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

KONSTANZ INSTITUT FÜR CORPORATE GOVERNANCE

KICG CMS-GUIDANCE 2014 –
zu den Leitlinien 1 bis 4 für das Management von Organisations- und Aufsichtspflichten

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

KONSTANZ INSTITUT FÜR CORPORATE GOVERNANCE

KICG CMS-GUIDANCE 2014 –

zu den Leitlinien 1 bis 4 für das Management von Organisations- und Aufsichtspflichten

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

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.

Vorwort

Diese Guidance ist gemeinsam mit den Leitlinien 1 bis 4 und dem Annex das Ergebnis eines am Konstanz Institut für Corporate Governance (KICG) durchgeführten und vom Bundesministerium für Bildung und Forschung (BMBF) geförderten Forschungsprojekts mit dem Titel ›Leitlinien für das Management von Organisations- und Aufsichtspflichten‹. Das Ziel der Guidance und der Leitlinien ist es, Unternehmen und ihren Entscheidungsträgern Empfehlungen für die Ausgestaltung von Management-Maßnahmen an die Hand zu geben, die angemessen und geeignet sind, die unternehmerischen Sorgfalts- und Aufsichtspflichten zu erfüllen. Dabei geht es vor allem um Maßnahmen, die im Rahmen eines umfassenden Compliance-Management-Systems (CMS) implementiert werden und dazu dienen, Fehlverhalten der Mitarbeiter zu verhindern und eine redliche und regelgetreue Führung der Geschäfte sicherzustellen (sog. Business Conduct Compliance-Maßnahmen). Intention der Guidance und Leitlinien ist es darüber hinaus, einen wesentlichen Beitrag zur Schließung der Lücke zu leisten, die sich zwischen einer Vielzahl rechtlicher Anforderungen im Bereich der Organisations- und Aufsichtspflichten und deren faktischen Interpretation und Umsetzung mittels entsprechender Management-Maßnahmen in Unternehmen auftut. Denn weder für die Ausgestaltung von CMS noch für einzelne Rechtsgebiete (Strafrecht sowie Ordungswidrigkeitenrecht, Kartellrecht, Exportkontrolle, Arbeits- und Sozialstandards etc.) liegen bislang konkrete Vorgaben für die Umsetzung der rechtlichen Anforderungen vor.

Um möglichst konkrete und spezifische Empfehlungen an Unternehmen sowie weitere Entscheidungsträger, die sich mit der Beurteilung der Funktionsfähigkeit und Angemessenheit von Compliance-Management-Systemen beschäftigen, geben zu können, richten sich die einzelnen Leitlinien jeweils an verschiedene Unternehmensgrößenklassen:

— Leitlinie 1: Unternehmen mit bis ca. 250 Mitarbeitern
— Leitlinie 2: Unternehmen mit ca. 250 bis 3.000 Mitarbeitern
— Leitlinie 3: Unternehmen mit ca. 3.000 bis 20.000 Mitarbeitern
— Leitlinie 4: Unternehmen mit mehr als ca. 20.000 Mitarbeitern

Durch die Unterscheidung dieser vier Leitlinien ist es möglich, die unterschiedlichen Voraussetzungen und Gegebenheiten verschiedener Unternehmenstypen (Organisationsstruktur, Ressourcenausstattung, Internationalisierungsgrad etc.), kurz: die jeweilige Compliance-Komplexität, in den Empfehlungen entsprechend berücksichtigen zu können.[01]

Um den Praxisbezug und die Praxisrelevanz sicherzustellen, wurde das interdisziplinäre betriebswirtschaftlich-juristische Forschungsprojekt von zahlreichen Partnern aus der Unternehmens- und Beratungspraxis unterstützt:

— ABB AG
— BASF SE
— BDO Deutsche Warentreuhand AG
— CMM Compliance Management Mittelstand GmbH
— Daimler AG
— Deloitte
— Deutsche Telekom AG
— Elma Hans Schmidbauer GmbH & Co. KG
— EnBW Energie Baden-Württemberg AG
— Ernst & Young GmbH
— Giesecke & Devrient GmbH
— Lahmeyer International GmbH
— Marsh GmbH
— Mazars GmbH
— Mörk Bau GmbH & Co. KG
— PauthnerDay
— Pfisterer AG
— PricewaterhouseCoopers AG
— RKW SE
— Siemens AG
— TaylorWessing
— TPA Horwath
— The AuditFactory
— Wilmer Cutler Pickering Hale and Dorr LLP (WilmerHale)
— ZF Lenksysteme GmbH

01 Die betriebswirtschaftlich-juristischen Studien und Working Papers, die im Rahmen des Forschungsprojekts erarbeitet wurden und die Grundlage der Guidance und der Leitlinien bilden, sind auf Nachfrage zu beziehen über compliance-pflichten@htwg-konstanz.de oder unter http://www.htwg-konstanz.de/KICG-Forschungspapiere.6620.0.html (16.04.2014) abrufbar.

Die Projektpartner haben durch ihre Expertise und Erfahrungen im Bereich Compliance Management, das sie dem Projektteam in ausführlichen Experteninterviews und im Rahmen einzelner Schwerpunktkonferenzen zur Verfügung gestellt haben, maßgeblich zur Erarbeitung der Guidance, Leitlinien und des Annex beigetragen. Allen Projektpartnern möchten wir an dieser Stelle ganz herzlich für Ihre Unterstützung danken!

Frau Christine Schweikert und Herr Maximilian Jantz haben dieses wichtige und alle Projektbeteiligten inhaltlich und zeitlich äußerst fordernde Forschungsprojekt in hervorragender Weise mitgestaltet, organisatorisch und inhaltlich betreut sowie ganz wesentlich dazu beigetragen, dass es fristgerecht und mit Erfolg abgeschlossen wurde. Für das große Engagement und die ausgezeichneten Leistungen sind wir sehr dankbar!

Wir hoffen, mit der Erarbeitung der Leitlinien eine Diskussion zu den Anforderungen an die Ausgestaltung von Compliance-Maßnahmen zwischen Unternehmen und Unternehmensverbänden, Rechtsanwaltskanzleien, Wirtschaftsprüfungsgesellschaften, Berufsfachverbänden sowie staatlichen Stellen (u.a. Justizministerien, Staatsanwaltschaften) anzustoßen, mit dem Ziel, ein möglichst hohes Maß der Konkretisierung und Verbindlichkeit von Standards der Organisationspflichten in diesem Bereich und damit eine erhebliche Steigerung der Rechtssicherheit zu erreichen. Kommentierungen, Anregungen, Ergänzungen und Feedback zu den Leitlinien sind jederzeit unter compliance-pflichten@htwg-konstanz.de willkommen.

Konstanz, im April 2014

Prof. Dr. Stephan Grüninger
Herausgeber/Projektleiter
Direktor KICG
HTWG Konstanz

RAuN Dr. Roland Steinmeyer
Projektleiter
Partner
WilmerHale

Prof. Dr. Josef Wieland
Projektleiter
Direktor LEIZ
Zeppelin Universität

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-Systems (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 Guidance und der Leitlinien ist, im Detail auf die sich aus den unterschiedlichen spezifischen Gesetzen ergebenden Organisations- und Sorgfaltspflichten der Unternehmensleitung 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 von Unternehmen in die vier Leitlinien bildet die Compliance-Komplexität eines 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.[02] 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.

02 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.[03] 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 Stake-holder (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.

03 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 Unternehmensleitung 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 1.6 ›COMPLIANCE-REMEDIATION NACH ENTDECKTEM SYSTEMATISCHEM FEHLVERHALTEN‹ IM ANNEX).

Compliance-Management-Systeme in der Praxis

KAPITEL

1. Zweck und Zielsetzung von Compliance-Management-Systemen

Compliance bedeutet, Normen und Regeln einzuhalten, und bezieht sich in diesem Zusammenhang auf die Einhaltung von gesetzlichen und regulatorischen Anforderungen, von Soft Law (rechtlich nicht bindende, aber praktisch relevante Empfehlungen und Stellungnahmen internationaler Organisationen und Behörden) sowie von internen Regelungen und Verhaltensstandards durch die Unternehmensleitung, Führungskräfte und Mitarbeiter. Ein Compliance-Management-System dient somit der Sicherstellung von Compliance im Unternehmen durch geeignete Maßnahmen mit dem Ziel der Herstellung und Erhaltung einer integren und regeltreuen Unternehmensführung. Dabei geht es nicht nur um Themen wie Korruptionsbekämpfung und Fairness im Wettbewerb (insbesondere Kartellrecht), die aufgrund zahlreicher Fälle in diesen Bereichen im Fokus der öffentlichen Debatte stehen, sondern auch um die Themen Umwelt, Menschenrechte, Arbeit- und Sozialstandards (Social Compliance) sowie um weitere, beispielsweise branchenbezogene Themen.

Jedoch ist ein CMS nicht in der Lage, sämtliche Compliance-Verstöße, Fehlverhalten und Straftaten im Unternehmen stets zu unterbinden. Ziel eines CMS kann und muss es aber sein, die für ein spezifisches Unternehmen besonders schwerwiegenden Compliance-Risiken erheblich zu mildern und systematisches Fehlverhalten der Organisation und ihrer Mitglieder (z.B. Beteiligung oder Duldung durch das Top-Management, Fehlsteuerungen durch Compliance-dysfunktionale Anreiz- und Sanktionssysteme) auszuschließen. Dabei darf Compliance Management nicht ausschließlich als Kontrollsystem verstanden werden, das die Handlungen der Unternehmensleitung und Mitarbeiter einschränkt und überwacht – eine Kontroll- und Überwachungsfunktion erfüllt ein CMS natürlich auch! –, sondern vielmehr geht es darum, den handelnden Akteuren im Unternehmen Orientierung und Handlungsanleitung zu geben und durch die Etablierung eines CMS im Unternehmen gegenüber den Kooperationspartnern des Unternehmens (u.a. Mitarbeiter, Lieferanten, Kunden, Investoren, aber auch Öffentlichkeit) ein Versprechen abzugeben, auf welche Art ein Unternehmen Geschäfte machen will und auf welche Art nicht. So verstanden und umgesetzt, kann ein CMS einen wesentlichen Beitrag zum Erwerb, zum Erhalt oder auch zur Wiedererlangung einer Reputation als vertrauenswürdiger Kooperationspartner und für integres Verhalten im Geschäftsverkehr leisten.

Chancen aus Compliance Management

- ✓ Vermeidung und Prävention von Straftaten und Fehlverhalten im Unternehmen
- ✓ Hilfestellung und Handlungsorientierung für Mitarbeiter
- ✓ Risikovermeidung und Risikomanagement, v.a. hinsichtlich Compliance-Risiken
- ✓ Integration von bestehenden Unternehmensfunktionen und -prozessen
- ✓ Erwerb und Erhalt einer Reputation für Vertrauenswürdigkeit und Integrität, auch Schutz vor Reputationsschäden
- ✓ Schaffung von Vertrauen seitens der Kooperationspartner (Stakeholder) des Unternehmens
- ✓ Erfüllung der unternehmerischen Verantwortung (Corporate (Social) Responsibility)
- ✓ Sicherung von Kooperationsbeziehungen
- ✓ Nachhaltige Sicherung der Geschäftstätigkeit
- ✓ CMS als Wettbewerbsvorteil
- ✓ Bindung und Gewinnung von Mitarbeitern und High Potentials

Mögliche negative Folgen von Non-Compliance

- **Rechtlich**
  - Haftstrafen und Entlassungen für straffällige Mitarbeiter, aber auch Unternehmensleitung und Organe
  - Geldbußen/Geldstrafen
  - Gewinnabschöpfung
- **Ökonomisch**
  - Kosten der Fallaufarbeitung
  - Strafzahlungen, Gewinnabschöpfungszahlungen
  - Aktienkursverlust, Verlust von Investoren
  - Verlust von Kunden
  - Blacklisting, Ausschluss von Ausschreibungsverfahren (z.B. Weltbank, Europäische Bank für Wiederaufbau und Entwicklung)
- **Schädigung der Reputation**
- **Gefährdung von Geschäftsbeziehungen**
- **Unternehmen als Ganzes nimmt Schaden und**
  - muss Mitarbeiter entlassen
  - kann Pensionszusagen nicht mehr auszahlen
  - Kunden verlieren einen Lieferanten
  - Lieferanten verlieren einen Kunden
  - Zinsen an Geldgeber können nicht bezahlt werden
  - die Gesellschaft nimmt Schaden aufgrund des Verlustes des Unternehmens

2. Funktionen eines Compliance-Management-Systems

Ein Compliance-Management-System erfüllt drei Funktionen: An erster Stelle dient das CMS der Vermeidung von Fehlverhalten und der Förderung integren Verhaltens im Unternehmen (Präventionsfunktion, ›Prevent‹). Zudem umfasst ein CMS zweitens Maßnahmen zur Aufdeckung von Fehlverhalten (Aufdeckungsfunktion, ›Detect‹) und drittens eine reaktive Komponente, die eine angemessene Sanktion entdeckter Fälle von Non-Compliance beinhaltet und einen (kontinuierlichen) Verbesserungsprozess anstößt (Reaktionsfunktion, ›Respond‹).

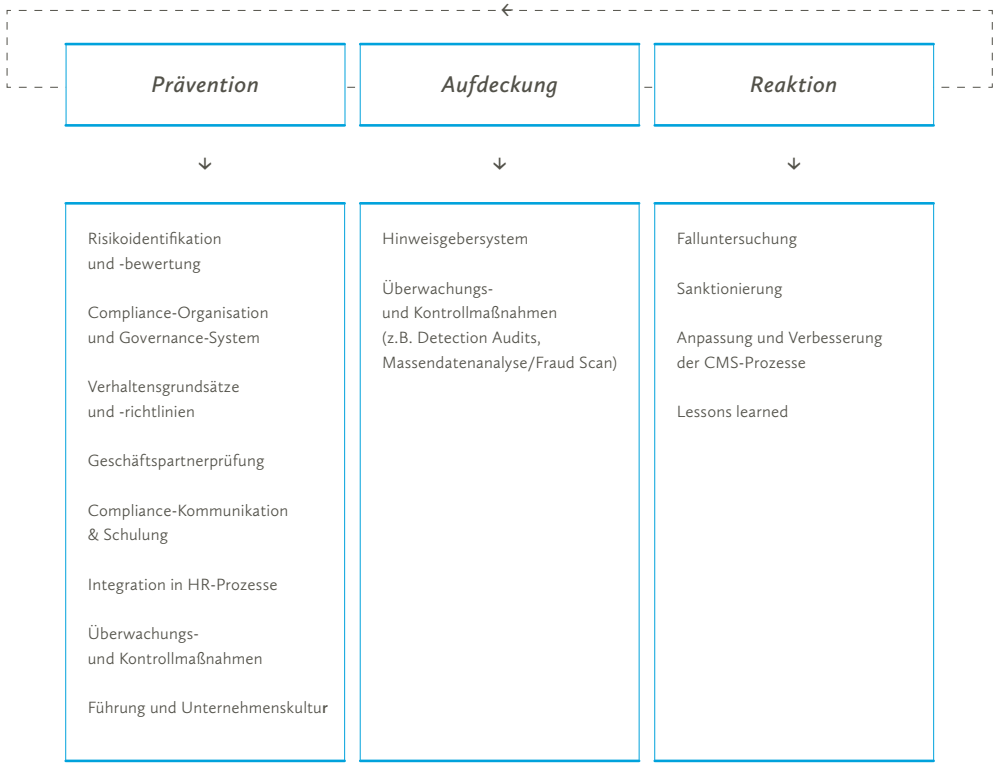

Abbildung 01 / CMS-Kreislauf: Prävention – Aufdeckung – Reaktion

2.1 Prävention (Prevent)

»*If you think compliance is expensive, try non-compliance!*«[04] – Es gibt vermutlich keinen geeigneteren Slogan für die Bedeutung wirksamer Prävention im Rahmen des Compliance Managements. Die Vermeidung von Fehlverhalten ist aus Sicht des Risikomanagements die beste Option. Eine erfolgreiche Prävention schützt das Unternehmen bestmöglich vor Schäden in rechtlicher sowie ökonomischer Hinsicht und trägt mit Blick auf die externen Interessengruppen des Unternehmens (Kunden, Lieferanten, Investoren, Öffentlichkeit etc.) wesentlich zur Herausbildung einer Reputation eines vertrauenswürdigen, integren Kooperationspartners bei. Nicht ohne Grund liegt ein Schwerpunkt von Compliance-Management-Systemen im Bereich der Prävention.

2.2 Aufdeckung (Detect)

Wie eben dargestellt, ist es die erste Funktion eines CMS, Fehlverhalten im Unternehmen vorzubeugen und bestmöglich zu verhindern. Jedoch ist ein CMS nicht in der Lage, Non-Compliance in 100 von 100 Fällen vollständig auszuschließen. Ein lückenloses Kontroll- und Regelsystem ist schon allein aus Kostengründen nicht zu haben. Unternehmen müssen sich daher stets darüber bewusst sein, dass trotz aller Compliance-(Präventions-)Maßnahmen Fehlverhalten möglich bleibt. Aus diesem Grund ist es wichtig, dass ein CMS neben der Prävention eine aufdeckende Komponente beinhaltet, die Maßnahmen umfasst, die der Aufdeckung von Fehlverhalten im Unternehmen dienen. Dazu gehören beispielsweise die Implementierung eines Hinweisgebersystems, in dem sowohl interne als auch externe Personen mögliches Fehlverhalten melden können, regelmäßige angekündigte wie unangekündigte Kontrollen der festgelegten Compliance-Prozesse (Einhaltung des Vier-Augen-Prinzips, von Freizeichnungsprozessen oder Dokumentationsvorschriften bei sensiblen Zahlungsvorgängen etc.) oder auch routinemäßig durchgeführte und IT-gestützte Analysen von Unternehmensdaten – unter strikter Beachtung der landesspezifischen Datenschutzregeln – im Hinblick auf Unregelmäßigkeiten und Auffälligkeiten. Für die Funktionsfähigkeit und Wirksamkeit eines CMS bildet die Aufdeckungsfunktion eine notwendige Grundlage.

2.3 Reaktion (Respond)

Die Reaktionsfunktion des CMS schließt den Kreislauf zwischen Aufdeckung und Prävention. Um die Glaubwürdigkeit des unternehmerischen Engagements im

04 Former U.S. Deputy Attorney General Paul McNulty

Bereich Compliance Management gegenüber den Mitarbeitern sowie gegenüber Geschäftspartnern, Behörden, der Öffentlichkeit etc. zu erhalten, sind bei der Aufdeckung von Fehlverhaltensfällen von Seiten der Unternehmensleitung angemessene Konsequenzen zu ergreifen. Dazu gehört zum einen, Fehlverhalten im Unternehmen konsequent und transparent zu sanktionieren, und zum anderen, aus den strafbaren oder unethischen, unerwünschten Verhaltensmustern Erkenntnisse für die Notwendigkeit der Anpassung und Verbesserung bestehender Prozesse zur Vermeidung zukünftigen Fehlverhaltens zu ziehen.

Die drei Funktionen eines Compliance-Management-Systems — Prävention, Aufdeckung und Reaktion — bilden somit einen Kreislauf, der im Zeitverlauf zu einer kontinuierlichen Verbesserung des gesamten CMS führt.

Die einzelnen CMS-Elemente und -Maßnahmen, die in → KAPITEL III detailliert dargestellt sind, lassen sich, wie in → ABBILDUNG 01 dargestellt, anhand ihrer Zielsetzung den verschiedenen CMS-Funktionen zuordnen. Verschiedene CMS-Elemente dienen dabei nicht ausschließlich der Erfüllung einer einzigen Funktion, sondern tragen in unterschiedlicher Weise zur Erfüllung mehrerer Funktionen bei. So kommt beispielsweise der Einführung von Prozesskontrollen zum einen eine aufdeckende Funktion zu. Aufgrund der abschreckenden Wirkung von Kontrollen und der von ihnen ausgehenden Erhöhung der Entdeckungswahrscheinlichkeit beinhalten Prozesskontrollen zum anderen auch immer eine präventive Komponente. Für die Implementierung eines funktionsfähigen CMS ist die eindeutige Zuordnung aller CMS-Elemente zu nur einer Funktion jedoch nicht entscheidend. Vielmehr dient die Systematisierung dazu aufzuzeigen, dass die Funktionsfähigkeit eines CMS (Prävention von Fehlverhalten, Aufdeckung von Fehlverhalten, Reaktion auf Fehlverhalten) mittels der acht identifizierten CMS-Elemente erreicht werden kann. Die Funktionen sind universal, d.h. sie gelten für alle Unternehmen unabhängig der jeweiligen Unternehmens- und Compliance-Komplexität.

3. Prüfung und Beurteilung von Compliance-Management-Systemen

Die Nachfrage nach der Überprüfung und Zertifizierung unternehmerischer CMS ist in der letzten Zeit stark gestiegen. Zahlreiche Dienstleister aus der Beratungs- und Wirtschaftsprüfungsbranche bieten Unternehmen unterschiedlich tiefe Prüfungsleistungen an. So verabschiedete im April 2011 das Institut der Wirtschaftsprüfer für die Überprüfung von CMS einen eigenen Prüfungsstandard (›Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen‹, IDW PS 980).

Für ein Unternehmen gibt es verschiedene Anlässe und Gründe, sein CMS einer externen Prüfung und Beurteilung bezüglich dessen Wirksamkeit zu unterziehen. So sind oftmals Compliance-Verstöße in der Vergangenheit Anlass für die Beauftragung einer externen Prüfung, mit der man nun z.B. dem Aufsichtsrat, Aktionären oder auch Behörden zeigen will, dass es eine gewisse ›Selbstreinigung‹ gab und nun im Unternehmen wieder alles funktioniert. Ein weiterer Grund für die Prüfung und Beurteilung kann sich aus den §§ 111 Abs. 1, 107 Abs. 3 AktG sowie den Empfehlungen des DCGK (vgl. Ziff. 5.3.2) ergeben, wonach der Aufsichtsrat (Prüfungsausschuss) verpflichtet ist, die Wirksamkeit eines eingerichteten internen Kontrollsystems zu überwachen und im Rahmen dieser Überwachung sich von der Angemessenheit und Funktionsfähigkeit des CMS überzeugen will. Für kleine und mittelständische Unternehmen hingegen kann die Beauftragung einer Prüfung des CMS auch eine strategische Komponente beinhalten. Große Unternehmen erwarten mehr und mehr sowohl von ihren bestehenden als auch potenziell neuen Lieferanten den Nachweis, dass diese bestimmte Compliance-Maßnahmen implementiert haben. Ein Unternehmen, das sein CMS bzw. bestimmte getroffene Compliance-Maßnahmen einer externen Prüfung unterzogen hat, kann auf diesem Wege seinem Kunden die angefragten Nachweise zukommen lassen. Für neue Lieferanten kann dies ein maßgebliches Kriterium sein, um als Lieferant des Kunden qualifiziert zu werden, und für Bestandslieferanten kann der Nachweis eines positiven Prüfurteils bei einer Lieferantenbewertung durch den Kunden zu einem positiven Ergebnis führen und dem Lieferanten einen Wettbewerbsvorteil bei der Vergabe neuer Aufträge verschaffen.

Und schließlich wird es in vielen Fällen auch um die Frage nach der Haftung der Leitungsgremien bzw. Organmitglieder gehen, also danach, ob diese ihre Organisations- und Sorgfaltspflichten erfüllt haben. Aus juristischer Perspektive ist eine Überprüfung und Beurteilung des CMS vor allem mit Blick auf eine Haftungsvermeidung bzw. -reduzierung für die Unternehmensorgane nach der Aufdeckung eines Compliance-Vorfalls erstrebenswert. Dabei darf Ziel einer Prüfung und Beurteilung – unabhängig von der Frage, ob und inwieweit ein positives Prüfurteil letztendlich überhaupt zu einer persönlichen Haftungsvermeidung führen kann – nicht das alleinige Ansinnen sein, die Leitungsgremien bei Auftreten von Compliance-Verstößen zu ›enthaften‹. Wird ein als ›Alibi-Funktion‹ eingerichtetes und lediglich auf dem Papier stehendes CMS nur aus Enthaftungsgesichtspunkten einer Prüfung unterzogen, so wird es selbst im Falle eines positiven Prüfurteils seine Ziele, nämlich Prävention, Aufdeckung und Reaktion auf lange Sicht nicht erfüllen können. Die Prüfung eines CMS sollte neben dem durchaus zulässigen Ziel einer Haftungsmilderung mit der primären Zielsetzung verbunden sein, im Wege einer integren und verantwortungsvollen Unternehmensführung zu beurteilen, ob die implementierten Maßnahmen angemessen und geeignet sind, Risiken aus Non-Compliance erheblich zu mildern und systemisch bedingtes Fehlverhalten auszuschließen.

Erste Vorstöße in dieser Richtung bilden beispielsweise der Prüfungsstandard 980 des Instituts der Wirtschaftsprüfung ›Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen‹ (IDW PS 980) oder auch der ComplianceProgram-Monitor[ZfW]. Der vorliegende Leitfaden steht in einer Reihe mit diesen Ansätzen mit der Intention, die bestehenden Bestrebungen weiter zu konkretisieren und zur Diskussion zu stellen. Dabei sollen die Guidance, die Leitlinien und der Annex zum einen den Leitungs- und Aufsichtsgremien von Unternehmen Hilfestellung für die Beurteilung der Erfüllung ihrer Organisations- und Aufsichtspflichten geben und so zu einer Milderung der bestehenden Unsicherheit beitragen. Zum anderen sollen diese Empfehlungen dem Compliance-Verantwortlichen im Unternehmen als Orientierungshilfe bei der Umsetzung eines funktionierenden CMS oder zur Beurteilung der Funktionsfähigkeit des CMS dienen. Die Frage der Funktionsfähigkeit von CMS beschäftigt nicht nur die Leitungs- und Aufsichtsgremien von Unternehmen, sondern auch deren Abschlussprüfer und andere Prüfer sowie Staatsanwälte und Richter, die im Rahmen von Verfahren über vorgefallene Straftaten beurteilen müssen, ob die Organisations- und Aufsichtspflichten bezüglich der Ausgestaltung des CMS erfüllt wurden. Und schließlich sollen diese Empfehlungen Grundlage für notwendige Diskussionen zwischen Unternehmen, Verbänden, Beratungs- und Wirtschaftsprüfungsunternehmen sowie dem Gesetzgeber und rechtssprechenden Organen bilden mit dem Ziel, mehr Verbindlichkeit und Sicherheit für Unternehmen hinsichtlich der Reichweite unternehmerischer Organisations- und Aufsichtspflichten sowie der Möglichkeit derer Erfüllung zu schaffen.

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 Guidance mit den Hinweisen und Empfehlungen einen Beitrag zur weiteren Konkretisierung von Anforderungen an die Ausgestaltung angemessener Compliance-Management-Systeme 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 dieser Guidance finden Unternehmen jeglicher Unternehmensgröße 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 Unternehmensleitung 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 Gesetze sowie anerkannter, einschlägiger Standards im Bereich Compliance und Integrity Management:

Für Wertpapierdienstleistungsunternehmen hat der deutsche Gesetzgeber insbesondere in § 33 WpHG[05] sowie in § 25 a KWG[06] spezifische Organisationspflichten und in § 25 c KWG[07] bestimmte interne Sicherungsmaßnahmen statuiert. Darüber hinaus hat die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) mit ihrem im Juni 2010 veröffentlichten Rundschreiben für Wertpapierdienstleistungsunternehmen Mindestanforderungen an die Compliance-Funktion und die weiteren Verhaltens-, Organisations- und Transparenzpflichten (MaComp)[08] konkretisiert. Obgleich diese spezifischen Normen sowie die MaComp für Industrieunternehmen nicht gelten und der Gesetzgeber für Industrieunternehmen bislang keine vergleichbaren konkreten regulatorischen Vorgaben zur Einführung und Ausgestaltung eines CMS erlassen hat, kann es dennoch auch für Unternehmen außerhalb des Finanzsektors empfehlenswert sein, sich mit diesen Vorschriften zu befassen. Zum einen ist die weitere Entwicklung nicht absehbar, weshalb eine künftige Ausstrahlungswirkung von spezifischen regulatorischen Anforderungen an Kreditinstitute auf Unternehmen aus dem Nichtfinanzsektor nicht ausgeschlossen werden kann. Und zum anderen können die Anforderungen aus dem WpHG, dem KWG und den MaComp zumindest für solche Instrumente und Maßnahmen, die nicht unmittelbar im Zusammenhang mit der Tätigkeit von Kredit- und Finanzdienstleistungsunternehmen stehen (z.B. die Einrichtung eines Risikomanagementsystems, die Einrichtung von Kontrollen, umfassende Dokumentation der Geschäftstätigkeit), als Orientierungshilfe dienen.

05 Nach §33 WpHG (Wertpapierhandelsgesetz) hat ein Wertpapierdienstleistungsunternehmen u.a. eine dauerhafte und wirksame Compliance-Funktion einzurichten, wirksame und transparente Verfahren für eine angemessene und unverzügliche Bearbeitung von Beschwerden durch Privatkunden vorzuhalten sowie sicherzustellen, dass die Geschäftsleitung und das Aufsichtsorgan in angemessenen Zeitabständen, zumindest einmal jährlich, Berichte der mit der Compliance-Funktion betrauten Mitarbeiter erhalten.

06 In §25 a Kreditwesengesetz (KWG) werden für Kreditinstitute und Finanzdienstleistungsinstitute besondere organisatorische Pflichten konkretisiert. Hiernach müssen diese Institute über eine ordnungsgemäße Geschäftsorganisation verfügen. Diese hat u.a. ein angemessenes und wirksames Risikomanagement zu umfassen, die Einrichtung interner Kontrollverfahren sowie eine vollständige Dokumentation der Geschäftstätigkeit sicherzustellen.

07 Nach §25 c KWG haben Kredit- und Finanzdienstleistungsinstitute interne Sicherungsmaßnahmen zu treffen, die der Verhinderung von Geldwäsche, Terrorismusfinanzierung oder sonstiger strafbarer Handlungen dienen, die zu einer Gefährdung des Vermögens des Instituts führen können.

08 Rundschreiben 4/2010 der BaFin in der Fassung vom 30.11.2012, abrufbar unter http://www.bafin.de/SharedDocs/Downloads/DE/Rundschreiben/dl_rs_1004_MaComp_Fassung_nov_2012.html (16.04.2014).

Auf internationaler Ebene ist im Jahr 2011 das Antikorruptionsgesetz des Vereinigten Königreichs, der UK Bribery Act, in Kraft getreten, nach dem – im Gegensatz zum (bisherigen) deutschen Recht[09] – sich auch Unternehmen selbst strafbar machen können, wenn eine Korruptionstat im Zusammenhang mit Geschäften für das Unternehmen begangen wird und das Unternehmen es versäumt hat, geeignete Antikorruptionsmaßnahmen zu ergreifen. Einer Haftung kann das Unternehmen nach dem UK Bribery Act nur entgehen, wenn es im Falle festgestellter Korruptionsverstöße nachweisen kann, dass es adäquate Vorkehrungen zur Bekämpfung von Korruption eingerichtet hatte.[10] Die Mindestanforderungen an die adäquaten Vorkehrungen formuliert das britische Justizministerium in seiner Guidance zum UK Bribery Act. Den Empfehlungen zum Bribery Act folgend müssen alle Unternehmen, die eine Verbindung zum Vereinigten Königreich unterhalten, ein (Compliance-Management-)System etablieren, das die folgenden sechs Prinzipien erfüllt: (1) proportionate procedures; (2) top-level commitment; (3) risk-assessment; (4) due diligence; (5) communication (including training); (6) monitoring & review.

Mit Blick auf die weiterhin fortschreitende Globalisierung und Internationalisierung der Wertschöpfungsketten kann mit einer hohen Wahrscheinlichkeit davon ausgegangen werden, dass die Mehrzahl aller Unternehmen, insbesondere die Unternehmen mit mehr als 250 Mitarbeitern, international tätig ist und daher Geschäftsbeziehungen zum Vereinigten Königreich haben wird. Da die Normen des Bribery Act über das Hoheitsgebiet des Vereinigten Königreichs hinaus Anwendung finden (sog. extraterritoriale Wirkung) und der Anwendungsbereich u.a. auch ausländische juristische Personen umfasst, die Geschäfte oder auch nur Teile des Geschäfts auf dem Hoheitsgebiet des Vereinigten Königreichs tätigen, werden die Prinzipien des Bribery Act daher als ein allgemein verbindlicher Mindeststandard für die Ausgestaltung funktionsfähiger CMS zugrunde gelegt. Die Prinzipien der Guidance des britischen Justizministeriums zum Bribery Act finden sich daher in den notwendigen CMS-Elementen der Leitlinien wieder. Die Festlegung der notwendigen CMS-Elemente deckt sich überdies mit weiteren einschlägigen Standards: Der Prüfungsstandard PS 980 des Instituts der Wirtschaftsprüfer ›Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen‹ identifiziert als CMS-Grundelemente: (1) Compliance-Kultur, (2) Compliance-Ziele, (3) Compliance-Risiken, (4) Compliance-Programm, (5) Compliance-Organisation, (6) Compliance-Kommunikation und (7) Compliance-Überwachung und Verbesserung. Auch die Elemente des Red Book der Open Compliance and Ethics Group (OCEG) stimmen inhaltlich mit den Prinzipien des UK Bribery Act überein. Eine Auflistung der wichtigsten relevanten und anerkannten Standards und Leitfäden im Bereich Compliance und Integrity Management findet sich in → KAPITEL V der GUIDANCE.

Die Beurteilung der Angemessenheit eines CMS richtet sich nach der Eignung und Angemessenheit der entwickelten und umgesetzten Maßnahmen für die jeweiligen Elemente. Welche Maßnahmen für ein bestimmtes Unternehmen als angemessen zu beurteilen sind, ist u.a. abhängig von der Unternehmensgröße, der Internationalität des Geschäfts, der Rechtsform und der Branche. Die vorliegende Guidance zeigt für die acht wesentlichen Elemente eines CMS auf, welche *Zielsetzungen* jeweils mit den einzelnen Elementen verfolgt werden und welche *Maßnahmen* für Unternehmen unterschiedlicher Unternehmensgröße geeignet sind, um diese Ziele erreichen zu können.

09 Der Justizminister des Landes Nordrhein-Westfalen hat am 14. November 2013 auf der Justizministerkonferenz in Berlin den Gesetzentwurf des Landes NRW ›Entwurf eines Gesetzes zur Einführung der strafrechtlichen Verantwortlichkeit von Unternehmen und sonstigen Verbänden‹ für ein bundesweites Unternehmensstrafrecht vorgestellt, wonach künftig bei Wirtschaftsdelikten wie Korruption oder Steuerbetrug die juristische Person selbst zu empfindlichen Strafen verurteilt werden kann. Der Gesetzesantrag soll demnächst über den Bundesrat in das Gesetzgebungsverfahren eingebracht werden. Auch im aktuellen Koalitionsvertrag zwischen CDU, CSU und SPD ist im Rahmen der Kriminalitätsbekämpfung die Prüfung eines Unternehmensstrafrechts für multinationale Konzerne vorgesehen, vgl. S. 145 des Koalitionsvertrages, abrufbar unter http://www.cdu.de/koalitionsvertrag (16.04.2014).

10 Vgl.1 auch → ABSCHNITT I.2 des ANNEX.

Risikoidentifikation und -bewertung

Warum ist die Risikoidentifikation und -beurteilung für die Funktionsfähigkeit des CMS wichtig?

Um welche Risiken geht es?

Wie können Compliance-Risiken erfasst werden?

Anhand welcher Kriterien und Methoden können Compliance-Risiken beurteilt werden?

