit, zu erfolgen
  - Zur Vermeidung von Doppelverantwortlichkeiten sind klare Kompetenzen und eindeutige Verantwortlichkeiten festzulegen
  - Die Geschäftsleitung hat entsprechende Überwachungs- und Kontrollmaßnahmen vorzunehmen, ob die delegierten Compliance-Aufgaben von den jeweiligen Personen ordnungsgemäß ausgeführt werden. Werden Überwachungsaufgaben delegiert, so sind auch die mit Überwachungs- und Kontrollaufgaben betrauten Personen regelmäßig daraufhin zu überwachen, ob sie ihren Kontrollaufgaben ordnungsgemäß nachgekommen sind

- ✓ Der Compliance-Funktion sind ausreichende Ressourcen für die ordnungsgemäße Erfüllung der Compliance-Aufgaben zur Verfügung zu stellen. Hierzu zählen insbesondere

  Angemessene Ressourcenausstattung der Compliance-Organisation
  - ausreichende personelle Ressourcen (mindestens 1 Vollzeitäquivalent je 2.000 Mitarbeiter)
  - die Ausstattung der Compliance-Funktion sowie der mit Compliance beauftragten Personen mit den notwendigen Kompetenzen, Kenntnissen, finanziellen Mitteln, erforderlichen Zeit etc.

Aufgaben und Tätigkeitsbereich der Compliance-Funktion

- ✓ Zu den wesentlichen Aufgaben der Compliance-Funktion gehören:[18]

  Wesentliche Aufgaben der Compliance-Funktion
  - Die Ermittlung und Beurteilung der Compliance-Risiken des Unternehmens
  - Die Pflicht zur Verhinderung von geplanten Straftaten im Unternehmen, von denen sie Kenntnis erlangt
  - Die Erstellung, Einführung und Kommunikation von Verhaltensgrundsätzen und -richtlinien
  - Sicherstellung funktionsfähiger Due Diligence-Maßnahmen und Beratung der durchführenden Funktionen
  - Die Veranlassung und ggf. Durchführung von Sensibilisierungs- und Schulungsmaßnahmen zu Compliance und Integrity
  - Die Veranlassung und Durchführung von Kontroll- und Überwachungsmaßnahmen
  - Zur Verfügung stehen als Berater und Ansprechpartner für die Geschäftsleitung, Führungskräfte und Mitarbeiter zu Compliance-relevanten Themen
  - Die Durchführung bzw. Veranlassung von Untersuchungsmaßnahmen bei möglichen Compliance-Verstößen
  - Das Ergreifen von Abhilfemaßnahmen im Falle der Kenntnis von Compliance-Defiziten
  - Eine regelmäßige Berichterstattung an die Geschäftsleitung, sofern die Compliance-Funktion oder einzelne Compliance-Aufgaben delegiert worden sind

[18] Empfehlungen zu der Umsetzung der verschiedenen Compliance-Aufgaben finden sich in den weiteren Ausführungen zu dem jeweiligen Compliance-Element in dieser Leitlinie.

Einrichtung eines Berichtswesens zu Compliance

- ✓ Die Geschäftsleitung hat ein Informationswesen einzurichten, damit die verantwortlichen Unternehmensorgane über Compliance-relevante Vorgänge und Themen stets informiert sind

  Einrichtung eines Berichtswesens zu Compliance

  - Wird die Compliance-Funktion von der Geschäftsleitung selbst ausgeübt, so hat die Geschäftsleitung gegenüber den Mitarbeitern klar zu kommunizieren, dass festgestellte Compliance-Mängel, auftretende Risiken etc. der Geschäftsleitung mitzuteilen sind
  - Wurde die Compliance-Funktion von der Geschäftsleitung delegiert, so

    Berichtspflicht des Compliance-Verantwortlichen

    - sind die Berichtspflicht und Berichtslinie des Compliance-Beauftragten festzulegen (es empfiehlt sich entweder eine direkte Berichtslinie an die Geschäftsleitung bzw. an das mit Compliance verantwortete Mitglied der Geschäftsleitung oder eine Berichtspflicht an den unmittelbaren Vorgesetzten des Compliance-Beauftragten festzulegen, der wiederum der Geschäftsleitung entsprechend zu berichten hat)
    - hat eine regelmäßige und ad-hoc Berichterstattung des Compliance-Beauftragten an die Geschäftsleitung, z.B. im Rahmen von Jours Fixes oder Besprechungen, zu erfolgen
    - sollte der Zugang des Compliance-Beauftragten zur Geschäftsleitung jederzeit möglich sein

      Jederzeitiger Zugang des Compliance-Verantwortlichen zur Geschäftsleitung

- ✓ Hat das Unternehmen ein Aufsichtsgremium (Aufsichtsrat/Beirat), so hat dieses die Geschäftsführung zu überwachen. Zur ordnungsgemäßen Ausübung der Überwachungsaufgaben ist erforderlich, dass die Geschäftsleitung das Aufsichtsgremium auch entsprechend über das CMS im Unternehmen unterrichtet, weshalb mindestens jährlich sowie ad-hoc eine Compliance-Berichterstattung der Geschäftsleitung an das Aufsichtsgremium zu erfolgen hat
- ✓ Die Berichterstattung ist entsprechend zu dokumentieren

  Dokumentation der Berichterstattung

Spezielle Governance-Strukturen bezüglich des Aufsichtsrats/Beirats

- ✓ Bei Aktiengesellschaften ist ein Aufsichtsrat zwingend vorgesehen, dem eine Beratungs- sowie Überwachungsfunktion im Unternehmen zukommt

  Überwachungs- und Beratungsfunktion des Aufsichtsrats

- ✓ Bei anderen Gesellschaftsformen wie der GbR, OHG, GmbH etc. kann es sich empfehlen, die Einrichtung eines Beirats mit Beratungs- und Überwachungsfunktion zu beschließen
- ✓ Aufsichtsrat und Beirat sind bei der Kenntnisnahme von Missständen im Unternehmen zum Einschreiten verpflichtet

Verhaltensgrundsätze
und -richtlinien

3

CMS-ELEMENT

Die Komplexität unternehmerischen Handelns verlangt die Implementierung von internen Verhaltensgrundsätzen und -richtlinien, um Mitarbeitern die notwendige Orientierung für die Ausübung ihrer geschäftlichen Tätigkeit zu geben. Geeignete allgemeine Verhaltensgrundsätze und -richtlinien basieren auf den schriftlich niedergelegten oder tradierten spezifischen Unternehmenswerten und legen die von der Geschäftsleitung gewünschte Geschäftsethik und die daraus hervorgehenden Erwartungen an das Verhalten von Führungskräften und Mitarbeitern im täglichen Geschäft fest. Dabei geht es jedoch nicht nur darum, Regeln und Verbote aufzustellen. Vielmehr sollen die Verhaltensgrundsätze und -richtlinien den Rahmen abstecken, in dem Führungskräfte und Mitarbeiter selbstverantwortlich für das Unternehmen handeln. Die Verhaltensgrundsätze und -richtlinien geben den Mitarbeitern Handlungsorientierung.

Wichtig dabei ist, die Verhaltensgrundsätze und -richtlinien klar und eindeutig an alle Mitarbeiter zu kommunizieren. Denn erst wenn die Erwartungen des Managements an das Verhalten der Mitarbeiter klar sind, werden Verhaltensgrundsätze und -richtlinien zur Zielerreichung – der Vermeidung kriminellen und unethischen Verhaltens im Geschäftsverkehr – auch tatsächlich beitragen.

Zielsetzungen des CMS-Elements
Verhaltensgrundsätze und -richtlinien

- ✓ Wissensvermittlung zu den geltenden Regeln im Geschäftsverkehr
- ✓ Handlungsorientierung für die Mitarbeiter
- ✓ Förderung von Vertrauen und Motivation der Mitarbeiter
- ✓ Schaffung von Vertrauen und Verbindlichkeit gegenüber den relevanten Stakeholdern (Anteilseigner, Mitarbeiter, Geschäftspartner, Öffentlichkeit etc.)

INSTRUMENTE Für Unternehmen mit einer Mitarbeiteranzahl von	LEITLINIE 1 bis 250	LEITLINIE 2 250 – 3.000	LEITLINIE 3 3.000 – 20.000	LEITLINIE 4 mehr als 20.000
	↓	↓	↓	↓
Verhaltenskodex (Code of Ethics/Code of Conduct)	**erwartet**	**erwartet**	**erwartet**	**erwartet**
Schriftliche Fixierung eines Verhaltenskodex und Bekanntmachung an die Mitarbeiter	erwartet	erwartet	erwartet	erwartet
Schriftliche Fixierung und Bekanntmachung von Verhaltensrichtlinien, die die Regelungen des Verhaltenskodex spezifizieren (z.B. Richtlinie zum Umgang mit Geschenken und Zuwendungen, Antikorruptionsrichtlinie)	im Ermessen	empfohlen	erwartet	erwartet
Schriftliche Fixierung eines Notfallplans (Checklisten, Handlungsanweisungen) im Falle des Auftretens unvorhergesehener Umstände (z.B. schwerwiegende Compliance-Verstöße, Umgang mit unvorhergesehenen behördlichen Durchsuchungen, Beschlagnahmen) und Vermittlung an relevante Mitarbeiter	erwartet	erwartet	erwartet	erwartet

Empfehlungen und Hinweise für die Umsetzung

Verhaltenskodex

Schriftliche Fixierung und Bekanntmachung eines Verhaltens-kodex

- ✓ Die allgemeinen Verhaltensgrundsätze sind in einem Verhaltenskodex – auch Code of Conduct oder Code of Ethics genannt – schriftlich zu fixieren und den Mitarbeitern bekannt zu machen
- ✓ Die allgemeinen Erwartungen zum Mitarbeiterverhalten im Rahmen der dienstlichen Tätigkeit sind grundsätzlich abzuleiten aus
  - den geltenden Rechtsvorschriften
  - der vom Unternehmen definierten Werte/Geschäftsethik (wie z.B. fairer Umgang mit Mitarbeitern, Kollegen und Geschäftspartnern)
  - allgemeinen Werten wie Ehrlichkeit, Zuverlässigkeit, Vertrauen, gegenseitiger Respekt
- ✓ In kleineren Unternehmen kann ein knapp gehaltener Verhaltenskodex, in dem die wesentlichen Unternehmenswerte schriftlich festgehalten sind, ausreichend sein