In welcher Funktion bzw. Position im Unternehmen ist die Aufgabe der Compliance-Risikoidentifikation und -beurteilung am besten anzusiedeln?

Wie ist mit den identifizierten Compliance-Risiken umzugehen? Was folgt aus der Compliance-Risikoidentifikation und -beurteilung?

Zielsetzung

Unternehmen, kleine wie große, agieren in einer hochkomplexen Umwelt, die von großer Unsicherheit geprägt ist. Die Unsicherheit, z.B. über die wirtschaftliche Entwicklung oder auch das Verhalten anderer Teilnehmer am Markt, tritt Unternehmen in Form von Risiken entgegen. Um nachhaltig erfolgreich wirtschaften zu können, müssen Unternehmen ihre Risiken kennen und entsprechende Präventions- oder Risikoreduzierungsmaßnahmen ergreifen. Für die Funktionsfähigkeit des CMS ist die Risikoidentifikation wichtig, damit das CMS so ausgestaltet werden kann, dass die wesentlichen Risiken bestmöglich vermieden bzw. gemindert und die im Unternehmen zur Verfügung stehenden Ressourcen (finanziell und personell) sinnvoll und effizient eingesetzt werden. Bei der Risikoidentifikation und -beurteilung geht es also um Kenntnis des Geschäfts, Fokussierung der Maßnahmen und Ressourceneffizienz.

— Unsicherheit

— Risikomanagement

Die Notwendigkeit und Zulässigkeit der Risikoorientierung des CMS ergibt sich auch aus dem Gesetz. Nach der Rechtsprechung besteht für Unternehmen eine Rechtspflicht zur Umsetzung möglicher, erforderlicher und zumutbarer Maßnahmen zur Erfüllung der unternehmerischen Organisations- und Aufsichtspflichten.[11] Übertragen auf die angemessene Ausgestaltung von CMS bedeutet dies, dass das Unternehmen solche Compliance-Maßnahmen implementieren muss, die möglich, erforderlich und zumutbar sind. Dabei bieten insbesondere die Attribute ›erforderlich‹ und ›zumutbar‹ einen Ermessenspielraum für die Unternehmen. Die Erfordernis und Zumutbarkeit von Compliance-Maßnahmen bemisst sich an ihrem Nutzen in Relation zum entstehenden Mehraufwand (finanziell und personell).[12] Daraus kann abgeleitet werden, dass das CMS danach auszurichten ist, wo die größten Risiken und Bedrohungen für das Unternehmen liegen und die Eintrittswahrscheinlichkeit dieser Risiken am höchsten ist (Risikoorientierung).[13] Auch der UK Bribery Act verlangt einen risikoorientierten Compliance-Management-Ansatz.[14] Nach dem ersten Grundsatz des Leitfadens zum UK Bribery Act (Guidance) müssen die Maßnahmen und Prozesse zur Vermeidung von Fehlverhalten (der UK Bribery Act fokussiert ausschließlich Fehlverhalten im Bereich der Korruption) in einem angemessenen Verhältnis zu den entsprechenden Risiken, aber auch zur Komplexität des Unternehmens und dessen Geschäftstätigkeit stehen.[15]

Wortlaut der Bribery Act Guidance:
»A commercial organisation's procedures to prevent bribery by persons associated with it are proportionate to the bribery risks it faces and to the nature, scale and complexity of the commercial organisation's activities.«

Im Mittelpunkt des CMS stehen die Vermeidung und Reduzierung von Compliance- und Integrity-Risiken (im Weiteren Compliance-Risiken genannt). Compliance-Risiken sind Risiken, die sich aus der Nichtbefolgung und Missachtung von Gesetzen, internen Regelungen und Normen im Unternehmen ergeben. Genauer handelt es sich dabei um Risiken aus Fehlverhalten und Regelverstößen von Mitarbeitern, Führungskräften und/oder (Top-)Managern des Unternehmens. Im Fachjargon werden diese Risiken häufig auch als Corporate Misconduct oder Fraud bezeichnet. Diese Sichtweise von Compliance-Risiken ist sehr breit angelegt und umfasst eine Vielzahl von Delikten. Aufgrund ihres potenziellen Schadens und möglichen negativen Auswirkungen für Unternehmen stehen insbesondere Risiken aus den Deliktbereichen Korruption, Vermögensschädigung (z.B. Untreue, Betrug, Diebstahl) sowie Kartelle und Absprachen (z.B. Preisabsprachen, Aufteilung von Märkten/Gebietsabsprachen, Absprachen über Produktions- bzw. Verkaufsbeschränkungen) im Fokus. Korruption, Kartelle/Absprachen sowie Vermögensschädigung durch Beschäftigte könnte man somit als die klassischen Compliance-Risiken bezeichnen. Darüber hinaus sind jeweils unternehmens- und branchenspezifische Risiken zu berücksichtigen. Auch die Geschäftspraktiken von Geschäftspartnern können Risiken für das Unternehmen darstellen. Die Zusammenarbeit mit internationalen Geschäftspartnern und Vertriebsmittlern ist daher ebenso wie Geschäftsaktivitäten im Ausland auf mögliche Risiken zu untersuchen (vgl. hierzu auch das CMS-Element → 4 GESCHÄFTSPARTNERPRÜFUNG).

— Compliance-Risiken

Dem Prüfungsstandard 980 ›Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen‹ des Instituts der Wirtschaftsprüfer folgend können sich Compliance-Risiken insbesondere aus Verstößen bzw. Fehlverhalten in den folgenden Teilbereichen ergeben:

— **Rechtsgebiete**

  — Wettbewerbs- und Kartellrecht

[11] Vgl. bspw. Bock, D. (2010): Strafrechtlich gebotene Unternehmensaufsicht (Criminal Compliance) als Absenkung des Schadenserwartungswerts aus unternehmensbezogenen Straftaten. In: HRRS 7-8/2010, 316 f.

[12] Vgl. Geismar, A.-G. (2011): Der Tatbestand der Aufsichtspflichtverletzung bei der Ahndung von Wirtschaftsdelikten (Kiel, Univ., Diss.). Baden-Baden: Nomos, 103.

[13] Ebenso argumentiert der BGH in Bezug auf die Erfordernis von Sicherungsmaßnahmen: *»Dabei sind Sicherungsmaßnahmen umso eher zumutbar, je größer die Gefahr und die Wahrscheinlichkeit ihrer Verwirklichung sind (vgl. Senatsurteil vom 5. Oktober 2004 - VI ZR 294/03 - VersR 2005, 279, 280 f.).«* (BGH VersR 2007, 72,73; VI ZR 223/05).

[14] Vgl. Ministry of Justice (2011): The Bribery Act 2010 – Guidance about procedures which relevant commercial organisations can put into place to prevent persons associated with them from bribing (section 9 of the Bribery Act 2010), S. 7.

[15] Vgl. Ministry of Justice (2011): The Bribery Act 2010 – Guidance about procedures which relevant commercial organisations can put into place to prevent persons associated with them from bribing (section 9 of the Bribery Act 2010), S. 21.

- Antikorruptionsrecht
  (z.B. §299 StGB oder Foreign Corrupt Practices Act – FCPA)
- Börsenrecht (z.B. Vorschriften zum Insiderhandel
  oder zu Ad-hoc-Meldepflichten)
- Vorschriften zur Unternehmensführung und -überwachung
  (z.B. nach dem Deutschen Corporate Governance Kodex)
- Geldwäschegesetz
- Umweltrecht
- Außenwirtschaftsrecht und Exportkontrolle
- Außensteuerrecht
- Datenschutz- und Datensicherheitsvorschriften
- Arbeitsrecht und Persönlichkeitsrechte
  (z.B. Allgemeines Gleichstellungsgesetz)
- Arbeitssicherheitsrecht
- Zollrecht
- Patentrecht
- Produkthaftungsrecht

- **Geschäftsbereiche bzw. Unternehmensprozesse**
  - Ausschreibung und Vergabe (Einkauf)
  - Provisionszahlungen (Vertrieb)
  - Arbeitssicherheit und technische Sicherheit (Produktion)
  - Vertragsmanagement
- **Organisation der Einhaltung von Selbstverpflichtungen
  (z.B. der Prinzipien des United Nations Global Compact)**

Die Handlungsempfehlungen in dieser Guidance, den Leitlinien und dem Annex schließen sich dieser Sichtweise grundsätzlich an und legen im Wesentlichen ihren Fokus auf die Vermeidung und Minimierung der Risiken aus den Deliktbereichen Korruption, Vermögensschädigung sowie dem Wettbewerbs- und Kartellrecht.

Konsequenzen von Non-Compliance

Compliance-Risiken sind für Unternehmen insbesondere deshalb kritisch, weil ihre negativen Auswirkungen auf das Unternehmen beträchtlich sein können: In ökonomischer und finanzieller Hinsicht zeigen sich die Auswirkungen von Fehlverhalten im Unternehmen beispielsweise in hohen Kosten für die Fallaufarbeitung, Bußgeldzahlungen oder Strafen in Form von Gewinnabschöpfung sowie auch im Rückgang des Börsenkurses. Darüber hinaus kann entdecktes Fehlverhalten eine beachtliche negative Öffentlichkeitswirkung entfalten und die Unternehmensreputation erheblich und langfristig schädigen. Nicht zu unterschätzen sind ebenso die strafrechtlichen Konsequenzen, die sich sowohl für den/die Täter selbst ergeben können, als auch für die verantwortlichen Personen in den Leitungs- und Aufsichtsgremien des Unternehmens, wenn sie ihren Organisations- und Aufsichtspflichten nicht entsprechend nachgekommen sind.

Für die Risikoorientierung des CMS ist besonders wichtig, dass die Risikoidentifikation und -bewertung keine einmaligen und in sich abgeschlossenen Prozesse sind, sondern die Risiken im Umfeld des Unternehmens kontinuierlich beobachtet und beurteilt werden müssen. Nur so können Veränderungen im Unternehmensumfeld und sich daraus ergebende Risiken früh erkannt und das CMS gegebenenfalls frühestmöglich angepasst werden.

Kontinuierliche Risikoidentifikation und -bewertung

Empfehlungen für die Umsetzung

Risikoidentifikation

Identifikation der Compliance-/ Integrity-Risiken

Für eine risikoorientierte Ausgestaltung des CMS sind zunächst die Risiken des Unternehmens systematisch zu erfassen. Dies schließt ein, dass sich die verantwortlichen Personen im Unternehmen Kenntnis über die relevanten Gesetze, die mit der Geschäftstätigkeit des Unternehmens in Zusammenhang stehen, verschaffen. Compliance-Risiken ergeben sich aber nicht nur aus möglichen Verstößen gegen geltendes Recht (z.B. Bestechlichkeit und Bestechung im geschäftlichen Verkehr vgl. §299 StGB, Vorteilsgewährung und Bestechung von Amtsträgern vgl. §§333, 334 StGB, Betrug vgl. §263 StGB), vielmehr ergeben sie sich auch aus dem Geschäft und werden maßgeblich vom Geschäftsmodell, der Branche, der Internationalität des Unternehmens wie auch der Organisationsstruktur beeinflusst. Alle diese Faktoren sollten daher in einem systematischen Risikoscreening zusammenfließen.

Verantwortung und Aufsicht für die Risikoidentifikation liegen bei der Unternehmensleitung. Die Risikoidentifikation hat vor allem mit der Kenntnis des eigenen Geschäfts und Unternehmens zu tun, das bedeutet, dass für die Risikoidentifikation nicht zwingend externe Expertise von Beratungsdienstleistern o.ä. hinzugezogen werden muss.

Für mittelständische Unternehmen und Unternehmen mit geringerer Unternehmensgröße kann bezüglich der Risikoidentifikation ein Vorteil darin liegen, dass ein vergleichsweise kleiner Personenkreis das Wissen über die Geschäftsstruktur, das Geschäftsmodell und die Unternehmensorganisation in sich vereint und sich so binnen kurzer Zeit, z.B. im Rahmen mehrerer Arbeitssitzungen, einen Überblick über kritische Risiken sowie die Risikolage insgesamt verschaffen kann (zentrale Risikoerhebung). Überdies ermöglicht die weniger formalisierte Organisationsstruktur und die häufig zutreffende räumliche Nähe in kleineren Unternehmen, Mitarbeiter in Schlüsselfunktionen verschiedener Unternehmensbereiche und mit unterschiedlicher Expertise in die Entwicklung des Risikoprofils einzubinden. So kann zum einen sichergestellt werden, dass sich aus den verschiedenen Perspektiven ein umfassendes Bild über das Risikoprofil des Unternehmens ergibt. Zum anderen bewirkt die Einbindung von Mitarbeitern eine höhere Akzeptanz für die Notwendigkeit des Prozesses sowie ein höheres Bewusstsein für Compliance-Risiken, auch hinsichtlich der Verbindlichkeit in der Umsetzung daraus hervorgehender Compliance-Maßnahmen im täglichen Geschäft. In größeren Unternehmen kann zur Operationalisierung des Austauschs zwischen der Compliance-Funktion und relevanten Fachabteilungen über die Einrichtung eines Risk-Committee/Risiko-Ausschusses nachgedacht werden.

Zentrale Risikoidentifikation

Einrichtung eines Risk-Committee/ Risiko-Ausschusses

Mit zunehmender Unternehmensgröße und einer damit einhergehenden höheren Compliance-Komplexität aufgrund verstärkter internationaler Tätigkeit, stärker dezentraler Organisationsstrukturen und ggf. Diversifizierung des Produktportfolios wird es der Unternehmensleitung nicht mehr möglich sein, die Risiken ausschließlich zentral zu erfassen und zu beurteilen. Aus diesem Grund ist es erforderlich, die zentrale Risikoidentifikation um eine dezentrale Risikoidentifikation zu ergänzen und die Ergebnisse zusammenzuführen. Dies bedeutet jedoch nicht, dass nicht auch in kleineren und mittelständischen Unternehmen eine dezentrale Risikoidentifikation erwogen werden kann. Je nach Organisationsstruktur, (De-)Zentralität der Geschäftseinheiten und Geschäftsmodell kann eine ergänzend vorgenommene dezentrale Risikoidentifikation wesentliche Erkenntnisse für die Risikoexposition im Hinblick auf Compliance- und Integrity-Risiken liefern. Im Rahmen einer dezentralen Risikoidentifikation sind regelmäßig aus allen zentralen und dezentralen Geschäftseinheiten sowie den relevanten zentralen Abteilungen entsprechende Risikoerhebungen und -beurteilungen anzufordern und von der Compliance-Abteilung, ggf. unterstützt durch Experten anderer relevanter Abteilungen (z.B. Revision, Controlling, Recht), zu einem Compliance-Risikoprofil zusammenzuführen und zu aggregieren. Zur Sicherstellung der Qualität der dezentralen Risikoidentifikation und -bewertung sollte die Compliance-Abteilung den Prozess beratend begleiten und einheitliche Vorgaben und Anforderungen an die Risikoidentifikation, z.B. in Form von Checklisten oder Formularen, an die einzelnen Geschäftseinheiten herausgeben.

Dezentrale Risikoidentifikation

Einheitliche Vorgaben und Anforderungen für die Risikoidentifikation und -bewertung

In Unternehmen mit geringer Unternehmensgröße eignen sich als Methoden zur Risikoidentifikation Kreativtechniken wie Brainstorming oder Mindmapping, mithilfe derer sich idealerweise die Unternehmensleitung in gemeinsamen Workshops mit leitenden Mitarbeitern einen Überblick über die Risikofelder verschaffen und mögliche Zusammenhänge und Abhängigkeiten zwischen den verschiedenen Risikobereichen grafisch dargestellt werden können. Daneben können Expertenbefragungen (z.B. aus Verbänden, Handelskammern aber auch von Mitarbeitern in Schlüsselfunktionen) oder auf den Risikofeldern basierende Szenariobildung weitere wichtige Erkenntnisse über das Risikoprofil des Unternehmens liefern. Mit zunehmender Unternehmensgröße und -komplexität sollten auch die Methoden zur Risikoidentifikation erweitert und die Durchführung der Risikoerhebung systematisiert werden. Größere Unternehmen sollten daher Erkenntnisse aus der Tätigkeit der Internen Revision, der Risikoabteilung oder dem internen Kontrollsystem sowie aus Compliance-Vorfällen aus der Vergangenheit systematisch in die Risikoerhebung integrieren. Weitere wichtige Informationsquellen zum Risikoprofil liefern Studien und Umfragen in den Bereichen Compliance Management und Compliance-Risiken sowie eine systematische Auswertung von Branchen-, Börsen- und Medieninformationen.

Risikobewertung

Nicht alle identifizierten Risiken sind für ein Unternehmen gleich relevant, d.h. die Risiken erfordern unterschiedliche Strategien der Risikosteuerung: manche Risiken werden von der Unternehmensleitung bewusst in Kauf genommen (z.B. Investitionen in Produktentwicklungen) wohingegen andere Risiken mit allen Mitteln bestmöglich zu vermeiden sind, da ihr Eintritt für das Unternehmen existenzbedrohende Konsequenzen haben könnte. Compliance-Risiken gehören, wie oben bereits erläutert, in die zweite Kategorie. Um die identifizierten Risiken angemessen adressieren zu können, ist eine Bewertung der Risiken bezüglich ihrer Relevanz sowie insbesondere ihres Schadenspotenzials und ihrer Eintrittsmöglichkeit vorzunehmen.

Grundlegende Voraussetzung für eine ›richtige‹ Bewertung der wesentlichen Compliance-Risiken und der darauf aufbauenden risikoorientierten CMS-Ausgestaltung ist eine ehrliche und ungeschönte Einschätzung der Risiken, um Fehlsteuerungen und falschen Schwerpunktsetzungen entgegenzuwirken. Die Risiken sind zunächst als *Brutto*risiken zu erfassen, d.h. ohne die Auswirkungen bereits getroffener Gegenmaßnahmen einzubeziehen. In einem zweiten Schritt sind die Bruttorisiken den bereits implementierten Präventions- und Reduzierungsmaßnahmen sowie Kontroll- und Überwachungsprozessen gegenüberzustellen und zu beurteilen, ob die getroffenen Maßnahmen und Prozesse geeignet sind, den Compliance-Risiken angemessen vorzubeugen, bzw. wo

Bewertung der Compliance-/ Integrity-Risiken

Defizite und Verbesserungsbedarf im CMS bestehen (*Netto*risiko). Eine Risikobewertung im klassischen Sinne nach der zu erwartenden Schadenshöhe und der Eintrittswahrscheinlichkeit bzw. nach dem sich daraus berechnenden Erwartungswert als Indikator für akzeptierbare bzw. nicht-akzeptierbare Risiken ist für die Bewertung von Compliance-Risiken nur bedingt geeignet. Zum einen liegen verlässliche Anhaltspunkte für spezifische Angaben zur Schadenshöhe und Eintrittswahrscheinlichkeit häufig nicht vor (auch weil Erfahrungswerte oftmals fehlen) und ungenaue Schätzungen sind eher wenig hilfreich. Zum anderen kann eine solche klassische Bewertung der Compliance-Risiken zu falschen Schlussfolgerungen für die Risikosteuerung führen. Compliance-Risiken sind für alle Unternehmen reale Risiken mit einer gewissen qualitativen Eintrittswahrscheinlichkeit, aber einem erheblichen Schadenspotenzial. Vor allem die Beurteilung der Eintrittswahrscheinlichkeiten von Compliance-Risiken kann schnell zu falschen Schlüssen für die Risikosteuerung führen, weil hierzu eine Einschätzung individuellen Verhaltens – genauer die Wahrscheinlichkeit von Fehlverhalten der Mitarbeiter – in der Zukunft vorzunehmen ist. Diese Einschätzung allein stellt schon eine Herausforderung dar. Kommt noch hinzu, dass Unternehmen in der Regel von ihren Mitarbeitern nicht annehmen, dass sie sich gesetzeswidrig oder nicht integer verhalten, sind falsche Schlussfolgerungen bezüglich der Eintrittswahrscheinlichkeit schnell gezogen. Aus diesem Grund empfiehlt es sich bei der Bewertung von Compliance-Risiken, die Bewertung der Eintrittswahrscheinlichkeit durch die generelle Eintritts*möglichkeit* von Compliance-Risiken zu ersetzen. Die Beurteilung der Eintrittsmöglichkeiten von Compliance-Risiken kann beispielsweise szenariobasiert erfolgen: Ist es möglich, dass das Compliance-Risiko X, z.B. die Bestechung von Amtsträgern, um einen Auftrag zu gewinnen, in unserem Unternehmen eintritt? Die festgestellten Eintrittsmöglichkeiten bilden die Basis für die Einleitung von Präventionsmaßnahmen und damit Grundlage des CMS, mit dem Ziel, die Eintrittsmöglichkeiten bestmöglich zu verhindern.

— Eintrittsmöglichkeit von Compliance-Risiken

Bei der Risikobewertung und -steuerung im Rahmen des CMS sollten sich Unternehmen zunächst auf die Risiken fokussieren, die rechtlich, ökonomisch und ethisch schwerwiegend sind, und das Risikomanagement im Rahmen eines kontinuierlichen Verbesserungsprozesses anpassen und verfeinern. Anhaltspunkte für eine realitätsgetreue Risikobewertung liefern anerkannte Checklisten und Rankings, wie beispielsweise der Corruption Perceptions Index (CPI), der jährlich von der Antikorruptionsbehörde Transparency International erhoben wird und Aufschluss über die Wahrnehmung von Korruption bei Amtsträgern und Politikern in unterschiedlichen Ländern gibt, das Risk Rating des Kreditversicherers COFACE[16] sowie Studien und Befragungen von Beratungs- und Wirtschaftsprüfungsunternehmen zu Compliance-Risiken und dem Status von CMS in Unternehmen. Für die Beurteilung der Risiken aus internationaler

— Indikatoren für Compliance-Risiken

[16] http://www.coface.de/Economic-studies (16.04.2014)

Tätigkeit ist insbesondere von Bedeutung, aus welchen Bereichen/Branchen die Geschäftspartner im Ausland sind (öffentliche Auftraggeber (→ *höheres Risiko*) oder private Auftraggeber) und wie die Geschäfte abgewickelt werden (Einschaltung von Beratern oder Vertriebsmittlern (→ *höheres Risiko*) oder Abwicklung als Direktgeschäft). In jedem Fall sind die Dienstleistungen und Entlohnungsmodi der Geschäftspartner genau auf mögliche Risiken zu überprüfen.

Risikosteuerung

Dem klassischen Risikomanagementprozess folgend ergeben sich aus der Risikoidentifikation und -bewertung vier Strategien zur Risikobewältigung, anhand derer Risiken auch klassifiziert werden können:

- Risiko vermeiden
- Risiko vermindern
- Risiko überwälzen (z.B. auf eine Versicherung)
- Risiko selbst tragen/akzeptieren

Für die Steuerung von Compliance-Risiken kann aber auch eine beispielsweise nach der *Risikoursache* (systemisch bedingt vs. Individualmotivation) oder nach der *Art und Wirkung auf die unmittelbare Haftung des Unternehmens und/oder seiner Organe* vorgenommene Klassifizierung sinnvoll sein. Aus den in der Risikobewertung ermittelten Nettorisiken sind dann im Rahmen der Risikosteuerung notwendige Maßnahmen zur Risikovermeidung und -verminderung sowie – falls im Unternehmen bereits ein CMS installiert ist – Defizite und Verbesserungspotenzial im bestehenden CMS abzuleiten.

— Compliance-Risikosteuerung

An diesem Punkt, der Steuerung von Compliance-Risiken durch ein angemessenes und funktionsfähiges CMS, setzen jeweils die im Folgenden dargestellten Elemente und Maßnahmen eines CMS an, die darauf zielen, Compliance-Risiken zu vermeiden sowie Fehlverhalten aufzudecken und ggf. notwendige Reaktionsmaßnahmen durchzuführen.

Für eine nachhaltige und funktionsfähige Risikoidentifikation und -ausrichtung des CMS ist eine fortlaufende Beobachtung des Risikoumfeldes bezüglich Veränderungen, die z.B. durch einen Unternehmenszukauf oder den Eintritt in neue Märkte entstehen, unerlässlich, so dass veränderte oder neue Risiken frühzeitig erkannt und die

— Fortlaufende Analyse des Risikoumfeldes

CMS-Elemente und -Maßnahmen entsprechend ergänzt oder angepasst werden können. Zusätzlich ist eine regelmäßige, systematische Gesamtprüfung der Compliance- und Integrity-Risiken vorzunehmen, um die Funktionsfähigkeit der im Rahmen des CMS implementierten Risikosteuerungsmaßnahmen dauerhaft sicherzustellen. Erfolgt neben der zentralen Analyse der Compliance-Risiken zusätzlich eine dezentrale Erhebung und Bewertung ist z.B. im Rahmen eines regelmäßigen Risikoreportings sicherzustellen, dass Veränderungen im Risikoumfeld frühzeitig erkannt und ggf. erforderliche Gegenmaßnahmen eingeleitet werden können.

— Systematische Gesamtprüfung der Compliance-/ Integrity-Risiken

— Risikoreporting

Compliance-Organisation und Governance-System

2

Welches Ziel wird mit einer Compliance-Organisation verfolgt?

Welches sind die Aufgaben der Compliance-Organisation und der Personen, die im Unternehmen mit der Umsetzung von Compliance betraut sind?

Wer trägt die Verantwortung für Compliance im Unternehmen?

Kann Compliance an bestimmte Personen bzw. Funktionen im Unternehmen delegiert werden?

Braucht jedes Unternehmen eine eigene Compliance-Organisation?

Welche Personen bzw. Funktionen sind für die Übernahme von Compliance-Aufgaben im Unternehmen geeignet?

Gibt es eine Richtgröße, wie viele Mitarbeiter im Unternehmen Compliance-Aufgaben wahrnehmen sollten?

Welche Funktionen kommen Kontrollorganen wie dem Aufsichtsrat oder Beirat im Hinblick auf Compliance zu?

Zielsetzung

Die Unternehmensleitung trägt die Verantwortung, dass Führungskräfte und Mitarbeiter sowie die Organmitglieder und Mitarbeiter von Tochterunternehmen sich im Rahmen der dienstlichen Tätigkeit an die einschlägigen Gesetze halten (sog. Legalitätspflicht der Unternehmensleitung). Mit der Organisation von Compliance soll diese Legalitätspflicht sichergestellt werden, d.h. Rechtsverstöße sollen bestmöglich vermieden werden. Dabei hat die Organisation von Compliance nicht zum Ziel, eine 100%ige Sicherheit im Unternehmen herzustellen. Es wird immer einzelne Mitarbeiter geben, die sich vorsätzlich über Gesetze und interne Richtlinien hinwegsetzen und kriminelle Verstöße begehen. Dieses potenzielle (Rest-)Risiko lässt sich auch nicht durch eine Compliance-Organisation vollständig eliminieren. Mit der Einrichtung einer Compliance-Organisation werden vielmehr systematisches, bewusstes oder gar kriminelles Fehlverhalten erschwert sowie unbeabsichtigte Verstöße bestmöglich verhindert. Über eine Organisation erhält das Thema Compliance somit Strukturen, die das Schadensrisiko für das Unternehmen erheblich verringern.

Legalitätspflicht der Unternehmensleitung

»Der Vorstand hat für die Einhaltung der gesetzlichen Bestimmungen und der unternehmensinternen Richtlinien zu sorgen und wirkt auf deren Beachtung durch die Konzernunternehmen hin (Compliance).«
Ziff. 4.1.3 Deutscher Corporate Governance Kodex

Zur Erfüllung ihrer gesellschaftsrechtlichen Organisations- und Sorgfaltspflichten kommt die Unternehmensleitung deshalb nicht umhin, entsprechende organisatorische Maßnahmen zu ergreifen. Kommt es zu Verstößen und kann die Unternehmensleitung keine oder nur unzulänglich implementierte organisatorische Maßnahmen vorweisen, so läuft sie Gefahr, dass gegen sie und das Unternehmen ein Bußgeld wegen Verletzung der Organisations- und Aufsichtspflichten verhängt wird (vgl. §§30, 130 OWiG). Daneben trägt die Unternehmensleitung von Kapitalgesellschaften das Risiko, bei Verletzung ihrer gesellschaftlichen Organisations- und Sorgfaltspflichten der Gesellschaft gegenüber für einen entstanden Schaden persönlich zur Verantwortung gezogen zu werden.[17] Der deutsche Gesetzgeber hat zwar mit der Kodifizierung der aus den USA stammenden Business Judgement Rule in §93 Abs.1 S.2 AktG[18] dem Umstand Rechnung getragen, dass unternehmerische Tätigkeit zwangsläufig das Eingehen von Risiken beinhaltet und die Unternehmensleitung ihre gesellschaftsrechtlichen Organisations- und Sorgfaltspflichten nicht verletzt, wenn sie sich vor einer Entscheidung hinreichend informiert hat, sich nicht in einem Interessenkonflikt befand und darauf vertrauen durfte, zum Besten der Gesellschaft zu handeln. Allerdings gilt das Privileg der Business Judgement Rule nur für unternehmerische Entscheidungen, nicht hingegen für die Erfüllung der Legalitätspflicht, also die Einhaltung von gesetzlichen Vorschriften. Insofern steht die Frage, ob Compliance im Unternehmen einer Organisation und Umsetzung bedarf, nicht zur Disposition der Unternehmensleitung. Es gilt schlicht, dass jedes Unternehmen die Organisation von Compliance vorzunehmen hat. Zu der Frage, wie die Organisation von Compliance auszugestalten ist, gibt es bislang keine konkreten gesetzlichen Vorgaben. So existiert für Unternehmen (bislang) auch keine gesetzliche Pflicht, eine formale eigenständige Compliance-Abteilung einzurichten. Der Unternehmensleitung obliegt diesbezüglich vielmehr ein Ermessensspielraum, wie und mit welchen Mitteln sie die Organisation ausgestalten möchte. Mag es für kleinere Unternehmen ausreichend sein, weniger formale Organisationsstrukturen einzurichten, so werden jedoch mit zunehmender Unternehmensgröße und Komplexität des Geschäfts die Anforderungen an die Organisation im Hinblick auf Umfang und Formalisierungsgrad steigen und bei Erreichen einer bestimmten Unternehmenskomplexität in einer umfassenden Compliance-Abteilung enden müssen. Letztendlich trägt die Unternehmensleitung die Verantwortung dafür, eine auf das Unternehmen zugeschnittene und funktionierende Compliance-Organisation einzurichten.

Privileg der Business Judgement Rule gilt nicht für die Erfüllung der Legalitätspflicht

Ermessensspielraum der Unternehmensleitung

[17] Erst im vergangenen Dezember 2013 verurteilte das Landgericht München I in einem zivilrechtlichen Haftungsprozess den ehemaligen CFO eines großen deutschen Konzerns zur Zahlung von Schadensersatz in Höhe von 15 Mio. Euro an seinen ehemaligen Dienstherrn. Das Vorstandsmitglied habe seine Organisations- und Aufsichtspflichten verletzt und Schmiergeldzahlungen seitens Mitarbeiter nicht nachhaltig verhindert (Urteil LG München I vom 10.12.2013, Az.: 5HK O 1387/10).

[18] Die im Aktienrecht kodifizierte Business Judgement Rule (§93 Abs.1 S.2 AktG) gilt nach der Rechtsprechung nicht nur für Vorstände einer AG, sondern entsprechend für Geschäftsführer einer GmbH (vgl. Urteil BGH vom 04.11.2002 – Az. II ZR 224/00, in NJW 2003, 358; Urteil OLG Frankfurt a.M. vom 25.10.2011 – Az. 5 U 27/10, in BeckRS 2011, 27373).

Empfehlungen für die Umsetzung

Compliance-Aufgaben

Nachdem das Unternehmen seine spezifischen Risiken definiert hat, gilt es, in den entsprechenden Risikobereichen die erforderlichen Maßnahmen zu implementieren, um Rechtsverstöße – seien sie vorsätzlich oder unbeabsichtigt begangen – bestmöglich zu vermeiden.

Dabei liegt die Primärverantwortung für Compliance bei der Unternehmensleitung. Die Unternehmensleitung hat dafür Sorge zu tragen, dass die erforderlichen Compliance-Aufgaben im Unternehmen entsprechend umgesetzt werden. Zu den wesentlichen Compliance-Aufgaben zählen insbesondere die Maßnahmen, die in den einzelnen Leitlinien und dieser Guidance zu den 8 CMS-Elementen (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) näher beschrieben sind. Danach gehören zu den Compliance-Aufgaben unter anderem:

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
- die Veranlassung und Durchführung von Sensibilisierungs-, Kommunikations- und Schulungsmaßnahmen zu Compliance-relevanten Themen
- Beratung von Management und Mitarbeitern bei auftretenden Fragen zum Thema Compliance
- die Veranlassung und Durchführung von Kontroll- und Überwachungsmaßnahmen
- die Mitwirkung bei der Durchführung bzw. Veranlassung von Untersuchungsmaßnahmen bei möglichen Compliance-Verstößen
- eine regelmäßige Compliance-Berichterstattung an die Unternehmensleitung und ggf. weitere Adressaten wie Aufsichtsgremien und weitere Stakeholder
- das Ergreifen von Abhilfemaßnahmen im Falle der Kenntnis von Compliance-Defiziten

Compliance-Governance und operative Umsetzung von Compliance

Um die Compliance-Aufgaben im Rahmen einer verantwortungsvollen Unternehmensorganisation ordnungsgemäß erfüllen zu können, hat die Unternehmensleitung entsprechende auf das Unternehmen zugeschnittene Organisationsstrukturen einzurichten.

Wahrnehmung der Compliance-Funktion durch Unternehmensleitung

In kleinen Unternehmen, für die sich aufgrund ihrer Geschäftstätigkeit keine besonderen Risiken ergeben, werden in der Regel auch keine gesteigerten Compliance-Anforderungen zu erwarten sein. Die Einrichtung einer eigenen Compliance-Abteilung wird grundsätzlich ebenso entbehrlich sein wie die Ausübung der Compliance-Aufgaben als Vollzeitbeschäftigung. Für kleine Unternehmen, in denen die Unternehmensleitung selbst stark in das Tagesgeschäft eingebunden ist, die Mitarbeiter alle persönlich kennt und überwiegend selbst das Geschäft und die einzelnen Prozesse steuert und

lenkt, kann es sich daher anbieten, die Umsetzung der Compliance-Aufgaben vollständig bei der Unternehmensleitung zu belassen. Neben den Kostenvorteilen liegen die Vorzüge insbesondere darin, dass die Unternehmensleitung, die sich selbst des Themas annimmt, sowohl nach innen als auch nach außen demonstriert, dass das Thema Compliance für das Unternehmen eine wichtige Bedeutung hat und einen sehr hohen Stellenwert einnimmt. In solchen Fällen dürfte zu erwarten sein, dass bei den Beschäftigten das Thema Compliance, das unmittelbar vom Chef aus wahrgenommen wird, eine größere Akzeptanz erfährt, als bei der Delegation auf nachgeordnete Unternehmensebenen (vgl. auch das CMS-Element → 8 FÜHRUNG UND UNTERNEHMENSKULTUR).

Gesamtverantwortung aller Unternehmensleitungsmitglieder

Besteht die Unternehmensleitung (Geschäftsführung, Vorstand) aus mehreren Personen, so gilt nach deutschem Recht eine Gesamtverantwortlichkeit aller Mitglieder der Unternehmensleitung für alle Angelegenheiten der Gesellschaft, insbesondere für die Erledigung sämtlicher Geschäfte, die der Betrieb des Unternehmens mit sich bringt. Wird ein Aufgabenbereich im Rahmen einer zulässigen Geschäftsverteilung an ein Mitglied der Unternehmensleitung delegiert, so entbindet dies allerdings die anderen Mitglieder der Unternehmensleitung nicht von ihrer gesellschaftsrechtlichen Gesamtverantwortung. Die Gesamtverantwortung wandelt sich vielmehr in eine Ressortüberwachungspflicht mit der Folge, dass jedes Unternehmensleitungsmitglied grundsätzlich weiterhin verpflichtet bleibt, die Verhältnisse in den einem anderen Mitglied der Unternehmensleitung übertragenen Geschäftsbereichen im Auge zu behalten. Insbesondere große Unternehmen werden im Hinblick auf die Vielzahl und Komplexität der Geschäftsführungsaufgaben nicht umhinkommen, im Wege der Ressortverteilung die verschiedenen Verantwortungsbereiche auf die einzelnen Mitglieder der Unternehmensleitung zu delegieren. Dabei sollte auch der Bereich Compliance unter dem Gesichtspunkt der Leitungsverantwortung einer verantwortungsvollen Unternehmensorganisation einem Mitglied der Unternehmensleitung übertragen werden – von großen multinationalen Unternehmen ist dies im Sinne einer guten Corporate Governance letztendlich sogar zu erwarten. Erfolgt eine entsprechende Ressortverteilung, so ist darauf zu achten, dass die Delegation insbesondere klar und eindeutig erfolgt und entsprechend schriftlich festgehalten wird, welches Organmitglied in welchem Umfang zuständig ist.

Ressortüberwachungspflicht

Delegation von Compliance

Mit zunehmender Unternehmensgröße werden die Aufgaben von Compliance nicht mehr von der Unternehmensleitung bzw. dem Unternehmensleitungsmitglied, dem die Ressortverantwortung für Compliance zugeteilt worden ist, allein zu erfüllen sein. Um das operative Geschäft zu erleichtern und die Unternehmensleitung zu entlasten, wird es weiterhin erforderlich sein, die Compliance-Aufgaben an nachgeordnete Personen im Unternehmen zu delegieren. Art und Umfang der Delegation von Compliance-Aufgaben werden von der jeweiligen Unternehmensgröße und -komplexität abhängen. Mag es bei kleineren Unternehmen zur Unterstützung der

Unternehmensleitung, welche die Compliance-Funktion ausübt, ausreichend sein, dass lediglich bestimmte Aufgaben delegiert werden, so wird mit zunehmender Unternehmensgröße die Notwendigkeit einer umfassenden Delegation und mithin umfassenden Compliance-Organisation notwendig sein.

Eine Delegation von Compliance-Aufgaben an nachgeordnete Unternehmensebenen erfordert zunächst eine sorgfältige Auswahl der mit Compliance-Aufgaben betrauten Personen. Die Unternehmensleitung hat sicherzustellen, dass die Auswahl auf fachlich kompetente und zuverlässige Personen fällt. Als geeignete Personen können z.B. Bereichs- bzw. Abteilungsleiter der verschiedenen Fachabteilungen wie Recht oder Revision mit Compliance beauftragt werden. Von Vorteil ist, dass diese Personen über erforderliche juristische und/oder betriebswirtschaftliche Kenntnisse verfügen, die für die Wahrnehmung der Compliance-Aufgaben unerlässlich sind.

Stehen kleinen Unternehmen entsprechende Ressourcen intern nicht zur Verfügung und ist es auch der Unternehmensleitung nicht möglich, die Compliance-Aufgaben wahrzunehmen, so ist für kleine bis mittelständische Unternehmen eine Ausgliederung von (bestimmten) Compliance-Aufgaben an externe Dienstleister/Experten denkbar. Allerdings ist hierbei in Betracht zu ziehen, dass ein Outsourcen von Compliance an externe Dritte das Risiko bergen kann, dass die Wichtigkeit des Themas und der Stellenwert von Compliance von den Mitarbeitern im Unternehmen nicht ernst genommen werden, weshalb es im Falle einer Ausgliederung der Compliance-Aufgaben für die Unternehmensleitung umso mehr unerlässlich sein wird, für ein klares Bekenntnis zur Compliance und Integrität im Geschäftsalltag durch regelmäßige Kommunikation und entsprechendes Vorbildverhalten zu sorgen (vgl. hierzu CMS-Element → 8 FÜHRUNG UND UNTERNEHMENSKULTUR).

Outsourcing von Compliance

Da jedoch auch in kleineren Unternehmen aufgrund gesetzlicher Regelungen bestimmte Unternehmensbeauftragte wie der Datenschutzbeauftragte, der Exportkontrollbeauftragte u.a. zu bestellen sind, kann als weitere Möglichkeit in Betracht gezogen werden, die Compliance-Funktion oder zumindest bestimmte Compliance-Aufgaben an diese Personen zu delegieren.[19] Denn aufgrund ihrer Bestellung als Unternehmensbeauftragte werden diese Personen in vielen Fällen nicht nur über gute Kenntnisse des eigenen Unternehmens insgesamt, sondern auch über bestimmte juristische (Grund-) Kenntnisse verfügen.

Delegation an Unternehmensbeauftragte

[19] Eine Übersicht zu den betrieblichen Unternehmensbeauftragten ist im ANNEX im → KAPITEL IV zu finden.

Für Unternehmen, die aufgrund einer entsprechenden Unternehmensgröße und -komplexität bereits über Fachabteilungen, wie eine Rechts- und oder Revisionsabteilung verfügen, bietet sich an, die Wahrnehmung der Compliance-Aufgaben einer solchen Abteilung zu übertragen. In diesen Fällen werden die Compliance-Aufgaben üblicherweise von einem internen Unternehmensjuristen oder Innenrevisor in der Regel neben der eigentlichen Hauptaufgabe wahrgenommen. Dennoch ist die Wahrnehmung von Compliance-Aufgaben nicht auf diesen Personenkreis beschränkt. Als weitere geeignete Personen im Unternehmen können beispielsweise die Personalleitung oder die Leitung einer anderen Fachabteilung in Betracht kommen.

Delegation an Fachabteilung

Je größer und komplexer ein Unternehmen ist, umso größer sind die organisatorischen Anforderungen an Compliance, um die sorgfältige Aufgabenerfüllung zu gewährleisten. Für größere Unternehmen (Unternehmen der Leitlinien 3 und 4) wird es zur Erfüllung der Compliance-Aufgaben häufig erforderlich sein, eine eigenständige Compliance-Abteilung einzurichten. Eine solche kann zwar durchaus an bestehende Unternehmensfunktionen wie z.B. Recht, Revision, HR angesiedelt werden, wobei in diesen Fällen zur Vermeidung von Interessenkonflikten gewährleistet sein muss, dass die Compliance-Funktion möglichst keine weitere Funktion im Unternehmen ausübt. Die Compliance-Funktion sollte daher im Hinblick auf mögliche Interessenkonflikte nicht gleichzeitig Leiter der Rechtsabteilung oder Leiter der Revisionsabteilung sein.[20] Für große multinationale (DAX-)Unternehmen dürfte eine eigenständige Compliance-Abteilung mit einem zentralen Compliance-Beauftragten (auch Compliance Officer oder Chief Compliance Officer), der für die Umsetzung von Compliance im gesamten Unternehmensverbund verantwortlich ist und direkt an das für Compliance verantwortliche Ressortmitglied der Unternehmensleitung regelmäßig über den Stand des CMS, ggf. über Fehlverhalten und Compliance-Vorfälle sowie die Umsetzung von Compliance und Integrität im Unternehmen insgesamt berichtet, unerlässlich sein. Es ist wichtig, die Compliance-Verantwortung zentral in der Person des Compliance-Beauftragten zu bündeln. Nur so kann sichergestellt werden, dass alle wichtigen Compliance-Themen wie z.B. auftretende Compliance-Fälle in der zentralen Compliance-Organisation ankommen und von dieser entsprechend bearbeitet werden. Eine Kombination der Compliance-Funktion mit weiteren Aufgabenbereichen wie z.B. Recht und Revision wird daher in der Regel eher bei (größeren) mittelständischen Unternehmen noch als geeignete Organisationsmaßnahme angesehen werden können.

Eigenständige Compliance-Abteilung

In kleinen und mittelständischen Unternehmen kann auch die Übertragung der Umsetzungsverantwortung für die Compliance-Aufgaben an ein autonomes kollegiales

[20] Vgl. Grüninger, S./Steinmeyer, R./Strenger, C. (im Erscheinen): Compliance und Aufsicht. In: Wieland, J., Steinmeyer, R., Grüninger, S. (Hrsg.): Handbuch Compliance-Management, 2. Auflage.

Compliance-Gremium (auch Compliance-Expertengruppe oder Compliance-Committee genannt), bestehend aus Vertretern der verschiedenen relevanten Fachbereiche des Unternehmens wie z.B. Recht, Revision, HR, Einkauf, Vertrieb, Technik in Betracht gezogen werden. Das Compliance-Gremium kann dabei als bloßes Beratungsgremium oder als Gremium mit Beratungs- und zusätzlicher Steuerungs- und Lenkungsfunktion ausgestaltet werden. Der wesentliche Vorteil ist darin zu sehen, dass ohne erhebliche Zusatzkosten auf bereits bestehende Ressourcen im Unternehmen zurückgegriffen werden kann. Ein derartiges Modell kann jedoch nur funktionieren, wenn diesen ins Compliance-Gremium berufenen Personen neben ihrer Haupttätigkeit auch tatsächlich die erforderliche Zeit für die Compliance-Aufgaben zur Verfügung gestellt wird. Des Weiteren sind aufgrund der größeren Gefahr von Überlappungen und der grundsätzlich fehlenden Weisungsgebundenheit der Personen untereinander klare Kompetenz- und Aufgabenzuschreibungen der einzelnen Personen erforderlich. Andernfalls besteht die Gefahr, dass sich letztlich keine der verantworteten Personen verantwortlich fühlt und Aufgaben und Pflichten nicht erfüllt werden. Und schließlich ist über ein klar definiertes Berichtswesen festzulegen, welche Person(en) des Compliance-Gremiums der Unternehmensleitung gegenüber zu Compliance-relevanten Themen zu berichten hat (haben). Während für kleinere mittelständische Unternehmen ein Compliance-Gremium eine geeignete Alternative zu einer Compliance-Abteilung darstellen kann, ist für große Unternehmen ein solches Gremium aufgrund der zunehmenden Unternehmenskomplexität und sich daraus ergebenden steigenden Arbeitsbelastung für die Compliance-Funktion grundsätzlich nicht als Ersatz einer Compliance-Abteilung geeignet. Dennoch empfiehlt sich, auch in diesen Unternehmen zur Unterstützung der Compliance-Funktion die Einrichtung eines entsprechenden Compliance-Gremiums in Betracht zu ziehen. Auch falls ein Unternehmen sich gegen die Einsetzung eines Compliance-Committee entscheidet, ist zu empfehlen, die unterschiedlichen im Unternehmen vorhandenen Ressourcen sinnvoll zu bündeln und im Wege effektiver, aufeinander abgestimmter Strategien effizient im Unternehmen einzusetzen (Integration von Governance, Risk und Compliance (GRC)).

Compliance-Gremium/ Compliance-Committee

Integration von GRC

Wird die Compliance-Funktion nicht unmittelbar durch die Unternehmensleitung selbst wahrgenommen, sondern an eine nachgeordnete Stelle oder Person im Unternehmen delegiert, so ist sicherzustellen, dass die mit der Compliance-Funktion verantwortete Person nicht nur über die erforderlichen fachlichen und persönlichen Kompetenzen verfügt, sondern für die ordnungsgemäße Aufgabenwahrnehmung unabhängig ist und ihr hierfür entsprechend weitreichende Befugnisse eingeräumt werden. So sieht beispielsweise die Rechtsprechung es als erforderlich an, dass der Compliance-Beauftragte die Befugnis haben muss, eigene interne Untersuchungen durchzuführen.[21]

[21] Vgl. Moosmayer, K. (2012): Modethema oder Pflichtprogramm guter Unternehmensführung? – Zehn Thesen zu Compliance. In: NJW 2012, S. 3014.

Aus diesem Grund ist es erforderlich, dass der Compliance-Beauftragte einer entsprechend hohen Hierarchiestufe angehört. Auch die weiteren mit Compliance-Aufgaben betrauten Personen sind nicht nur sorgfältig auszuwählen, sondern auch durch geeignete Aus- und Fortbildungsmaßnahmen entsprechend zu befähigen (vgl. CMS-Element → 5 COMPLIANCE-KOMMUNIKATION & SCHULUNG). Bei der Aufgabenverteilung bzw. -zuweisung sind klare Kompetenzen und Verantwortlichkeiten festzulegen und Doppelverantwortlichkeiten sowie Kompetenzüberschneidungen unbedingt zu vermeiden. Andernfalls besteht die Gefahr, dass sich letztlich keine der verantworteten Personen verantwortlich fühlt und Aufgaben und Pflichten nicht erfüllt werden. Klar definierte Verantwortungsbereiche legen den jeweiligen Handlungsrahmen fest und bieten dadurch Orientierung für die Verantwortlichen und führen zu Sicherheit bei der Entscheidung. Zu Dokumentations- und Beweiszwecken sollten festgelegte Kompetenzen und Verantwortlichkeiten sowie deren Delegation schriftlich festgehalten werden. Dies wird in großen Unternehmen grundsätzlich z.B. in den jeweiligen Stellenbeschreibungen sowie in einem Unternehmensorganigramm geschehen und wird auch kleineren Unternehmen empfohlen.

Hierarchische Einordnung des Compliance-Beauftragten

Festlegung klarer Kompetenzen und Verantwortlichkeiten

»Wer Verantwortung gem. §130 OWiG delegiert, hat darauf zu achten, daß Kompetenzüberschneidungen vermieden werden«
OLG Düsseldorf, Beschluss vom 12.11.1998 - 2 Ss OWI 385–98 - (OWI) 112–98 III

In Unternehmen mit inländischen sowie ausländischen Beteiligungsgesellschaften ist die zentrale Compliance-Abteilung durch Compliance-Beauftragte in den Beteiligungsgesellschaften vor Ort zu unterstützen. Ohne den Einsatz solcher dezentralen Compliance-Beauftragten wird es einem Unternehmen schwerlich möglich sein, Compliance in sämtlichen Unternehmenseinheiten und Geschäftsbereichen sachgerecht umzusetzen und die Funktionalität von Compliance im Unternehmensverbund zu gewährleisten. Über dezentrale Compliance-Beauftragte lassen sich nicht nur Maßnahmen vor Ort leichter umsetzen und implementieren, sondern auch eine umfassende Berichterstattung über Compliance-relevante Vorkommnisse besser sicherstellen. In welchen Beteiligungsgesellschaften sowie in welchem Umfang dezentrale Compliance-Beauftragte einzusetzen sind, wird sich an der Größe, Komplexität und dem Risiko der zugeordneten Geschäftseinheit orientieren müssen.

Dezentrale Compliance-Beauftragte

Damit die Compliance-Organisation eines Unternehmens ihre Aufgaben erfüllen kann, ist sie mit den notwendigen finanziellen und personellen Ressourcen auszustatten. Gesetzliche Vorgaben gibt es weder zu der erforderlichen Anzahl an Mitarbeitern, die im Unternehmen mit Compliance-Aufgaben zu betrauen sind, noch zu dem Umfang zu notwendigen finanziellen Mitteln. Die erforderliche Anzahl an Compliance-Mitarbeitern im Unternehmen sowie die erforderlichen finanziellen Mittel hängen vielmehr von dem Inhalt der zu bewältigenden Aufgaben ab. In kleinen und mittleren Unternehmen mit übersichtlichem Geschäftsmodell und niedriger Risikoexposition

Angemessene Ressourcenausstattung der Compliance-Organisation

kann es ausreichend sein, dass die Compliance-Funktion neben ihrer Haupttätigkeit nur einen geringen Anteil für die Compliance-Aufgaben aufzuwenden hat. Für mittelgroße und große Unternehmen hingegen wird es im Hinblick auf die zunehmende Unternehmenskomplexität und der damit verbundenen vielseitigen und umfassenden Compliance-Aufgaben erforderlich sein, einen eigens hierfür verantwortlichen Compliance-Beauftragten – in der Regel Compliance Officer oder Chief Compliance Officer genannt – für die ordentliche Erfüllung von Compliance zu bestellen, der mindestens 50% seiner Arbeitszeit für die Aufgabenwahrnehmung aufbringt.

Personelle Ausstattung der Compliance-Funktion

Auch der Compliance-Funktion selbst sind zur Erfüllung der Compliance Aufgaben die notwendige Zeit einzuräumen und ausreichende Sach- und Finanzmittel sowie personelle Ressourcen zur Verfügung zu stellen. Entsprechend wissenschaftlicher Studien sowie Fällen aus der Praxis sollte der Compliance-Funktion je 2.000 Mitarbeiter im Unternehmen eine vollzeitäquivalente Arbeitskraft für Compliance zur Verfügung stehen.[22] Dieser Wert darf allerdings nicht als starre Größe angesehen werden. Vielmehr kommt es für die Ressourcenausstattung auf weitere Faktoren wie das jeweilige Geschäftsmodell, den Internationalisierungsgrad etc. an.[23] Letztendlich liegt es im Ermessen der Unternehmensleitung, die Angemessenheit der Ressourcen zu beurteilen und festzulegen. Um eine angemessene Ressourcenfestlegung sicherzustellen, hat sich die Unternehmensleitung intensiv und gründlich mit den erforderlichen unternehmensspezifischen Compliance-Aufgaben auseinanderzusetzen. Kommt es im Unternehmen zu Compliance-Verstößen und stellt sich heraus, dass Compliance mangels ausreichend zur Verfügung gestellter Ressourcen nicht funktioniert hat, so trägt die Unternehmensleitung das Risiko, wegen Verletzung der Organisations- und Sorgfaltspflichten für die dem Unternehmen entstandenen Schäden zur Verantwortung gezogen zu werden.

»Im Fall einer Delegierung von Verantwortung nach § 130 OWiG trifft den an sich Verantwortlichen zwar eine Aufsichtspflicht. Die zu verlangenden Aufsichtsmaßnahmen müssen jedoch zumutbar und praktisch durchführbar sein.«
OLG Düsseldorf, Beschluss vom 12.11.1998 - 2 Ss OWI 385–98 - (OWI) 112–98 III

Aufgrund ihrer Primärverantwortung für Compliance ist die Unternehmensleitung im Falle der Delegation von Compliance oder einzelner Compliance-Aufgaben verantwortlich, entsprechende Aufsichtsmaßnahmen einzurichten und zu überprüfen, ob sämtliche delegierten Compliance-Aufgaben auch ordnungsgemäß ausgeführt werden. Werden auch Überwachungs- und Kontrollaufgaben seitens der Unternehmensleitung delegiert, so ist sie auch zur Aufsicht der mit Überwachungs- und Kontrollaufgaben verantworteten Personen verpflichtet.

Überwachung der mit Compliance beauftragten Personen

[22] Zu dem gleichen Wert vgl. die PwC-Studie ›Wirtschaftskriminalität und Unternehmenskultur 2013‹, S. 30.

[23] So gibt es z.B. Unternehmen mit einem großen Anteil an Produktionsmitarbeitern im Verhältnis zur Gesamtmitarbeiterzahl oder reine Handelsunternehmen mit einer sehr großen Mitarbeiterzahl, aber überwiegend nationaler Geschäftstätigkeit. In beiden genannten Fällen dürfte das Unternehmen in der Regel eher geringeren Compliance-Risiken ausgesetzt sein, was eine geringere personelle Ausstattung der Compliance-Funktion durchaus rechtfertigen kann.

Einrichtung eines Berichtswesens

Da die Gesamtverantwortung für Compliance auch bei zulässiger Delegation stets bei der Unternehmensleitung verbleibt, ist es unabdingbar, dass sie über alle wesentlichen Vorgänge im Unternehmen sowie über alle relevanten Informationen Kenntnis erlangt (von unten nach oben). Nur so wird es der Unternehmensleitung möglich sein, erforderliche und wichtige Entscheidungen treffen zu können und Compliance-Gefahren und Risiken rechtzeitig abzuwenden. Daher stellt die Einrichtung und Sicherstellung eines funktionierenden Berichtswesens im Unternehmen eine weitere wichtige organisatorische Aufgabe der Unternehmensleitung dar.

Regelmäßige Jours Fixes

Nimmt die Unternehmensleitung die Compliance-Funktion selbst wahr, so kann die Informationsbeschaffung z.B. über regelmäßige Jours Fixes erfolgen, in denen ein gegenseitiger Informationsaustausch zwischen der Unternehmensleitung und den Mitarbeitern bzw. den (Bereichs-)Leitern zu Compliance-Themen erfolgt.

Berichtspflicht des Compliance-Beauftragten an Unternehmensleitung

Wurden Compliance-Aufgaben hingegen delegiert, so ist zur Sicherstellung eines funktionierenden Informationswesens erforderlich, dass eine Informationspflicht des Compliance-Beauftragten festgelegt wird, die ihn zu einer *regelmäßigen* Berichterstattung gegenüber der Unternehmensleitung verpflichtet. Ein Berichtswesen, das eine Compliance-Berichterstattung in das Ermessen des Compliance-Beauftragten stellt und nur eine Ad-hoc-Berichterstattung vorsieht, birgt erhebliche Gefahren. So kann der Compliance-Beauftragte z.B. fälschlicherweise zu der Einschätzung kommen, dass bestimmte Compliance-Vorfälle als nicht relevant anzusehen sind und er eine entsprechende Berichterstattung unterlässt. Kommt es zu erneuten gleichartigen Verstößen und stellt sich heraus, dass diese vermieden worden wären, falls über die vorherigen Verstöße Bericht erstattet worden wäre, so wird die Funktionsfähigkeit des CMS schnell in Frage stehen. In großen Unternehmen ist daher eine mindestens jährlich erfolgende, schriftliche Berichtspflicht des Compliance-Beauftragten an die Unternehmensleitung festzulegen.

Die Informationspflicht des Compliance-Beauftragten sollte in großen Unternehmen über eine direkte Berichtslinie an das Mitglied der Unternehmensleitung

festgelegt werden, dem im Rahmen der Geschäfts- bzw. Ressortverteilung das Thema Compliance zugeteilt worden ist. Damit der Informationsfluss auch tatsächlich funktionieren kann, ist es gerade in großen Unternehmen, in denen die Unternehmensleitung grundsätzlich schwerer erreichbar ist als in kleinen Unternehmen, erforderlich, dass der Compliance-Beauftragte neben der regelmäßigen Berichterstattung auch jederzeit ad-hoc Zugang zur Unternehmensleitung hat, um unverzüglich über besondere und wichtige Vorkommnisse berichten zu können. Insbesondere in Krisensituationen ist es für den Compliance-Beauftragten von erheblicher Bedeutung, einen schnellen Zugang zur Unternehmensleitung zu haben, um sicherzustellen, dass die Unternehmensleitung erforderliche wichtige Entscheidungen schnellst möglich treffen kann.

Direkte Berichtslinie des Compliance-Beauftragten an Unternehmensleitung

Jederzeitiger Zugang des Compliance-Verantwortlichen zur Unternehmensleitung

Gerade in großen Unternehmen, die überwiegend als (Kapital-)Gesellschaften mit Aufsichtsgremium (Beirat/Aufsichtsrat) formiert sein werden, wird die Unternehmensleitung nicht umhinkommen, ein Berichtswesen einzurichten und die Erwartungen daran klar zu kommunizieren, damit sie ihrer gesetzlichen Auskunfts- und Berichtspflicht ordnungsgemäß nachkommen kann.[24] Neben der Berichtpflicht des Compliance-Beauftragten an die Unternehmensleitung ist darüber zu entscheiden, inwieweit der Compliance-Beauftragte ein Recht auf direkte Berichtsmöglichkeit/direktes Informationsrecht gegenüber dem Aufsichtsrat haben soll. Grundsätzlich steht nach der herrschenden Literatur dem Vorstand das sogenannte Informationsmonopol zu, wonach eine Direktberichterstattung des Compliance-Beauftragten an den Aufsichtsrat ohne Einverständnis des Vorstands grundsätzlich nicht zulässig ist. Allgemein anerkannt ist jedoch die Ausnahme hiervon, wenn ein Verdacht besteht, dass Vorstandsmitglieder selbst in Compliance-Verstöße verwickelt sind. Ferner ist eine direkte Berichterstattung des Compliance-Beauftragten an den Aufsichtsrat sowie ein Recht des Aufsichtsrats, direkt beim Compliance-Beauftragten Berichte anzufordern, dann zulässig, wenn in der

Berichtsmöglichkeit des Compliance-Beauftragten gegenüber Aufsichtsrat

[24] Z.B. die Berichts- und Auskunftspflicht des Vorstands (gem. §90 AktG gegenüber dem Aufsichtsrat, gem. §131 AktG gegenüber der Hauptversammlung) sowie die jährliche Erklärungspflicht von Vorstand und Aufsichtsrat von börsennotierten Gesellschaften zum Deutschen Corporate Governance Kodex (§161 AktG). Am 16. April 2013 hat die Europäische Kommission einen Vorschlag für eine Richtlinie *zur Änderung der Richtlinien 78/660/EWG und 83/349/EWG des Rates im Hinblick auf die Offenlegung nichtfinanzieller und die Diversität betreffender Informationen durch bestimmte große Gesellschaften und Konzerne* übernommen, die die Transparenz bestimmter großer Unternehmen in sozialen und ökologischen Fragen verbessern soll. Mit dieser Richtlinie sollen die Bilanzierungs-Richtlinien (Vierte und Siebte Rechnungslegungs-Richtlinien über den Jahresabschluss und den konsolidierten Abschluss, 78/660/EWG und 83/349/EWG) ergänzt werden mit dem Ziel, die Transparenz und die Verfolgung ökologischer und sozialer Aspekte von Unternehmen in der EU zu erhöhen und damit einen wirksamen Beitrag zu langfristigem wirtschaftlichen Wachstum und Beschäftigung zu leisten. Nach diesem Gesetzesvorschlag sollen künftig Gesellschaften, die durchschnittlich **mehr als 500 Mitarbeiter** beschäftigen **und** entweder eine **Bilanzsumme von mehr als 20 Mio. Euro oder einen Nettoumsatz von mehr als 40 Mio. Euro aufweisen**, u.a. in ihrem Lagebericht eine Erklärung abgeben müssen, die mindestens wesentliche Angaben zu Umwelt-, Sozial- und Arbeitnehmerbelangen, zur Achtung der Menschenrechte und zur Bekämpfung von Korruption und Bestechung enthält. Verfolgt eine Gesellschaft in einem oder mehreren dieser Bereiche keine spezielle Politik, so soll sie künftig erklären müssen, warum dies der Fall ist. Der Vorschlag der Richtlinie ist abrufbar unter: http://ec.europa.eu/internal_market/accounting/non-financial_reporting/index_de.htm (16.04.2014).

Satzung oder in der Berichtsordnung zwischen Vorstand und Aufsichtsrat ein direkter Berichtsweg vertraglich festgeschrieben wurde. Daher sollte in großen Unternehmen im Hinblick auf eine verantwortungsvolle Unternehmensorganisation die Berichtspflicht des Compliance-Beauftragten an die Unternehmensleitung um eine zwischen Vorstand und Aufsichtsrat vertraglich festgelegte jederzeitige Berichtsmöglichkeit (*dotted line*) sowie um eine jährliche Berichtspflicht des Compliance-Beauftragten an das Aufsichtsgremium ergänzt werden. Hierdurch wird letztendlich sichergestellt, dass auch die Aufsichtsgremien ihrer gesetzlichen Überwachungs- und Einlenkungspflicht besser gerecht werden können.

Hat das Unternehmen dezentrale Compliance-Beauftragte eingesetzt, so ist mit zunehmender Unternehmensgröße und Komplexität insbesondere auf ein effizientes Berichtssystem innerhalb der Compliance-Organisation zu achten. Dies erfordert auch eine Berichtspflicht der dezentralen Compliance-Beauftragten, die von der Unternehmensleitung einzufordern ist. Die Berichterstattung der dezentralen Compliance-Beauftragten kann sowohl an den jeweiligen Fachvorgesetzten (z.B. den Leiter einer Geschäftseinheit), an übergeordnete Compliance-Beauftragte (z.B. sog. Regional Compliance Officer) als auch direkt an die zentrale Compliance-Abteilung erfolgen.

Berichtspflicht der dezentralen Compliance-Beauftragten

Schließlich ist die im Rahmen der Berichterstattung erfolgte Kommunikation entsprechend zu dokumentieren. So kann nicht nur im Streitfall zwischen der Unternehmensleitung und den Compliance-Beauftragten, sondern auch bei Auftreten von Verstößen gegenüber Ermittlungsbehörden, der entsprechende Nachweis über eine erfolgte Berichterstattung erbracht werden.

Dokumentation der Berichterstattung

Spezielle Governance-Strukturen bezüglich des Aufsichtsrats/Beirats

Bei kleinen Unternehmen wird der Aufsichtsrat keine zentrale Rolle spielen, es sei denn, sie sind als Aktiengesellschaft formiert. Jedoch kann auch für kleine Unternehmen die Bestellung eines freiwilligen Beirats von Vorteil sein. Ein *außenstehender* Beirat mit *Beratungsfunktion* und einem kritischen und unbefangenen Blick von außen kann dem Unternehmen wertvolles Expertenwissen über wirtschaftliche, juristische oder technische Zusammenhänge liefern, das im Unternehmen selbst u. U. nicht vorhanden ist. Auf diesem Wege lässt sich gerade auch für kleine Unternehmen das Risiko unternehmerischer Fehlentscheidungen reduzieren. Ein Unternehmen hat ferner die Möglichkeit, Beiräte zu bestellen, die neben einer Beratungsfunktion auch eine *Überwachungsfunktion* ausüben. Dies kann sich beispielsweise bei Unternehmen mit Eigentü-

Aufsichtsrat

Beratungsfunktion

Überwachungsfunktion

merfamilienstrukturen empfehlen, indem der Beirat den Familieneinfluss gegenüber einem fremd eingesetzten Management wahrt.

Mit zunehmender Unternehmensgröße werden sich Unternehmen überwiegend als Kapitalgesellschaften, insbesondere als Aktiengesellschaften formieren. Als Gesellschaftsorgan sind die Aufsichtsratsmitglieder verpflichtet, die ihnen übertragenen Aufgaben mit der Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters zu erfüllen und dürfen sich hierbei allein von den Interessen der Gesellschaft leiten lassen.

Zu den wesentlichen Aufgaben eines Aufsichtsrats gehören die Kontrolle der grundlegenden unternehmerischen Entscheidungen der Unternehmensleitung sowie die Beratung der Unternehmensleitung im Rahmen der Überwachung. Um diesen Aufgaben gerecht zu werden, sind zusätzliche (organisatorische) Anforderungen sowohl an die Unternehmensleitung als auch an das Aufsichtsgremium selbst zu stellen. Im Rahmen seiner Überwachungspflicht ist dem Aufsichtsrat zu empfehlen, sich insbesondere auch mit der Prüfung der Angemessenheit und Funktionsfähigkeit des CMS zu befassen.[25] Wichtige Voraussetzung für eine funktionierende Überwachung ist hierbei eine umfassende Compliance-Berichterstattung an den Aufsichtsrat. Denn für eine sachgerechte und effektive Kontrolle des CMS durch den Aufsichtsrat ist es unerlässlich, dass dem Aufsichtsrat hierzu auch alle relevanten Informationen vorliegen. Aus diesem Grund hat der Vorstand unabhängig von der Unternehmensgröße regelmäßig schriftlich – mindestens jährlich – sowie ad-hoc dem Aufsichtsrat über die Compliance-Themen und ihre Entwicklung im Unternehmen zu berichten. In kleineren Unternehmen, die kein umfassendes CMS eingerichtet haben, sollte die Berichterstattung insbesondere die Themen wie die spezifischen Compliance-Risiken des Unternehmens, die Compliance-Bemühungen des Unternehmens sowie ggf. aufgetretene Compliance-Fälle und die getroffenen Gegenmaßnahmen zum Inhalt haben. Bloße Mitteilungen seitens des Vorstands und des Compliance-Beauftragten zu aufgetretenen Verdachtsfällen dürften z.B. nicht ausreichen, damit sich der Aufsichtsrat ein umfassendes Bild von der Funktionalität des CMS machen kann. Im Gegenzug darf sich der Aufsichtsrat nicht ›blind‹ darauf verlassen, dass der Vorstand seiner Berichtspflicht nachkommt. Dem Aufsichtsrat steht daher ein entsprechendes Informationsrecht zu, von dem er auch entsprechend Gebrauch machen muss. In großen Unternehmen kann es zusätzlich, wie bereits oben ausgeführt wurde, empfehlenswert sein, dem Compliance-Beauftragten zusätzlich eine jederzeitige direkte

Berichterstattung des Vorstands an den Aufsichtsrat

Berichtsmöglichkeit an den Aufsichtsrat

[25] §107 Abs. 3 AktG konkretisiert die Aufgaben des Prüfungsausschusses beziehungsweise des Aufsichtsrats, wonach diese unter anderem dazu verpflichtet sind, die Wirksamkeit des Internen Kontroll- und Risikomanagementsystems zu überwachen. Nach Ziff. 5.3.2 des DCGK soll der Aufsichtsrat einen Prüfungsausschuss (Audit Committee) einrichten, der sich u.a. auch mit der Compliance des Unternehmens befasst – falls kein anderer Ausschuss damit betraut ist.

Berichtsmöglichkeit sowie eine mindestens jährliche Berichtspflicht gegenüber dem Aufsichtsorgan einzuräumen.

Für den Aufsichtsrat empfiehlt sich überdies – entsprechend der Empfehlung in Ziff. 3.4 des DCGK – zur Sicherung eines angemessenen Informationsflusses zwischen Vorstand und Aufsichtsrat eine Informationsordnung erlassen, welche die Berichtspflichten des Vorstands im Einzelnen einschließlich der Berichterstattung über Fälle von Non-Compliance regelt. In großen Unternehmen kann der Erlass einer entsprechenden Informationsordnung durch den Aufsichtsrat im Hinblick auf eine verantwortungsvolle Wahrnehmung seiner Überwachungs- und Kontrollaufgaben erwartet werden. Die notwendigen Informationen für die Feststellung der Effektivität des CMS kann sich der Aufsichtsrat z.B. über die Einsicht in die Prüfungsberichte der Internen Revision, durch Einsicht in die Berichte des Vorstands oder durch Einsicht in die Berichterstattung über intern oder extern erfolgte Prüfungsmaßnahmen beschaffen. Nimmt der Aufsichtsrat im Rahmen seiner Überwachung auch eine Beratung des Vorstands vor, so hat der Aufsichtsrat hierbei zu berücksichtigen, dass er primär das Unternehmensinteresse zu wahren hat und eine Beratung des Vorstands daher im Interesse der Gesellschaft zu erfolgen hat.

Informationsordnung des Aufsichtsrats

Sowohl die Überwachungs- als auch die Beratungsaufgaben des Aufsichtsrats erfordern entsprechenden Sachverstand und Unabhängigkeit (vgl. Ziff. 5.4.1 und 5.4.2 des DCGK). Mit zunehmender Größe und Komplexität des Unternehmens werden die Anforderungen an die Befähigung der Aufsichtsratsmitglieder zur Erfüllung ihrer Aufgaben steigen. Große Unternehmen haben daher insbesondere dafür Sorge zu tragen, dass eine sorgfältige Auswahl und Besetzung des Aufsichtsrats erfolgt und die erforderliche Unabhängigkeit und Fachkenntnis der Aufsichtsratsmitglieder gegeben sind. Fehlen notwendige Kenntnisse und Fähigkeiten zum Bereich Compliance, so hat das Unternehmen den Aufsichtsrat zu spezifischen Compliance-Themen zu schulen.