Implementierung des Verhaltenskodex

Implementierung des Verhaltens-kodex und der Verhaltens-richtlinien

- ✓ Um Verständnis und Akzeptanz des Verhaltenskodex seitens der Mitarbeiter zu erreichen, sollten die Mitarbeiter frühzeitig in den Entstehungsprozess des Verhaltenskodex (z.B. Definition der Unternehmenswerte) eingebunden werden
- ✓ Der Verhaltenskodex ist klar und in einfacher Sprache zu verfassen, damit er von jedem Mitarbeiter verstanden werden kann
- ✓ Die Bekanntmachung des Verhaltenskodex kann erfolgen durch
  - Aushändigung eines Exemplars an jeden Mitarbeiter
  - Aushänge/Poster an zentralen Stellen im Unternehmen
  - Emailversand
- ✓ Es empfiehlt sich, die zentralen Inhalte des Verhaltenskodex den Mitarbeitern stets präsent zu halten z.B. in Form von Aushängen, Postern

Implementierung eines Notfallplans

Notfallplan

- ✓ Schriftliche Fixierung eines Notfallplans (z.B. Checklisten mit konkreten Handlungsanweisungen), der Handlungsorientierung in unerwarteten Situationen gibt (z.B. im Falle der Kenntnisnahme von schwerwiegenden Compliance-Verstößen; bei unvorhergesehenen behördlichen Durchsuchungen und Beschlagnahmen)
- ✓ In einem solchen Notfallplan ist z.B. festzulegen, wie die Beschäftigten sich in unvorhergesehenen Situationen zu verhalten haben sowie welche Personen zwingend zu informieren sind und wer dessen Stellvertreter sind, falls die verantwortliche Person nicht erreicht werden kann
- ✓ Die Checklisten, Handlungsanweisungen etc. sind den relevanten Mitarbeitern (z.B. Empfang, Pforte) zu vermitteln
- ✓ Das richtige Verhalten im Notfall sollte mit den relevanten Mitarbeitern (z.B. durch Simulierung des Notfalls) entsprechend trainiert werden

Geschäftspartnerprüfung

CMS-ELEMENT

4

Unternehmen arbeiten mit den unterschiedlichsten Geschäftspartnern – wie Lieferanten, Kunden, Vermittler, Joint-Venture-Partnern – zusammen. Je größer dabei ein Unternehmen ist, desto unterschiedlicher und zahlreicher werden auch die Geschäftspartner wie z.B. Kunden, Lieferanten, Handelsvertreter, Geschäftsvermittler, Joint-Venture-Partner, Berater, Zollagenten, Personaldienstleister sein. Die Gefahren, die von der Zusammenarbeit mit unseriösen Geschäftspartnern ausgehen können, sind für das Unternehmen sehr groß. Denn rechtswidriges Verhalten sowie ethisch fragwürdige Praktiken eines Geschäftspartners bergen neben operativen und finanziellen Risiken ein hohes Reputationsrisiko für das Unternehmen selbst.

Mit einer Geschäftspartnerprüfung sollen sowohl die rechtlichen, wirtschaftlichen und Reputationsrisiken für das eigene Unternehmen als auch die Chancen einer geschäftlichen Zusammenarbeit mit Dritten geprüft und beurteilt werden. Eine Überprüfung der Geschäftspartner auf deren Integrität und Zuverlässigkeit hin ermöglicht dem Unternehmen, sich ein Bild von seinen Geschäftspartnern zu machen und sich zu vergewissern, ob es sich um einen integren und vertrauenswürdigen Partner handelt oder ob eher Abstand von der Zusammenarbeit genommen werden sollte. Somit lassen sich die Risiken aus einer Zusammenarbeit mit Dritten erheblich reduzieren und dienen mithin dem Schutz des Unternehmens und seiner Mitarbeiter vor Schäden.

Zielsetzungen des CMS-Elements Geschäftspartnerprüfung

- ✓ Vermeidung bzw. Reduzierung von rechtlichen, wirtschaftlichen und Reputationsrisiken, die aus einer geschäftlichen Beziehung entstehen können
- ✓ Prüfung von Chancen einer geschäftlichen Zusammenarbeit mit Dritten

INSTRUMENTE Für Unternehmen mit einer Mitarbeiteranzahl von	LEITLINIE 1 bis 250	LEITLINIE 2 250 – 3.000	LEITLINIE 3 3.000 – 20.000	LEITLINIE 4 mehr als 20.000
Sorgfältige Auswahl der Geschäftspartner	**erwartet**	**erwartet**	**erwartet**	**erwartet**
Stammdaten-Erhebung zu jedem Geschäftspartner	erwartet	erwartet	erwartet	erwartet
Kurze Überprüfung jedes Geschäftspartners auf erhöhtes Risiko anhand von Checklisten, Red Flags etc.	erwartet	erwartet	erwartet	erwartet
Standardisierter Abgleich von Geschäftspartnern mit Sanktions- und Anti-Terrorlisten	erwartet	erwartet	erwartet	erwartet
Durchführung intensiverer Prüfungsmaßnahmen bei Geschäftspartnern mit erhöhtem Risiko	erwartet	erwartet	erwartet	erwartet
Festlegung von Entscheidungverantwortlichkeiten/ Genehmigungsprozessen	**erwartet**	**erwartet**	**erwartet**	**erwartet**
Bei erhöhtem Risiko Einbindung des Compliance-Beauftragten bzw. anderer geeigneter Stellen in die Genehmigungsprozesse (unter Wahrung des Prinzips der Funktionstrennung)	erwartet	erwartet	erwartet	erwartet
Aufrechterhaltung der Geschäftsbeziehungen	**erwartet**	**erwartet**	**erwartet**	**erwartet**
Einbindung von Compliance-Klauseln in Verträge mit Geschäftspartnern oder Einholung schriftlicher Compliance-Erklärungen der Geschäftspartner	empfohlen	empfohlen	erwartet	erwartet

INSTRUMENTE Für Unternehmen mit einer Mitarbeiteranzahl von	LEITLINIE 1 bis 250	LEITLINIE 2 250 – 3.000	LEITLINIE 3 3.000 – 20.000	LEITLINIE 4 mehr als 20.000
	↓	↓	↓	↓
Schriftliche Festlegung von vertraglicher Leistung und Provisionshöhe bei Verträgen mit Vertriebsmittlern/-agenten	erwartet	erwartet	erwartet	erwartet
Überprüfung bestehender Geschäftspartner bei Eintritt besonderer Umstände (z.B. Veränderungen der Eignerstruktur, Bekanntwerden negativer Hinweise)	erwartet	erwartet	erwartet	erwartet
Regelmäßige und turnusmäßige Überprüfung aller im Rahmen der Compliance-Risikoanalyse als risikobehaftet identifizierten Geschäftspartner inkl. Vertragsprüfung	empfohlen	empfohlen	empfohlen	erwartet

Empfehlungen und Hinweise für die Umsetzung

Sorgfältige Auswahl der Geschäftspartner

Grundlegende Prüfungsmaßnahmen (Basisprüfung)

- ✓ Zu jedem Geschäftspartner sind grundlegende Prüfungsmaßnahmen (Basisprüfung) erforderlich. Diese umfassen die Erhebung der wesentlichen Stammdaten wie z.B.
  - Kontaktdaten, wie Name, Adresse, Telefonnummer
  - Bank- und Steuerdaten
  - Rechtsform und Eigentümerstruktur
  - Handelsregisternummer
  - Rechnungsanschrift
- ✓ Es ist eine kurze Risikoprüfung vorzunehmen, ob besondere Umstände auf ein erhöhtes Risiko aus einer vertraglichen Beziehung mit dem Geschäftspartner hindeuten können. Merkmale für ein erhöhtes Risiko können sein:
  - Der Geschäftspartner ist nahezu unbekannt und hat den Sitz im Ausland
  - Der Geschäftspartner hat seinen Sitz in einem ausländischen Staat mit politisch oder wirtschaftlich instabiler bzw. ungewisser Lage
  - Erhöhtes Branchenrisiko des Geschäftspartners (z.B. Rüstungsindustrie)
  - Das beabsichtigte Geschäft überschreitet ein bestimmtes vom Unternehmen festgelegtes, kritisches Auftragsvolumen
  - Mit dem Geschäftspartner soll eine Unternehmenskooperation (z.B. Joint Venture) eingegangen werden
  - Bei dem Geschäftspartner handelt es sich um ein Zielunternehmen, das von dem Unternehmen käuflich erworben werden soll
  - Der Geschäftspartner soll für das Unternehmen im Ausland Beratungsdienstleistungen erbringen

Intensivere Prüfungsmaßnahmen

- ✓ Intensivere Prüfungsmaßnahmen hat das Unternehmen vorzunehmen,
  - wenn im Rahmen der zuvor vorgenommenen Risikobewertung des Geschäftspartners bzw. der Geschäftsbeziehung Umstände festgestellt werden, die auf ein erhöhtes Risiko im Falle einer vertraglichen Beziehung hinweisen
  - falls dem Unternehmen im Laufe einer bereits bestehenden Geschäftsbeziehung besondere Umstände bekannt werden. Hierzu zählen z.B.