Sachverstand und Unabhängigkeit des Aufsichtsrats

Unternehmen, die als Kapitalgesellschaft formiert sind, sollten grundsätzlich die Empfehlungen des DCGK, insbesondere zur Bildung von Ausschüssen, z.B. Prüfungsausschuss (Audit Committee), Nominierungsausschuss, berücksichtigen (vgl. → ABSCHNITT I.1 ›KAPITALMARKTORIENTIERUNG‹ des ANNEX). Gerade große, multinationale Unternehmen werden sich bei Nichtbeachtung der Empfehlungen des Kodex und im Falle von Compliance-Verstößen schwerlich auf ein funktionierendes CMS berufen können und sich vielmehr dem Vorwurf der Nichterfüllung der unternehmerischen Organisations- und Sorgfaltspflichten ausgesetzt sehen.

Einrichtung eines Prüfungsausschusses

Erlangt der Aufsichtsrat Kenntnis von (Compliance-)Missständen im Unternehmen, so hat er entsprechende Gegenmaßnahmen einzuleiten und einzufordern

(vgl. auch → ABSCHNITT I.1 ›KAPITALMARKTORIENTIERUNG‹ des ANNEX). Gleiches dürfte gelten, wenn im Unternehmen schwerwiegende Compliance-Verstöße bekannt werden und die Funktionalität des CMS in Frage steht.

— Einleitung von Gegenmaßnahmen bei Kenntnis von (Compliance-) Missständen

Verhaltensgrundsätze und -richtlinien

3

Weshalb benötigt ein Unternehmen Verhaltensgrundsätze und -richtlinien?

Welche Funktion hat ein Verhaltenskodex?

Zu welchen Themen sollte ein Unternehmen weitere Verhaltensrichtlinien implementieren?

Wie sollten Verhaltensgrundsätze und -richtlinien den Mitarbeitern bekanntgemacht werden?

Mit welchen Mitteln kann die Akzeptanz von Verhaltensgrundsätzen und -richtlinien seitens der Mitarbeiter gefördert werden?

Welche Besonderheiten sind für ausländische Tochter- und Beteiligungsgesellschaften zu beachten?

Zielsetzung

Verhaltensgrundsätze und -richtlinien zielen darauf ab, den Mitarbeitern Orientierung zu geben, sich bei der Ausübung ihrer geschäftlichen Tätigkeit innerhalb des rechtlich Erlaubten sowie innerhalb des seitens des Unternehmens selbst auferlegten Handlungsrahmens zu halten. Es geht dabei in erster Linie um die Vermeidung krimineller sowie unethischer Handlungen. Mit Verhaltensgrundsätzen und -richtlinien wird nicht nur die Sensibilisierung der Mitarbeiter und mithin integres Verhalten im Geschäftsalltag gefördert, sondern auch eine Haftungs- und Schadensminimierung für das Unternehmen als auch für seine Beschäftigten selbst erreicht.

Verhaltensgrundsätze und -richtlinien bieten den Mitarbeitern Orientierung

Geeignete Verhaltensgrundsätze und -richtlinien enthalten nicht nur Handlungsbeschränkungen, sondern legen vielmehr einen Handlungs*spielraum* fest, der den Beschäftigten zugleich Handlungsmöglichkeiten schafft, innerhalb derer sie eigenverantwortlich ihre Aufgaben ausüben können. Dies stärkt nicht nur das gegenseitige Vertrauen, sondern schafft und fördert zugleich die Eigenmotivation der Mitarbeiter, was sich wiederum aus ökonomischer Sicht positiv auf die Leistungsbereitschaft der Mitarbeiter auswirken kann.

Festlegung des Handlungsspielraums

Verhaltensgrundsätze und -richtlinien, die zudem nach außen kommuniziert werden, signalisieren den Vertragspartnern wie Kunden, Lieferanten etc. sowie der Öffentlichkeit, dass das Unternehmen an sich selbst hohe Erwartungen an verantwortungsvolles und rechtmäßiges Handeln stellt. Da letztendlich der Erfolg eines Unternehmens insbesondere vom Vertrauen aller Stakeholder sowie der Öffentlichkeit in seine Integrität und Fachkompetenz abhängt, stellen Verhaltensgrundsätze und -richtlinien auch geeignete Maßnahmen dar, die Kooperationsbeziehungen mit sämtlichen Stakeholdern langfristig zu sichern.

Sicherung der Kooperationsbeziehungen mit den Stakeholdern

Empfehlungen für die Umsetzung

Verhaltenskodex (auch Code of Conduct/Code of Ethics)

Allgemeine Verhaltensgrundsätze dienen als Grundlage für integres Verhalten und bieten den Mitarbeitern Orientierung zu dem von ihnen erwarteten Verhalten im Geschäftsalltag.. Die Basis der allgemeinen Verhaltensanforderungen bilden dabei grundsätzlich die vom Unternehmen definierten spezifischen Unternehmenswerte.

Allgemeine Verhaltensgrundsätze

Spezifische Unternehmenswerte

Daraus lassen sich die allgemeinen (globalen) Grundsätze für gesetzestreues und ethisches Verhalten (wie Zuverlässigkeit, Ehrlichkeit, Respekt, Vertrauen, fairer Umgang mit Mitarbeitern, Kollegen und Geschäftspartnern) ableiten. Diese allgemeinen Verhaltensanforderungen werden typischerweise in einem zentralen, für alle Mitarbeiter geltenden sogenannten Verhaltenskodex (auch Code of Conduct oder Code of Ethics genannt) festgehalten. Sie sind in der Regel allgemein formuliert und enthalten grundlegende Verhaltensanforderungen wie z. B. zu Antikorruption, Antigeldwäsche, Kartellrecht, Leitlinien für Umwelt und Nachhaltigkeit. Diese allgemeinen Verhaltensgrundsätze gelten für alle Beschäftigten gleichermaßen.

Code of Conduct/ Code of Ethics

Um den Mitarbeitern die notwendige Orientierung für das von ihnen erwartete Verhalten im Geschäftsalltag zu geben, haben Unternehmen unabhängig von ihrer Größe einen schriftlichen Verhaltenskodex zu erstellen und an die Mitarbeiter bekannt zu machen. In kleinen Unternehmen mit übersichtlicher Mitarbeiterzahl und schlanken Organisationsstrukturen kann ein kurzer und einfach gehaltener Kodex, der z. B. die wesentlichen Unternehmenswerte und die daraus abgeleiteten Verhaltensanforderungen festhält, bereits genügen. Denn gerade in kleinen Unternehmen, in denen die Unternehmensleitung in das Tagesgeschäft mit eingebunden ist und in besonderer Nähe zu den Mitarbeitern steht, kann sich die wesentliche Orientierung für die Mitarbeiter anstatt aus schriftlichen Verhaltensgrundsätzen vielmehr unmittelbar aus dem kompromisslosen Vorleben der Unternehmenswerte durch die Unternehmensleitung ergeben. Die Verschriftlichung trägt zusätzlich dazu bei, die Bedeutung und Wichtigkeit der Erwartung an rechtstreues und ethisches Verhalten hervorzuheben. Um den Kodex über die Bekanntmachung hinaus den Mitarbeitern stets präsent zu halten, wird auch kleinen Unternehmen empfohlen, diesen zumindest in einer Kurzfassung durch Aushänge an zentralen Stellen im Unternehmen (z. B. in Form von Postern, Druckfassung) öffentlich vorzuhalten.

Typischer Inhalt eines Code of Conduct

In (großen) Unternehmen enthält ein Verhaltenskodex typischerweise insbesondere folgende Bestandteile:[26]

[26]

- Vorwort der Unternehmensleitung, in dem sie die Bedeutung und Wichtigkeit des Kodex darlegt
- ein klares Statement der Unternehmensleitung zu ihrer Sichtweise und Haltung bzgl. der Art und Weise, wie das Unternehmen Geschäfte machen will und wie nicht (sog. Commitment)
- Festlegung des konkreten Geltungsbereiches des Verhaltenskodex. Dies ist vor allem wichtig, wenn das Unternehmen Filialen, Zweigstellen etc. hat, da mit der konkreten Festlegung Missverständnisse vermieden werden können.

- eine klare Definition der erwarteten Mindestverhaltensanforderungen an die Beschäftigten
  - Einhaltung geltenden Rechts und der vom Unternehmen definierten Werte/Geschäftsethik
  - Verbot der Diskriminierung und respektvoller Umgang mit Mitarbeitern, Kollegen, Geschäftspartnern etc.
- den Hinweis auf Meldemöglichkeiten der Mitarbeiter bei der Feststellung von Compliance-Verstößen
- den Hinweis auf strikte Verbindlichkeit des Verhaltenskodex sowie auf Sanktionen (strafrechtlich, zivil- und arbeitsrechtlich) bei Missachtung der Verhaltensregeln
- Beschreibung der Compliance-Organisation und Benennung der Ansprechpartner zu Compliance-relevanten Themen und Fragen für die Mitarbeiter
- Bezugnahme/Hinweis auf weitere, ergänzende Verhaltensrichtlinien zu den wesentlichen Compliance-Risiken wie z.B. Antikorruptionsrichtlinie, Geschenkerichtlinie, Kartellrechtsrichtlinie, Umgang mit Spenden und Sponsoring

Spezifische Verhaltensrichtlinien

Mit zunehmender Komplexität der Geschäftstätigkeit steigen auch die zu erfüllenden rechtlichen sowie ethischen Anforderungen an das Unternehmen und seine Beschäftigten und somit die Risiken für das Unternehmen, die sich aus der Missachtung von Normen und ethischen Standards ergeben können. Eine Festlegung sämtlicher Anforderungen an die Mitarbeiter in einem allumfassenden Verhaltenskodex dürfte kaum zu bewerkstelligen sein, ohne dass ein solches Regelwerk für die Anwender zu komplex und überfrachtet ist und letztendlich die gewünschte Wirkung verfehlt. Neben den allgemeinen Verhaltensanforderungen muss das Unternehmen daher über weitere geeignete spezifische Verhaltensrichtlinien sowie Dienstanweisungen verfügen, welche die im Verhaltenskodex allgemein gehaltenen Anforderungen an das gewünschte Mitarbeiterverhalten konkretisieren und ergänzen, um strafbare Handlungen bestmöglich zu verhindern. Mit den spezifischen Verhaltensrichtlinien erfahren die Mitarbeiter konkrete Verhaltensregeln, die sich insbesondere aus den definierten wesentlichen Compliance-Risiken bzw. Compliance-Bereichen ableiten (z.B. Wettbewerbs- und Kartellrechtsrichtlinie für den Vertrieb, Richtlinie für die Forschungs- und Entwicklungsabteilung in Bezug auf Vertraulichkeit und Umgang mit Forschungs- und Entwicklungsergebnissen, Richtlinie für die Exportkontrollabteilung bzgl. des Umgangs mit sog. Dual-Use-Gütern etc.). Mitarbeiter müssen entsprechend sensibilisiert werden und den genauen Handlungsspielraum kennen. Denn erst wenn die Erwartungen der Unternehmensleitung an die Beschäftigten klar sind, kann die Unternehmensleitung im Fall von Compliance-Verstößen auch entsprechende Maßnahmen durchsetzen.

Spezifische Verhaltensrichtlinien

Bauen die spezifischen Verhaltensrichtlinien auf den allgemeinen Verhaltensgrundsätzen des Code of Conduct auf, so kann dies bei den Beschäftigten weiteres Bewusstsein für die Wichtigkeit und Bedeutung integren Verhaltens in der zunehmend komplexeren Arbeitswelt schaffen. Kleine Unternehmen werden auch hier u.U. auf die Verschriftlichung spezifischer Verhaltensrichtlinien verzichten können, sofern das Vorleben der Unternehmenswerte durch die Unternehmensleitung auch als Orientierung zur Vermeidung von spezifischen Unternehmensrisiken wie Korruption, Wettbewerbsverstößen etc. geeignet ist. Größere Unternehmen haben für weitere schriftliche Verhaltensrichtlinien zu sorgen. Andernfalls wird es schwer möglich sein, den Mitarbeitern die erforderliche Orientierung im Wege von detaillierteren Verhaltensanforderungen, die aufgrund zunehmender Unternehmenskomplexität notwendig sind, zu geben.

Im Gegensatz zum Code of Conduct, der als allgemeine Verhaltensrichtlinie für alle Mitarbeiter unternehmensweit einheitlich gilt, sind spezifische Verhaltensrichtlinien nicht für alle Mitarbeiter bzw. Geschäftsbereiche im Unternehmen gleichermaßen relevant. Daher ist in jeder Verhaltensrichtlinie der jeweilige Geltungsbereich klar festzulegen (z.B. Einkauf/ Vertrieb bzgl. der Überprüfung der Geschäftspartner).

Typische Themenfelder, für weitere konkretere Ge- und Verbote in spezifischen Verhaltensrichtlinien sind:

Richtlinien – Themenfelder

- Antikorruption
- Wettbewerbs- und Kartellrecht (Antitrust Law)
- Geschäftstätigkeit mit Amtsträgern
- Umgang mit der Annahme und Vornahme von Zuwendungen (Geschenke, Bewirtungen und sonstige Einladungen)
- Umgang mit Spenden und Sponsoring
- Umgang und Prüfung von Geschäftspartnern

[26] Ausführliche Empfehlungen bezüglich der Entwicklung und Implementierung eines Code of Conduct siehe Grüninger, S. (2005): Codes of Conduct – Grundsätze für integres Unternehmensverhalten entwickeln und implementieren. In: KPMG Audit Committee Institute (Hrsg.): Audit Committee Quarterly, Nr. 3.

— Umgang mit Eigentum des Unternehmens und Dritter sowie mit vertraulichen Daten und sensiblen Informationen

— Umgang mit Interessenkonflikten

Zu welchen Themen ein Unternehmen spezifische Verhaltensrichtlinien implementieren sollte, wird sich weniger an der Unternehmensgröße, sondern vielmehr an der jeweiligen Risikoexposition des Unternehmens aufgrund seines Geschäftsmodells, seiner Produkte, dem Internationalisierungsgrad etc. auszurichten haben. Auch kleinere Unternehmen haben diesbezüglich zu berücksichtigen, dass es auch für sie erforderlich sein kann, für die Mitarbeiter bestimmte spezifische Verhaltensrichtlinien schriftlich festlegen.

— Umgang mit der Annahme und Vornahme von Zuwendungen

Das Thema *Umgang mit der Annahme und Vornahme von Zuwendungen* hat insbesondere aufgrund größerer Korruptionsskandale in der jüngeren Vergangenheit an Brisanz gewonnen und ist für jedes Unternehmen – unabhängig von der Größe und Komplexität – von Bedeutung. Unternehmen haben verschiedene Möglichkeiten, einem Korruptionsrisiko zu begegnen. So können Unternehmen festlegen, dass weder die Vergabe noch die Annahme jedweder Art von Geschenken zulässig ist. Eine derartige Unternehmenspolitik mag zwar generell das Ziel verfolgen, von vornherein jeglichen Anschein einer möglichen Bestechung bzw. Bestechlichkeit der Beschäftigten zu vermeiden. Es dürfte jedoch fraglich sein, ob derartige Instrumente tatsächlich geeignet sind, das gewünschte Ziel – nämlich die Vermeidung von Korruption – zu erreichen. Denn das Gesetz verbietet nicht per se das Gewähren bzw. die Annahme von Geschenken. Von Bedeutung ist unter anderem vielmehr der Anlass, aus dem eine Zuwendung getätigt bzw. ein Präsent überreicht wird. Geringfügige Aufmerksamkeiten zu Weihnachten, zu Jubiläen oder Essenseinladungen aus geschäftlichem Anlass sind in der Regel unbedenklich, sofern sie dem Gebot der Höflichkeit entsprechen, d.h. ein übliches Maß nicht übersteigen, und sofern sie nicht getätigt werden, um eine Gegenleistung zu erhalten. Daher haben die Unternehmen für ihre Mitarbeiter klare Regeln für den Umgang mit Zuwendungen festzulegen, um den Mitarbeitern die notwendige Orientierung zu geben, was tabu und was erlaubt ist.[27] Im Rahmen von sogenannten Geschenkerichtlinien sind insbesondere folgende Punkte zu beachten:

[27] Einen ausführlichen Überblick zum Umgang mit Zuwendungen an Amtsträger findet sich in dem vom Bundesministerium des Innern herausgegebenen *Fragen-/Antwortenkatalog zum Thema Annahme von Belohnungen, Geschenken und sonstigen Vorteilen (Zuwendungen)*. Die darin enthaltenen Informationen und Hinweise sollen sowohl den Beschäftigten der Bundesverwaltung als auch den Adressaten aus der Wirtschaft Verständnis dafür vermitteln, welche dienstrechtlichen Grenzen für Verwaltungsbeschäftigte in Bezug auf den Umgang mit Geschenken und Zuwendungen einzuhalten sind. Der Fragenkatalog ist abrufbar unter: http://www.bmi.bund.de/SharedDocs/Pressemitteilungen/DE/2011/mitMarginalspalte/12/korruptionspraevention.html (16.04.2014).

— Bei der Gewährung bzw. Annahme von Zuwendungen muss jeder Anschein vermieden werden, für persönliche Vorteile empfänglich zu sein.

— Zuwendungen dürfen nicht mit einem (bevorstehenden) Geschäftsabschluss in Zusammenhang stehen.

— Damit beim Umgang mit Geschenken die Angemessenheit, eine einheitliche Handhabung innerhalb des Unternehmens sowie Transparenz sichergestellt sind, können Wertgrenzen festgelegt werden, an denen sich die Mitarbeiter orientieren können.

— Des Weiteren können Zustimmungserfordernisse festgelegt werden, falls Wertgrenzen überschritten werden.

— Bargeldzuwendungen sind strikt zu untersagen.

— Zuwendungen haben transparent zu sein. Zuwendungen an private Anschriften des Geschäftspartners sollten grundsätzlich untersagt sein.

Neben Antikorruptionsmaßnahmen kommt auch der Kartellrechts-Compliance eine wesentliche Rolle im Unternehmen zu, denn Verstöße gegen kartellrechtliche Vorschriften können zu schwerwiegenden Sanktionen für das Unternehmen führen. So kann nach §81 Abs. 4 S.2, 3 GWB bzw. Art. 23 Abs. 2 VO 1/2003[28] gegen das Unternehmen eine maximale Geldbuße in Höhe von bis zu 10 Prozent des weltweiten Jahreskonzernumsatzes verhängt werden. Unternehmen haben zu beachten, dass auch im Rahmen von Zusammentreffen mit Unternehmensvertretern derselben Branche (z.B. auf Verbandssitzungen wie Arbeitskreisen, Jahresversammlungen) bestimmtes Verhalten kartellrechtlich unzulässig ist und Verstöße hiergegen erhebliche Risiken bergen. Um beispielsweise der Gefahr eines unzulässigen Informationsaustausches oder verbotener Absprachen über wettbewerbsrelevante Themen, wie z.B. Preise, Preiserhöhungen, Rohstoffpreissteigerungen auf derartigen Treffen vorzubeugen, müssen die Verantwortlichen im Unternehmen daher die relevanten kartellrechtlichen Vorschriften und Haftungsrisiken sowie ihren unternehmerischen Handlungsspielraum kennen, insbesondere welche Verhaltensweisen rechtlich zulässig, welche bedenklich und welche verboten sind. Unternehmen jeglicher Unternehmensgröße sollten daher ihren Mitarbeitern entsprechende interne Verhaltensrichtlinien zum Wettbewerbs- und Kartellrecht vorhalten.

Mit zunehmender Unternehmensgröße nimmt die Komplexität der unternehmerischen Geschäftstätigkeit zu. An große Unternehmen werden hierbei Erwartungen verschiedenster Stakeholder gestellt, die es notwendig machen, sich umfassend

[28] VERORDNUNG (EG) Nr. 1/2003 DES RATES vom 16. Dezember 2002 zur Durchführung der in den Artikeln 81 und 82 des Vertrags niedergelegten Wettbewerbsregeln, abrufbar unter: http://europa.eu/legislation_summaries/competition/firms/l26092_de.htm (16.04.2014).

mit diesen Erwartungen auseinanderzusetzen und zur Risikominimierung geeignete weitere Verhaltensrichtlinien für die betroffenen Mitarbeiter und Geschäftsbereiche zu erstellen. Für große Unternehmen gewinnt das Thema Social Compliance (Verbot von Kinderarbeit in der Wertschöpfungskette, Gewährung angemessener Löhne, Einhaltung von Umwelt- und Sicherheitsstandards in Drittländern) zunehmend an Bedeutung und wird im Rahmen von Verhaltensstandards bzw. -richtlinien thematisiert werden müssen.

Implementierung der Verhaltensgrundsätze und -richtlinien

Verhaltensgrundsätze und -richtlinien werden zur Zielerreichung, nämlich die Vermeidung strafbaren und unethischen Verhaltens, nur dann geeignet sein, wenn sie bei den Mitarbeitern auf Verständnis und Akzeptanz stoßen und von diesen tatsächlich bei der täglichen Arbeit gelebt werden. Neben Sensibilisierungs- und Schulungsmaßnahmen (vgl. hierzu das CMS-Element → 5 COMPLIANCE-KOMMUNIKATION & SCHULUNG) kann insbesondere der Entstehungsprozess von Verhaltensgrundsätzen und -richtlinien ganz entscheidend zur Erreichung bzw. Förderung von Akzeptanz beitragen. Werden z. B. Mitarbeiter frühzeitig in den Implementierungsprozess mit eingebunden, z. B. bei der Definition der Unternehmenswerte und im Rahmen der Entwicklung entsprechender Verhaltensgrundsätze, so kann dies zu einer größeren Verbindlichkeit und Zustimmung seitens der Beschäftigten führen. Gerade in kleineren Unternehmen dürfte aufgrund der überschaubareren Strukturen die Einbindung der Beschäftigten umfangreicher möglich sein als bei Großunternehmen. Um auch in großen Unternehmen eine Mitarbeiterbeteiligung zu ermöglichen, kann es sich anbieten, die Mitarbeiter bzw. Führungskräfte beispielsweise über die Bildung von Arbeits- oder Fokusgruppen mit einzubinden.

Implementierungsprozess

Einbindung von Mitarbeitern und Führungskräften

Auch die beste Richtlinie kann ihren Zweck nur dann erfüllen, wenn sie den Mitarbeitern entsprechend bekanntgemacht worden ist. Die Bekanntmachung kann auf unterschiedliche Weise erfolgen, wobei sichergestellt werden muss, dass alle Mitarbeiter, für die die Verhaltensgrundsätze und -richtlinien gelten sollen, entsprechend informiert werden. Dabei empfiehlt sich bei (erstmaliger) Einführung oder Änderung einer Verhaltensrichtlinie eine persönliche Mitteilung durch die Unternehmensleitung. Denn einer persönlichen Bekanntgabe durch die Unternehmensleitung wird eine größere Bedeutung zukommen als die bloße schriftliche Mitteilung. Die persönliche Bekanntgabe kann z. B. im Rahmen eines Meetings (sofern alle Mitarbeiter anwesend sind), bei Betriebsversammlungen oder Informationsveranstaltungen erfolgen. Um die Wichtigkeit und Bedeutung der Richtlinien hervorzuheben eignet sich insbesondere für kleinere und mittelgroße Unternehmen auch die Verteilung eines persönlichen Exemplars an die Beschäftigten wie z. B. in Form von Merkblättern, Informationsbroschüren. In großen

Bekanntmachung des Verhaltenskodex und der Richtlinien

Unternehmen kann sich auch der Einsatz von Multimedia (z. B. Kurzfilme mit einem Statement der Unternehmensleitung, die per E-Mail versendet werden oder auf der Intranetseite präsentiert werden) als geeignetes Mittel zur Erreichung der jeweiligen Adressaten anbieten. Dennoch hat neben einer mündlichen Bekanntgabe zumindest in den größeren Unternehmen insbesondere aus Dokumentationsgründen auch eine zusätzliche schriftliche Mitteilung und Bekanntgabe zu erfolgen, um sicherzustellen alle Adressaten tatsächlich erreicht zu haben. Das bloße Versenden per E-Mail oder das bloße Einstellen im Intranet des Unternehmens dürfte für eine wirkungsvolle Bekanntmachung der Verhaltensrichtlinien nur dann als geeignet gelten, wenn hierauf durch die Unternehmensleitung nachhaltig und unternehmensweit hingewiesen wird. Den Unternehmen wird grundsätzlich empfohlen, zumindest ihren schriftlichen Verhaltenskodex nicht nur intern gegenüber den Beschäftigten, sondern auch extern z. B. durch die Möglichkeit der Einsicht auf der allgemein zugänglichen Unternehmenswebsite, bekannt zu machen. Eine allgemeine Veröffentlichung des Verhaltenskodex ermöglicht die Kontrolle seitens der Stakeholder, ob die verankerten Werte und Vorgaben im Kodex vom Unternehmen so auch gelebt werden (z. B. Umgang mit Kundenbeschwerden etc.) und stärkt damit die Glaubwürdigkeit des Wertesystems im Unternehmen.

Veröffentlichung des Verhaltenskodex auf der Unternehmenswebsite

Neben der (erstmaligen) Bekanntgabe der schriftlichen Verhaltensgrundsätze und -richtlinien ist sicherzustellen, dass die Verhaltensgrundsätze und -richtlinien den Mitarbeitern weiterhin jederzeit in der jeweils aktuellsten Version zugänglich sind. Hierfür eignet sich beispielsweise die elektronische Ablage im Intranet. Der Vorteil einer elektronischen Speicherung/Ablage ist darin zu sehen, dass die Mitarbeiter mit Zugang zur EDV jederzeit schnell auf die aktuelle/neueste Version Zugriff nehmen können. In Unternehmen, in denen nicht alle Mitarbeiter Zugang zum Intranet haben (z. B. Mitarbeiter aus Montage, Produktion), ist sicherzustellen, dass der Verhaltenskodex sowie diejenigen weiteren Richtlinien, welche auch für diese Mitarbeiter relevant sind, zusätzlich in Papierform an zentralen, für diese Mitarbeiter zugänglichen Orten im Unternehmen wie dem ›schwarzen Brett‹, in Aufenthaltsräumen etc., ausgehängt sind.

Zugang zur jeweils aktuellen Version der Richtlinien

Verhaltensgrundsätze und -richtlinien sind klar und in einfacher Sprache zu verfassen, damit sie von jedem Mitarbeiter verstanden werden können. Verhaltensgrundsätze und -richtlinien dürfen nicht verklausuliert sein, da andernfalls die Gefahr besteht, dass sie ihre Orientierungswirkung verlieren. Deshalb sollten die Verhaltensgrundsätze und -richtlinien als praktische Anleitungen konzipiert sein, um den Mitarbeitern verständlich darzulegen, was sie zu tun bzw. zu unterlassen haben. Detaillierte Ausführungen in den Richtlinien mögen zwar rechtlich richtig sein, sind als Handlungsanweisung und Orientierung im alltäglichen Geschäftsleben allerdings oft dann nicht geeignet, wenn sie zu kompliziert verfasst sind und von den Beschäftigten nicht verstanden werden. Daher kann es unter Umständen zwingend erforderlich sein, den

Klare einfache Sprache

Beschäftigten kurze praktische Anleitungen z.B. im Rahmen von Checklisten, in denen Compliance-Maßnahmen mit aufgenommen sind, zur Verfügung zu stellen.

Anpassung der Richtlinien

Verhaltensgrundsätze und -richtlinien müssen an geänderte Faktoren (z.B. Gesetzesänderungen, Änderung der Risikolage) angepasst werden. Dabei wird der Fokus weitgehend auf den einzelnen Verhaltensrichtlinien und weniger auf dem Code of Conduct liegen, da letzterer in der Regel meist eher allgemein gehalten ist und von Gesetzesänderungen oder sonstigen Änderungsfaktoren weniger, wenn gar überhaupt nicht betroffen sein wird. Für kleine Unternehmen bietet sich an, die notwendigen Informationen zu (bevorstehenden) Gesetzesänderungen über die verschiedenen Branchenverbände oder frei zugängliche Newsletter von Experten, Institutionen zu besorgen, um entscheiden zu können, ob Anpassungen erforderlich sind.

Richtlinien-management

Große Unternehmen werden nicht umhinkommen ein geeignetes Richtlinienmanagement einzuführen, mit dem sichergestellt wird, dass sämtliche Verhaltensgrundsätze und -richtlinien (konzernweit) regelmäßig auf ihre Notwendigkeit und Relevanz hin überprüft und ggf. an geänderte Faktoren (z.B. Gesetzesänderungen, Änderung der Risikolage) angepasst werden. Es sind umfassende Prozesse für die Umsetzung und die anschließende Kontrolle der ordnungsgemäßen Durchführung erforderlich. Zu geeigneten Maßnahmen zählen hierbei u.a. die Festlegung einer begrenzten Gültigkeitsdauer der jeweiligen Richtlinie sowie die Bestimmung von Prozesseigentümern der jeweiligen Richtlinien, welche die Verantwortung für die Anpassung und Umsetzung dieser Richtlinie tragen und entsprechende Berichtspflichten gegenüber bestimmter Organisationseinheiten (z.B. der Compliance-Organisation) haben.

Eventuelle Mitbestimmungs-rechte des Betriebsrats beachten

Existiert in dem Unternehmen ein Betriebsrat, so hat das Unternehmen darauf zu achten, dass bei der Implementierung von Verhaltensgrundsätzen und -richtlinien unter Umständen eine Mitbestimmung des Betriebsrats zwingend erforderlich sein kann. Grundsätzlich sind ethisch-moralische Programmsätze, Leitlinien zur ›Unternehmensphilosophie‹ oder inhaltliche Bezugnahmen auf Gesetze *mitbestimmungsfrei*. Einem Mitbestimmungsrecht des Betriebsrats unterliegen dagegen Regelungen über das sog. Ordnungsverhalten im Betrieb (§87 I Nr. 1 BetrVG). Letzteres trifft nach der Rechtsprechung z.B. auf eine in der Verhaltensrichtlinie enthaltene Regelung zu, nach der die Mitarbeiter Verstöße über ein sog. ›Whistleblowing-System‹ melden sollen[29] (zum Whistleblowing vgl. auch das CMS-Element → **5 COMPLIANCE-KOMMUNIKATION & SCHULUNG**). Werden Richtlinien unter Missachtung eines Mitbestimmungsrechts erlassen, so kann der Betriebsrat gegen eine solche Regelung der Verhaltensrichtlinie gerichtlich vorgehen und sie aushebeln. Zur Vermeidung bzw. Minimierung unnützer Aufwendungen und Kosten empfiehlt es sich daher, den Betriebsrat frühzeitig zu den (mitbestimmungspflichtigen) Regelungen einer Verhaltensrichtlinie mit einzubinden und dessen Zustimmung vor weiteren kostspieligen Implementierungsmaßnahmen einzuholen. Im Rahmen der Gespräche mit dem Betriebsrat sollte klar und deutlich das mit der Maßnahme verfolgte Ziel, nämlich der Schutz des Unternehmens und seiner Beschäftigten vor Schäden, dargelegt werden.

[29] Vgl. Urteil des BAG, 22.07. 2008 – 1 ABR 40/07.

Ausländische Tochter- und Beteiligungs-gesellschaften

Hat das Unternehmen ausländische Tochter- und Beteiligungsgesellschaften, so hat es im Wege geeigneter Maßnahmen sicherzustellen, dass die konzernweit festgelegten Verhaltensgrundsätze und -richtlinien nicht gegen lokale Gesetze verstoßen (z.B. Arbeitsrecht, Datenschutz). Je nach Art und Umfang der Richtlinien kann es erforderlich werden, hierzu entsprechende externe Fachexpertise in Anspruch zu nehmen. Auch Mitarbeiter in den ausländischen Beteiligungsgesellschaften müssen von den Verhaltensanforderungen Kenntnis haben und diese verstehen. Lokale Richtlinien sollten daher die jeweils konkreten rechtlichen Grundlagen der jeweiligen Jurisdiktion nennen sowie eventuelle kulturelle/lokale, gesetzliche Besonderheiten mitberücksichtigen. Die Konzernmutter hat für die ausländischen Beteiligungsgesellschaften die Verhaltensgrundsätze und -richtlinien zumindest in englischer Sprache vorzuhalten. Bei Beteiligungen in Ländern mit Beschäftigten mit fehlenden oder unzureichenden Englischkenntnissen sollten die Verhaltensgrundsätze und -richtlinien in der jeweiligen Landessprache erstellt werden. Die Notwendigkeit für die Übersetzung in die jeweilige Landessprache kann sich aus der Größe der zu erreichenden Zielgruppe in der ausländischen Tochter- und Beteiligungsgesellschaft sowie aus dem von der Zielgruppe ausgehenden Risiko ergeben.

Neben den allgemeinen und spezifischen Verhaltensrichtlinien sollten Unternehmen ihren Mitarbeitern weitere konkrete Arbeitshilfen, Checklisten etc. zur Orientierung bieten, die konkrete Maßnahmen, Verfahrens- sowie Genehmigungsabläufe vorgeben und ihnen im Tagesgeschäft damit wertvolle Unterstützung liefern.

Implementierung eines Notfallplans

Krisen- bzw. Notfallplan

Kein noch so gutes CMS kann eine 100%ige Vermeidung von Fehlverhalten sicherstellen, vielmehr besteht für jedes Unternehmen ein unvermeidliches Restrisiko. Der Eintritt einer Krise kann sich aus dem Bekanntwerden schwerwiegender Compliance-Verstöße oder aufgrund überraschender behördlicher Durchsuchungsaktionen (sog. ›Dawn Raids‹) wegen angezeigter Straftaten ergeben. Tritt ein unvorhergesehener Ernstfall ein, so sollten Unternehmen hierauf vorbereitet sein, um eine bestmögliche Schadensminimierung zu gewährleisten. Es gilt daher, in einem Krisen- bzw. Notfallplan die

wesentlichen Verhaltensanforderungen für die Mitarbeiter festzuhalten. Ein Notfallplan sollte beispielsweise konkrete Weisungen beinhalten,[30]

- wie sich die Mitarbeiter im Falle von behördlichen Untersuchungen gegenüber den Ermittlungsbehörden und Ermittlungsbeamten zu verhalten haben,
- welche Personen im Unternehmen (z.B. Geschäftsleitung, Compliance-Beauftragter, Leiter Recht) zu unterrichten sind,
- ob sowie ggf. welche externen Berater wie z.B. im Strafrecht spezialisierte Rechtsanwälte hinzuzuziehen sind,
- wer für die Kommunikation verantwortlich ist bzw. wie die Kommunikation nach innen (Mitarbeiter) und außen (Geschäftspartner, Öffentlichkeit, Medien) zu erfolgen hat

In kleinen Unternehmen kann ein Notfallplan bestehend aus kurzen, übersichtlichen Checklisten zu dem geforderten Mitarbeiterverhalten, zu Namens- und Telefonnummern der zu informierenden Personen etc. bereits ausreichend sein, während in großen Unternehmen ein umfassendes Krisenmanagement im Rahmen eines zeitgerechten und effektiven Risikomanagements als unverzichtbar anzusehen ist.

Dabei gilt es, den Notfallplan den Mitarbeitern nicht nur bekannt zu machen, sondern darüber hinaus bestimmte Ernstfälle zu simulieren und mit den Mitarbeitern einzuüben, um sicherzustellen, dass die vorgesehenen Maßnahmen tatsächlich greifen und auch die verantwortlichen Personen wissen, wie sie in einem Krisenfall vorzugehen haben.

30 Eine detaillierte Übersicht zu Verhaltensempfehlungen im Krisenfall findet sich bei Campos Nave, J., Bonenberger, S. (2008): Korruptionsaffären, Corporate Compliance und Sofortmaßnahmen für den Krisenfall, in: BetriebsBerater, Nr. 15/2008, S. 734.

Geschäftspartnerprüfung

4

Warum ist die Geschäftspartnerprüfung aus Compliance-Sicht so wichtig?

Welche Arten von Risiken können sich aus der Zusammenarbeit mit Geschäftspartnern für das Unternehmen ergeben?

Welche Geschäftspartner sollten überprüft werden?

Aus welchem Anlass und wie häufig sollten Geschäftspartner überprüft werden?

Welche Prüfungsmaßnahmen sind geeignet und erforderlich?

Wonach sollte sich der Umfang der Prüfungsmaßnahmen richten?

Was sind geeignete Präventionsmaßnahmen zur Minderung der Risiken, die sich aus einer Geschäftspartnerbeziehung ergeben können?

Zielsetzung

Mit einer Geschäftspartnerprüfung werden die rechtlichen und wirtschaftlichen Risiken aber auch Chancen einer geschäftlichen Zusammenarbeit mit Dritten wie Kunden, Lieferanten, Dienstleistern, Vertriebsmittlern usw. überprüft. Ziel dabei ist, die Geschäftspartner auf ihre Integrität und Zuverlässigkeit hin zu analysieren. Für Unternehmen ist es wichtig, sich ein Bild von ihrem Geschäftspartner zu machen und sich zu vergewissern, ob es sich um einen ›integren‹ Geschäftspartner handelt. Denn das Unterlassen einer Geschäftspartnerprüfung kann für ein Unternehmen schwerwiegende Folgen haben und eine Sorgfaltspflichtverletzung seitens der Unternehmensleitung darstellen. Aus haftungsrechtlicher Sicht besteht für Unternehmen das Risiko, im Bereich der Korruption nicht nur für das Fehlverhalten der eigenen Mitarbeiter, sondern auch für Verstöße von Geschäftspartnern zur Verantwortung gezogen zu werden. Begehen eingeschaltete Vertriebspartner wie Agenten oder Mittler Bestechungshandlungen, so können derartige Verstöße für das Unternehmen zu Geldstrafen, Bußgeldern und Schadensersatzzahlungen sowie zum Ausschluss von öffentlichen Aufträgen führen.

Wirtschaftliche Risiken und Chancen der Zusammenarbeit

Haftungsrisiko für Verstöße von Geschäftspartnern

Eine Geschäftspartnerprüfung ist ferner dann erforderlich, wenn für das Unternehmen die Gefahr bestehen kann, dass bereits die Eingehung einer Geschäftsbeziehung mit einem Vertragspartner einen Rechtsverstoß darstellen würde. So verbieten beispielsweise verschiedene Anti-Terror-Gesetze und -Verordnungen Warenlieferungen oder Zahlungen an mutmaßliche terroristische Personen, Gruppierungen und Organisationen.[31] Verstöße gegen die Verbote und Beschränkungen dieser Verordnungen sind strafbewehrt und werden mit Geld- oder Freiheitsstrafe geahndet.

Anti-Terror-Gesetze und -Verordnungen

Aber nicht nur aus haftungsrechtlichen Gesichtspunkten, sondern auch zum Schutz der eigenen Reputation und damit zum Schutz vor finanziellen Schäden hat jedes Unternehmen geeignete Maßnahmen für eine Geschäftspartnerprüfung zu implementieren. Schließlich können auch rechtlich zulässige, jedoch ethisch fragwürdige Praktiken der Geschäftspartner – wie z. B. Kinderarbeit bei ausländischen Lieferanten, Umweltskandale – zu erheblichen Schäden für das eigene Unternehmen führen.

Reputationsschutz

[31] Vgl. Verordnung (EG) Nr. 881/2002 vom 16.01.2002 sowie Verordnung (EG) Nr. 2580/2001 vom 27.12.2001. In diesen Listen sind mutmaßliche terroristische Personen, Gruppierungen und Organisationen aufgeführt, mit denen keine Geschäfte getätigt werden dürfen. In diesen Listen finden sich nicht nur Personen und Unternehmen aus dem Ausland, sondern auch aus Deutschland. Das Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA) hat das Merkblatt ›Länderunabhängige Embargomaßnahmen zur Terrorismusbekämpfung‹ mit weiteren Einzelheiten und Informationen zu den verschiedenen Sanktionsmaßnahmen erstellt. Das Merkblatt kann kostenfrei auf der Internetseite des BAFA unter http://www.ausfuhrkontrolle.info/ausfuhrkontrolle/de/embargos/terrorismus/ (16.04.2014) abgerufen werden. Darüber hinaus existiert eine Vielzahl weiterer internationaler Sanktionslisten, wie z. B. die US Denied Persons List, die von sämtlichen Unternehmen zu beachten sind. Diese Liste enthält Namen von Personen, an die weder von US- noch von ausländischen (deutschen) Unternehmen Waren mit US-Ursprung geliefert oder bezogen werden dürfen.

Unternehmen, deren eigene Integrität und Zuverlässigkeit aufgrund einer geschäftlichen Beziehung zu unredlichen Geschäftspartnern in Frage steht, laufen Gefahr, dass Kunden, Verbraucher und die Öffentlichkeit sich von dem Unternehmen abwenden und bestehende Geschäftsbeziehungen beenden. Oftmals wiegen derartige Folgen für das Unternehmen schwerer als verhängte Geldstrafen und Bußgelder. Und schließlich wird es im Interesse eines Unternehmens liegen, finanzielle Schäden aufgrund betrügerischer Aktivitäten von Geschäftspartnern bestmöglich zu vermeiden.

Je mehr Informationen dem Unternehmen über den potenziellen Geschäftspartner vorliegen, desto sicherer und realistischer wird das Bild des Unternehmens zu der Frage sein, ob es sich um einen zuverlässigen Partner handelt. Die Einführung einer systematischen Geschäftspartner-Prüfung dient daher dem Schutz des Unternehmens und seiner Mitarbeiter vor solchen Risiken.

Empfehlungen für die Umsetzung

Die Geschäftspartnerprüfung ist so auszugestalten, dass das Unternehmen ein realistisches Bild von seinen Geschäftspartnern bekommt und die Zusammenarbeit auf solche Geschäftspartner begrenzen kann, die redlich und vertrauenswürdig sind.

Sorgfältige Auswahl der Geschäftspartner

Eine unternehmerische Tätigkeit bringt eine Vielzahl unterschiedlicher Geschäftsbeziehungen mit sich. Um eine effiziente, schnelle sowie kontinuierliche Prüfung von Geschäftspartnern zu gewährleisten und den Aufwand einer Geschäftspartnerprüfung sowohl für kleine als auch große Unternehmen in einem wirtschaftlich zumutbaren Maß zu halten, empfiehlt sich die Durchführung einer risikobasierten Geschäftspartnerprüfung. Bei dieser werden die Geschäftspartner anhand verschiedener Kriterien in verschiedene Risikoklassen wie z. B. niedrig und hoch eingeteilt und die Intensität einer anschließenden Prüfung dabei von der jeweiligen Risikoklassifizierung abhängig gemacht. Eine Einteilung der Geschäftskontakte in unterschiedliche Risikoklassen bietet Unternehmen den Vorteil, sich auf die kritischen Risiken zu konzentrieren. Dieses risikobasierte Vorgehen ist einerseits sehr ressourceneffizient und kann andererseits das Geschäftspartnerrisiko erheblich reduzieren. Da das Risiko einer Geschäftsbeziehung (Großhändler, Kunden, Lieferanten, Berater, Handelsvertreter, Zielobjekt im Rahmen von Mergers & Acquisitions etc.) unterschiedlich ausfallen kann, empfiehlt sich in einem

Risikobasierte Geschäftspartnerprüfung

ersten Schritt, eine Identifizierung aller bestehenden und neuen Geschäftsbeziehungen vorzunehmen.

Kleinere Unternehmen, deren Geschäftspartnerstruktur und unternehmerische Tätigkeit übersichtlich sind, werden vielmals lediglich einem geringen Geschäftspartnerrisiko ausgesetzt sein. Ein geringes Geschäftspartnerrisiko kann beispielsweise für Unternehmen angenommen werden, die weder kritische Produkte/Dienstleistungen[32] vertreiben noch von Geschäftspartnern beziehen, keine kritischen Geschäftsmodelle wie der Einsatz von Vertriebsmittlern und -agenten praktizieren und überwiegend mit Bestandsgeschäftspartnern Geschäfte betreiben, mit denen bereits eine längere und zuverlässige Geschäftsbeziehung besteht. Gleiches dürfte gelten, wenn das Unternehmen überwiegend mit neuen, dem Unternehmen bekannten Geschäftspartnern Geschäfte tätigen will, die ihren Sitz in Deutschland oder innerhalb der westlichen EU-Länder haben. Dennoch können sich auch für kleine Unternehmen verschiedene Risiken aus einer geschäftlichen Beziehung mit Dritten ergeben, weshalb kleinere Unternehmen ebenfalls zumindest eine kurze Einschätzung/Prüfung der Partner dahingehend vorzunehmen haben, ob besondere Umstände auf ein erhöhtes Risiko hindeuten, wenn mit diesem Geschäftspartner eine geschäftliche Beziehung eingegangen wird.

Überprüfung des Geschäftspartners auf Hinweise auf erhöhtes Risiko

Merkmale für ein potenziell erhöhtes Geschäftspartnerrisiko, für alle Unternehmen, unabhängig von ihrer Größe, sind:

- Der Geschäftspartner ist nahezu unbekannt und hat den Sitz im Ausland. Ein erhöhtes Risiko ergibt sich z.B., wenn sich der Sitz des Geschäftspartners oder das Land, in dem das Geschäft getätigt werden soll, in einem sog. Hochrisikoland für Korruption[33] befinden.
- Der Geschäftspartner hat seinen Sitz in einem ausländischen Staat mit politisch oder wirtschaftlich instabiler bzw. ungewisser Lage.
- Der Geschäftspartner ist in einer bestimmten Branche tätig (z.B. Rüstungsindustrie oder andere Branchen mit hohen Compliance-Risiken): Für das Unternehmen kann sich anhand der Exportkontrollvorschriften eine Prüfungspflicht bzgl. der (End-)Verwendung der gelieferten Ware durch den Geschäftspartner oder dessen Endkunden ergeben.
- Das beabsichtigte Geschäft überschreitet ein bestimmtes vom Unternehmen festgelegtes, kritisches Auftragsvolumen.
- Bei dem Geschäftspartner handelt es sich um einenn Agenten/Vertriebsmittler, der für das Unternehmen (im Ausland) Beratungsdienstleistungen erbringen sollen. Ein erhöhtes Risiko kann sich insbesondere aus dem Geschäftsmodell mit Vertriebsmittlern ergeben, z.B. indem das Unternehmen mit dem Vertriebspartner ein/e außergewöhnlich hohe/s Honorar/Provision vereinbaren und dieser einen Teil seines Honorars/seiner Provision für korruptive Handlungen verwenden würde, um einen Geschäftsabschluss zu erreichen.
- Bei dem Geschäftspartner handelt es sich um ein Zielobjekt, das vom Unternehmen käuflich erworben werden soll, oder mit dem Geschäftspartner ist eine Unternehmenskooperation (z.B. Joint Venture) geplant. Werden nach Abschluss des Kaufes oder des Kooperationsvertrages Korruptionsfälle, Umwelt- oder medienwirksame Skandale von Führungskräften des Geschäftspartnerunternehmens bekannt, so kann das erhebliche Schäden für das eigene Unternehmen zur Folge haben. Zum einen besteht die Gefahr, dass der Wert des Zielunternehmens drastisch einbricht und zum anderen die Gefahr der Haftung des Unternehmens als Rechtsnachfolger. Denn mit Wirkung zum 30.06.2013 wurde mit der 8. Novelle des Gesetzes gegen Wettbewerbsbeschränkungen[34] dem §30 OWiG ein neuer Absatz 2a eingefügt , der vorsieht, dass künftig eine Unternehmensgeldbuße nunmehr auch gegenüber Rechtsnachfolgern eines Unternehmens (zum Beispiel in Fällen der Verschmelzung oder Aufspaltung des Unternehmens) verhängt werden kann. Zudem wurde die Höhe des maximalen Bußgeldes gegen juristische Personen von bislang 1 Mio. Euro auf 10 Mio. Euro festgesetzt. Aufgrund der Gesetzesänderung wird es aus Risikogesichtspunkten umso wichtiger sein, den Geschäftspartner gründlich auf mögliche Compliance-Verstöße aus der Vergangenheit hin zu untersuchen. Neben haftungsrechtlichen Konsequenzen können Verstöße des Zielunternehmens auch zu erheblichen Reputationsschäden des Käuferunternehmens selbst führen.

Textbox 01: Merkmale für ein erhöhtes Geschäftspartnerrisiko

Diese vorgenannten Beispiele legen lediglich exemplarisch die Bedeutung einer risikobasierten Geschäftspartnerprüfung dar und sind keinesfalls als abschließende Faktoren und Kriterien zu betrachten. Jedes Unternehmen hat eine auf das eigene Unternehmen zugeschnittene, risikobasierte Prüfung seiner Geschäftspartner durchzuführen.

32 Zu den kritischen Produkten/Dienstleistungen zählen z.B. Rüstungsgüter bzw. sog. Dual-Use-Güter.

33 Vgl. z.B. Korruptionswahrnehmungsindex von Transparency International abrufbar unter: http://www.transparency.org/research/cpi/overview (16.04.2014).

34 Die 8. Novelle des Gesetzes gegen Wettbewerbsbeschränkungen, BGBL I,Jahr 2013, Seite 1738, ist abrufbar unter: http://www.bgbl.de/Xaver/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl113s1738.pdf#__Bundesanzeiger_BGBl__%2F%2F*[%40attr_id%3D%27bgbl113s1738.pdf%27]__1394706673853 (16.04.2014).

Grundlegende Prüfungsmaßnahmen (Basisprüfung)

Grundlegende Prüfungsmaßnahmen (Basisprüfung)

Bei kleinen Unternehmen, deren Geschäftspartnerstruktur übersichtlich ist und deren unternehmerische Tätigkeit mit Dritten lediglich geringe Risiken birgt, werden vornehmlich grundlegende Prüfungsmaßnahmen im Wege einer Basisprüfung ausreichen. Eine Basisprüfung bezieht sich insbesondere auf die wesentlichen (Stamm-) Daten, die in der Regel für die Durchführung des Geschäfts notwendig sind, und daher zu jedem potenziellen Geschäftspartner erhoben werden müssen. Zu den Basisinformationen zählen insbesondere die wesentlichen Stammdaten des Geschäftspartners wie z.B.:

Stammdaten-Erhebung

- Kontaktdaten wie Name, Adresse, Telefonnummer
- Bank- und Steuerdaten
- Rechtsform und Eigentümerstruktur
- Handelsregisternummer bzw. Kopie des Handelsregisterauszugs
- Rechnungsanschrift
- ggf. vorhandene Zertifizierungen (ISO 9001, 14001 etc.)

Mit zunehmender Unternehmensgröße und wachsender Zahl der unterschiedlichsten Geschäftspartner werden Art und Umfang der Basisprüfungsmaßnahmen entsprechend umfangreicher ausfallen müssen. So sollten im Unternehmen beispielsweise im Rahmen der Prüfung der Eigentümerstruktur des Geschäftspartners klare Prozesse definiert sein, wann und unter welchen Umständen, z.B. durch Beschaffung eines entsprechenden Handelsregisterauszugs, die Gesellschaftsverhältnisse des Geschäftspartnerunternehmens zu überprüfen sind, sowie unter welchen Umständen die jeweiligen Gesellschafter einer näheren Prüfung zu unterziehen sind.

Geschäftspartnerabgleich mit Sanktions- und Anti-Terrorlisten

Unabhängig von der Unternehmensgröße hat jedes Unternehmen einen klaren standardisierten Prozess zu schaffen, wann und welche Geschäftspartner mit den verschiedenen Sanktions- und Anti-Terrorlisten abzugleichen sind (vgl. hierzu → FUSSNOTE 31). Inwieweit einem Unternehmen hierbei ggf. noch ein manueller Abgleich möglich sein sollte bzw. wann ein automatischer datenbankbasierter Abgleich erforderlich sein wird, wird von verschiedenen Faktoren abhängig sein. So ist es z.B. für Unternehmen, die eine Vielzahl unterschiedlicher internationaler Geschäftsbeziehungen unterhalten, zur Erfüllung ihrer Organisations- und Sorgfaltspflichten unumgänglich, seine Geschäftspartner unter Zuhilfenahme datenbankgestützter Lösungen mit den verschiedenen Anti-Terrorlisten abzugleichen. Ist es dem einen kleinen Unternehmen aufgrund geringer Risiken aus der Geschäftstätigkeit, übersichtlicher und homogener Geschäftspartnerstruktur u.U. noch möglich, einen gelegentlichen, bedarfsbezogenen Abgleich manuell vorzunehmen,[35] so wird kleinen Unternehmen, die beispielsweise im Rüstungsbereich tätig sind und verschiedene Kunden weltweit bedienen, ein manuell betriebener Aufwand kaum mehr möglich sein, weshalb die Basisprüfungsmaßnahmen bei diesen Unternehmen ebenso wie bei größeren Unternehmen durch den Einsatz entsprechender technischer Mittel erweitert werden müssen.

Ferner werden nach dem Geldwäschegesetz (GWG) in bestimmten Fällen u.a. auch Unternehmen, die gewerblich mit Gütern handeln – unabhängig von ihrer Größe – gesetzlich verpflichtet, ihre Vertragspartner/Kunden zu identifizieren.[36] Daher hat jedes Unternehmen entsprechende Prozesse festzulegen, welche die gesetzlichen Anforderungen aus dem GWG sicherstellen.

Intensivere Prüfungsmaßnahmen

Intensivere Prüfungsmaßnahmen

Geschäftsbeziehungen, die in die Kategorie eines erhöhten Risikos eingestuft worden sind, müssen aus Risikogesichtspunkten einer intensiveren Prüfung unterzogen werden. Dies gilt sowohl für neue Geschäftspartner als auch für Bestandsgeschäftspartner, falls dem Unternehmen im Laufe der Zeit besondere Umstände bekannt werden, die Rückschlüsse auf ein erhöhtes Risiko zulassen können. Solche Umstände können z.B. der Eintritt von wesentlichen Veränderungen in der Eigentümerstruktur des Geschäftspartners oder das Bekanntwerden von negativen Hinweisen über den Geschäftspartner (drohende Insolvenz des Geschäftspartners, kriminelles Verhalten, ethisch fragwürdige Geschäftspraktiken etc.) sein.

Ohne erheblichen Aufwand können auch kleine Unternehmen bei Vorliegen eines erhöhten Geschäftspartnerrisikos ihre Standardprüfungsmaßnahmen durch intensivere Prüfungsmaßnahmen wie Hintergrundrecherchen zu dem Geschäftspartner über allgemein zugängliche Quellen wie z.B. das Internet ergänzen. Hierbei kann bereits die einfache Maßnahme wie das ›googeln‹ eines Geschäftspartners Informationen über dessen mögliches kriminelles Fehlverhalten oder Geschäftspraktiken, die in der Öffentlichkeit als unredlich angesehen wurden, liefern. Ebenso lassen sich auch die

35 Z.B. kann über die Internetseite des Justizportals des Bundes und der Länder (http://www.finanz-sanktionsliste.de/fisalis/jsp/index.jsf (16.04.2014)) eine Prüfung der in den Sanktions-Verordnungen der EU gelisteten Personen, Gruppen oder Organisationen vorgenommen werden.

36 Nach §3 Abs.2 Nr. 4 GWG haben bspw. auch Güterhändler bei der Annahme von Bargeld im Wert von 15.000 Euro oder mehr bestimmte im GWG normierte Identifizierungspflichten zu erfüllen.

Unternehmensdaten des Geschäftspartners durch Vorlage eines Handelsregisterauszugs leicht auf Richtigkeit und Vollständigkeit oder das Kreditausfallrisiko über spezielle Dienstleister überprüfen oder Informationen über einen Geschäftspartner zu möglichem korruptiven Verhalten in der Vergangenheit, z. B. über die Korruptionsregister verschiedener Bundes-länder, einholen. Die Tiefe und der Umfang intensiver Prüfungsmaßnahmen haben sich dabei insbesondere an den sich aus der Geschäftsbeziehung spezifisch ergebenden Risiken für das Unternehmen zu orientieren.

Prüfungsmaßnahmen bei Mergers & Acquisitions

Intensive Prüfungsmaßnahmen sind insbesondere im Rahmen von Unternehmenszukäufen (Mergers & Acquisitions) sowie bei Eingehen von Unternehmenskooperationen (z. B. Joint Ventures) erforderlich. Hierbei ist das Zielunternehmen (das Kaufunternehmen bzw. der Kooperationspartner) einer intensiven Geschäftspartnerprüfung (auch Due Diligence genannt) zu unterziehen. Laufende Verfahren gegen das Zielunternehmen wie z. B. wegen Korruptionsverdacht, Kartellrechts- oder Umweltverstößen sowie eine drohende Insolvenz der Zielgesellschaft oder ethisch fragwürdige Verhaltensweisen des Zielunternehmens können sich (nachträglich) nachteilig auf den Wert des erworbenen Unternehmens sowie auf die Reputation des eigenen Unternehmens auswirken. Das Unterlassen einer Due Diligence durch die Geschäftsführung des kaufenden Unternehmens stellt daher in der Regel eine gesellschaftsrechtliche Sorgfaltspflichtverletzung gegenüber dem eigenen Unternehmen dar. Erleidet die Gesellschaft einen Schaden, so ist die Unternehmensleitung der eigenen Gesellschaft gegenüber zum Schadensersatz verpflichtet.

Spezifische Länderrisiken/ Korruptionswahrnehmungsindex (CPI)

Mit zunehmender Internationalität der Geschäftsbeziehungen werden die entsprechenden Prüfmaßnahmen erweitert werden müssen. So sind insbesondere bei ausländischen Geschäftspartnern oder Geschäften im Ausland die spezifischen Länderrisiken (z.B. Korruptionswahrnehmungsindex (CPI)) mit einzubeziehen und sich daraus ableitende intensivere Prüfmaßnahmen vorzunehmen. Ein Abgleich des Geschäftspartners mit Sanktionslisten darf sich in der Regel nicht mehr auf die Europäischen Listen beschränken, sondern ist im Falle internationaler Geschäftsbeziehungen um den Abgleich mit den internationalen Listen zu erweitern. Für größere Unternehmen, deren Unternehmensmarke das wesentliche Unternehmenskapital darstellt, sollten im Rahmen der intensiven Prüfungsmaßnahmen auch weitergehende Integritätschecks des Geschäftspartners miteinbezogen werden. Denn Informationen über den Geschäftspartner, wie z.B. ob er ein eigenes CMS hat, ob und wie er ein eigenes CMS nach außen kommuniziert (Unternehmenswebsite etc.), ob es ein Commitment der Unternehmensleitung des Geschäftspartners zu Umwelt-, Sozialbelangen etc. gibt und ob und inwieweit er CSR im Rahmen der Wertschöpfungskette (nach oben und unten) mit einbindet, lassen Rückschlüsse auf die Zuverlässigkeit des Geschäftspartners und der Ernsthaftigkeit seiner implementierten Compliance-Maßnahmen zu. Integritätschecks können z.B. über eine Selbstauskunft des Geschäftspartners anhand eines detaillierten Fragebogens mit anschließendem Abgleich der zur Verfügung gestellten Daten mit den öffentlich zugänglichen Informationen erfolgen. Wird die Selbstauskunft vom Geschäftspartner nur lückenhaft ausgefüllt oder verweigert oder ergeben sich Unstimmigkeiten, so können dies Zweifel an der Zuverlässigkeit und Integrität des Geschäftspartners begründen. In diesen Fällen ist beim Geschäftspartner nach den fehlenden Informationen bzw. bei fehlender Plausibilität entsprechend nachzufassen.

Vor-Ort-Besichtigung/ Audits

Vor allem Vor-Ort-Besichtigung/Audits beim Geschäftspartner sind geeignete Maßnahmen, um sich einen umfassenden Eindruck zu dessen Zuverlässigkeit zu verschaffen. Über Vor-Ort-Besuche lässt sich beispielsweise feststellen, wie der Geschäftspartner tatsächlich technisch und personell aufgestellt ist und ob es sich nicht gar um eine Briefkastenfirma handelt. Eine Vor-Ort-Besichtigung eignet sich insbesondere zur Überprüfung, ob und inwieweit Arbeitssicherheitsbedingungen, sicherheitstechnische Standards, Umweltstandards oder Sozialstandards (wie z. B. Verbot von Kinderarbeit, menschenwürdige Arbeitsbedingungen) beim Geschäftspartner vorhanden sind und beachtet werden (sog. (technisches) Audit). Eine solche Untersuchung (Audit) kann sowohl vom Unternehmen selbst als auch – falls beispielsweise eine unabhängige Zertifizierung gewünscht ist oder der Geschäftspartner seinen Sitz im Ausland hat und das Unternehmen entweder nicht die notwendigen Kenntnisse oder Kapazitäten für die Durchführung eines Audits hat – über externe Dienstleister erbracht werden.

Einbeziehung spezialisierter Dienstleister

Verdichten sich im Rahmen der Geschäftspartnerprüfung die Warnhinweise auf ein hohes Geschäftspartnerrisiko (sog. Red Flags), so sind die Prüfungsmaßnahmen weiter zu intensivieren, ggf. unter Einbeziehung spezialisierter Dienstleister.

Durchführung der Überprüfung, Entscheidungsverantwortlichkeiten und Genehmigungsprozesse

Prüfung von Neugeschäftspartnern

Sämtliche erforderliche Prüfungsmaßnahmen (Basisprüfungsmaßnahmen als auch intensive Prüfungsmaßnahmen) müssen bei Neugeschäftspartnern frühzeitig, also bereits während der Vertragsanbahnung spätestens vor Vertragsabschluss, durchgeführt sein. Bei bestehenden Geschäftspartnern sind die Prüfungsmaßnahmen danach auszurichten, ob die Geschäftsbeziehung als geringes oder erhöhtes Risiko eingestuft worden ist.

Beschränkt sich das Unternehmen im Falle eines lediglich geringen Geschäftspartnerrisikos nur auf die Basisprüfungsmaßnahmen, so läuft es Gefahr, dass unter Umständen Informationen über den Geschäftspartner unberücksichtigt bleiben, die für

eine realistische Risikoeinschätzung von wesentlicher Bedeutung wären. Daher haben die Unternehmen auch im Falle eines vom Geschäftspartner ausgehenden geringen Risikos abzuwägen, ob der Umfang der Prüfungsmaßnahmen generell über die Basisprüfung hinausgehen sollte.

Prüfung von Bestandsgeschäftspartnern

Mit zunehmender Unternehmensgröße und Komplexität wird die Zahl der Bestandsgeschäftspartnern eines Unternehmens ansteigen und damit einen erheblichen Aufwand einfordern, will man jeden Bestandsgeschäftspartner einer nachträglichen intensiven Überprüfung unterziehen. Um den Aufwand im Hinblick auf ein potenzielles Risiko dennoch in einem wirtschaftlich zumutbaren Rahmen zu halten, empfiehlt es sich, die Prüfungsmaßnahmen für Bestandsgeschäftspartner entsprechend risikobasiert vorzunehmen.

Hat ein Unternehmen seine bisherigen Geschäftspartner bislang keiner Überprüfung unterzogen, so sind erstmalige Prüfungsmaßnahmen zumindest zu den Bestandsgeschäftspartnern nachzuholen, deren Kategorisierung auf ein erhöhtes Risiko hinweist (vgl. oben → TEXTBOX 01 ›MERKMALE FÜR EIN ERHÖHTES GESCHÄFTSPARTNERRISIKO‹). Hat ein Unternehmen beispielsweise bestehende Geschäftsbeziehungen zu ausländischen Vertriebsagenten/Beratern, die zudem auch noch in einem als korruptionsanfällig geltenden Land Beratungs- oder Vermittlungstätigkeit erbringen, so ist diese Geschäftsbeziehung als ein hohes Risiko einzustufen und macht auch eine Überprüfung des Bestandsgeschäftspartners aus Risikogesichtspunkten zwingend erforderlich. In diesem Beispielsfall hätte das Unternehmen insbesondere zu prüfen, ob mit dem Geschäftspartner schriftliche Verträge bestehen, ob die zu erbringende Leistung konkret beschrieben ist sowie ob die Vergütung in einem angemessenen, üblichen Umfang zu der zu erbringenden Leistung steht. Ist der Inhalt der Geschäftsbeziehung nicht umfassend transparent, so hat das Unternehmen intensive Klärungsmaßnahmen herbeizuführen. Ebenso sind (wiederholende) Prüfungsmaßnahmen dann erforderlich, wenn Änderungen beim Geschäftspartner wie z.B. hinsichtlich der Eigentümerstruktur, hinsichtlich der Finanzlage etc. bekanntwerden oder wesentliche rechtliche oder ethisch verwerfliche Verstöße des Geschäftspartners zu Tage treten. Da wesentliche Änderungen, negative Hinweise etc. jederzeit eintreten können, sollten diejenigen Geschäftsbeziehungen, die von dem Unternehmen als hohes Risiko (z.B. Geschäftspartner aus riskanten Branchen, Geschäftspartner mit Sitz in sog. Hochrisikoländern) eingestuft werden, einer turnusmäßigen Wiederholungsprüfung unterzogen werden.

Weiterhin kann unter Risikogesichtspunkten für ein Unternehmen nicht nur eine Prüfung eines unmittelbaren Geschäftspartners, sondern ggf. auch der weiteren Beteiligten entlang der Wertschöpfungskette erforderlich sein. Lässt ein Unternehmen beispielsweise Waren über Geschäftspartner in Entwicklungs- oder Schwellenländern

herstellen und verstößt ein Unterlieferant des eigenen Geschäftspartners gegen unzureichende Arbeits- und Sicherheitsbedingungen, gegen das Verbot von Kinderarbeit etc., so können derartige Verstöße auf reges öffentliches und mediales Interesse stoßen und den guten Ruf des eigenen Unternehmens in Mitleidenschaft ziehen und nachhaltige Schäden für das Unternehmen verursachen.

Festlegung der Verantwortlichkeit der Prüfungsdurchführung

Unternehmen sollten ein entsprechendes Informationswesen schaffen, mit dem sichergestellt wird, dass das Bekanntwerden von negativen Hinweisen oder veränderten Umständen, die ggf. Rückschlüsse auf ein erhöhtes Risiko aus der Geschäftsbeziehung zulassen, intern im Unternehmen an die verantwortliche(n) Stelle(n) entsprechend kommuniziert wird, damit die weiteren Prüfungsmaßnahmen unverzüglich eingeleitet werden können. Mit der Durchführung der Geschäftspartnerprüfung sind geeignete Mitarbeiter zu betrauen. Dabei ist klar zu definieren, wer für die Durchführung der Prüfungsmaßnahmen zuständig ist. In kleineren Unternehmen kann es sich anbieten, die Durchführung der Prüfungsmaßnahmen einer oder wenigen Personen im Unternehmen (z.B. der Buchhaltung oder dem Vertrieb oder Einkauf) zu übertragen. Größere Unternehmen werden hierfür eine entsprechend größere Zahl an Mitarbeitern beauftragen müssen. Hier kann es sich anbieten, die Durchführung der Prüfungsmaßnahmen bereichsbezogen festzulegen (z.B. Prüfung von Lieferanten durch den Einkauf, Prüfung von Kunden durch den Verkauf). Der Vorteil ist darin zu sehen, dass die entsprechenden Prüfungsmaßnahmen im Rahmen der jeweiligen Prozesse, wie der Lieferanten- bzw. Kundenanlage, eingebunden werden können und damit einen effizienten Ressourceneinsatz ermöglichen.

Je größer das Unternehmen ist und je unterschiedlicher und zahlreicher die Geschäftspartner sein werden, desto umfassender und systematisierter muss der Prüfprozess der Geschäftspartnerbeziehung ausgelegt und dokumentiert werden, um einen einheitlichen Prüfprozess im Unternehmen sicherzustellen. Insbesondere bei international agierenden Unternehmen bringen die Geschäftsbeziehungen komplexe Netzwerke unterschiedlicher Geschäftspartner wie eine Zusammenarbeit mit Absatzmittlern, Lieferanten, Handelskooperationen/-vertretern und lokalen Beratungsunternehmen hervor. Dabei ist insbesondere für große Unternehmen, die mehrere tausend Geschäftspartnerbeziehungen unterhalten, der Einsatz von entsprechender spezifischer Software unumgänglich, um ein zuverlässiges Geschäftspartnermanagement sicherzustellen.

Geschäftspartnerprüfung anhand von Checklisten/ Red Flags

Den mit den Prüfmaßnahmen betrauten Mitarbeitern sind detaillierte Prozessbeschreibungen zur Verfügung zu stellen. Bereits einfache Checklisten, die Maßnahmen oder zu beachtende Punkte beinhalten, wie die Vornahme der Kategorisierung der Geschäftsbeziehungen in unterschiedliche Risikoklassen zu erfolgen hat, welche Stammdaten zu erfassen sind, welche intensiven Prüfungsmaßnahmen hilfreich bzw.

zwingend erforderlich sind, welche besonderen Warnhinweise (Red Flags) auf ein erhöhtes Risiko hindeuten, leisten den Mitarbeitern die wichtige Orientierung.

Mit zunehmender Zahl an verschiedensten Geschäftsbeziehungen sind im Hinblick auf die damit verbundene Zunahme der Risiken für das Unternehmen erhöhte Anforderungen an den Prüfprozess zu stellen. Dies erfordert auch die Implementierung geeigneter prozessintegrierter Kontrollmaßnahmen (vgl. CMS-Element → 7 ÜBERWACHUNGS- UND KONTROLLMASSNAHMEN). So hat das Unternehmen grundsätzlich eine klare Funktionstrennung dahingehend sicherzustellen, dass der für die Durchführung der Geschäftspartnerprüfung verantwortliche Mitarbeiter nicht zugleich die Entscheidung über die Annahme oder Ablehnung des Geschäftspartners trifft, sondern diese Entscheidung von einer anderen, unabhängigen Stelle im Unternehmen getroffen wird. Kleine Unternehmen, in denen die Unternehmensleitung stark ins Tagesgeschäft eingebunden ist und über die wesentlichen Vorkommnisse im Unternehmen Bescheid weiß, bedürfen dabei weniger formalisierten Maßnahmen, wenn die Entscheidung dadurch letztendlich auf der Unternehmensleitung beruht. Größere Unternehmen haben jedoch die Entscheidungskompetenzen klar festzulegen. Entscheidungen sollten hierbei dezentral von der jeweils betroffenen Fachabteilung getroffen werden. Dies ermöglicht nicht nur einen effizienten Einsatz der Personalressourcen, sondern sichert auch die Qualität des Entscheidungsprozesses. Im Rahmen des Prozesses ist ferner zu bestimmen, wie mit Hinweisen auf ein erhöhtes Geschäftspartnerrisiko konkret umzugehen ist, wer im Unternehmen die Entscheidungskompetenz für die Ablehnung oder Freigabe eines Geschäftspartners hat bzw. unter welchen Umständen eine Entscheidung bzw. Genehmigung des Vorgesetzten erforderlich ist. Auch empfiehlt sich, im Prozess klar festzuhalten, unter welchen Umständen der Compliance-Verantwortliche in die weiteren Prüfungs- und Genehmigungsprozesse eingebunden werden kann bzw. einzubinden ist. Dies kann z.B. erforderlich werden, wenn den Verantwortlichen bei der Prüfung des Geschäftspartners Zweifel an dessen Zuverlässigkeit oder Integrität aufkommen oder bestimmte Red Flags auf ein erhöhtes Risiko des Geschäftspartners hindeuten.