- Eintritt von wesentlichen Veränderungen beim Geschäftspartner (z.B. Änderungen in der Eigentümerstruktur)
- Bekanntwerden von negativen Hinweisen über den Geschäftspartner (wie z.B. kriminelles Verhalten oder ethisch fragwürdige Geschäftspraktiken, drohende Insolvenz)

✓ Die Tiefe und der Umfang der intensiveren Prüfungsmaßnahmen haben sich an der Höhe des Risikos der beabsichtigen Geschäftsbeziehung mit dem Geschäftspartner auszurichten. Zu geeigneten intensiveren Prüfungsmaßnahmen zählen z.B. — Tiefe und Umfang der Prüfungsmaßnahmen

- Einholung einer Selbstauskunft des Geschäftspartners
- Beschaffung eines Handelsregisterauszugs (insbesondere zur Prüfung der Eigentümerstruktur)
- eigene Prüfung über frei verfügbare Quellen wie das Internet (z.B. können über den elektronischen Bundesanzeiger Veröffentlichungen, Bekanntmachungen und rechtlich rrelevante Unternehmensnachrichten gesucht werden; googeln; Pressemeldungen etc.)
- Prüfung des Kreditausfallrisikos (Insolvenzrisiko, Branchenrisiko)
- Bei ausländischen Geschäftspartnern oder Geschäften im Ausland sind die Länderrisiken zu prüfen (z.B. CPI, Abgleich des Geschäftspartners mit den Anti-Terrorlisten der Europäischen Union und/oder USA)
- Prüfung der Verträge mit Vertriebsmittlern und -agenten, ob die vertraglich geschuldete Leistung schriftlich fixiert wurde und zu der Provisionshöhe in einem angemessenen Verhältnis steht
- Vor-Ort-Besichtigung/Audit beim Geschäftspartner

Durchführung der Überprüfung, Entscheidungsverantwortlichkeiten und Genehmigungsprozesse

✓ Bezüglich neuer Geschäftspartner müssen sämtliche erforderliche Prüfungsmaßnahmen bereits während der Vertragsanbahnung, spätestens vor Vertragsabschluss erfolgt sein — Durchführung der Prüfungsmaßnahmen

✓ In kleineren Unternehmen, deren jährlicher Neukundenzuwachs in einem überschaubaren Rahmen liegt, kann es sich empfehlen, die Durchführung der Prüfungsmaßnahmen einer Person im Unternehmen zuzuweisen, z.B. der Buchhaltung, einem Vertriebsmitarbeiter

✓ Mit zunehmender Anzahl unterschiedlichster Geschäftspartner wie Kunden, Lieferanten etc. kann es empfehlenswert sein, die Durchführung der Geschäftspartnerprüfung bereichsbezogen festzulegen (z.B. Prüfung von Lieferanten durch den Einkauf, Prüfung von Kunden durch den Verkauf)

✓ Bei Vorliegen eines erhöhten Geschäftspartnerrisikos

- ist die Geschäftsleitung bzw. der Compliance-Beauftragte oder eine andere entsprechend bevollmächtigte Person im Unternehmen zur Entscheidung über die weiteren Handlungsoptionen hinzuziehen. — Entscheidungsverantwortlichkeiten
- ist der Genehmigungsprozess so festzulegen, dass die Genehmigung durch eine von der mit der Durchführung der Geschäftspartnerprüfung beauftragten Person unabhängige Stelle erfolgt (Funktionstrennungsprinzip) — Genehmigungsprozess

✓ Sämtliche Prüfungsmaßnahmen (Basisprüfung sowie intensivere Prüfung) sollten anhand von Checklisten oder einfachen Fragebögen erfolgen, um die Einheitlichkeit und Vollständigkeit der Datenerfassung sicherzustellen. Checklisten oder einfache Fragebögen können Orientierung geben

- bzgl. der Kategorisierung der Geschäftspartner in die jeweilige Risikoklasse
- zu der Stammdatenerfassung
- bzgl. der vorzunehmenden intensiveren Überprüfungsmaßnahmen
- zu besonderen Warnhinweisen (sog. Red Flags), die sofort auf ein erhöhtes Risiko hinweisen
- unter welchen Voraussetzungen der Vorgesetzte hinzuzuziehen ist

✓ Im Unternehmen ist ein Prozess festzulegen, wie und unter welchen Voraussetzungen ein Abgleich von Geschäftspartnern mit Sanktions- und Anti-Terrorlisten zu erfolgen hat — Abgleich von Geschäftspartnern mit Sanktions- und Anti-Terrorlisten

✓ Bei der Durchführung der Geschäftspartnerprüfung sind von dem Unternehmen die geltenden Datenschutzregelungen zu beachten

✓ Das Unternehmen sollte im Vorfeld verschiedene Entscheidungsoptionen festlegen wie z.B. — Festlegung von Entscheidungsoptionen

- Eingehen der Geschäftsbeziehung ohne weitere erforderliche Maßnahmen z.B. weil Stammdaten des Geschäftspartners ohne Schwierigkeiten vollständig zu beschaffen und keine Umstände bekannt sind, die auf ein erhöhtes Risiko aus einer Geschäftsbeziehung hindeuten

- Vornahme weiterer intensiver Prüfungsmaßnahmen ggf. unter Einbeziehung spezialisierter Dienstleister/Experten im Falle von Hinweisen auf ein erhöhtes Risiko einer Geschäftspartnerbeziehung
- Nichtaufnahme bzw. der Abbruch der Geschäftsbeziehung z.B. falls Negativmeldungen über den Geschäftspartner zu kriminellem Verhalten oder ethisch fragwürdigen Geschäftspraktiken bekannt werden

Aufrechterhaltung von Geschäftsbeziehungen

- ✓ Für den Abschluss von Verträgen empfiehlt es sich,
  - schriftliche Compliance-Erklärungen der Geschäftspartner anzufordern oder
  - Compliance-Klauseln in die Verträge einzubinden (z.B. Erwartungen des Unternehmens von legalem und integrem Geschäftsgebaren des Partners, Grunderwartungen an das CMS des Geschäftspartners, Sonderkündigungsrechte des Unternehmens im Falle schwerer Compliance-Verstöße durch den Geschäftspartner)

  Anfordern schriftlicher Compliance-Erklärungen oder Einbindung von Compliance-Klauseln in Verträge
- ✓ In Verträgen mit Vertriebsagenten/Mittlern sind die vertragliche Leistung sowie die entsprechende Provisionshöhe schriftlich festzulegen
- ✓ Wiederholte Prüfung von Geschäftspartnern bei Bekanntwerden besonderer Umstände (z.B. Veränderungen der Eignerstruktur, Bekanntwerden negativer Hinweise zu dem Geschäftspartner)
- ✓ Geschäftspartner, die im Rahmen der Compliance-Risikoanalyse als risikobehaftet eingestuft worden sind, sollten nicht nur vor Geschäftsaufnahme, sondern regelmäßig und turnusmäßig überprüft werden. Dabei sollte die Überprüfung auch eine erneute Prüfung der bestehenden Verträge umfassen.

  Regelmäßige und turnusmäßige Prüfung von Geschäftspartnern

Compliance-Kommunikation & Schulung

5

CMS-ELEMENT

Compliance Management kann nur dann funktionieren, wenn die einzelnen Compliance-Maßnahmen im Geschäftsalltag umgesetzt werden und die Unternehmenswerte die Basis für das tägliche Handeln im Unternehmen bilden. Damit die Mitarbeiter das CMS durch ihr Handeln mit Leben füllen können, liegt es in der Verantwortung der Geschäftsleitung, durch geeignete Compliance-Kommunikations- und Schulungsmaßnahmen eine Sensibilisierung und ein Bewusstsein für Compliance und Integrität im Geschäftsalltag zu schaffen sowie Kenntnis über und Verständnis für die mit dem CMS einhergehenden Erwartungen an das Verhalten der Mitarbeiter in ihrer geschäftlichen Tätigkeit zu erreichen. Dabei geht es nicht nur um die Vermittlung von Regeln, Vorgaben und Verboten, sondern vielmehr geht es darum, die Mitarbeiter zu integrem und selbstverantwortlichem Handeln zu befähigen und ihnen Handlungsorientierung für die Umsetzung von Compliance und Integrity im Rahmen ihrer beruflichen Tätigkeit zu geben.

Ein funktionsfähiges CMS schließt neben der Compliance-Kommunikation von oben nach unten ebenso einen Kommunikationskanal von unten nach oben ein. Die Compliance-Kommunikation ›bottom-up‹ ist insbesondere für die Aufdeckung von Missständen und Fehlverhalten im Unternehmen, aber auch für die kontinuierliche Verbesserung des CMS auf Basis von Rückmeldungen der Führungskräfte und Mitarbeiter unverzichtbar.

Zudem erstreckt sich Compliance-Kommunikation nicht nur auf die Mitarbeiter des Unternehmens, sondern auch auf externe Interessengruppen wie Kunden, Lieferanten und Fremdkapitalgeber. Zielsetzung externer Compliance-Kommunikation ist es, die Ernsthaftigkeit und Umsetzung des CMS glaubwürdig und transparent darzustellen, um so eine Reputation für Vertrauenswürdigkeit aufzubauen und die Geschäftsbeziehungen langfristig aufrechtzuerhalten.