Wahrung der Funktionstrennung im Genehmigungsprozess

Einbindung des Compliance-Verantwortlichen

Schließlich hat das Unternehmen sicherzustellen, dass sämtliche vom Unternehmen getroffenen Entscheidungen und die zugrundeliegenden Gründe dokumentiert werden und die Mitarbeiter bei der Durchführung der Geschäftspartnerprüfung die geltenden Datenschutzregelungen beachten.

Festlegung von Entscheidungsoptionen

Für die mit der Durchführung der Prüfungsmaßnahmen verantwortlichen Mitarbeiter sollten verschiedene Entscheidungsoptionen festgelegt sein, wie z.B. die Voraussetzungen einer Freigabe und Zustandekommen oder Ablehnung der Geschäftsbeziehung bzw. eine eventuelle Vornahme weiterer Prüfungsschritte unter Einbeziehung spezialisierter Dienstleister/Experten aufgrund von Hinweisen auf ein hohes Risiko.

Festlegung von Entscheidungsoptionen

Einbeziehung spezialisierter Dienstleister/Experten

Das Vorliegen eines erhöhten Risikos sollte nicht grundsätzlich der Anlass für den Abbruch einer Geschäftsbeziehung sein. Vielmehr sollen Hinweise auf ein potenziell erhöhtes Risiko das Unternehmen zu weiteren (Überprüfungs-)Maßnahmen veranlassen und damit die Chance bieten, eine Entscheidung zu fällen, die auf eine umfassenden Informationsbasis gestützt ist. So kann sich als Option zur Durchführung einer weiteren Recherche die Beauftragung von externen spezialisierten Dienstleistern anbieten, wenn das Unternehmen einen neuen Markt in einem sog. Hochrisikoland betreten möchte und hierfür Vertriebsagenten zum Einsatz bringen möchte, die es nicht (gut) kennt. Spezialisierten und eventuell vor Ort sitzenden Experten steht in der Regel ein größeres Informationsnetzwerk für eine umfassende Integritätsprüfung des Geschäftspartners und seines Umfelds zur Verfügung.

Letztendlich ist aber auch die Option zu erwägen, von einer Geschäftsanbahnung Abstand zu nehmen bzw. eine bestehende Geschäftsbeziehung unter Umständen abzubrechen. Solche Maßnahmen können in Betracht gezogen werden, wenn über den Geschäftspartner Kenntnisse zu kriminellem Verhalten oder ethisch fragwürdigen Geschäftspraktiken bekannt werden und diese Negativmeldungen nachhaltig auf das Unternehmen und seine Marke zurückfallen und erheblichen (Reputations-)Schaden anrichten können.

Nach einer Studie aus dem Jahr 2012 können nicht nur die Qualität oder der Preis eines Produktes, sondern insbesondere auch die Reputation eines Unternehmens, einen wesentlichen Einfluss auf die Kaufentscheidung von Kunden nehmen: *»70% of the consumers report that they avoid buying a product if they don't like the company behind the product«*

Vgl. Weber Shandwick (Eds.) (2012), S. 8: ›The company behind the brand: in reputation we trust.‹ *http://www.webershandwick.eu/home/news/673 (16.04.2014)*

Aufrechterhaltung von Geschäftsbeziehungen

Je größer sich das Schadensrisiko für ein Unternehmen darstellt, das aus einer Geschäftsbeziehung mit Dritten hervorgehen kann, desto umfassender sollte ein

Unternehmen geeignete vertragliche Präventionsmaßnahmen implementieren. Als geeignete Präventionsmaßnahmen kommen verschiedenste Möglichkeiten in Betracht.

Festlegung von vertraglichen Präventionsmaßnahmen

Bereits das Anfordern von schriftlichen Compliance-Erklärungen vom Geschäftspartner hebt die Bedeutung und Wichtigkeit von Compliance für das Unternehmen hervor und kann zu einer zusätzlichen Sensibilisierung des Geschäftspartners führen.

Einholung von Compliance-Erklärungen

Ein weiteres probates Mittel stellt die Einbindung von vertraglichen Compliance-Klauseln in die jeweiligen Verträge mit den Geschäftspartnern dar. Solche präventiven Compliance-Klauseln sollen gegenüber dem Vertragspartner die Wichtigkeit und Bedeutung der Einhaltung gesetzlicher und vertraglicher Normen aufzeigen und beinhalten in der Regel besondere Rechte des Unternehmens oder (negative) Folgen für den Geschäftspartner, falls dieser gegen bestimmte (Compliance-)Regelungen verstößt, wie z.B. Vertragsstrafen oder (pauschalierte) Schadensersatzzahlungen des Geschäftspartners im Falle der Verletzung festgelegter Compliance-Verhaltensweisen. Sonderkündigungsrechte bieten dem Unternehmen die Möglichkeit, sich fristlos von einer Geschäftsbeziehung zu lösen, falls der Geschäftspartner sich als unzuverlässig erwiesen hat und für das Unternehmen ein erhebliches Compliance-Risiko darstellt.

Vertragliche Compliance-Klauseln

Als eine wichtige Compliance-Klausel ist in diesem Zusammenhang die sog. Audit-Klausel anzusehen, mit der sich das Unternehmen von seinem Geschäftspartner das Recht einräumen lässt, eigene Untersuchungen und Überprüfungen zur Einhaltung von Compliance beim Geschäftspartner vornehmen zu dürfen. Ohne eine entsprechende Audit-Klausel dürften die weiteren vertraglichen Compliance-Klauseln ihre Wirkung verfehlen, wenn ein Unternehmen keine Prüfungsmöglichkeiten hat, ob der Geschäftspartner sich auch tatsächlich an die Compliance-Vereinbarungen hält. Eine Audit-Klausel sollte dabei klar definieren, welche Prüfungsmaßnahmen sowie aus welchen Anlässen das Unternehmen solche vornehmen darf. Ferner ist den Unternehmen zu empfehlen, sich vertragliche Ansprüche auf Informations- und Auskunftserteilung einräumen zu lassen. Dies kann für das Unternehmen z.B. im Rahmen von Joint-Venture-Beteiligungen empfehlenswert sein, falls Unregelmäßigkeiten in der eigenständigen und unabhängigen Beteiligungsgesellschaft bekannt werden und das Unternehmen aus Compliance-Risikogesichtspunkten sich ein umfassendes Bild verschaffen möchte und ohne diese vertraglichen Regelungen keine oder nur schwer durchsetzbare Informationsansprüche hätte.[37] Aufgrund ihrer abschreckenden Wirkung stellen Compliance-Klauseln ein geeignetes Mittel dar, den Geschäftspartner von unerwünschtem Fehlverhalten abzuhalten.

Audit-Klausel

[37] Sind in einem Joint-Venture-Unternehmen bspw. zwei Joint-Venture-Partner mit jeweils 50% beteiligt, so steht grundsätzlich keinem der Joint-Venture-Partner ohne Einverständnis des jeweils anderen Joint-Venture-Partners das Recht zu, in dem gemeinsamen Joint-Venture-Unternehmen Prüfungsmaßnahmen durchzuführen bzw. durchführen zu lassen. Über eine Audit-Klausel zwischen den beiden Joint-Venture-Partnern können entsprechende Rechte eingeräumt werden.

Verträge mit Geschäftspartnern sollten aus Transparenz- und Dokumentationsgesichtspunkten stets schriftlich abgeschlossen werden. Dabei sind die Verträge zu bestimmten Geschäftspartnern wie Vertriebsmittlern oder exklusiven Vertragshändlern einer intensiveren Compliance-Prüfung dahingehend zu unterziehen, ob die jeweiligen Verträge eine detaillierte und nachvollziehbare Beschreibung der zu erbringenden Leistung enthalten sowie ob Provisionsvereinbarungen/Honorare in geschäftsüblichem, angemessenem Verhältnis zur vereinbarten und erbrachten Leistung stehen. Die Verträge mit den im Rahmen der Compliance-Risikoanalyse als risikobehaftet identifizierten Geschäftspartnern sollten ebenso wie diese Geschäftspartner selbst einer regelmäßigen und turnusmäßigen Prüfung unterzogen werden.

Abschluss schriftlicher Verträge

Weiter kann es sich anbieten, die Verträge mit potenziell hochriskanten Geschäftspartnern nur befristet abzuschließen und einen Prozess im Unternehmen zu implementieren, wonach das Unternehmen nach Ablauf der Vertragsdauer eine erneute Vertragsverlängerung nur dann vornehmen darf, wenn eine erneute Vertrags- und Geschäftspartnerprüfung vorgenommen worden ist. Allerdings ist zu beachten, dass befristete Verträge in der Regel nur im Wege eines Sonderkündigungsrechts beendet werden können. Will das Unternehmen sich von einem (unliebsamen) Geschäftspartner trennen, liegen allerdings keine Gründe für eine Sonderkündigung vor oder ist der Nachweis für die Zulässigkeit einer Sonderkündigung nicht oder nur schwer zu erbringen, so läuft das Unternehmen Gefahr, sich nicht ohne weiteres vor Ablauf der Befristung von der bestehenden Geschäftsbeziehung mit dem Geschäftspartner lösen zu können.

Abschluss befristeter oder unbefristeter Verträge

Und schließlich sollten Unternehmen während einer laufenden Geschäftsbeziehung mit Vertriebsmittlern und Agenten bzw. spätestens nach Ablauf der vereinbarten Laufzeit überprüfen, ob die vertraglich geschuldete Leistung auch tatsächlich entsprechend erbracht worden ist. Die Feststellungen dieser Überprüfung sollten wesentliche Grundlage für die weiteren Entscheidungen sein, wie z.B. ob dieser Geschäftspartner für weitere Projekte in Betracht zu ziehen ist oder von einer weiteren Geschäftsbeziehung abgesehen werden sollte. Prozesse, die sicherstellen, dass die Auszahlungen von Vergütungen oder Provisionen nur auf Grundlage einer nachvollziehbaren Dokumentation über die tatsächlich erbrachte Leistung vorgenommen werden und eine Überweisung grundsätzlich nur auf ein Bankkonto im Land des Sitzes des Geschäftspartners veranlasst werden darf, dienen beispielsweise der Geldwäscheprävention und der Verdachtsvermeidung, an betrügerischen Verhaltensweisen des Geschäftspartners beteiligt zu sein.

Überprüfung der tatsächlichen Leistungserbringung

Compliance-Kommunikation & Schulung

5

Welche Rolle spielen Kommunikation und Schulung für ein funktionierendes CMS?

Welche Themen und Inhalte sollen kommuniziert und geschult werden?

Welche Medien eignen sich zur Kommunikation von Compliance-Themen?

Welche Personen und Personengruppen im Unternehmen sollen (spezifisch) zu Compliance-Themen geschult werden? Wie häufig?

Welche Aspekte sind bei der Entwicklung eines Compliance-Schulungsprogramms zu beachten?

Wie können Mitarbeiter zu Compliance-Themen geschult werden? Welche Schulungsmethoden eignen sich für die Vermittlung von Compliance-Themen? Worauf ist bei der Auswahl der Schulungsmethode zu achten?

Wie kann ein Unternehmen sicherstellen, dass die Mitarbeiter Fragen und Anliegen zum CMS aber auch Beobachtungen von Fehlverhalten an die Compliance-Verantwortlichen kommunizieren können?

Braucht jedes Unternehmen ein eigenes Hinweisgebersystem (Whistleblowing-System)?

Worauf ist bei der Implementierung eines Hinweisgebersystems zu achten?

Zielsetzung

Die Kommunikation von Compliance insgesamt, deren Ziele, Inhalte und Erwartungen an die Mitarbeiter bilden einen wichtigen Erfolgsfaktor für ein funktionsfähiges CMS und damit ein wesentliches Kriterium für die Beurteilung der Angemessenheit und Wirksamkeit des CMS. Der beste Verhaltenskodex nützt nur wenig, wenn diejenigen, die sich daran halten sollen und denen er Orientierung geben soll, nicht davon erfahren oder nicht wissen, inwiefern er sie in ihrer Arbeit betrifft und welche Erwartungen im Verhaltenskodex an ihr Handeln im Geschäftsalltag gestellt werden. Damit das CMS erfolgreich umgesetzt werden kann, muss es bei denen ›ankommen‹ und ›wahrgenommen‹ werden – eben an die kommuniziert werden –, die es umsetzen sollen: die Mitarbeiter des Unternehmens. Compliance-Kommunikation schließt aber auch die Kommunikation an die weiteren Interessengruppen des Unternehmens, Lieferanten, Kunden, Investoren, Gesellschaft etc. ein. Compliance-Kommunikation an externe Interessengruppen ist Erwartungsmanagement, d.h. das Unternehmen vermittelt seinen Geschäftspartnern im Rahmen der Compliance-Kommunikation, z.B. durch Weitergabe des Verhaltenskodex oder Veröffentlichung von Informationen zum CMS auf der Unternehmenswebsite, auf welche Art und Weise das Unternehmen Geschäfte macht und welcher Stellenwert Compliance und Integrität in Geschäfts- und Entscheidungssituationen beigemessen wird.

Compliance-Kommunikation intern

Compliance-Kommunikation extern

Für die Erreichung der verschiedenen Zielgruppen ist die Auswahl geeigneter Kommunikationsmedien entscheidend. Ebenso sind die Inhalte der Kommunikation entsprechend der Zielgruppe anzupassen und aufzubereiten, d.h. die Botschaft muss verständlich und relevant für die jeweilige Zielgruppe kommuniziert werden. Nur so kann sichergestellt werden, dass die Mitarbeiter, als wichtigste Zielgruppe der Compliance-Kommunikation, die Botschaft verstehen und begreifen, was die Botschaft für ihr Handeln im Geschäftsalltag bedeutet.

Zielgruppenorientierung und Relevanz der Inhalte

Zielsetzung wirksamer Compliance-Kommunikation ist es, bei den Mitarbeitern Verständnis und Akzeptanz des CMS im Allgemeinen zu schaffen und ihnen Orientierung zu geben, damit die Unternehmenswerte und Compliance-Zielsetzungen von den Beschäftigten im Geschäftsalltag umgesetzt und tatsächlich gelebt werden (können). Mit Blick auf externe Interessengruppen wie Kunden, Lieferanten und Fremdkapitalgeber ist das Ziel der Compliance-Kommunikation, die Ernsthaftigkeit und Umsetzung des CMS glaubwürdig und transparent darzustellen, um so eine Reputation für Vertrauenswürdigkeit aufzubauen und die Geschäftsbeziehungen langfristig zu stabilisieren. Darüber hinaus kann glaubwürdige Compliance-Kommunikation auch im Bereich des Employer Branding und bei der Gewinnung von Fach- und Führungskräften eine wichtige Rolle spielen.

Verständnis und Akzeptanz des CMS

Der Erfolg der Compliance-Kommunikation steht und fällt mit dem Tone from the Top, dem Verhalten der Unternehmensleitung und Führungskräfte und der Führungs- und Unternehmenskultur. Mit ihrem Handeln und aktiven Vorleben von Compliance und Integrität im Geschäftsalltag beeinflussen die Unternehmensleitung und Führungskräfte ganz maßgeblich, wie Compliance im Unternehmen wahrgenommen und das CMS umgesetzt – mit Leben gefüllt – werden (vgl. hierzu auch das CMS-Element → 8 FÜHRUNG UND UNTERNEHMENSKULTUR).

Tone from the Top

Wirksame Compliance-Kommunikation und Sensibilisierung der Mitarbeiter für Compliance und Integrität ist eng verbunden mit Schulungen und Trainings in diesem Bereich. Neben der reinen Wissensvermittlung besteht das Ziel von Compliance-Schulungen darin, den Mitarbeitern und Führungskräften Handlungsorientierung zu geben und sie zu integrem und selbstverantwortlichem Handeln im Geschäftsalltag zu befähigen.

Compliance-Schulungen und Trainings

Neben der Kommunikation und Schulung von Compliance von oben nach unten, d.h. von der Unternehmensleitung, den oberen Führungsebenen und Compliance-Verantwortlichen an die Mitarbeiter, darf die Kommunikation ›bottom-up‹, also von unten nach oben, nicht vernachlässigt werden. Zum einen ist es für die Beurteilung der Wirksamkeit von Compliance-Kommunikation und Schulungen wichtig, von den Beschäftigten Rückmeldung darüber zu bekommen, wie Compliance und das CMS allgemein im Unternehmen wahrgenommen werden, welche kommunizierten Inhalte die Mitarbeiter wie erreichen und wo ggf. Notwendigkeit zur Anpassung besteht. Zum anderen ist es für die Aufdeckung von Compliance-Verstößen im Unternehmen erforderlich, dass Mitarbeiter und Führungskräfte Fehlverhalten und Missstände melden können. In bestimmten Fällen kann es sinnvoll sein, das Meldesystem auch externen Interessengruppen zugänglich zu machen, so dass beispielsweise auch Missstände in der vor- oder nachgelagerten Wertschöpfungskette durch Geschäftspartner gemeldet werden können. Häufig werden solche Systeme als Hinweisgeber- oder auch Whistleblowing-System bezeichnet. Neben der Aufdeckungsfunktion dient ein solches System der Abschreckung potenzieller Täter, indem es die Entdeckungswahrscheinlichkeit für Fehlverhalten deutlich erhöht. Die Einräumung der Möglichkeit einer anonymen Hinweisgabe kann dazu beitragen, dass auch Fehlverhalten angezeigt wird, das bei öffentlicher Meldung aufgrund von Angst vor Repressalien gegenüber dem Meldenden nicht angezeigt würde. Darüber hinaus können eingehende Meldungen auf bestehende Lücken im CMS hinweisen, was zur Verbesserung des CMS insgesamt beitragen kann. Bei der Entwicklung und Umsetzung eines Hinweisgebersystems im Unternehmen ist insbesondere auf den Schutz der Hinweisgeber sowie auf die geltende Rechtslage der verschiedenen nationalen Gesetzgebungen zu achten.

Kommunikation *bottom-up*

Hinweise von Unternehmensinternen sind noch immer die wichtigste Hinweisquelle für Fehlverhalten im Unternehmen, vgl. KPMG (2012): Wirtschaftskriminalität in Deutschland 2012, S. 18 und 28.

Aufdeckung und Meldemöglichkeit von Compliance-Verstößen

Hinweisgebersystem

Empfehlungen für die Umsetzung

Compliance-Kommunikation

Tone from the Top und Vorbildverhalten der Führungskräfte

An der ersten Stelle erfolgreicher Compliance-Kommunikation steht der Tone from the Top, also die Kommunikation durch Vorbildverhalten und Vorleben von Compliance und Integrität durch die Unternehmensleitung und Führungskräfte (vgl. hierzu auch das CMS-Element → 8 FÜHRUNG UND UNTERNEHMENSKULTUR). Gerade für kleinere und mittelständische Unternehmen kann ein Vorteil in der Umsetzung funktionsfähiger Compliance-Kommunikation darin liegen, dass die Unternehmensleitung in der direkten Zusammenarbeit und im Dialog im Geschäftsalltag einen Großteil der Mitarbeiter erreichen und auf direktem Wege kommunizieren kann. Hinzu kommt, dass vor allem inhabergeführte und Familienunternehmen sehr stark durch den (die) Eigentümer(-familie) und dessen (deren) Werte geprägt sind. Der (die) Eigentümer(-familie) kann daher allein durch sein (ihr) eigenes Vorbildverhalten und Commitment die Bedeutung und Relevanz von Compliance und Integrity für eine erfolgreiche Geschäftstätigkeit wirkungsvoll in das Unternehmen tragen und dazu beitragen, das CMS mit Leben zu füllen. In größeren Unternehmen erfolgt die direkte und persönliche Compliance-Kommunikation von der Unternehmensleitung über die Führungskräfte an die einzelnen Mitarbeiter. Dabei ist die Compliance-Kommunikation in bestehende Termine und Veranstaltungen, wie z.B. Betriebsversammlungen, einzubinden. Zudem empfiehlt es sich, dass Compliance einen regelmäßigen Tagesordnungspunkt in Führungskräfte-, Abteilungs- oder Teammeetings bildet und in Zielvereinbarungsgesprächen thematisiert wird (vgl. hierzu auch das CMS-Element → 6 INTEGRATION IN HR-PROZESSE). Entscheidend für eine funktionierende und wirkungsvolle Compliance-Kommunikation ist, dass die Kommunikation klar, eindeutig und konsistent erfolgt und die Unternehmensleitung sowie die Führungskräfte in der täglichen Zusammenarbeit mit ihren Mitarbeitern ihre Haltung zu Compliance und Integrity sowie ihre diesbezüglichen Erwartungen an die Mitarbeiter klar kommunizieren.

Tone from the Top & Tone from the Middle
Die Kommunikation der Unternehmensleitung und der Führungskräfte ist das einflussreichste Medium der Compliance-Kommunikation. Durch ihr Verhalten in der täglichen Zusammenarbeit mit ihren Mitarbeitern und ihre Haltung zu bzw. ihr Commitment für Compliance und Integrity im Geschäft beeinflussen sie maßgeblich das Verhalten aller Mitarbeiter im Unternehmen.

Compliance-Kommunikationsmedien
Bekanntmachung und Verteilung des Verhaltenskodex

Bezüglich der Ausgestaltung von Compliance-Medien sind den Unternehmen grundsätzlich keine Grenzen gesetzt. Es gilt jedoch zu beachten, dass die Kommunikationsmedien der Zielgruppe entsprechend auszuwählen und zu gestalten sind. Der Verhaltenskodex sowie die wesentlichen Bestandteile des CMS sind allen Mitarbeitern beispielsweise in Form einer ansprechend gestalteten und in einer einfachen Sprache gehaltenen Broschüre bekannt zu machen. Um zu vermeiden, dass veraltete Broschüren oder Versionen von Richtlinien im Unternehmen im Umlauf sind, und um die Dokumente für Mitarbeiter dauerhaft und jederzeit in der aktuellen Version zugänglich zu machen, bietet sich die Einrichtung eines Compliance-Bereichs im Intranet oder Internet an, in dem alle relevanten Dokumente zum CMS (Verhaltenskodex, Richtlinien, Schulungsunterlagen etc.) zum Download bereit stehen sowie weitere Informationen zum Thema und die jeweiligen Ansprechpartner zu finden sind. Außerdem können über eine solche Plattform Neuigkeiten im Bereich Compliance und Integrität kommuniziert und Antworten auf häufige Fragen zur Umsetzung von Compliance im Geschäftsalltag veröffentlicht werden. Vor allem für größere Unternehmen mit zunehmendem Komplexitäts- und Formalisierungsgrad, die eine Vielzahl an Mitarbeitern in vermehrt dezentral organisierten Geschäftseinheiten mit der Compliance-Kommunikation erreichen müssen, stellt ein solcher IT-basierter Compliance-Bereich ein geeignetes und unverzichtbares Kommunikationsmedium dar. Bei einer verstärkten Informationsbereitstellung über digitale Medien ist zu bedenken, dass unter Umständen nicht alle Mitarbeiter durch solche Medien erreicht werden (z.B. Mitarbeiter in der Produktion, die über keinen Arbeitsplatz mit Internet-/Intranetzugang verfügen). Um diese Mitarbeiter ebenso zu erreichen, kann der Verhaltenskodex beispielsweise in Plakatform oder als Druckfassung an einer geeigneten zentralen Stelle ausgehängt bzw. ausgelegt werden. Neben klassischen Kommunikationsmedien wie Plakaten und Mailings an die Mitarbeiter können in der Compliance-Kommunikation auch (eher) unkonventionelle Maßnahmen dazu beitragen, die Mitarbeiter für das Thema Compliance zu sensibilisieren, zu interessieren und zu informieren. Die Bandbreite reicht hier von Comics, über Quizzes, einen ›Compliance-Tipp der Woche‹, Compliance-Wikis als Nachschlagewerk sowie zum Austausch und zur Diskussion von Compliance-Themen, Compliance-Apps bis hin zu ›Compliance-Key-Cards‹ mit den 10 wichtigsten Do's und Don'ts.

Internet- oder Intranet-Portal zu Compliance-Themen

Unternehmensinterne Verbreitung des Verhaltenskodex

Unternehmen, in denen die Unternehmensleitung den größten Teil der Mitarbeiter in der täglichen Zusammenarbeit nicht mehr persönlich erreicht, müssen regelmäßig und strukturiert zu Compliance kommunizieren (Compliance-Newsletter, Beiträge zu Compliance in der Betriebszeitung etc.). Je nach internationaler Ausrichtung des Unternehmens kann es aus Gründen der Reichweite und der Sensibilisierungswirkung sinnvoll sein, die einzelnen Kommunikationsmaßnahmen in verschiedenen Sprachen zur Verfügung zu stellen sowie ggf. bei der Auswahl geeigneter Kommunikationsmaßnahmen und -medien kulturelle Aspekte zu berücksichtigen.

Compliance-Kommunikation bei Neueinführung eines CMS

Mit Blick auf den Inhalt der Compliance-Kommunikation ist vor allem bei der Neueinführung eines CMS von Bedeutung, den Mehrwert und das Ziel der Compliance-Bemühungen für das Unternehmen und für den einzelnen Mitarbeiter zu vermitteln. Hierbei sollte den Mitarbeitern aufgezeigt werden, dass Compliance nichts neues, keine

Modeerscheinung, ist, sondern dass integres Verhalten selbstverständlich ist und erwartet wird, dass sich die Beschäftigten an geltendes Recht sowie interne Regelungen halten. Die Überzeugungsarbeit von Topmanagement, Führungskräften und Compliance-Abteilung besteht darin, den Mitarbeitern glaubwürdig zu vermitteln, dass das CMS mit seinen Verhaltensrichtlinien nicht nur Einschränkungen für die tägliche Arbeit der Mitarbeiter mit sich bringt, sondern ihnen einen Handlungsrahmen gibt, in dem sie ihre Aufgaben integer und in Einklang mit Recht und Gesetz erfüllen können, also Handlung wiederum auch ermöglicht. Basis für die Compliance-Kommunikation bildet der Verhaltenskodex des Unternehmens, der in Schriftform an die Mitarbeiter z.B. im Wege der Gehaltsabrechnung oder durch den Versand per Email an die Mitarbeiter zu verteilen ist (vgl. hierzu auch das CMS-Element → 3 VERHALTENSGRUNDSÄTZE UND -RICHTLINIEN). Ergänzend zur Schriftform empfiehlt es sich, die Verteilung des Kodex mit einer Schulung der Mitarbeiter zu den im Kodex angesprochenen Themen zu unterstützen. Im Rahmen einer solchen Schulung kann den Mitarbeitern vermittelt werden, welche Bedeutung Compliance und Integrity für die Geschäftstätigkeit des Unternehmens insgesamt haben und welche Relevanz die Implementierung des CMS und des Verhaltenskodex für die eigene Arbeit haben. Neben der Vermittlung von Wissen bieten Schulungen die Möglichkeit, z.B. in Case Studies oder anhand von Fallbeispielen kritische Situationen und Lösungswege aufzuzeigen sowie auf Fragen und Unklarheiten seitens der Mitarbeiter direkt eingehen zu können.

Compliance-Kommunikation erfolgt aber nicht nur ›top-down‹ durch die Unternehmensleitung sowie durch die Compliance-Funktion. Auch die Führungskräfte und direkten Vorgesetzten sind in der Verantwortung, ihren Mitarbeitern (in der täglichen Arbeit oder z.B. im Rahmen bestehender Teammeetings oder anderer Termine) den Stellenwert von Compliance und Integrity für die Geschäftstätigkeit zu kommunizieren, für Rückfragen ansprechbar zu sein und – auch indem sie eine Vorbildposition einnehmen – auf die Umsetzung von Compliance und Integrity im eigenen Verantwortungsbereich mit Engagement hinzuwirken. Zur Unterstützung der direkten Kommunikation zwischen den Vorgesetzten und ihren Mitarbeitern sowie zur Qualitätssicherung der (informalen) Schulungen in den jeweiligen Fachabteilungen und Teams sollten von der Compliance-Funktion entsprechende Materialien zur Schulung und Kommunikation zur Verfügung gestellt werden, an denen sich die Vorgesetzten orientieren können.

Compliance-Kommunikation durch Führungskräfte und Vorgesetzte

Bereitstellung von Schulungs- und Informationsmaterial zu Compliance und Integrity

Neben der Vermittlung von Wissen zu Compliance/Integrity und Fähigkeiten zum Umgang mit kritischen Situationen, die zumeist top-down erfolgt, ist es genauso wichtig, den Mitarbeitern eine Möglichkeit zu bieten, Fragen und Unsicherheiten, die sich im täglichen Geschäft aus Compliance-Sicht ergeben können, aber auch Feedback an die Verantwortlichen (Unternehmensleitung oder Compliance-Funktion) richten zu können. In kleineren Unternehmen wird diese Zuständigkeit bei der Unternehmensleitung direkt liegen. Dabei ist sicherzustellen, dass die Unternehmensleitung für die Anliegen der Mitarbeiter erreichbar ist und den Mitarbeitern kommuniziert wird, dass sie sich mit ihren Anliegen an die Unternehmensleitung wenden können. In größeren Unternehmen, in denen die Unternehmensleitung aufgrund der gestiegenen Komplexität in der Organisationsstruktur und der Geschäftsführung diese Aufgabe nicht mehr zusätzlich leisten kann, ist diese Aufgabe zu delegieren. Dies kann z.B. durch Benennung eines Ansprechpartners für Compliance oder die Einrichtung eines Compliance-Helpdesks o.ä. erfolgen, an den sich Mitarbeiter vertrauensvoll mit Fragen und Anliegen wenden können.

Ansprechpartner für Compliance-Anliegen

Um bei den Mitarbeitern ein besseres Verständnis und eine höhere Akzeptanz für das CMS und notwendige Maßnahmen zu schaffen, können persönliche Betroffenheit und Emotionen eine wichtige Rolle spielen. Hier gilt es, den Mitarbeitern aufzuzeigen, dass Compliance dazu beiträgt, (bessere) Geschäfte zu machen und das Unternehmen und seine Marke, vor Schäden (Reputationsschäden, finanzielle Schäden etc.) zu schützen. Vor allem bei kleinen Unternehmen kann es wirkungsvoll sein, den Schutz der Marke/des Unternehmens ins Zentrum der Compliance-Kommunikation zu stellen, da in diesen Unternehmen häufig ein sehr enger Bezug zum Unternehmen besteht. In eigentümergeführten Unternehmen kann es insbesondere sinnvoll sein, die Compliance-Kommunikation eng an den Unternehmerwerten auszurichten, da sich die Mitarbeiter dieser Unternehmen oftmals stark mit diesen Werten identifizieren.

Förderung von Verständnis und Akzeptanz für das CMS durch Betroffenheit und Emotion

In Unternehmen mit bereits existierendem CMS kommt es bei der Compliance-Kommunikation darauf an, sowohl die Inhalte als auch die Kommunikation selbst attraktiv zu halten. D.h. die Themen sollten variiert werden, es können gezielt Schwerpunkte gesetzt oder aktuelle Entwicklungen oder Vorfälle aufgegriffen werden sowie verschiedene Kommunikationsmedien genutzt werden. Die Kommunikation von Verstößen und Fehlverhalten, daraus folgenden Konsequenzen und Verbesserungsmaßnahmen kann zu einer offenen Kommunikationskultur beitragen und ähnliche Vorfälle in der Zukunft vermeiden. Als ›real cases‹ können solche Vorfälle genutzt werden, um Lösungsstrategien in schwierigen Situationen aufzuzeigen. Jedoch ist bei der Kommunikation von Compliance-Vorfällen auf einen sensiblen Umgang mit der Situation und Informationen zu den beteiligten Personen zu achten, um Reputationsschäden zu vermeiden und die Beteiligten zu schützen.

Attraktivität der Compliance-Kommunikation

Real cases und Fallstudien

Für die Gewinnung neuer Geschäftspartner, aber auch zur Stabilisierung bestehender Geschäftsbeziehungen sowie zur Festigung der Unternehmensreputation muss Compliance, z.B. durch den Versand oder Übergabe des Verhaltenskodex, ebenso an externe Stakeholder (Kunden, Lieferanten, Kapitalgeber, Öffentlichkeit etc.) kommuniziert werden. Auch für kleinere Unternehmen kann es sinnvoll sein, die Bemühungen

Compliance-Kommunikation an Stakeholder

im Bereich Compliance gezielt nach außen darzustellen. Eine Darstellung des CMS und der Compliance-Funktion sowie die Veröffentlichung des Verhaltenskodex auf der Unternehmenswebsite bieten eine wenig aufwändige, aber wirkungsvolle Kommunikationsmöglichkeit. Von größeren Unternehmen wird die externe Kommunikation von Compliance vermehrt erwartet und ist aktiv zu betreiben (z.B. Internetauftritt der Compliance-Funktion, Stellungnahme im Geschäftsbericht, Austausch und aktive Teilnahme in Verbänden und Arbeitskreisen, Publikationen und Vorträge der Unternehmensleitung und der Compliance-Verantwortlichen zum Thema).

Veröffentlichung des Verhaltenskodex im Internet

Internetauftritt der Compliance-Funktion

Abschließend bleibt zur Compliance-Kommunikation anzumerken, dass die Kommunikation von Compliance nie vollendet ist, sondern regelmäßig und kontinuierlich erfolgen muss, um nachhaltig wirksam sein zu können. Ein ›Compliance-Overkill‹ ist jedoch zu vermeiden.

Regelmäßige und kontinuierliche Kommunikation

Schulung

Compliance-Schulungen sind darauf ausgerichtet, die Mitarbeiter eines Unternehmens für Compliance und Integrity zu sensibilisieren und zu integrem und selbstverantwortlichem Handeln im Geschäftsalltag zu befähigen. Aufgrund der unterschiedlichen mit den einzelnen Positionen, Geschäftseinheiten und Abteilungen im Unternehmen verbundenen Compliance-Risiken empfiehlt sich für die Umsetzung der Compliance-Schulungen ein abgestuftes, risikogruppenorientiertes Schulungskonzept. Dabei ist darauf zu achten, dass Führungskräfte sowie Mitarbeiter in sensiblen Funktionen zusätzlich zu einer grundlegenden Sensibilisierung zu Compliance und Integrity sowie den Inhalten des Verhaltenskodex – die für alle Mitarbeiter zu empfehlen ist – regelmäßige funktions- und aufgabenspezifische Schulungen zu relevanten Compliance-Themen erhalten. Daneben ist es wichtig, dass die regelmäßigen Präsenzschulungen, die in der Regel durch die Compliance-Funktion oder externe Referenten durchgeführt werden, durch eine regelmäßige informale Sensibilisierung durch die Führungskräfte oder den Compliance-Beauftragten zu Compliance und Integrity anhand von Alltagsbeispielen (z.B. im Rahmen von Jours Fixes, Teammeetings) begleitet werden.

Abgestuftes, zielgruppenorientiertes Compliance-Schulungskonzept

Grundlegende Schulung zu Compliance und Integrity

Informale Compliance-Schulung durch Führungskräfte

Grundsätzlich ist zu gewährleisten, dass die Mitarbeiter bei Neueinführung eines CMS im Rahmen einer Schulung eine grundlegende Sensibilisierung zu Compliance und Integrity erhalten und im Zeitverlauf regelmäßig zu relevanten Themen Auffrischungsschulungen stattfinden. Neue Mitarbeiter sollten zeitnah in das laufende Schulungsprogramm integriert werden und können z.B. im Rahmen einer grundlegenden Schulung oder einem Einführungsgespräch mit der Compliance-Funktion bzw. dem Vorgesetzten zu Compliance und Integrity sensibilisiert werden. In der grundlegenden Compliance-Sensibilisierung/-Schulung sollten die für die Mitarbeiter relevanten geltenden Gesetze und Regelungen sowie die Inhalte des Verhaltenskodex dargestellt und aufgezeigt werden, welche Implikationen daraus für die eigene Arbeit folgen. Entlang konkreter Fallbeispiele können Handlungsoptionen und Lösungsstrategien in Dilemmasituationen aufgezeigt werden. Nach dieser ersten Schulung sollten die Mitarbeiter verstehen, warum die Einhaltung von Gesetzen, internen Regelungen und Unternehmenswerten so wesentlich für die Geschäfte des Unternehmens ist, dass die Unternehmensleitung die Beachtung des CMS erwartet und dass (vorsätzliches) Fehlverhalten nicht toleriert und konsequent sanktioniert wird. Bei der Darstellung möglicher negativer Konsequenzen für den Mitarbeiter und das Unternehmen ist darauf zu achten, dass sich die Art und Weise, wie hier kommuniziert wird, auf das Bild und die Wahrnehmung von Compliance beim Mitarbeiter und im Unternehmen insgesamt auswirken kann. Liegt der Fokus der Kommunikation in der Abschreckung wird Compliance eher als einschränkend, als Aufpasser oder *Polizei* im Unternehmen wahrgenommen werden. Schulungen, v.a. in Verbindung mit Fallstudien und dem direkten Dialog mit den Mitarbeitern, bieten hier eine geeignete Möglichkeit, Compliance als beratende, unterstützende, eben auch geschäftsermöglichende Funktion darzustellen und so ggf. vorhandene Skepsis gegenüber dem CMS auszuräumen.

Direkter Dialog mit Mitarbeitern

Die Implementierung eines abgestuften, risikogruppenorientierten Schulungskonzeptes empfiehlt sich – auch aus ökonomischen Gründen – für alle Unternehmen unabhängig ihrer Organisationskomplexität. Ein möglicher Vorteil kleinerer Unternehmen bei der Planung und Durchführung von Compliance-Schulungen liegt in der geringen Organisationsgröße. Es besteht häufig ein enger und direkter Kontakt zwischen Unternehmensleitung und Mitarbeitern, d.h. Schulungen können in kleineren Gruppen oder – weniger formalisiert – auch im direkten Dialog zwischen Unternehmensleitung und Mitarbeitern durchgeführt werden (informale Schulung). Die persönliche Nähe stellt den Zugang und die Erreichbarkeit der Unternehmensleitung für die Mitarbeiter sicher und schafft Vertrauen. Damit in größeren Unternehmen sichergestellt werden kann, dass alle Mitarbeiter adäquat zu Compliance und Integrity geschult werden, ist ein unternehmensweites Compliance-Schulungsprogramm zu entwickeln. Basis des Schulungsprogramms bildet, wie oben bereits ausgeführt, eine grundlegende Schulung aller relevanten Mitarbeiter zu Compliance und Integrity sowie insbesondere zu den Inhalten des Verhaltenskodex.[38] Je nach Unternehmensgröße und -struktur kann diese web-basiert oder unterstützt durch neue Informationstechnologien (z.B. Apps, Podcasts) erfolgen. Der Vorteil von Online-Schulungen liegt in der großen Reichweite und dem geringen logistischen Aufwand, mit dem innerhalb kurzer Zeit ein Großteil der Mitarbeiter zu erreichen ist, sowie in der zeitlichen Flexibilität, die solche Schulungsformate den Mitarbeitern bezüglich der Durchführung der Schulung bieten. Web-basierte Schulungen sind zudem für die bedarfsorientierte Schulung z.B. bei neuen Mitarbeitern

[38]

Neue Informationstechnologien für Compliance-Schulung und Kommunikation

Web-basierte Compliance-Schulungen

gut geeignet. Damit die gewünschte Sensibilisierung und Vermittlung von Kenntnissen und Verhaltenserwartungen auch im Rahmen solcher Online-Schulungen erreicht wird, ist eine attraktive und zielgruppenorientierte Gestaltung der Inhalte, ggf. unterstützt durch Kontroll- und Verständnisfragen, die zur Reflexion des vermittelten Wissens anregen, wichtig. Im Gegensatz zu Präsenzschulungen, die seitens der Mitarbeiter in der Regel mit einer höheren Verbindlichkeit zur Teilnahme verbunden sind (weil die Teilnahme über Anwesenheitslisten einfach nachzuprüfen ist und die Notwendigkeit, die Nichtteilnahme im Vorfeld gegenüber dem Vorgesetzten oder der Compliance-Funktion aktiv zu kommunizieren, Mitarbeiter davon abhalten kann, die Schulung zu versäumen), ist die Teilnahme einzelner Mitarbeiter an einer Online-Schulung schwerer nachvollziehbar und somit ist es für Mitarbeiter einfacher, die Teilnahmeaufforderung zu ignorieren. Hier liegt es an der Compliance-Funktion sowie an den jeweiligen Vorgesetzten, die Mitarbeiter von der Relevanz der Schulung für ihre Arbeit und für die Teilnahme an der Online-Schulung zu überzeugen. Aufbauend auf der ersten grundlegenden Compliance-Schulung sollte das Schulungskonzept regelmäßig auffrischende Schulungen zu relevanten und aktuellen Themen im Bereich Compliance/Integrity beinhalten, um die Themen präsent zu halten und die Bedeutung von integrem Handeln langfristig im Denken und Handeln der Mitarbeiter zu verankern.

Regelmäßige Präsenzschulungen zu relevanten Themen

Abhängig von der Unternehmensgröße und den spezifischen Compliance- und Integrity-Risiken aufgrund von Auslandstätigkeit, Branche etc. sind für bestimmte Mitarbeitergruppen zusätzlich spezifischere Schulungen notwendig. Führungskräfte, Compliance-Beauftragte sowie Mitarbeiter in sensiblen Funktionen und Positionen mit erhöhtem Compliance-Risiko (z.B. Vertrieb, Einkauf) sind entsprechend ihrer Tätigkeit und dem Umfeld, in dem sie handeln, aufgaben- und funktionsspezifisch sowie intensiver im Rahmen von Präsenzveranstaltungen zu schulen. Auch hier sind reale und spezifische Geschäftssituationen in die Schulungen zu integrieren, entlang derer potenziell auftretende Dilemmasituationen aufgezeigt und Lösungsstrategien entwickelt werden. Damit die Führungskräfte ihrer Verantwortung für die Kommunikation und Umsetzung von Compliance und Integrity im eigenen Verantwortungsbereich nachkommen können, müssen sie im Rahmen der Personalentwicklung (PE) in entsprechenden Seminaren und Trainings mit den entsprechenden Kenntnissen, Fähigkeiten und

Zielgruppenorientierte Compliance-Schulungen für Mitarbeiter und Führungskräfte in sensiblen Funktionen

Compliance und Integrity als Bestandteile von PE-Seminaren

[38] Der Begriff ›relevante Mitarbeiter‹ wird in diesem Zusammenhang verwendet, um herauszuheben, dass jedes Unternehmen jeweils selbstständig zu beurteilen hat, ob alle Mitarbeiter im Rahmen einer Präsenz- oder web-basierten Schulung zu Compliance und Integrity zu sensibilisieren sind oder ob es eventuell Mitarbeitergruppen gibt (z.B. in der Produktion), die besser und ausreichend durch andere geeignete Kommunikationsmedien, wie z.B. Aushang des Verhaltenskodex, und durch den direkten Dialog mit dem eigenen Vorgesetzten für Compliance und Integrity sensibilisiert werden können. Diese Beurteilung hängt maßgeblich von den identifizierten Compliance-Risiken ab. Wird beispielsweise Diebstahl in der Produktion als eines der größten Compliance-Risiken identifiziert, gehören die Mitarbeiter in der Produktion durchaus zu den ›relevanten‹ Mitarbeitern und sind entsprechend zu schulen und zu sensibilisieren.

Fertigkeiten ausgestattet werden. In ein umfassendes Schulungsprogramm sind darüber hinaus ebenso die Leitungsgremien des Unternehmens (Vorstand/Geschäftsführung sowie Aufsichtsrat/Beirat) zu integrieren. Dabei geht es nicht darum, die Unternehmensleitung und Mitglieder des Aufsichtsgremiums in festen Abständen und in einem festen Schulungsformat pflichtbewusst zu schulen, ›nur damit geschult wurde‹. Vielmehr geht es darum, dass auch die Mitglieder der Unternehmensleitung und des Aufsichtsgremiums regelmäßig und bei bestimmten Anlässen (z.B. aufgrund relevanter Veränderungen in der Gesetzgebung, Unternehmenszukauf, Eintritt in neue Märkte) zu relevanten Compliance- und Integrity-Themen geschult werden bzw. zu diesen Themen eine entsprechende Sensibilisierung stattfindet (interner oder externer Workshop/Präsenzschulung etc.). Nur so kann sichergestellt werden, dass *alle* Mitglieder der Leitungsgremien Kenntnis über die wesentlichen Compliance- und Integrity-Risiken des eigenen Geschäfts haben und ihre Vorbildfunktion für die Umsetzung von Compliance und Integrity im Geschäftsalltag erfüllen können. Bei kleineren und mittleren Unternehmen kann eine solche Sensibilisierung der Leitungsgremien auch auf eher informalem Wege, z.B. durch Selbststudium relevanter Literatur oder moderierte Workshops der Unternehmensleitung zu relevanten Themen, erfolgen.

Schulung von Unternehmensleitung und Aufsichtsrat/Beirat

Zielsetzung eines risikogruppenorientierten Compliance-Schulungsprogramms ist es, die Mitarbeiter, Führungskräfte und Leitungsgremien entsprechend ihrer Funktion und Position im Unternehmen mit den relevanten Kenntnissen und Fähigkeiten zu Compliance und Integrity auszustatten. Um sicherzustellen, dass die Mitarbeiter die entsprechenden Schulungen erhalten haben, ist es erforderlich, die Teilnahme an den Schulungen jeweils zu dokumentieren. In Unternehmen mit eigener Compliance-Abteilung werden die Schulungen von dieser initiiert und entweder selbst oder unterstützt durch externe Referenten durchgeführt. Mit zunehmender Unternehmensgröße wird die Compliance-Abteilung allerdings auf unterstützende Maßnahmen wie z.B. auf den sog. Coaching-Ansatz bzw. das Train-the-Trainer-Konzept angewiesen sein, um die Kommunikation- und Schulungsanforderungen im Unternehmen zu erfüllen. Hier werden ausgewählte Personen, z.B. die Unternehmensleitung, der Compliance-Beauftragte oder Führungskräfte, speziell geschult und dazu befähigt, dass sie selbstständig im Unternehmen grundlegende Schulungen zu Compliance und Integrity durchführen und ihr Wissen so ins Unternehmen weitertragen können. Aber auch für kleinere

Dokumentation der Schulungsteilnahmen

Coaching-Konzept

›Train-the-Trainer‹ Konzept

Praxisnähe und Relevanz der Schulungsthemen
Damit die Mitarbeiter die ihnen vermittelten Inhalte begreifen und verstehen, welche Auswirkungen und Erwartungen durch das CMS für ihre Tätigkeit entstehen, ist es wichtig, die Schulungen praxisnah und relevant für die jeweilige Zielgruppe zu gestalten. So sollten Fallstudien oder Compliance-kritische Beispielsituationen dem tatsächlichen Geschäft entnommen bzw. aus diesem heraus entwickelt werden, damit den Mitarbeitern bewusst wird, dass sie selbst auch einmal in solch eine Situation geraten können. Die Einbindung praktischer und relevanter (realer) Fälle in die Schulungen erhöht die Betroffenheit seitens der Mitarbeiter und regt zu Diskussionen und Nachfragen an.[39] Mitarbeiter bekommen ein besseres Verständnis und Bewusstsein für schwierige und compliance-kritische Situationen und erlernen mögliche Lösungs- und Auswege.

[39]

und mittlere Unternehmen mit schlanker Compliance-Organisation kann das Train-the-Trainer-Konzept ein gangbarer (im Sinne von ressourcenschonend) Weg sein.

Einholung von Feedback

Um die Wahrnehmung und Wirksamkeit der Schulungen seitens der Mitarbeiter beurteilen und ggf. nachbessern zu können, wird empfohlen, in regelmäßigen Abständen Feedback der Mitarbeiter sowohl zu den Kommunikations- als auch Schulungsmaßnahmen einzuholen. Dies kann beispielsweise direkt nach einer Schulung mittels Feedbackbögen oder im Rahmen einer Mitarbeiterbefragung erfolgen. Aber auch die Registrierung von Klicks auf der Compliance-Intranetseite oder der direkte Dialog zwischen Unternehmensleitung/Compliance-Funktion und Mitarbeitern im Tagesgeschäft gibt Aufschluss über die Wahrnehmung der Schulungen bei den Mitarbeitern und die Aufmerksamkeit für Compliance und Integrity im Unternehmen insgesamt (vgl. hierzu auch CMS-Element → 8 FÜHRUNG UND UNTERNEHMENSKULTUR).

Hinweisgebersystem

Aufdeckung und Meldemöglichkeit von Fehlverhalten

Eine funktionsfähige Meldemöglichkeit für Fehlverhalten, in diesem Zusammenhang häufig als ein Hinweisgebersystem bezeichnet, ist Voraussetzung für die Erfüllung der Aufdeckungsfunktion des CMS und stellt für die Unternehmensleitung eine unentbehrliche und ungefilterte Hinweisquelle für Fehlverhalten im Unternehmen dar. Unternehmen müssen einen geeigneten Kanal zur Verfügung stellen sowie einen Prozess zur Meldemöglichkeit definieren, wie Mitarbeiter auf Missstände und Fehlverhalten im Unternehmen hinweisen und um Rat zu solchen Situationen suchen können. Dieser Prozess ist den Mitarbeitern z.B. im Verhaltenskodex zu kommunizieren. Die Einrichtung eines Hinweisgebersystems im Rahmen des CMS zielt keineswegs darauf, die gängigen Meldewege von Beschwerden oder Hinweisen im Unternehmen (z.B. an die Personalabteilung, den Betriebsrat oder den direkten Vorgesetzten) abzuschaffen. Auch die direkte Meldemöglichkeit an die Unternehmensleitung bleibt von einem solchen System unberührt. Vielmehr bietet ein Hinweisgebersystem eine ergänzende Alternative, an die sich Mitarbeiter vertraulich und ggf. anonym wenden können, wenn sie Kenntnis von schwerwiegendem Fehlverhalten im Unternehmen erlangen. Bei der Einrichtung anonymer Hinweisgebersysteme sowie bei der Etablierung eines Hinweisgebersystems in verschiedenen Ländern ist besonders darauf zu achten, dass ggf. von

Prozess zur Meldung von Fehlverhalten

39 Das Schulungsinstrument RESIST, das gemeinsam von der International Chamber of Commerce, von Transparency International, dem United Nations Global Compact und dem World Economic Forum entwickelt wurde, liefert 22 Fallbeispiele und Szenarien sowie passende Reaktionen und mögliche Lösungswege zu Bestechungsanforderungen und Dilemmasituationen aus der realen Unternehmenspraxis (http://www.iccwbo.org/products-and-services/fighting-commercial-crime/resist/ (16.04.2014)).

Unternehmen, die an einer US-amerikanischen Börse notiert sind, sind nach Section 301 des Sarbanes-Oxley-Act verpflichtet, ein Hinweisgebersystem einzurichten, das den Mitarbeitern ermöglicht, fragwürdige Buchführungspraktiken vertraulich und anonym zu melden (vgl. auch Moosmayer, K. (2012): Compliance – Praxisleitfaden für Unternehmen. München: C.H. Beck, S. 56)

40

Etablierung eines Hinweisgebersystems in kleineren Unternehmen
Die Einrichtung eines Hinweisgebersystems ist auch in kleineren Unternehmen mit geringeren Ressourcen ohne hohen Aufwand umsetzbar. Neben dem direkten Meldeweg über den jeweiligen Vorgesetzten kann die Unternehmensleitung eine interne Vertrauensperson (z.B. ein Mitglied der Unternehmensleitung oder der Compliance-Beauftragte) bestellen, die über das notwendige Fachwissen verfügt und an die sich Mitarbeiter mit Hinweisen wenden können. Zusätzlich kann über die Einrichtung eines elektronischen Briefkastens für Hinweise oder die Bestellung einer Ombudsperson nachgedacht werden.

der deutschen Gesetzgebung abweichende spezifische nationale arbeits- und datenschutzrechtliche Bestimmungen zu beachten sind. Aus Gründen der Transparenz und Akzeptanz eines Hinweisgebersystems im Unternehmen empfiehlt es sich, den Betriebsrat frühzeitig in die Entwicklung und Umsetzung des Systems einzubinden und seine Zustimmung einzuholen.[40]

Meldemöglichkeit an Unternehmensleitung

Grundsätzlich ist bei kleineren Unternehmen aufgrund ihrer geringen Organisationsgröße und dem geringeren Formalisierungsgrad davon auszugehen, dass der direkte Kanal, d.h. die Ansprache von Missständen oder Fehlverhalten beim Vorgesetzten oder bei der Unternehmensleitung selbst, der wichtigste Kanal für Hinweise ist. Daher sollte diese Möglichkeit der Hinweisgabe im Sinne einer offenen Kommunikationskultur im Unternehmen gegenüber den Mitarbeitern auch so kommuniziert werden. In manchen Fällen, falls beispielsweise der Vorgesetzte selbst in fragwürdige Vorfälle verwickelt ist und die direkte Ansprache der Situation beim Vorgesetzten keine Alternative ist, kann jedoch die Möglichkeit einer anonymen Hinweisgabe oder die Meldung an eine interne oder externe Vertrauensperson (Ombudsperson) angebracht sein (s.u.). Ein weiteres geeignetes Instrument für eine anonyme Hinweisgabe ist ein elektronischer Briefkasten, der von der Unternehmensleitung/dem Compliance-Beauftragten oder auch von einem externen Anwalt betreut wird.

Anonyme Hinweisgabe

Interne/externe Vertrauensperson

Ombudsperson

Für Unternehmen aller Größenklassen ist die Bestellung einer externen Ombudsperson eine gute Lösung für ein Hinweisgebersystem. Die Ombudsperson, häufig ein unternehmensexterner Rechtsanwalt mit entsprechender Fachkenntnis, nimmt die Hinweise an und steht dem Hinweisgeber beratend zur Seite. Sie leitet, je nach Absprache mit dem beauftragenden Unternehmen, die Hinweise entsprechend an den Compliance-Beauftragten oder die Unternehmensleitung weiter oder leitet falls nötig selbstständig weitere Schritte ein. Gegenüber dem Unternehmen gibt die Ombudsperson nur die Informationen weiter, zu deren Offenlegung sie vom Hinweisgeber autorisiert wurde, und

40 Vgl. hierzu auch das CMS-Element → 3 ›VERHALTENSGRUNDSÄTZE UND -RICHTLINIEN‹ sowie das Urteil des BAG, 22.07.2008 – 1 ABR 40/07.

bleibt im weiteren Verlauf des Vorgangs im Kontakt mit dem Hinweisgeber. Je nach Unternehmensgröße, ist es möglich, dass eine Ombudsperson mehrere Unternehmen betreut. So ist ihre Tätigkeit auch für kleinere und mittlere Unternehmen oder bei begrenzten Ressourcen finanzierbar. Die Bestellung einer Ombudsperson bietet gegenüber internen Meldewegen vor allem den Vorteil (auch für kleinere und mittlere Unternehmen), dass die Ombudsperson eine vom Unternehmen unabhängige Stelle mit der notwendigen Fachkenntnis und grundsätzlich zur Verschwiegenheit gegenüber dem Unternehmen verpflichtet ist, was die Hemmschwelle zur Meldung von Auffälligkeiten durch Mitarbeiter (die z.B. aus Angst vor Repressalien entstehen kann) senken kann. Durch die Einrichtung einer solchen, vom Unternehmen unabhängigen Meldemöglichkeit, bezeugt die Unternehmensleitung die Ernsthaftigkeit und das Interesse an der Aufdeckung und Aufklärung von Auffälligkeiten zur Sicherstellung von Compliance und Integrität im Geschäft und verdeutlicht gleichzeitig, wie wichtig ihr der Schutz der Hinweisgeber vor Repressalien ist (siehe unten). Somit schafft sie einen weiteren Anreiz für die Mitarbeiter, Unregelmäßigkeiten zu melden.

Elektronisches Hinweisgebersystem

Telefonhotline

Für große Unternehmen ist aufgrund ihrer Dezentralität und der hohen Mitarbeiterzahl die Einrichtung einer anonymen Hotline oder eines elektronischen Hinweisgebersystems unverzichtbar, um die Erreichbarkeit für alle Mitarbeiter jederzeit sicherzustellen. Meldungen sollten mindestens in den festgelegten Konzernsprachen möglich sein. Um eine jederzeitige Erreichbarkeit und Möglichkeit der Hinweisgabe in mehreren Sprachen sicherzustellen, kann die Beauftragung eines externen Dienstleisters erforderlich sein.

Prozess zu Meldungen und dem Umgang mit Meldungen von Fehlverhalten

Für den Umgang mit Hinweisen und der Bearbeitung von Meldungen zu schwerwiegendem Fehlverhalten ist vor allem in größeren Unternehmen ein Prozess festzulegen, der regelt, welche Person(en) bzw. Abteilung für die Einleitung und Durchführung weiterer Maßnahmen zuständig und welche Maßnahmen im Einzelnen zu ergreifen sind. Die Festlegung von Verantwortlichkeiten und Zuständigkeiten für die Bearbeitung von Hinweisen empfiehlt sich auch für Unternehmen geringerer Größe. In jedem Fall sind bei der Bearbeitung von Hinweisen die geltenden daten- und arbeitsschutzrechtlichen Regelungen zu beachten.

Schutz des Hinweisgebers

Ein sehr wichtiges Thema für die Funktionsfähigkeit aber auch für die Legalität des Hinweisgebersystems ist der Schutz der Hinweisgeber. Es liegt in der Pflicht der Unternehmensleitung, den Hinweisgeber vor Repressalien, Mobbing oder weiteren negativen Konsequenzen zu schützen, auch um zu verhindern, dass Hinweise aus Angst vor Repressalien nicht gegeben werden. Mobbing oder anderes negatives Verhalten der Mitarbeiter gegenüber dem Meldenden sind von der Unternehmensleitung klar und deutlich zu untersagen und konsequent zu sanktionieren. In diesem Zusammenhang

Anonyme Hinweisgabe

spielt die Frage, ob eine *anonyme* Meldemöglichkeit ein geeignetes sowie zulässiges Mittel darstellt, eine zentrale Rolle. Während Unternehmen, die dem US-amerikanischen Sarbanes-Oxley-Act unterfallen, eine anonyme Hinweisgabe zu ermöglichen haben (vgl. → ABSCHNITT 1.2.2 des ANNEX), verbieten hingegen verschiedene europäische Rechtsordnungen wie z.B. Spanien und Portugal die Einrichtung von anonymen Hinweisgebersystemen.[41] Dennoch ist ein Hinweisgeber durch die Möglichkeit einer anonymen Hinweisgabe am besten vor negativen Konsequenzen zu schützen. Für kleinere Unternehmen dürfte die Problematik bezüglich der Zulässigkeit von anonymen Hinweisgebersystemen nur von untergeordneter Rolle sein, da bereits die Sinnhaftigkeit einer anonymen Meldemöglichkeit in kleinen Unternehmen in Frage zu stellen ist. Aufgrund ihrer geringen Unternehmensgröße ist vor allem in kleineren Unternehmen die Anonymität des Hinweisgebers im Einzelfall häufig nur schwierig zu wahren. Vor allem wenn Untersuchungen eingeleitet werden, kann unter Umständen aufgrund von Spezialwissen in den Hinweisen leicht auf die Identität des Hinweisgebers geschlossen werden. Es dürfte daher zweifelhaft sein, ob ein anonym eingerichtetes Hinweisgebersystem in kleinen Unternehmen überhaupt von den Mitarbeitern in Anspruch genommen wird und somit sein Ziel und Zweck erreichen kann. Gerade deshalb steht die Unternehmensleitung bei kleineren Unternehmen besonders in der Pflicht, bei den Mitarbeitern Vertrauen zu schaffen und klare Regelungen zu treffen, welche die Hinweisgeber im Falle einer Meldung vor jedweden Repressalien durch andere Mitarbeiter schützen. Größere Unternehmen werden allerdings aufgrund ihrer zunehmenden internationalen Geschäftstätigkeit bei der Entwicklung und Umsetzung eines Hinweisgebersystems nicht umhin kommen, die jeweils geltende Rechtslage der verschiedenen nationalen Gesetzgebungen genau zu überprüfen und ihr Hinweisgebersystem den Anforderungen entsprechend ggf. länderspezifisch auszugestalten.

Akzeptanz des Hinweisgebersystems

Für die Akzeptanz des Hinweisgebersystems im Unternehmen ist es wichtig, gegenüber den Mitarbeitern zu kommunizieren, welcher Zweck mit dessen Einrichtung verfolgt wird. Es ist klar herauszustellen, dass es bei der Meldung von Hinweisen nicht darum geht, Kollegen oder Vorgesetzten zu schaden oder sie zu denunzieren. Die Mitarbeiter sind davon zu überzeugen, dass das Hinweisgebersystem für sie eine Möglichkeit bietet, an die sie sich vertraulich wenden können, wenn sie Kenntnis über schwerwiegende Verstöße erlangen und Unsicherheit oder Vorbehalte darüber bestehen, den Verstoß direkt bei ihrem eigenen Vorgesetzten anzusprechen (z.B. weil der Vorgesetzte selbst in die Verstöße verwickelt ist), und dass es die moralische Verantwortung und Integrität jedes Einzelnen erfordert, Fehlverhalten zu melden. Für die Glaubwürdigkeit

[41] Für eine ausführliche Darstellung der (rechtlichen) Rahmenbedingungen von Whistleblowing-Systemen in verschiedenen Ländern vgl. ›Global Guide to Whistleblowing Programs‹ der World Law Group, abrufbar unter http://www.theworldlawgroup.com/?cm=Doc&ce=details&primaryKey=53535 (16.04.2014).

und Akzeptanz des Hinweisgebersystems ist es überdies wichtig, den Mitarbeitern zu kommunizieren, dass ihre Hinweise ernst genommen werden und ihnen nachgegangen wird und dass die Hinweisgeber bei Meldung eines berechtigten Hinweises in gutem Glauben keine disziplinarischen oder sonstigen negativen Konsequenzen für sich selbst fürchten müssen. Zur Vermeidung eines Missbrauchs des Hinweisgebersystems ist jedoch auch klar herauszustellen, dass das System nicht für das Anbringen allgemeiner Beschwerden oder sonstiger Verleumdungen gedacht ist, sondern ausschließlich ein Kanal für die Meldung schwerwiegender Verstöße und Fehlverhalten. Der Missbrauch des Hinweisgebersystems ist durch die entsprechenden Abteilungen konsequent zu sanktionieren.

Amnestieprogramm

Erhält die Unternehmensleitung Kenntnis oder ausreichend Grund für die Vermutung von systemischem, großflächigem Fehlverhalten und Kollusionen innerhalb des Unternehmens, ist über die Einrichtung eines Amnestieprogramms bzw. einer Kronzeugenregelung nachzudenken, um das Netz von Fehlhandlungen und -prozessen vollständig aufzudecken. Im Rahmen eines solchen Amnestieprogramms verzichtet das Unternehmen auf die Geltendmachung von Schadensersatzansprüchen und die Auflösung des Arbeitsverhältnisses gegenüber Mitarbeitern, die bei der Untersuchung uneingeschränkt kooperieren und relevante Hinweise geben. Eine strafrechtliche Verfolgungsmöglichkeit durch Behörden bleibt hiervon jedoch unberührt. Gegenüber den verschiedenen Interessengruppen des Unternehmens vermittelt die Einrichtung eines Amnestieprogramms die konsequente Durchsetzung der Nichttolerierung von Fehlverhalten und kann dadurch zu einer Stärkung der Glaubwürdigkeit des CMS beitragen. Jedoch ist bei der Einrichtung und Durchführung von Amnestieprogrammen mit einer großen Sorgfalt vorzugehen und unter allen Umständen zu vermeiden, dass die gewährte Amnestie nicht zu einem Freibrief für Fehlverhalten oder zu ›Einmal-ist-keinmal‹-Denkweisen unter den Mitarbeitern führt. Aus diesem Grund ist die Amnestie ausschließlich Mitwissern des Systems zu gewähren, um an die Drahtzieher des Systems zu kommen, und niemals diesen Drahtziehern selbst (vgl. hierzu auch → ABSCHNITT I.6 ›COMPLIANCE-REMEDIATION NACH ENTDECKTEM SYSTEMATISCHEM FEHLVERHALTEN‹ IM ANNEX).

Integration in HR-Prozesse

6

Warum ist die Integration von Compliance in Personalprozesse so wichtig?

Welche Personalprozesse haben insbesondere Berührungspunkte mit Compliance? Wie sind diese anzupassen?

Durch welche Personalmaßnahmen kann die Umsetzung von Compliance im Unternehmen unterstützt und gefördert werden?

Warum ist das Ergreifen geeigneter personeller Maßnahmen bei der Entdeckung von Compliance-Verstößen wichtig?

Wie ist bei der Entdeckung von Fehlverhalten im Unternehmen zu reagieren?

Zielsetzung

Mitarbeiter sind die wichtigste Ressource eines Unternehmens. Sie sind es auch, die das Compliance-Management-System mit Leben erfüllen und umsetzen. Die Funktionsfähigkeit und Angemessenheit des CMS hängt daher auch davon ab, ob das CMS in die entsprechenden Personalprozesse integriert und in der Personalarbeit verankert ist. Konsistente und transparente Personalprozesse fördern die Mitarbeitermotivation und stärken die Loyalität der Mitarbeiter zum Unternehmen. Eine wichtige Rolle spielen in diesem Zusammenhang geeignete Anreiz- und Personalentwicklungskonzepte aber auch die konsequente Reaktion auf und Sanktionierung von Fehlverhalten oder Fällen von Non-Compliance (Abschreckungsfunktion). Auf diese Weise wird eine Sensibilisierung der Mitarbeiter für integres und erwünschtes Verhalten erreicht, die die Verbindlichkeit des CMS gegenüber Mitarbeitern wie auch externen Kooperationspartnern erhöht und die Glaubwürdigkeit des CMS insgesamt stärkt.

Mitarbeiter als wichtigste Ressource des Unternehmens

Anreiz- und Personalentwicklungskonzepte

Reaktion und Sanktionierung

»In looking for people to hire, you look for three qualities: integrity, intelligence, and energy. And if they don't have the first, the other two will kill you.«
Warren Buffett, CEO Berkshire Hathaway

Mit Blick auf Compliance-Risiken, die in den meisten Fällen aus individuellem Fehlverhalten hervorgehen, kommt der Auswahl von Mitarbeitern und Führungskräften eine besonders bedeutende Rolle zu. Unternehmen müssen dafür Sorge tragen, dass Personen, die in der Vergangenheit straffällig geworden sind oder deren Integrität in Zweifel gezogen wird, nicht eingestellt oder in verantwortungsvolle Positionen befördert werden. Zur Minimierung solcher Verhaltensrisiken ist es daher erforderlich, das CMS vor allem in die Personalauswahl, aber auch in die Personalentwicklungsprozesse zu integrieren. Dann kann die Ausgestaltung und Umsetzung konsistenter und transparenter Personalprozesse einen wichtigen Beitrag zur Funktionsfähigkeit und Angemessenheit des CMS sowie zur Herausbildung einer werteorientierten Unternehmenskultur leisten.

Sorgfältige Personalauswahl

Empfehlungen für die Umsetzung

Für die Integration von Compliance in Personalprozesse sind drei Bereiche besonders wesentlich: (1) Personalauswahl, (2) Personalentwicklung und Personalprozesse und (3) Reaktion auf Fehlverhalten. Zunächst muss das Unternehmen dafür Sorge tragen, die ›richtigen‹ Mitarbeiter einzustellen und zu befördern.

Personalauswahl

Die Einbindung von Compliance-Maßnahmen in den Personalauswahlprozess muss nicht mit hohem Aufwand verbunden sein, wird aber in der Regel mit zunehmender Unternehmensgröße und abhängig von der zu besetzenden Position (Mitarbeiter in Führungs- oder Schlüsselfunktionen sowie Mitarbeiter in der Compliance-Abteilung oder in Positionen mit erhöhtem Compliance-Risiko) komplexer. D.h. der sogenannte *Backgroundcheck* potenzieller Mitarbeiter (Überprüfung des Bewerbers vor Einstellung anhand unterschiedlicher Quellen) wird in aller Regel umfassender und gründlicher ausfallen müssen.

Grundsätzlich soll eine knappe Hintergrundprüfung potenzieller Mitarbeiter Bestandteil jedes Einstellungsprozesses sein. Erste grundlegende Prüfungsmaßnahmen können z.B. im Wege einer Google-Suche erfolgen.[42] Zusätzlich ist zu empfehlen, die in der Bewerbung eingereichten Zeugniskopien im Rahmen des Bewerbungsprozesses mit den Originaldokumenten abzugleichen, um Fälschungen auszuschließen. Solche Prüfungsmaßnahmen sind nur mit einem geringen Mehraufwand verbunden, jedoch durchaus effektiv, auch im Hinblick auf eine abschreckende Wirkung gegenüber unerwünschten Bewerbern. So wird beispielsweise eine Person, die Bewerbungsunterlagen und Zeugnisse gefälscht hat, mit allen Mitteln versuchen, Originalzeugnisse oder Referenzen nicht vorlegen zu müssen. Ein solches Verhalten sollte als ›Red Flag‹ bewertet werden und mindestens zu weiteren, intensiveren Prüfungen und ggf. ganz zum Abbruch der Bewerbungsgespräche führen. Bei Unsicherheit hinsichtlich des Bewerbers sowie bei Positionen mit erhöhtem Compliance-Risiko[43] sowie Positionen in Schlüsselfunktionen (Unternehmensleitung, Geschäftsführer der Tochtergesellschaften, Leiter der Fachabteilungen) sollten zusätzlich umfassendere Backgroundchecks erfolgen. Bei der Auswahl der anzuwendenden Prüfungsmaßnahmen ist insbesondere in international tätigen Unternehmen die Einhaltung der gesetzlichen Bestimmungen, v.a. im Bereich Datenschutz, zu beachten. Grundsätzlich sollte ein umfassender Backgroundcheck in Ländern, in denen es möglich ist, bei der Anforderung eines polizeilichen Führungs-

Grundlegende Prüfmaßnahmen bei Neueinstellungen

Backgroundchecks

42 Der Arbeitgeber darf sich grundsätzlich über einen Bewerber aus allen allgemein zugänglichen Quellen wie z.B. Zeitung oder Internet informieren. Nach dem derzeitigen Entwurf der Bundesregierung zur Neuregelung des Beschäftigtendatenschutzes (vgl. http://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/Entwuerfe/Entwurf_Beschaeftigtendatenschutz.html?nn=3314802) (29.04.2014) sollen die Informationsmöglichkeiten des Arbeitgebers jedoch eingeschränkt werden. Der Gesetzesentwurf sieht in §32 Abs. 6 vor, dass sich der Arbeitgeber durch soziale Netzwerke, die der elektronischen Kommunikation dienen wie z.B. facebook, schülerVZ, studiVZ, StayFriends, nicht über den Bewerber informieren darf. Soziale Netzwerke, die der Darstellung der beruflichen Qualifikation der Mitglieder dienen (z.B. Xing, LinkedIn), darf der Arbeitgeber bei seiner Recherche hingegen nutzen.