Zielsetzungen des CMS-Elements
Compliance-Kommunikation & Schulung

- ✓ Wissensvermittlung und Sensibilisierung der Mitarbeiter
- ✓ Handlungsorientierung für Mitarbeiter und Befähigung zur Umsetzung der Erwartungen
- ✓ Herstellung von Glaubwürdigkeit und Transparenz über Verhalten und Geschäft des Unternehmens, vor allem gegenüber externen Stakeholdern
- ✓ Aufdeckung von Fehlverhalten und Missständen

INSTRUMENTE Für Unternehmen mit einer Mitarbeiteranzahl von	LEITLINIE 1 bis 250	LEITLINIE 2 250 – 3.000	LEITLINIE 3 3.000 – 20.000	LEITLINIE 4 mehr als 20.000
Interne Vermittlung und Kommunikation der Compliance-Regeln	**erwartet**	**erwartet**	**erwartet**	**erwartet**
Sicherstellung der Verteilung des Verhaltenskodex an die Mitarbeiter (z.B. elektronischer Versand, Verteilung mit der Gehaltsabrechnung)	erwartet	erwartet	erwartet	erwartet
Compliance-Funktion stellt Schulungs- und Informationsmaterial zu Compliance/Integrity zur Verfügung	im Ermessen	empfohlen	erwartet	erwartet
Veröffentlichung des Verhaltenskodex an geeigneter zentraler Stelle (z.B. Intranet)	erwartet	erwartet	erwartet	erwartet
Benennung eines Ansprechpartners für Compliance-Anliegen der Mitarbeiter	erwartet	erwartet	erwartet	erwartet
Einrichtung eines Internet- bzw. Intranetportals zu Compliance-Themen	im Ermessen	im Ermessen	erwartet	erwartet
Externe Kommunikation zu Compliance und Integrity	**erwartet**	**erwartet**	**erwartet**	**erwartet**
Direkte Kommunikation des Verhaltenskodex gegenüber relevanten Stakeholdern (z.B. Kunden, Lieferanten)	erwartet	erwartet	erwartet	erwartet
Veröffentlichung des Verhaltenskodex im Internet	empfohlen	empfohlen	erwartet	erwartet
Internetauftritt der Compliance-Funktion (z.B. Veröffentlichung des Verhaltenskodex, Ansprechpartner, Hotline)	im Ermessen	im Ermessen	empfohlen	erwartet

INSTRUMENTE Für Unternehmen mit einer Mitarbeiteranzahl von	LEITLINIE 1 bis 250	LEITLINIE 2 250 – 3.000	LEITLINIE 3 3.000 – 20.000	LEITLINIE 4 mehr als 20.000
Schulung von Unternehmensleitung und Aufsichtsrat/Beirat	**erwartet**	**erwartet**	**erwartet**	**erwartet**
Regelmäßige informale Schulung von Unternehmensleitung und Aufsichtsrat	erwartet	erwartet	erwartet	erwartet
Präsenzschulung/Workshop (intern/extern) der Unternehmensleitung zu Compliance und Integrity	erwartet	erwartet	erwartet	erwartet
Präsenzschulung/Workshop des Aufsichtsrats/Beirats zu Compliance und Integrity	erwartet	erwartet	erwartet	erwartet
Schulung von Mitarbeitern	**erwartet**	**erwartet**	**erwartet**	**erwartet**
Regelmäßige informale Schulung durch die Führungskräfte oder den Compliance-Beauftragten zu Compliance und Integrity anhand von Alltagsbeispielen (z.B. im Rahmen von Jours Fixes, Teammeetings)	erwartet	erwartet	erwartet	erwartet
Grundlegende Schulung zu Compliance und Integrity, insbesondere zu den Inhalten des Verhaltenskodex	empfohlen	empfohlen	erwartet	erwartet
Regelmäßige Präsenzschulung zu relevanten Themen im Bereich Compliance/Integrity durch Compliance-Beauftragten und/oder externe Referenten	im Ermessen	im Ermessen	erwartet	erwartet
Nutzung neuer Informationstechnologien für Compliance-Kommunikation und -Schulung (z.B. App, Podcast)	im Ermessen	im Ermessen	im Ermessen	empfohlen

Schulung von Mitarbeitern in sensiblen Funktionen	**erwartet**	**erwartet**	**erwartet**	**erwartet**
Regelmäßige Präsenzschulung zu relevanten aufgaben- und funktionsbezogenen Compliance-Themen durch Compliance-Beauftragten und/oder externe Referenten	erwartet	erwartet	erwartet	erwartet
Zusätzliche Schulung von Führungskräften	**im Ermessen**	**im Ermessen**	**erwartet**	**erwartet**
Compliance und Integrity sind Bestandteile von Seminaren/Trainings im Rahmen der Personalentwicklung von Führungskräften	erwartet	erwartet	erwartet	erwartet
Präsenzschulung von Führungskräften in sensiblen Geschäftsbereichen zu Compliance und Integrity durch Compliance-Beauftragten und/oder externe Referenten	erwartet	erwartet	erwartet	erwartet
Befähigung der Führungskräfte zur Durchführung von Compliance-Schulungen durch ›Train-the-Trainer‹-Konzept	im Ermessen	empfohlen	erwartet	erwartet
Schulung neuer Mitarbeiter	**erwartet**	**erwartet**	**erwartet**	**erwartet**
Informale Einführungsschulung zu Compliance und Integrity im Einstiegsgespräch neuer Mitarbeiter in sensiblen Bereichen durch Compliance-Funktion	erwartet	erwartet	erwartet	erwartet
Compliance und Integrity als Bestandteil der Einführungsschulung für relevante Mitarbeiter (Erstsensibilisierung durch Compliance-Funktion)	erwartet	erwartet	erwartet	erwartet

INSTRUMENTE Für Unternehmen mit einer Mitarbeiteranzahl von	LEITLINIE 1 bis 250	LEITLINIE 2 250 – 3.000	LEITLINIE 3 3.000 – 20.000	LEITLINIE 4 mehr als 20.000
Meldemöglichkeiten/Hinweisgebersystem	**erwartet**	**erwartet**	**erwartet**	**erwartet**
Unternehmen hat einen Prozess zur Meldemöglichkeit von Fehlverhalten für Mitarbeiter definiert und kommuniziert	erwartet	erwartet	erwartet	erwartet
Meldemöglichkeit direkt an Unternehmensleitung	erwartet	erwartet	erwartet	erwartet
Benennung einer internen Vertrauensperson	empfohlen	alternativ	erwartet	erwartet
Ombudsperson (externe Vertrauensperson)	empfohlen	alternativ	alternativ	alternativ
Elektronisches Hinweisgebersystem (anonym)	im Ermessen	alternativ	alternativ	alternativ
Telefonhotline (anonym)	im Ermessen	alternativ	alternativ	alternativ
Schriftliche Prozessdefinition bezüglich Meldungen und Umgang mit Meldungen zu möglichem Fehlverhalten (Verantwortlichkeiten, Eskalationsstufen)	im Ermessen	empfohlen	erwartet	erwartet

Empfehlungen und Hinweise für die Umsetzung

Compliance-Kommunikation

- ✓ Die interne Vermittlung und Kommunikation von Compliance und Integrity erfolgt durch:
  - Verteilung und Kommunikation des Verhaltenskodex an alle Mitarbeiter
  - Veröffentlichung des Verhaltenskodex an geeigneter zentraler Stelle
  - Ggf. Einrichtung eines Intranet-/Internetportals zu Compliance-Themen, in dem der Hintergrund und die Bedeutung von Compliance und Integrity verständlich erklärt sind, die relevanten Dokumente, vor allem der Verhaltenskodex, in der aktuellen Version hinterlegt und die jeweiligen Ansprechpartner (Compliance-Beauftragter) mit ihren Kontaktdaten aufgeführt sind

  Verteilung und Kommunikation des Verhaltenskodex

  Veröffentlichung des Verhaltenskodex

  Internet- oder Intranetportal zu Compliance-Themen

- ✓ Die interne Compliance-Kommunikation (Zielgruppe: Führungskräfte und Mitarbeiter) findet statt durch die tägliche Zusammenarbeit zwischen Geschäftsleitung, Führungskräften und Mitarbeitern:
  - Vorleben von Compliance-konformen und integrem Verhalten der Geschäftsleitung und Führungskräfte im täglichen Geschäft und der täglichen Zusammenarbeit
  - Einforderung von Compliance-konformen und integrem Verhalten der Mitarbeiter durch die Geschäftsleitung und Führungskräfte

  Interne Kommunikation zu Compliance und Integrity

- ✓ Für eine funktionierende Compliance-Kommunikation im Unternehmen hat eine klare, eindeutige und verständliche Kommunikation der Haltung der Geschäftsleitung zu Compliance und Integrity und deren Erwartungen an die Mitarbeiter zu erfolgen

- ✓ Sicherstellung der Möglichkeit der Compliance-Kommunikation ›von unten nach oben‹ durch
  - Benennung eines Ansprechpartners für Compliance-Anliegen der Mitarbeiter (Zugang und Erreichbarkeit der Geschäftsleitung, des Compliance-Beauftragten und der Führungskräfte für die Mitarbeiter bei Fragen, Unsicherheiten, Hinweisen etc.)
  - Einholung von Feedback zur Wahrnehmung und Umsetzung des CMS bei den Mitarbeitern sowie Möglichkeit zur Anregung von Verbesserungen, z.B. durch ein offenes Ohr in der täglichen Zusammenarbeit oder aktives Nachfragen in Team-Besprechungen oder sonstigen Meetings

  Ansprechpartner für Compliance-Anliegen

- ✓ Das Unternehmen hat die Themen Compliance und Integrity auch extern zu kommunizieren (Zielgruppen: Kunden, Lieferanten, Kapitalgeber, Öffentlichkeit). Im Rahmen der externen Kommunikation

  - ist der Verhaltenskodex gegenüber relevanten Stakeholdern (z.B. relevanten Kunden und Lieferanten) direkt zu kommunizieren (z.B. durch persönliche Übergabe, Versand)
  - sollte die Kommunikation zu Compliance und Integrity in den direkten Gesprächen und Verhandlungen der Geschäftsleitung, Führungskräfte und jeweiligen Mitarbeiter mit den Geschäftspartnern und externen Stakeholdern erfolgen
  - kann sich die Veröffentlichung des Verhaltenskodex im Internet empfehlen

  Externe Kommunikation zu Compliance und Integrity

- ✓ Die Compliance-Kommunikation muss kontinuierlich, verständlich, eindeutig und konsistent erfolgen.

Schulungen

- ✓ Alle Mitarbeiter sind hinsichtlich der wesentlichen für sie geltenden gesetzlichen Regelungen und der Bedeutung von Integrität für die Geschäftstätigkeit zu schulen und bezüglich der Relevanz von Compliance und Integrity auf ihre Arbeit zu sensibilisieren:

  - Compliance und Integrity bilden die Basis der täglichen Zusammenarbeit zwischen Geschäftsleitung/Führungskräften und Mitarbeitern

    Informale Compliance-Schulung durch Führungskräfte
  - zusätzlich empfiehlt sich die Durchführung einer grundlegenden Schulung zu Compliance und Integrity sowie zu den Inhalten des Verhaltenskodex

    Grundlegende Schulung zu Compliance und Integrity
  - Einführung zu Compliance und Integrity und Erstsensibilisierung neuer Mitarbeiter im Rahmen des Einstellungsgesprächs oder der Orientierungswoche/Einführung für neue Mitarbeiter und anschließend Integration der neuen Mitarbeiter in das bestehende Compliance-Schulungskonzept

    Schulung neuer Mitarbeiter
  - Mitarbeiter in sensiblen Funktionen, z.B. Einkauf, Vertrieb, sind besonders auf mögliche Compliance-Risiken wie Korruption hinzuweisen und hinsichtlich des Umgangs mit Dilemmasituationen funktionsbezogen zu schulen

    Zielgruppenorientierte Compliance-Schulungen

- ✓ Die Führungskräfte sind aufgrund ihrer Multiplikatoren- und Vorbildfunktion spezifisch zu Compliance und Integrity zu schulen und mit den entsprechenden Kompetenzen und Fähigkeiten auszustatten:

  - Integration der Themen Compliance und Integrity in die Schulungen, die im Rahmen der Personalentwicklung (PE) von Führungskräften durchgeführt werden (z.B. interne/externe Seminare, Trainings)

    Compliance und Integrity als Bestandteile von PE-Seminaren
  - Durchführung spezifischer und funktionsbezogener Präsenzschulungen zu Compliance und Integrity durch den Compliance-Beauftragten und/oder externe Referenten für Führungskräfte in sensiblen Geschäftsbereichen

- ✓ Auch Geschäftsleitung und Aufsichtsgremium (wie Aufsichtsrat und Beirat) sind regelmäßig zu Compliance und Integrity zu schulen, z.B. im Wege von

  - informalen Schulungsformaten, z.B. in moderierten Diskussionen der Mitglieder der Geschäftsleitung oder durch Selbststudium relevanter Literatur,
  - Präsenzschulungen/Workshops, ggf. durch Unterstützung externer Referenten/Berater

  Schulung von Geschäftsleitung und Aufsichtsrat/Beirat

- ✓ Die Schulungs- und Sensibilisierungsmaßnahmen

  - können durch die Geschäftsleitung persönlich, ggf. durch Unterstützung externer Fachleute/Berater, erfolgen. Zur Sicherstellung der Qualität der Schulungen kann es sinnvoll sein, dass sich die Geschäftsleitung im Vorfeld z.B. durch ein Coaching durch einen externen Experten oder das sog. Train-the-Trainer-Konzept die erforderlichen Kenntnisse und Fähigkeiten aneignet.

    Durchführung der Schulungen

    ***Train-the-Trainer*-Konzept**
  - sind auf die jeweilige Zielgruppe (Mitarbeiter, Fachbereiche, Führungskräfte, Geschäftsführung etc.) auszurichten und praxisnah zu gestalten

    Zielgruppenorientierung und Praxisrelevanz
  - müssen die notwendigen Inhalte vermitteln wie u.a.

    Inhalte der Compliance-Schulungen

    - Inhalte des Verhaltenskodex und damit einhergehende Anforderungen und Erwartungen an das Verhalten der Mitarbeiter
    - Darstellung der relevanten geltenden Gesetze und Regeln
    - unternehmens- und branchenspezifische Compliance-/Integrity-Risiken
    - Praxisfälle und Fallstudien zum Aufzeigen und Einüben von Lösungsstrategien aus kritischen Situationen und als Handlungsorientierung
    - Konsequenzen bei Fehlverhalten

Meldemöglichkeiten/Hinweisgebersystem

- ✓ Die Geschäftsleitung muss sicherstellen, dass entdeckte Missstände oder Fehlverhalten gemeldet werden können. Der Prozess zur Meldemöglichkeit von Fehlverhalten ist an die Mitarbeiter zu kommunizieren.

  Prozess zur Meldung von Fehlverhalten

- ✓ Für die Meldung von Missständen oder Fehlverhalten
  - muss für die Mitarbeiter ein direkter Kanal zur Verfügung stehen, d.h. die Möglichkeit bestehen, Missstände oder Fehlverhalten bei der Geschäftsleitung, dem direkten Vorgesetzen oder beim Compliance-Beauftragten ansprechen zu können

    Meldemöglichkeit an Geschäftsleitung

  - können weitere Meldemöglichkeiten empfehlenswert sein wie z.B.
    - die Benennung einer internen Vertrauensperson, die über das notwendige Fachwissen verfügt

      Interne Vertrauensperson
    - die Einrichtung eines elektronischen Briefkastens, der von der Geschäftsleitung oder dem Compliance-Beauftragten betreut wird
    - die Bestellung einer externen Vertrauensperson (sog. Ombudsperson wie z.B. externer Anwalt)

      Ombudsperson

- ✓ Es ist klar herauszustellen, dass das Meldesystem nicht für das Anbringen allgemeiner Beschwerden oder sonstiger Verleumdungen gedacht ist. Missbrauch des Meldesystems ist konsequent zu sanktionieren.
- ✓ Für das Funktionieren des Meldesystems ist zwingend sicherzustellen, dass der Hinweisgeber keinerlei Sanktionen oder Repressalien seitens der Geschäftsleitung und/oder anderer Mitarbeiter ausgesetzt ist.

Integration in HR-Prozesse

6

CMS-ELEMENT

Mitarbeiter sind die wichtigste Ressource eines Unternehmens. Sie sind es, die Compliance im Geschäftsalltag mit Leben füllen und umsetzen. Es sind aber auch die Mitarbeiter und Führungskräfte und deren Handlungen im Rahmen ihrer geschäftlichen Tätigkeit, die für das Unternehmen ein großes Risiko darstellen. Compliance Management verstanden als die Steuerung und Vermeidung von Risiken aus Fehlverhalten ist Mitarbeiterführung und muss in die entsprechenden Personalprozesse integriert und in der Personalarbeit verankert sein. Compliance Management fängt daher bereits bei der Auswahl von Mitarbeitern und Führungskräften an und setzt sich in der Personalentwicklung fort. Die Geschäftsleitung trägt die Verantwortung für die Sicherstellung einer sorgfältigen Personalauswahl im Rahmen der Personaleinstellungs- und -entwicklungsprozesse. Darüber hinaus bilden integritätsorientierte Anreiz- und Vergütungskonzepte sowie die konsequente Reaktion auf und Sanktionierung von Fehlverhalten oder Fällen von Non-Compliance (Abschreckungsfunktion) wichtige Instrumente für die Vermeidung und Reduzierung von Verhaltensrisiken.

Die Einbindung von Compliance in Personalprozesse trägt zu einer Sensibilisierung der Mitarbeiter für integres und erwünschtes Verhalten bei, die die Verbindlichkeit des CMS gegenüber Mitarbeitern wie auch externen Kooperationspartnern erhöht und die Glaubwürdigkeit des CMS insgesamt stärkt. Darüber hinaus fördern konsistente und transparente Personalprozesse die Mitarbeitermotivation und stärken die Loyalität der Mitarbeiter zum Unternehmen.

Zielsetzungen des CMS-Elements
Integration in HR-Prozesse

- ✓ Vermeidung von Verhaltensrisiken durch sorgfältige Personalauswahl
- ✓ Mitarbeiterbindung und Förderung der Mitarbeitermotivation
- ✓ Schaffung einer werteorientierten Unternehmenskultur
- ✓ Demonstration der Ernsthaftigkeit der Compliance-Bemühungen und der Konsequenz in der Durchsetzung
- ✓ Abschreckung geplanter Handlungen durch konsequente Sanktionierung von Fehlverhalten

INSTRUMENTE Für Unternehmen mit einer Mitarbeiteranzahl von	LEITLINIE 1 bis 250	LEITLINIE 2 250 – 3.000	LEITLINIE 3 3.000 – 20.000	LEITLINIE 4 mehr als 20.000
Unterstützende Compliance-Maßnahmen bei der Personalauswahl	**erwartet**	**erwartet**	**erwartet**	**erwartet**
Durchführung grundlegender Prüfmaßnahmen bei Neueinstellungen (z.B. Einsicht der Originalzeugnisse)	erwartet	erwartet	erwartet	erwartet
Backgroundcheck bei Einstellung von Geschäftsführern, Vorständen	erwartet	erwartet	erwartet	erwartet
Backgroundcheck bei Einstellung von Führungskräften mit erhöhtem Compliance-Risiko	empfohlen	empfohlen	erwartet	erwartet
Potenzialanalyse von Kandidaten für Führungs- und Schlüsselpositionen mit erhöhtem Compliance-Risiko auch bezüglich der persönlichen Integrität	im Ermessen	im Ermessen	empfohlen	erwartet
Unterstützende Compliance-Maßnahmen in den Personalprozessen und der Personalentwicklung	**erwartet**	**erwartet**	**erwartet**	**erwartet**
Verhaltenskodex als Bestandteil des Arbeitsverhältnisses	erwartet	erwartet	erwartet	erwartet
Unterzeichnung einer Erklärung der Einhaltung des Verhaltenskodex im eigenen Verantwortungsbereich (Geschäftseinheit, Landesgesellschaft) im abgelaufenen Geschäftsjahr durch die oberen Führungskräfte	im Ermessen	empfohlen	erwartet	erwartet
Compliance und Integrity als systematisches/formales Beurteilungskriterium in Personalgesprächen/Mitarbeiterbeurteilungen	empfohlen	empfohlen	erwartet	erwartet
Compliance und Führungsverhalten sind Kriterien der Führungskräftebeurteilung	erwartet	erwartet	erwartet	erwartet

INSTRUMENTE Für Unternehmen mit einer Mitarbeiteranzahl von	LEITLINIE 1 bis 250	LEITLINIE 2 250 – 3.000	LEITLINIE 3 3.000 – 20.000	LEITLINIE 4 mehr als 20.000
	↓	↓	↓	↓
Integration von Zielen für die Umsetzung des CMS in Zielvereinbarungen für obere Führungskräfte	im Ermessen	im Ermessen	erwartet	erwartet
Wiederholung der Hintergrundrecherchen für Personen, die in Schlüsselpositionen befördert werden	empfohlen	empfohlen	empfohlen	erwartet
Führungskräfteentwicklungsprogramm beinhaltet Rotation in mit Kontrollaufgaben befasste Funktionen (Interne Revision, Compliance, Risikomanagement)	im Ermessen	im Ermessen	empfohlen	empfohlen
Reaktion auf Fehlverhalten	**erwartet**	**erwartet**	**erwartet**	**erwartet**
Konsequente Sanktionierung von Fehlverhalten	erwartet	erwartet	erwartet	erwartet
Kommunikation möglicher Sanktionen auf Fehlverhalten von Mitarbeitern (arbeitsrechtliche, zivilrechtliche und strafrechtliche Konsequenzen etc.)	erwartet	erwartet	erwartet	erwartet
Überprüfung der bestehenden CMS-Prozesse und -Maßnahmen auf Schwachstellen und ggf. Anpassung (Remediation)	erwartet	erwartet	erwartet	erwartet

Empfehlungen und Hinweise für die Umsetzung

Personalauswahl

- ✓ Die Personalauswahl muss sorgfältig erfolgen und umfasst bestimmte Hintergrundrecherchen (sogenannte Backgroundchecks)
  - Grundlegende Prüfmaßnahmen (z.B. Abgleich von Zeugniskopien mit den Originaldokumenten, Google-Suche) sind grundsätzlich bei allen Stellenbesetzungen durchzuführen
  - Abhängig von der zu besetzenden Position (Geschäftsführer, Mitarbeiter und Führungskräfte in Schlüsselfunktionen oder in Funktionen mit erhöhtem Compliance-Risiko) hat ein umfassenderer Backgroundcheck zu erfolgen, der weitere Maßnahmen beinhaltet wie z.B.
    - Überprüfung der angegebenen früheren Arbeitgeber, z.B. durch Google-Suche
    - Anforderung eines polizeilichen Führungszeugnisses
    - Einholung von Referenzen
    - ggf. Einschaltung externer Dienstleister
  - Kritische Erkenntnisse einer ersten grundlegenden Überprüfung können, müssen aber nicht zwingend zum Abbruch der Gespräche führen, erfordern jedoch die Durchführung weiterer Prüfungsmaßnahmen (ggf. unterstützt durch externe Dienstleister wie Auskunfteien oder Detekteien).

Backgroundchecks

Grundlegende Prüfmaßahmen bei Neueinstellungen

Umfassendere Prüfungs-maßnahmen

Personalprozesse und Personalentwicklung

- ✓ Der Verhaltenskodex ist Bestandteil des Arbeitsverhältnisses (z.B. als Bestandteil des Arbeitsvertrages, Anlage zum Arbeitsvertrag)
- ✓ In Personalgesprächen und Mitarbeiterbeurteilungen sollten Compliance und Integrity bzw. das Verhalten des Mitarbeiters thematisiert und in die Beurteilung miteinbezogen werden.
- ✓ Ebenso sind Compliance und das Führungsverhalten als Beurteilungskriterien in der Führungskräftebeurteilung zu berücksichtigen.

Verhaltenskodex als Bestandteil des Arbeitsverhältnisses

Compliance und Integrity in Mitarbeiter-beurteilungen

Compliance und Integrity in Führungs-kräftebeurteilung

- ✓ Bei anstehenden Beförderungen von Personen in Schlüsselpositionen oder sensible Funktionen sind die Hintergrundrecherchen ggf. zu wiederholen (beispielsweise durch Einholung von Referenzen der Vorgesetzten oder einen Blick in die Personalakte)

  Hintergrundrecherchen bei Beförderungen

- ✓ Im Rahmen der Erfüllung der Fürsorgepflicht des Arbeitgebers kann es sich empfehlen, bei der Beobachtung von Auffälligkeiten (z.B. auffälliges Urlaubs- und/oder Arbeitsverhalten, aufwändiger Lebensstil, persönliche Notlagen) Unterstützungsleistungen für betroffene Mitarbeiter anzubieten

- ✓ Compliance und Integrity sollten in den Anreiz- und Vergütungssystemen Verankerung finden, z.B. durch
  - Sicherstellung einer angemessenen Bezahlung für die erwartete Arbeitsleistung
  - Vermeidung falscher Anreizsetzung in Gehalts- und Vergütungssystemen: unethisches Verhalten oder die Nichteinhaltung der Grundwerte und der Verhaltensrichtlinien von Mitarbeitern im Geschäftsalltag sind im Rahmen der Vergütungspolitik zu berücksichtigen und führen z.B. zu einer Nicht-Gewährung variabler Gehaltsbestandteile.

- ✓ Weitere personalpolitische Maßnahmen, die zur Vermeidung von Verhaltensrisiken und Fehlverhalten beitragen können, sind:
  - ggf. Personalrotationspläne (v.a. in Compliance-kritischen Abteilungen, um Seilschaften zu durchbrechen bzw. nicht erst entstehen zu lassen)
  - Regelung der Genehmigungs- bzw. Anzeigepflicht von Nebentätigkeiten der Mitarbeiter
  - Fairness und Transparenz in Personalprozessen und Personalpolitik
  - Einbindung des/der Personalleiters/Personalabteilung in Compliance-Maßnahmen, z.B. Durchführung von Schulungen/Trainings, Einführung von Arbeitsanweisungen

Reaktion auf Fehlverhalten

- ✓ Fehlverhalten von Mitarbeitern darf nicht geduldet werden und ist konsequent zu sanktionieren.

  Konsequente Sanktionierung von Fehlverhalten

- ✓ Die möglichen Sanktionen von Fehlverhalten müssen den Mitarbeitern kommuniziert werden (z.B. im Verhaltenskodex).

  Kommunikation möglicher Sanktionen

- ✓ Die Sanktionierung von Fehlverhalten erfolgt auf allen Hierarchieebenen konsequent und transparent.

- ✓ Bei der Sanktionierung von Fehlverhalten ist grundsätzlich das gesamte Spektrum möglicher Disziplinarmaßnahmen zu prüfen (arbeits-, zivil- und strafrechtliche Sanktionierung) und entsprechend durchzusetzen.

- ✓ Entdecktes Fehlverhalten ist auf die entsprechenden Gründe und Ursachen zu untersuchen. Bestehende Kontrollprozesse und Regelwerke sind auf Lücken zu überprüfen und, falls erforderlich, anzupassen bzw. zu verbessern (›Lessons learned‹).

  Überprüfung und Anpassung der bestehenden CMS-Prozesse und -Maßnahmen

Überwachungs- und Kontrollmaßnahmen

7

CMS-ELEMENT

Compliance kann in Unternehmen nur dann funktionieren, wenn die implementierten Maßnahmen von den Mitarbeitern auch tatsächlich umgesetzt, also gelebt werden. Mit Überwachungs- und Kontrollmaßnahmen wird das Ziel verfolgt, Fehler und Unregelmäßigkeiten im Unternehmen zu verhindern bzw. zu vermeiden sowie aufzudecken. Durch das Implementieren von Überwachungs- und Kontrollmaßnahmen erhöht das Unternehmen die Aufdeckungswahrscheinlichkeit von Fehlverhalten und sorgt damit zugleich für eine präventive Komponente, da es hierdurch den Mitarbeitern vor Augen hält, dass Verstöße durch das Unternehmen entdeckt und entsprechend sanktioniert werden können.

Darüber hinaus dienen Überwachungs- und Kontrollmaßnahmen dazu, das CMS insgesamt auf den Prüfstand zu stellen und mögliche Schwachstellen im CMS aufzudecken. Aus den Erkenntnissen der Überwachung und Kontrolle lassen sich entsprechende Gegenmaßnahmen zur Verbesserung oder Anpassung des CMS an geänderte Gegebenheiten ableiten und implementieren und stellen eine nachhaltige und dauerhafte Funktionalität des CMS sicher.

Zielsetzungen des CMS-Elements
Überwachungs- und Kontrollmaßnahmen

- ✓ Erhöhung der Entdeckungswahrscheinlichkeit von Fehlverhalten
- ✓ Verhinderung von Fehlverhalten aufgrund Abschreckungsfunktion
- ✓ Sicherstellung der Funktionsfähigkeit und Beachtung festgelegter Prozesse
- ✓ Beurteilung der Angemessenheit und Funktionsfähigkeit des CMS

INSTRUMENTE Für Unternehmen mit einer Mitarbeiteranzahl von	LEITLINIE 1 bis 250	LEITLINIE 2 250 – 3.000	LEITLINIE 3 3.000 – 20.000	LEITLINIE 4 mehr als 20.000
Prozessintegrierte Kontrollen	**erwartet**	**erwartet**	**erwartet**	**erwartet**
Vier-Augen-Prinzip in Geschäftsprozessen/-transaktionen mit erhöhten Compliance-Risiken	erwartet	erwartet	erwartet	erwartet
Funktionstrennungsprinzip (Segregation of Duties) in Geschäftsprozessen/-transaktionen mit erhöhten Compliance-Risiken	empfohlen	empfohlen	erwartet	erwartet
Vergabe von Zugangs- und Zugriffsberechtigungen	erwartet	erwartet	erwartet	erwartet
Prozessunabhängige/aufdeckende Kontrollen	**erwartet**	**erwartet**	**erwartet**	**erwartet**
Durchführung aufdeckender Kontrollen durch Vorgesetzte (Unternehmensleitung, Abteilungsleiter), regelmäßige Überprüfung von Geschäftsvorfällen (Stichproben)	erwartet	erwartet	erwartet	erwartet
Durchführung von Ordnungsmäßigkeitsprüfungen durch die Interne Revision	im Ermessen	empfohlen	alternativ	alternativ
Durchführung von Ordnungsmäßigkeitsprüfungen durch externe Dienstleister	im Ermessen	empfohlen	alternativ	alternativ
Zentrale Koordination und Berichtswesen bezüglich der Ordnungsmäßigkeitsprüfungen	im Ermessen	erwartet	erwartet	erwartet

INSTRUMENTE Für Unternehmen mit einer Mitarbeiteranzahl von	LEITLINIE 1 bis 250	LEITLINIE 2 250 – 3.000	LEITLINIE 3 3.000 – 20.000	LEITLINIE 4 mehr als 20.000
Monitoring & Review	**erwartet**	**erwartet**	**erwartet**	**erwartet**
Prüfung der Funktionsfähigkeit und Umsetzung des CMS durch geeignete interne Stellen (z.B. Interne Revision): *mindestens alle 3 Jahre*	erwartet	erwartet	erwartet	erwartet
Prüfung der Funktionsfähigkeit und Umsetzung des CMS unter Hinzuziehung externer Sachverständiger (z.B. Rechtsanwälte, Wirtschaftsprüfer, sonstige Berater)	im Ermessen	im Ermessen	empfohlen	empfohlen
Überprüfung der Geschäftsprozesse auf ihre Anfälligkeit für dolose Handlungen (Geschäftsprozessaufnahmen, Überprüfung der Wirksamkeit von Kontrollen)	im Ermessen	im Ermessen	empfohlen	empfohlen
Auswertung der Berichterstattung zum IKS, Compliance-relevante Feststellungen sind in der CMS-Beurteilung zu berücksichtigen	im Ermessen	empfohlen	erwartet	erwartet
Externe Prüfung/Zertifizierung des CMS	im Ermessen	im Ermessen	im Ermessen	im Ermessen
Dokumentation	**erwartet**	**erwartet**	**erwartet**	**erwartet**
Schriftliche Dokumentation der Überwachungs- und Kontrollmaßnahmen	erwartet	erwartet	erwartet	erwartet

Empfehlungen und Hinweise für die Umsetzung

Aufsichts- und Überwachungsmaßnahmen

- ✓ Die Geschäftsleitung trägt die Verantwortung für die Aufsicht und Überwachung bezüglich der Einhaltung von Compliance im Unternehmen

- ✓ Implementierung von prozessintegrierten Überwachungs- und Kontrollmaßnahmen innerhalb der Arbeitsabläufe. Hierzu zählen insbesondere

  - die Umsetzung des Vier-Augen-Prinzips in sensiblen Geschäftsprozessen/-transaktionen sowie in Bereichen und Funktionen mit erhöhtem Compliance-Risiko, das in diesen Bereichen grds. um das Prinzip der Funktionstrennung (Segregation of Duties) erweitert werden sollte
  - die Vergabe von Zugangs- und Zugriffsberechtigungen zu sensiblen Informationen und Daten nur an berechtigte Personen (Prinzip der Mindestinformation)

  Prozessintegrierte Kontrollen

- ✓ Zusätzlich zu den prozessintegrierten Überwachungsmaßnahmen hat die Geschäftsleitung regelmäßige prozessunabhängige, aufdeckende Kontrollmaßnahmen vorzunehmen (sog. Ordnungsmäßigkeitsprüfungen), die überprüfen, ob die Mitarbeiter die definierten Prozessabläufe tatsächlich eingehalten haben

  - Die Prüfungsmaßnahmen haben unangekündigte Überprüfungen der Geschäftsvorfälle im Wege von Stichproben zu umfassen
  - Die Durchführung dieser Prüfungsmaßnahmen kann von der Geschäftsleitung an geeignete Personen im Unternehmen delegiert werden (z.B. Mitarbeiter aus Stabs- und Linienabteilungen)
  - Im Falle der Delegation der Überwachungs- und Kontrollaufgaben hat die Geschäftsleitung eine regelmäßige Überprüfung vorzunehmen, ob die mit den Kontrollaufgaben verantworteten Personen ihrer Überwachungspflicht nachgekommen sind

  Prozessunabhängige Kontrollen/aufdeckende Kontrollmaßnahmen (Ordnungsmäßigkeitsprüfungen)

  Stichprobenartige Überprüfungen

- ✓ Umfang und Intensität der Überwachungsmaßnahmen haben sich zu richten nach

  - dem Risiko der jeweiligen Unternehmensbereiche
  - der Sensibilität der Funktionen (z.B. Personen mit Überweisungs- bzw. Zahlungsbefugnissen oder mit Zugang zu sensiblen Daten/Informationen)
  - der Sensibilität der Prozesse/Vorgänge (z.B. Buchungs-/Zahlungsvorgänge)
  - der Anzahl festgestellter Verstöße gegen Gesetze, Vorschriften, Prozesse, Arbeitsanweisungen etc. durch Mitarbeiter

  Umfang und Intensität der Überwachungsmaßnahmen

Monitoring & Review

- ✓ Die Geschäftsleitung hat regelmäßig (mindestens alle 3 Jahre) über geeignete interne Stellen (z.B. Interne Revision) prüfen zu lassen, ob und inwieweit die implementierten Compliance-Maßnahmen zur Vermeidung von Fehlverhalten angemessen sind und tatsächlich funktionieren können

  — Funktions-fähigkeitsprüfung

- ✓ Fehlen im Unternehmen das notwendige Fachwissen und die Erfahrung zur Durchführung einer Funktionsfähigkeitsprüfung, so sind externe Berater hinzuzuziehen

- ✓ Eine vorzeitige anlassbezogene Prüfung des CMS bzw. Teilen davon ist vorzunehmen
  - bei Bekanntwerden bzw. bei Hinweisen auf Compliance-Verstöße
  - bei Veränderung wesentlicher Faktoren (Änderung von Gesetzen, Änderung des Risikoprofils des Unternehmens etc.)

- ✓ Zur Prüfung und Beurteilung der Funktionalität der implementierten Compliance-Maßnahmen empfehlen sich weitere Maßnahmen wie z.B.
  - Interviews mit den Mitarbeitern anhand von Checklisten und Fragebögen zur Beurteilung der Angemessenheit und Funktionsfähigkeit der implementierten Compliance-Maßnahmen
  - Zugrundelegung verschiedener Compliance-Prüfstandards, die als Orientierung für die Beurteilung der Funktionsfähigkeit des CMS dienen können

- ✓ Unter Umständen kann es für ein Unternehmen vorteilhaft sein, sein CMS oder Teile davon einer externen Prüfung/Zertifizierung bzgl. der Funktionsfähigkeit zu unterziehen.

  — Externe Prüfung/ Zertifizierung des CMS

Dokumentation

- ✓ Sämtliche Überwachungs- und Kontrollmaßnahmen im Unternehmen sind zu dokumentieren.

  — Dokumentation der Überwachungs- und Kontroll-maßnahmen

Führung und Unternehmenskultur

8

CMS-ELEMENT

Der Führungsstil und das Führungsverhalten (*Leadership*) sowie die Kultur eines Unternehmens (*Corporate Culture*) bilden den Rahmen und gleichzeitig das Fundament eines nachhaltigen und funktionsfähigen Compliance-Management-Systems. Die Geschäftsleitung trägt die Verantwortung für Compliance und Integrität im Geschäft. Damit ist es ihre Aufgabe, geeignete Maßnahmen zur Sicherstellung von Compliance im Unternehmen einzuleiten. Ein Unterlassen kann zum einen zu erheblichen Schädigungen des Unternehmens aus ökonomischer Sicht und mit Blick auf die Unternehmensreputation führen. Zum anderen können sich aus der Nichterfüllung von Organisations- und Aufsichtspflichten persönliche Folgen für die Mitglieder der Geschäftsleitung ergeben – vom Personalwechsel bis hin zur Strafverfolgung und persönlichen Haftung. Bei der Umsetzung des CMS muss die Geschäftsleitung daher an erster Stelle mit gutem Beispiel und persönlichem Engagement voran gehen, auch aus persönlichem Eigenschutz. Ohne sichtbares Engagement und klares Eintreten der Geschäftsleitung und der Mitglieder der oberen Führungsebenen für Compliance und Integrität im Unternehmen werden das CMS und die Bemühungen darum die Ziele nicht erreichen können.

Zielsetzungen des CMS-Elements
Führung und Unternehmenskultur

- ✓ Vermittlung von Glaubwürdigkeit und der Bedeutung von Compliance und Integrität gegenüber den Mitarbeitern und externen Interessengruppen
- ✓ Sicherstellung von Integrität und Compliance im Geschäftsalltag
- ✓ Orientierung und Handlungsanleitung durch persönliches Vorbildverhalten und Engagement der Geschäftsleitung und Führungskräfte
- ✓ Stabilisierung der Kooperationsbeziehungen

INSTRUMENTE Für Unternehmen mit einer Mitarbeiteranzahl von	LEITLINIE 1 bis 250	LEITLINIE 2 250 – 3.000	LEITLINIE 3 3.000 – 20.000	LEITLINIE 4 mehr als 20.000
Tone from the Top	**erwartet**	**erwartet**	**erwartet**	**erwartet**
Unternehmensleitung kommuniziert regelmäßig zu Compliance und Integrity und den wesentlichen Verhaltenserwartungen an die Mitarbeiter	erwartet	erwartet	erwartet	erwartet
Unternehmensleitung und obere Führungskräfte positionieren sich klar zu integrem Verhalten im Geschäftsverkehr, insbesondere zu risikobehafteten/ konfliktträchtigen Entscheidungssituationen	erwartet	erwartet	erwartet	erwartet
Unternehmensleitung und obere Führungskräfte haben sich mit den Compliance-Risiken auseinandergesetzt und positionieren sich klar dazu	erwartet	erwartet	erwartet	erwartet
Tone from the Middle	**erwartet**	**erwartet**	**erwartet**	**erwartet**
Regelmäßige Kommunikation der Führungskräfte zu Compliance und Integrity bezogen auf den eigenen Verantwortungsbereich (aufgaben- und funktionsbezogene Spezifizierung der Verhaltenserwartungen)	erwartet	erwartet	erwartet	erwartet
Beurteilung der Unternehmenskultur und -integrität	**erwartet**	**erwartet**	**erwartet**	**erwartet**
Gespräche zwischen Unternehmensleitung, Führungskräften und Mitarbeitern	erwartet	erwartet	erwartet	erwartet
Integration von Fragen zu Compliance und Integrity in die allgemeine Mitarbeiterbefragung	im Ermessen	empfohlen	empfohlen	empfohlen

INSTRUMENTE Für Unternehmen mit einer Mitarbeiteranzahl von	LEITLINIE 1 bis 250	LEITLINIE 2 250 – 3.000	LEITLINIE 3 3.000 – 20.000	LEITLINIE 4 mehr als 20.000
	↓	↓	↓	↓
Integrity Barometer (spezifische Mitarbeiterbefragung)	im Ermessen	im Ermessen	empfohlen	empfohlen
Einholung von Feedback zum Führungsverhalten von Vorgesetzten (z.B. von Mitarbeitern, Kollegen, Kunden, Lieferanten)	im Ermessen	im Ermessen	empfohlen	empfohlen
Auswertung von Kennzahlen (Fluktuationsrate etc.)	im Ermessen	im Ermessen	empfohlen	empfohlen

Empfehlungen und Hinweise für die Umsetzung

Tone from the Top & Tone from the Middle

- ✓ Die Geschäftsleitung kommuniziert regelmäßig zu Compliance und Integrity sowie zu den Verhaltenserwartungen an die Mitarbeiter. Vor allem
  - positioniert sich die Geschäftsleitung klar zu integrem Verhalten im Geschäftsverkehr sowie zum Umgang mit risikobehafteten und konfliktträchtigen Entscheidungssituationen und
  - legt für alle Mitarbeiter wie auch für das eigene Verhalten dieselben Verhaltensmaßstäbe an (Selbstverpflichtung und Vorbildverhalten der Geschäftsleitung).

  Kommunikation der Geschäftsleitung

  Klare Positionierung des Topmanagements zu integrem Verhalten

- ✓ Geschäftsleitung und Führungskräfte haben sich mit den Compliance-Risiken auseinandergesetzt und positionieren sich klar dazu

  Auseinandersetzung mit den Compliance-Risiken

- ✓ Wesentliche Aspekte für das Setzen des ›richtigen‹ Tone from the Top sind:
  - Die Kommunikation erfolgt persönlich durch die Geschäftsleitung und kann
    - in der direkten Zusammenarbeit zwischen Geschäftsleitung und Mitarbeiter erfolgen sowie
    - in bestehende Besprechungen oder Termine (z.B. Betriebsversammlungen, Führungskräfte- oder Teammeetings) integriert werden
  - im Rahmen des Einstiegsgesprächs oder der Einführungsveranstaltung für neue Mitarbeiter
    - sollte die Geschäftsleitung persönlich die Unternehmenswerte sowie die Inhalte des Verhaltenskodex vorstellen und
    - ihre Bedeutung für die Geschäfte des Unternehmens das Verhalten der Mitarbeiter darlegen

- ✓ Die Führungskräfte übernehmen eine Botschafter-, Vermittlungs- und Übersetzungsfunktion für die Umsetzung von Compliance und Integrity im Geschäftsalltag.
  - Sie sind wichtige Multiplikatoren für Compliance und Integrity und kommunizieren regelmäßig zu Compliance und Integrity mit ihren Mitarbeitern (aufgaben- und funktionsbezogene Spezifizierung der Verhaltenserwartungen).

  Regelmäßige Kommunikation der Führungskräfte zu Compliance und Integrity

- In der Zusammenarbeit mit den Mitarbeitern sind sie Vorbild für integres Verhalten im Geschäft und Ansprechpartner für Mitarbeiter in kritischen Situationen und bei Unsicherheit.

Unternehmenskultur und Beurteilung von Kultur und Integrität im Unternehmen

- ✓ Entwicklung, Festlegung und Kommunikation unternehmensspezifischer Werte als Basis der Geschäftstätigkeit sowie als Handlungsorientierung für alle Mitarbeiter.

  Unternehmenswerte

  - Durch die Einbindung von Mitarbeitern und Führungskräften aus verschiedenen Bereichen in die Entwicklung spezifischer Unternehmenswerte (z.B. im Rahmen von Workshops) kann von Beginn an eine breitere Akzeptanz der Unternehmenswerte erreicht werden.
  - Die Vermittlung der Unternehmenswerte erfolgt durch Geschäftsleitung und Führungskräfte in der täglichen Zusammenarbeit und im direkten Dialog mit den Mitarbeitern

- ✓ Förderung und Etablierung einer offenen Kommunikationskultur, in der Mitarbeiter Unsicherheiten und Fragen vertrauensvoll und möglichst frühzeitig ansprechen, indem die Geschäftsleitung und Führungskräfte ihre Mitarbeiter zu Nachfragen ermutigen und jederzeit für die Mitarbeiter ansprechbar sind.

  Offene Kommunikationskultur

- ✓ Für die Beurteilung der Unternehmenskultur und -integrität

  Beurteilung der Unternehmenskultur und -integrität

  - sind regelmäßige Gespräche zwischen Geschäftsleitung, Führungskräften und Mitarbeitern sowie eine kritische Reflexion des Feedbacks erforderlich
  - können weitere Instrumente zur Beurteilung der Unternehmenskultur und -integrität umgesetzt werden, wie z.B.
    - Integration von Fragen zu Compliance und Integrity in bestehende Mitarbeiterbefragungen
    - Durchführung spezifischer Mitarbeiterbefragungen zur Erhebung der Wahrnehmung und Umsetzung von Compliance und Integrity (sog. Integrity Barometer)
    - Einholung von Feedback zum Führungsverhalten von Vorgesetzten und Führungskräften (z.B. von Mitarbeitern, Kollegen, Kunden, Lieferanten)
    - Auswertung geeigneter Kennzahlen (z.B. Fluktuationsrate)

Projektbeteiligte

KAPITEL IV

Projektleitung

Prof. Dr. Stephan Grüninger

Wissenschaftlicher Direktor Konstanz Institut für Corporate Governance,

HTWG Konstanz

RAuN Dr. Roland Steinmeyer

Partner, WilmerHale

Prof. Dr. Josef Wieland

Direktor Leadership Excellence Instituts Zeppelin,

Zeppelin Universität Friedrichshafen

Projektmitarbeit

RA Maximilian Jantz

Dipl.-Betriebswirtin (FH) Christine Schweikert

Gestaltung

Stefan Klär

www.stefanklaer.de

Projektförderer

Bundesministerium für Bildung und Forschung (BMBF)

Förderkennzeichen: 17044X11

HOCHSCHULE KONSTANZ TECHNIK, WIRTSCHAFT UND GESTALTUNG

KICG

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

Projektpartner

ABB

BASF The Chemical Company

BDO

DAIMLER

Deloitte.

Elma

EnBW

EY Building a better working world

Giesecke & Devrient Creating Confidence.

LAHMEYER INTERNATIONAL

MARSH

MAZARS

MÖRK BAU

PAUTHNERDAY

PFISTERER

pwc

rkw

SIEMENS

TaylorWessing

T

The AuditFactory Prüfung. Beratung. Training.

TPA Horwath

WILMERHALE

ZF Lenksysteme

Leitlinien für das Management von
Organisations- und Aufsichtspflichten

Übersicht der Projektdokumente

KICG CMS-GUIDANCE 2014

Grüninger, S., Jantz, M., Schweikert, C., Steinmeyer, R. (2014):
Empfehlungen für die Ausgestaltung und Beurteilung von Compliance-Management-Systemen –
Guidance zu den Leitlinien 1 bis 4 für das Management von Organisations- und Aufsichtspflichten

KICG CMS-LEITLINIE 1 2014

Grüninger, S., Jantz, M., Schweikert, C., Steinmeyer, R. (2014):
Empfehlungen für die Ausgestaltung und Beurteilung von Compliance-Management-Systemen –
Leitlinie 1 für das Management von Organisations- und Aufsichtspflichten

KICG CMS-LEITLINIE 2 2014

Grüninger, S., Jantz, M., Schweikert, C., Steinmeyer, R. (2014):
Empfehlungen für die Ausgestaltung und Beurteilung von Compliance-Management-Systemen –
Leitlinie 2 für das Management von Organisations- und Aufsichtspflichten

KICG CMS-LEITLINIE 3 2014

Grüninger, S., Jantz, M., Schweikert, C., Steinmeyer, R. (2014):
Empfehlungen für die Ausgestaltung und Beurteilung von Compliance-Management-Systemen –
Leitlinie 3 für das Management von Organisations- und Aufsichtspflichten

KICG CMS-LEITLINIE 4 2014

Grüninger, S., Jantz, M., Schweikert, C., Steinmeyer, R. (2014):
Empfehlungen für die Ausgestaltung und Beurteilung von Compliance-Management-Systemen –
Leitlinie 4 für das Management von Organisations- und Aufsichtspflichten

KICG CMS-ANNEX 2014

Grüninger, S., Jantz, M., Schweikert, C., Steinmeyer, R. (2014):
Empfehlungen für die Ausgestaltung und Beurteilung von Compliance-Management-Systemen –
Annex – Spezifische Anforderungen und Risikotreiber für die Ausgestaltung von Compliance-
Management-Systemen

www.kicg.htwg-konstanz.de