43 Welche Positionen mit einem erhöhten Compliance-Risiko behaftet sind bzw. welche Positionen zu den Schlüsselfunktionen zählen, ist von jedem Unternehmen selbstständig und spezifisch anhand des Compliance-Risikoprofils zu beurteilen und festzulegen. Vgl. → FUSSNOTE 38.

zeugnisses beginnen. In Ländern mit weicheren Datenschutzregelungen (z.B. USA) besteht alternativ die Möglichkeit, Einsicht in Kriminalstatistiken zu nehmen und Namenssuchen durchzuführen (i.d.R. wird eine solche Prüfmaßnahme durch spezialisierte Anbieter durchgeführt werden). Anschließend sollten die wichtigsten Lebenslaufdaten (Hochschulabschluss, Examen etc.) im Rahmen eines Backgroundchecks mithilfe entsprechender Rückfragen bei Behörden o.ä. verifiziert werden. Darüber hinaus empfiehlt es sich, bei aussichtsreichen Bewerbern um einen Referenzkontakt (z.B. frühere Arbeitgeber) zu bitten und bei diesem entsprechende Referenzen einzuholen.

Potenzialanalyse bei Führungs- und Schlüsselpositionen

In umfangreicheren Einstellungsverfahren vor allem bei der Besetzung von Führungs- und Schlüsselpositionen in größeren Unternehmen empfiehlt es sich, für diese Kandidaten z.B. anhand konkreter Fallstudien, Rollenspielen oder Gruppendiskussionen gezielt eine Potenzialanalyse, auch bezüglich der persönlichen Integrität, vorzunehmen, die Aufschluss über die Motivation, Kompetenzen und Entwicklungspotenziale der Kandidaten gibt. Im Rahmen solcher Potenzialanalysen ist es darüber hinaus möglich, anhand spezifischer Situationsfragen, eine erste Einschätzung des Verhaltens der Person in schwierigen Compliance-Situationen vorzunehmen. Für die Durchführung der verschiedenen Prüfungsmaßnahmen ist i.d.R. eine Einwilligung der Person erforderlich. Kritische Erkenntnisse des Backgroundchecks können, müssen aber nicht zwingend, zum Abbruch der Gespräche führen, jedoch zur Durchführung weiterer Nachforschungen (ggf. unterstützt durch externe Dienstleister wie Auskunfteien oder Detekteien). In der Regel werden sich diese umfassenderen Prüfungsmaßnahmen auf externe Kandidaten, die sich auf Schlüssel- oder Führungspositionen bewerben, beschränken. Bei internen Mitarbeitern, die bereits langjährig im Unternehmen tätig sind und ein Führungskräfteprogramm durchlaufen haben und die sich auf eine Schlüssel- bzw. Führungsfunktion bewerben, ist im Einzelfall zu prüfen, in welchem Umfang Prüfungsmaßnahmen wie umfassendere Backgroundchecks erforderlich bzw. zu wiederholen sind.

Personalprozesse und Personalentwicklung

Verhaltenskodex als Bestandteil des Arbeitsverhältnisses

Grundlegendes personalpolitisches Instrument zur Unterstützung der Compliance-Bestrebungen im Unternehmen und für die Funktionsfähigkeit des CMS insgesamt bildet die Verankerung des Verhaltenskodex im Arbeitsverhältnis. Bei Neueinführung eines CMS ist es möglich, den Verhaltenskodex durch eine Änderung des Arbeitsvertrages zu dessen Bestandteil zu machen. Vor allem für größere Unternehmen mit großer Belegschaft ist dieses Vorgehen in der Umsetzung jedoch sehr aufwändig, da jedes bestehende Arbeitsverhältnis einzeln durch eine Änderung des Arbeitsvertrages angepasst werden müsste. Aus diesem Grund hat es sich in der Praxis eher bewährt, den Verhaltenskodex im Wege einer separaten Klausel als Anhang des Arbeitsvertrags zum Bestandteil des Arbeitsverhältnisses zu machen. Für neue Mitarbeiter ist es aber durchaus empfehlenswert, die Beachtung des Verhaltenskodex als Vertragsklausel direkt in den Arbeitsvertrag mit aufzunehmen.

Erklärung zur Einhaltung des Verhaltenskodex durch obere Führungskräfte

Um auf die Umsetzung des CMS in den jeweiligen Geschäftsbereichen und Landesgesellschaften hinzuwirken, kann es zusätzlich zur Verankerung des Verhaltenskodex im Arbeitsvertrag sinnvoll sein, von den oberen Führungskräften jeweils für das abgelaufene Geschäftsjahr eine Erklärung einzuholen, in der sie die Einhaltung des Verhaltenskodex in ihrer Geschäftseinheit, Landesgesellschaft etc. bestätigen. Vor allem für Unternehmen mit erhöhter Compliance- und Organisationskomplexität ist dies ein wirkungsvolles Instrument zur Umsetzung von Compliance und Integrity. Durch das aktive Einfordern einer solchen Erklärung werden die Führungsaufgabe und Verantwortung der oberen Führungskräfte, auf die Umsetzung von Compliance und Integrity im eigenen Verantwortungsbereich hinzuwirken, nochmals herausgestellt und ihrer Verbindlichkeit Nachdruck verliehen.

Compliance und Integrity in Mitarbeiterbeurteilungen

Für die Ernsthaftigkeit und dauerhafte Umsetzung des CMS im täglichen Geschäft ist es erforderlich, Compliance und Integrity als systematisches Beurteilungskriterium in Personalgesprächen zu integrieren. Dabei geht es nicht darum, integres Verhalten besonders zu honorieren – integres Verhalten bildet die Grundlage des Arbeitsverhältnisses –, vielmehr geht es darum, in den Personalgesprächen das Verhalten der Mitarbeiter zu reflektieren, Potenziale aufzuzeigen, Fehlverhalten anzusprechen und Handlungsmöglichkeiten in kritischen Situationen zu thematisieren, um Fehlverhalten in der Zukunft zu vermeiden. Dazu gehört im Einzelfall dann auch, Fehlverhalten in der Mitarbeiterbeurteilung entsprechend zu berücksichtigen. Bei der Beurteilung von Führungskräften kommt der Integration von Compliance und Integrity eine noch bedeutendere Rolle zu, weil sie im Unternehmen die Personen sind, deren Verhalten Vorbild für die Mitarbeiter sein soll bzw. ist. Zur Verstärkung der Bedeutung des Führungsverhaltens und Engagements der Führungskräfte für die Umsetzung von Compliance und Integrity sollten vor allem größere Unternehmen für die oberen Führungskräfte spezifische Ziele für die Umsetzung des CMS in die Zielvereinbarungen integrieren.

Compliance und Führungsverhalten in der Führungskräftebeurteilung

Zielvereinbarungen für obere Führungskräfte

Integritätsfördernde Anreiz- und Vergütungssysteme

Mit Blick auf integritätsfördernde Anreiz- und Vergütungssysteme sind zwei Aspekte zu beachten. Zunächst bildet eine angemessene Bezahlung im Austausch zur erwarteten Arbeitsleistung Grundlage für jedes Arbeitsverhältnis. Die Angemessenheit der Bezahlung ist Ausdruck der Wertschätzung der Arbeit und trägt wesentlich zur Vermeidung von Fehlverhalten bei, indem sie bestimmten Rationalisierungs- und Rechtfertigungsstrategien wirtschaftskrimineller Handlungen die Grundlage entzieht (wie beispielsweise Diebstahl, Betrug oder das Zugestehen gewisser Extras aufgrund gefühlter

besonderer Verdienste für das Unternehmen, die von diesem, nach eigenem Ermessen, nicht entsprechend gewürdigt werden). Zum anderen ist zu vermeiden, dass durch falsche Anreizsetzung unethisches Handeln implizit befördert wird, indem die Gewährung von Boni oder variablen Gehaltsbestandteilen ausschließlich an die Erreichung bestimmter Erfolgskennzahlen geknüpft ist, ungeachtet der angewendeten Mittel zur Zielerreichung. Darüber ob die Einhaltung von Compliance Auswirkung auf die Zielerreichung bzw. die Gewährung variabler Gehaltsbestandteile Einfluss nehmen soll, ist im Einzelfall zu entscheiden. Unethische Geschäftspraktiken oder unerwünschtes Verhalten von Mitarbeitern sollten sich jedoch grundsätzlich im Nichterreichen der Zielvereinbarungen und damit auch in der Nicht-Gewährung variabler Gehaltsbestandteile auswirken. In jedem Fall ist den Mitarbeitern zu kommunizieren, dass legales und integres Handeln die Grundlage für die Geschäftstätigkeit bildet und für die Mitarbeiter keine negativen Konsequenzen entstehen, auch und gerade dann wenn die integre Entscheidungsoption in einer Handlungssituation den Verlust eines Auftrages oder den Rückzug aus einem Geschäft bedeuten kann.

Compliance in der Personalentwicklung (PE)

Zusätzlich zur Integration von Compliance und Integrity in die Mitarbeiter- und Führungskräftebeurteilungen ist im Rahmen der Personalentwicklung und -beförderung darauf zu achten, dass auffällige Personen nicht in verantwortungsvolle Positionen befördert werden. Auffälliges oder unangemessenes Verhalten, Verwarnungen oder sonstige Sanktionen, die gegenüber einem Mitarbeiter ausgesprochen werden, sind in der Personalakte zu vermerken. Vor einer anstehenden Beförderung sind entsprechende Informationen zu dem jeweiligen Mitarbeiter einzuholen, entlang derer die Eignung des Mitarbeiters für die Beförderung kritisch zu prüfen ist. Geeignete Erkenntnisquellen für die Beurteilung der Eignung und Integrität zu befördernder Mitarbeiter sind z.B. die Personalakte oder Referenzen/Beurteilungen der bisherigen Vorgesetzten des Mitarbeiters. Im Rahmen der Personalentwicklung, insbesondere bei der Führungskräfteentwicklung und der Entwicklung in Compliance-sensible Positionen, ist sicherzustellen, dass die zu befördernden Mitarbeiter auf die neue Position und die damit verbundenen Verantwortlichkeiten und Zuständigkeiten vorbereitet sind. In Schulungen müssen die notwendigen Kenntnisse vermittelt und entsprechende Fähigkeiten erlernt und eingeübt werden.

Hintergrundrecherchen bei Beförderungen

Zur Integration von Compliance in die tägliche Personalarbeit gehört es, offensichtliche Auffälligkeiten, die auf kriminelle bzw. unethische Aktivitäten hinweisen können, bei Mitarbeitern zu beobachten und ggf. anzusprechen, um daraus möglicherweise hervorgehendes Fehlverhalten frühzeitig zu vermeiden. Entsprechende Warnsignale können beispielsweise ein aufwändiger Lebensstil oder persönliche Notlagen sowie ein auffälliges Urlaubs- und/oder Arbeitsverhalten sein (z.B. Person arbeitet immer allein, zu ungewöhnlichen Tageszeiten, auffallend oft am Wochenende, um kriminellen Aktivitäten möglichst heimlich und ungestört nachgehen zu können). Die allgemeine Fürsorgepflicht des Arbeitgebers verpflichtet diesen, den Mitarbeiter bei Auffälligkeiten anzusprechen und Unterstützung bzw. Hilfe anzubieten.

Fürsorgepflicht des Arbeitgebers

Weitere personalpolitische Maßnahmen, die zur Vermeidung von Verhaltensrisiken und Fehlverhalten beitragen können, sind Personalrotationspläne (v.a. in Compliance-sensiblen Abteilungen, um etwaige Seilschaften zu durchbrechen bzw. nicht erst entstehen zu lassen) oder auch die Rotation von Führungskräften in mit Kontrollaufgaben befasste Funktionen (z.B. Interne Revision, Compliance, Risikomanagement), um bei den Führungskräften eine zusätzliche Sensibilisierung bezüglich Compliance und Integrity und die Prozesse in diesen Abteilungen zu erreichen. Darüber hinaus sollte auch die Genehmigungs- bzw. Anzeigepflicht von Nebentätigkeiten der Mitarbeiter klar geregelt sein, um mögliche Interessenkonflikte frühzeitig zu erkennen bzw. nicht entstehen zu lassen. Grundsätzlich ist es für den Erfolg und die Funktionsfähigkeit des CMS wichtig, dass die Personalprozesse und -politik fair und transparent sind. Die Personalabteilung ist für die Anstrengungen im Rahmen des CMS ein wichtiger Partner, der bei der Umsetzung vieler Maßnahmen mit einzubeziehen ist (z.B. Entwicklung und Ausrollung des Verhaltenskodex, Durchführung von Schulungen/Trainings, Einführung von Arbeitsanweisungen etc.). Daher übernimmt die Personalabteilung für den Erfolg des CMS als Berater, Unterstützer, Betreuer sowohl für die Compliance-Abteilung/den Compliance-Beauftragten als auch für jeden einzelnen Mitarbeiter eine wichtige Funktion.

Personalrotation

Rotation in mit Kontrollaufgaben befasste Funktionen

Nebentätigkeiten

Reaktion auf Fehlverhalten

Bei vermutetem oder entdecktem Fehlverhalten ist die Bedeutung der Reaktion auf solches unerwünschte Verhalten nicht zu unterschätzen – vor allem im Hinblick auf die Vermeidung zukünftigen Fehlverhaltens. Dabei ist nicht in erster Linie die Form oder Härte der Bestrafung entscheidend, vielmehr geht es darum, *dass* von Seiten des Unternehmens *reagiert wird* – auch weil die Unternehmensleitung, unterstützt durch die entsprechenden Funktionen (HR, Compliance), durch eine angemessene Reaktion nachdrücklich heraushebt, wie ernst es ihr mit dem CMS und der Erwartung integren Verhaltens im Geschäftsverkehr ist. Die Duldung von Fehlverhalten könnte eine Unterminierung der gesamten Bestrebungen im Bereich Compliance und Integrity zur Folge haben.

Wichtig ist, *dass* reagiert wird

Vor dem Einleiten konkreter Reaktions- und Sanktionsmaßnahmen muss der Unternehmensleitung und den zuständigen Funktionen – vor allem bei vermutetem Fehlverhalten oder bei Hinweisen auf Verstöße – daran gelegen sein, den Hinweisen nachzugehen und die Umstände vollständig aufzuklären, um weitere Verfehlungen und

(noch) schwerer wiegende Konsequenzen und Schäden vom Unternehmen abzuwenden. Hierzu gilt es, ggf. unterstützt durch geeignete interne oder externe Funktionen (z.B. Interne Untersuchungen – sog. Internal Investigations –, externe Berater/Rechtsanwälte), entsprechende Nachforschungen einzuleiten, die die Hinweise erhärten und weitere Untersuchungen zur vollständigen Sachverhaltsaufklärung auslösen oder, sollte sich die Vermutung nicht bewahrheiten, zu einer Schließung des Vorgangs führen. Weitere Hinweise zum Umgang mit entdecktem systematischen Fehlverhalten finden sich im ANNEX, → ABSCHNITT I.6 ›COMPLIANCE-REMEDIATION NACH ENTDECKTEM SYSTEMATISCHEM FEHLVERHALTEN‹.

Überprüfung und Anpassung der bestehenden CMS-Prozesse und -Maßnahmen

Die Reaktionsmaßnahmen auf Compliance-Verstöße beschränken sich nicht auf die individuelle Sanktionierung des/der betroffenen Mitarbeiter(s). Zu einem angemessenen Reaktionsprozess gehört es auch, notwendige Prozessanpassungen oder -veränderungen vorzunehmen sowie Lücken in Kontrollprozessen oder Regelwerken zur Vermeidung zukünftigen Fehlverhaltens zu identifizieren und Defizite aufzuheben. Darüber hinaus kann es sinnvoll sein, aufgetretene Compliance-Verstöße im Rahmen von Schulungen (z.B. Case Studies) zu thematisieren, um die Mitarbeiter entsprechend zu sensibilisieren und ähnlichen Verfehlungen in der Zukunft vorzubeugen. Häufig ist in diesem Zusammenhang von ›lessons learned‹ die Rede.

Konsequente Sanktionierung von Fehlverhalten

Gleichwohl kommt der konsequenten Sanktionierung von Fehlverhalten für die Glaubwürdigkeit und Präventionswirkung des CMS eine wichtige Rolle zu. Grundsätzlich steht dem Unternehmen das gesamte Spektrum möglicher Sanktionsmaßnahmen zur Verfügung. Zu den klassischen Disziplinarmaßnahmen zählen u.a. Ermahnung, Abmahnung, Verlust von freiwilligen oder variablen Entgeltbestandteilen, Versetzung in eine andere Position sowie die außerordentliche Kündigung. Darüber hinaus ist zu entscheiden, ob weitere zivilrechtliche (z.B. Geltendmachung von Schadensersatzansprüchen) oder strafrechtliche Maßnahmen (Erstattung einer Strafanzeige) ergriffen werden sollen. Über die Sanktionierung von Compliance-Verstößen ist jedoch jeweils im Einzelfall zu entscheiden. Wichtig ist, dass die Unternehmensleitung z.B. im Verhaltenskodex gegenüber den Mitarbeitern kommuniziert, dass Fehlverhalten nicht geduldet und entsprechende Reaktionsmaßnahmen auslösen wird. Die Kommunikation sollte ebenso beinhalten, dass Fehlverhalten für die beteiligten Mitarbeiter zu schwerwiegenden Disziplinarmaßnahmen führen und ggf. weitere arbeits-, zivil- und strafrechtliche Konsequenzen zur Folge haben kann.

Kommunikation möglicher Sanktionen

Überwachungs- und Kontrollmaßnahmen

7

Welche Ziele verfolgen Überwachungs- und Kontrollmaßnahmen im Rahmen des CMS?

Sind Kontrollen überhaupt sinnvoll, führen sie nicht vielmehr zu einer Misstrauenskultur?

Wie können Überwachungs- und Kontrollmaßnahmen in die Unternehmensprozesse integriert werden?

In welcher Häufigkeit und in welchem Umfang sind Kontrollen im Unternehmen durchzuführen?

Wer ist für die Durchführung von Überwachungs- und Kontrollmaßnahmen zuständig?

Welches Ziel wird mit dem Monitoring des CMS verfolgt?

Zielsetzung

Die Unternehmensleitung trägt die Verantwortung dafür, dass sich Management und Mitarbeiter an die geltenden gesetzlichen sowie unternehmensinternen Regeln und Normen halten und Schäden von der Gesellschaft abgewendet werden (sog. Legalitätspflicht, vgl. CMS-Element → 2 COMPLIANCE-ORGANISATION UND GOVERNANCE-SYSTEM). Dies macht eine Aufsicht und Überwachung der Einhaltung von Compliance seitens der Beschäftigten zwingend erforderlich. Überwachungs- und Kontrollmaßnahmen zielen darauf ab, Fehler und Unregelmäßigkeiten zu verhindern, zu vermindern und aufzudecken. Kontrollen erhöhen nicht nur die Entdeckungswahrscheinlichkeit von Verstößen, sondern haben zugleich präventive Wirkung, da sie den Betriebsangehörigen vor Augen halten, dass Verstöße entdeckt und entsprechend geahndet werden können. Für die Gewährleistung der Glaubwürdigkeit der Unternehmensleitung, dass Fehlverhalten im Unternehmen nicht toleriert wird, sind Kontroll- und Aufsichtsmaßnahmen zur Aufdeckung von Verstößen von Mitarbeitern und Schwachstellen in den Prozessen notwendig. Aufsichtsmaßnahmen, die jedoch ausschließlich darauf abzielen, eine unternehmerische ›Polizei- und Überwachungsfunktion‹ zu errichten, um die Angst der Beschäftigten vor Entdeckung und Sanktionen zu schüren, werden auf Dauer schädlich und kontraproduktiv sein. Denn übertriebene Kontroll- und Aufsichtsmaßnahmen lähmen das operative Geschäft und werden sich nachteilig auf die Motivation der Mitarbeiter auswirken. Unternehmen müssen daher versuchen, die Balance zu halten zwischen zu übertrieben eingerichteten Kontroll- und Aufsichtsmaßnahmen, welche die Eigenverantwortlichkeit der Beschäftigten beschränken und damit zu einer Minderung der Mitarbeitermotivation führen, und zu lax gehaltenen Aufsichts- und Kontrollmaßnahmen, die den Mitarbeitern signalisieren, dass die Einhaltung von Compliance im Unternehmen keine (wesentliche) Bedeutung spielt und Verstöße nicht geahndet bzw. erst gar nicht festgestellt werden.

Erhöhung der Entdeckungswahrscheinlichkeit von Verstößen

Überwachungsmaßnahmen wie Monitoring und Review verfolgen das Ziel, das CMS dahingehend zu überprüfen und zu beurteilen, ob es angemessen ausgestaltet und funktionsfähig ist. Ob die entwickelten Maßnahmen tatsächlich geeignet sind, die verfolgten Ziele von Prävention und Detektion zu erfüllen, zeigt sich oft erst bei, während oder nach erfolgter Anwendung der Maßnahmen. Da Prozesse und Regularien einem stetigen Wandel unterliegen, ist das CMS in turnusmäßigen Abständen im Wege von Monitoring und Review auf seine Geeignetheit, Angemessenheit und Funktionsfähigkeit hin zu prüfen. Hierdurch lässt sich nicht nur feststellen, ob das CMS auf Änderungen und neue Anforderungen angepasst werden muss, sondern es lassen sich auch eventuelle Schwachstellen aufdecken, die behoben werden können. Dadurch kann das CMS einem kontinuierlichem Verbesserungsprozess unterzogen werden, um dessen

Monitoring und Review

Funktionalität auf Dauer sicherzustellen. Indem diese Überwachungsmaßnahmen auf die Beurteilung der Funktionsfähigkeit eines CMS abzielen, untermauern sie, dass der Unternehmensleitung ernsthaft daran gelegen ist, ein funktionierendes CMS zu betreiben.

Sämtliche Überwachungs- und Kontrollmaßnahmen zielen damit auf die Sicherstellung eines funktionierenden CMS ab und dienen letztendlich dem Schutz und Erhalt des Betriebsvermögens und sichern mithin die Existenz des Unternehmens.

Empfehlungen für die Umsetzung

Aufsichts- und Überwachungsmaßnahmen

Die Aufsichts- und Überwachungsmaßnahmen eines Unternehmens können dann als funktionsfähig angesehen werden, wenn sie regelkonformes Verhalten fördern, nicht leicht umgangen werden können und geeignet sind, systematisches Fehlverhalten zu verhindern. Geeignete Kontrollaktivitäten sind dabei sowohl in die Arbeitsprozesse zu integrieren als auch prozessunabhängig durchzuführen.

Aufsichts- und Überwachungsmaßnahmen

Bereits im Rahmen der Aufbau- und Ablauforganisation sind von den Unternehmen unabhängig von ihrer Größe und Komplexität bestimmte Überwachungs- und Kontrollmaßnahmen zu implementieren (sog. prozessintegrierte Maßnahmen). Aufgrund ihrer präventiven Wirkung stellen die klassischen prozessintegrierten Kontrollprinzipien wie das Funktionstrennungsprinzip, das Vier-Augen-Prinzip, das Transparenzprinzip sowie das Mindestinformationsprinzip geeignete Maßnahmen dar, die zu einer wesentlichen Reduzierung von Fehlverhalten beitragen. Mit einem Vier-Augen-Prinzip wird festgelegt, dass bestimmte Geschäftsprozesse einer Kontrolle oder Entscheidung seitens einer weiteren Person bedürfen. Das Vier-Augen-Prinzip ist allerdings nur dann ein funktionierendes Mittel, wenn die Kontrolle bzw. Freigabe auf einer unabhängigen und strikt durchgeführten Gegenprüfung beruht. Nimmt die für die Gegenkontrolle verantwortliche Person eine Prüfung – aufgrund von Vertrauen zu dem Mitarbeiter/Kollegen oder aufgrund von Arbeitsüberlastung nicht oder nur lückenhaft oder inkonsequent vor – so kommt dem Vier-Augen-Prinzip keine bzw. lediglich geringe Funktionalität zu. Über eine Funktionstrennung (sog. Segregation of duties) lässt sich diese (mögliche) Schwachstelle eines Vier-Augen-Prinzips abfedern, indem das Unternehmen sicherstellt, dass miteinander unvereinbare Funktionen nicht in einer Person oder Organisationseinheit vereint sind. Die Funktionstrennung dient dazu, verschiedene Funktionen und

Prozessintegrierte Maßnahmen

Vier-Augen-Prinzip

Funktionstrennungsprinzip

Verantwortungen sauber zu trennen, um Interessenkollisionen und somit Fehler oder kriminelle Aktivitäten zu vermeiden. Interessenkollisionen können u.a. vermieden werden, wenn beispielsweise die folgenden Funktionen voneinander getrennt sind:

- Einkauf und Rechnungsprüfung/Rechnungsanweisung
- Einkauf und Wareneingangsprüfung
- Vertrieb und Bonitätsprüfung (neuer) Kunden

Kleinen und mittleren Unternehmen mit beschränkten personellen Ressourcen wird es oft nicht möglich sein, eine umfassende Funktionstrennung im Bereich der Organisation einzurichten. Gleichwohl sollten auch diese Unternehmen das Vier-Augen-Prinzip zumindest in sensiblen bzw. risikobehafteten Prozessen (z.B. Anlage und Freigabe von Vertriebsmittlern in Hochrisikoländern, Unterschriftenregelung bei der Beschaffung von Waren, Gütern, Dienstleistungen ab einem bestimmten Auftragswert) sowie in Bereichen und Funktionen mit erhöhtem Compliance-Risiko um das Prinzip der Funktionstrennung erweitern. Beim Einsatz von IT sollten die Unternehmen das Funktionstrennungsprinzip ebenfalls, z.B. durch das Einrichten von bestimmten Benutzerrechten, gewährleisten.[44]

Auch im Bereich des Umgangs mit Daten sind prozessintegrierte Maßnahmen geeignete Mittel, die Risiken von Datenmanipulation, Datenklau oder sonstigem Datenmissbrauch zu minimieren. Hierzu eignet sich z.B. die Festlegung von Zugangs- und Zugriffsberechtigungen in den verschiedenen Geschäftsbereichen, die sicherstellen, dass sensible Informationen und Daten nur denjenigen Beschäftigten zur Verfügung stehen, die diese zur Ausübung ihrer Arbeit benötigen (Need-to-know-Prinzip).

Festlegung von Zugangs- und Zugriffsberechtigungen

Ein großer Vorteil und Nutzen von prozessintegrierten Kontrollaktivitäten ist darin zu sehen, dass sie von allen Unternehmen, unabhängig von ihrer Größe, ohne erhebliche Kosten und Implementierungsaufwand auf allen Hierarchieebenen des Unternehmens eingerichtet werden können. Prozessintegrierte Kontrollen können von den Geschäftsbereichen selbst durchgeführt werden. Die Verantwortung hierfür kann an die einzelnen Bereiche delegiert werden mit der Maßgabe, dass die Führungskräfte für die Kontrollen zuständig sind. Insbesondere eine gut ausgeprägte Funktionstrennung

Vorteile prozessintegrierter Kontrollen

44 Eine besondere Sorgfalt für die Einräumung von Berechtigungen kann bei Auszubildenden oder Trainees erforderlich sein, die im Rahmen der Ausbildung verschiedene Abteilungen durchlaufen und dort jeweils mit bestimmten Zugangs- und Zugriffsberechtigungen ausgestattet werden. Nach dem Ende der jeweiligen Station im Unternehmen sind den Auszubildenden/Trainees die Zugangsberechtigungen wieder zu sperren. Andernfalls läuft das Unternehmen Gefahr, dass sich diese Personen nach Ablauf der Ausbildung zu einer Art ›Superuser‹ mit allumfassenden Zugriffs- und Zugangsberechtigungen entwickeln.

in Verbindung mit dem Vier-Augen-Prinzip kann den Umfang von weiteren (prozessunabhängigen) Kontroll- und Überprüfungsmaßnahmen, ob die implementierten Kontrollprinzipien von den Mitarbeitern auch tatsächlich berücksichtigt werden, erheblich minimieren.

Dennoch darf die Unternehmensleitung im Rahmen ihrer Aufsichts- und Überwachungspflichten nicht gänzlich auf die Durchführung von regelmäßigen prozessunabhängigen Überwachungs- und Kontrollmaßnahmen verzichten, mit denen zu überprüfen ist, ob die Mitarbeiter die definierten Prozessabläufe tatsächlich eingehalten haben. Wird im Rahmen solcher Kontrollen Fehlverhalten aufgedeckt oder gibt es sonstige Hinweise auf Verstöße, so sind derartige Kontrollmaßnahmen hinsichtlich des Umfangs und Häufigkeit sogar zu intensivieren. In kleineren Unternehmen wird es der Unternehmensleitung oftmals möglich sein, derartige Prüfungen selbst durchzuführen. Mit zunehmender Unternehmensgröße und Komplexität der Geschäftstätigkeit hingegen werden die Anforderungen an die Kenntnis des Geschäfts des Unternehmens steigen. Um ihren Aufsichtspflichten gerecht zu werden, wird die Unternehmensleitung eine Delegation der Überwachungs- und Aufsichtsmaßnahmen an nachgeordnete Stellen vornehmen müssen. In kleineren Unternehmen bieten sich eine Controllingabteilung oder die besonderen Unternehmensbeauftragten wie beispielsweise der Compliance-Verantwortliche, der Risikomanager oder Datenschutzbeauftragte sowie die jeweiligen Abteilungsleiter in den verschiedenen Fachbereichen an. Insbesondere die Führungskräfte haben für ein funktionierendes internes Kontrollsystem innerhalb ihres eigenen Bereichs sicherzustellen, dass geeignete Kontrollen vorhanden sind. Größere Unternehmen haben darüber hinaus Ordnungsmäßigkeitsprüfungen durch eine unabhängige Stelle durchführen zu lassen, um eine neutrale und unvoreingenommene Beurteilung zu bekommen, ob die grundlegenden formalen Ordnungsprinzipien tatsächlich eingehalten werden. Ist im Unternehmen eine Interne Revision oder Compliance-Abteilung vorhanden, so werden üblicherweise diese Organisationseinheiten mit den Ordnungsmäßigkeitsprüfungen beauftragt. Daneben können auch externe Dienstleister mit der Wahrnehmung dieser Prüfungsmaßnahmen beauftragt werden. Ab einer bestimmten Unternehmensgröße und Komplexität ist eine zentrale Koordination der Ordnungsmäßigkeitsprüfungen unerlässlich. Diese zentrale Stelle ist neben der Bereitstellung der Prüfungsunterlagen auch für die Beantwortung der Prüfberichte und die Koordination von Abhilfemaßnahmen bei festgestellten Defiziten verantwortlich. Als Kontrollmaßnahmen eigenen sich bereits einfache Prüfungshandlungen wie die Befragung von Mitarbeitern, Beobachtung

Prozessunabhängige Kontrollen

»Kennt oder versteht der Betriebsinhaber wesentliche für seinen Geschäftsbetrieb geltende Bestimmungen nicht, so muss er sich zur Erfüllung seiner Überwachungspflicht entweder die für die Überwachungsaufgabe erforderlichen Kenntnisse verschaffen, um seiner Pflicht selbst nachkommen zu können, oder er hat ein innerbetriebliches Kontrollsystem zu organisieren, das er extern, etwa durch einen Steuerberater oder Wirtschaftsprüfer, überwachen lässt«
BayObLG, Beschluss vom 10.08.2001 - 3 ObOWi 51/2001

Ordnungsmäßigkeitsprüfungen

Zentrale Koordination und Berichtswesen bzgl. Ordnungsmäßigkeitsprüfungen

von Aktivitäten und Arbeitsabläufen, die Durchsicht von Dokumenten und Unterlagen sowie das Nachvollziehen der Durchführung bestimmter Geschäftsvorfälle, um einen Eindruck zu bekommen, ob und inwieweit sich die Mitarbeiter an die festgelegten Prozesse und Unternehmensrichtlinien halten. In multinationalen Unternehmen sind umfassende Maßnahmen erforderlich, die einen effizienten Einsatz aller zur Verfügung stehenden Ressourcen im Unternehmen für die Durchführung entsprechender Maßnahmen erfordern. Die Überprüfung der Compliance-Prozesse hat durch die Interne Revision in regelmäßigen Abständen zu erfolgen. Es empfiehlt sich, die Compliance-Abteilung in die Compliance-Prozesse (z.B. bzgl. Korruption, Kartellrechtsverstöße) mit einzubinden und die Prüfpläne und -prozesse zwischen Revision und der Compliance-Abteilung abzusprechen. Die Interne Revision sowie die Compliance-Abteilung sollten hierzu in einem engen Dialog und gegenseitigem Austausch stehen.

Überprüfung der Compliance-Prozesse durch Interne Revision

Überträgt die Unternehmensleitung die Erfüllung der Überwachungs- und Aufsichtspflichten auf nachgeordnete Stellen oder externe Dritte, so hat sie diese Beauftragten sorgfältig auszuwählen und deren Tätigkeit durch überraschende, regelmäßige Prüfungen zu überwachen. Dabei erfüllt die Unternehmensleitung nach der Rechtsprechung ihre Pflicht nur dann, wenn sie die von ihr nicht wahrgenommenen Aufsichtsmaßnahmen lückenlos verteilt und den Aufsichtspersonen den Inhalt ihrer Pflichten genau mitteilt.[45] Grundsätzlich sind aus Dokumentationsgründen die Instruktionen schriftlich zu fassen und an die Mitarbeiter zu kommunizieren (Transparenzprinzip). Bei kleineren Unternehmen mögen ggf. auch mündliche Instruktionen u.U. geeignet sein, wenn aufgrund der geringen Unternehmensgröße bereits über die enge Zusammenarbeit zwischen Unternehmensleitung und Beschäftigten oder der Beschäftigten untereinander eine grundsätzlich gegenseitige Kontrolle erfolgt. Dennoch wird auch kleineren Unternehmen empfohlen, sämtliche die Instruktionen und Arbeitsanweisungen zu Geschäftsprozessen schriftlich vorzuhalten.

»Kann er betriebliche Aufgaben und Pflichten nicht selbst erfüllen, so muß er [der Betriebsinhaber – Anm. d. Verf.] dafür geeignete und zuverlässige Personen bestellen und diese gelegentlich entweder selbst überprüfen oder durch andere - etwa eine Revisionsabteilung - kontrollieren lassen. Dabei sind stichprobenartige, überraschende Prüfungen erforderlich und regelmäßig auch ausreichend, um vorsätzliche Zuwiderhandlungen gegen gesetzliche Vorschriften und Anweisungen der Betriebsleitung zu verhindern.«
BGH, Beschluss vom 25.06.1985 - KRB 2/85 (KG)

Umfang und Intensität der Aufsichts- und Überwachungsmaßnahmen haben sich an Faktoren wie der Größe des Unternehmens, Anzahl der Mitarbeiter, Verstöße in der Vergangenheit etc. auszurichten. Sollten bestimmte prozessabhängige Kontrollaktivitäten wie z.B. die Funktionstrennung und das Vier-Augen-Prinzip aufgrund der Betriebsgröße nicht bzw. nur beschränkt durchführbar sein, so sind die unregelmäßigen, stichprobenartigen prozessunabhängigen Kontrollen zu verstärken. Was Häufigkeit und die Nichtankündigung von Kontrollmaßnahmen anbelangt, so befindet sich das Unternehmen in einem nicht unerheblichen Spannungsverhältnis. Denn zu häufig durchgeführte Kontrollmaßnahmen lähmen nicht nur den Betriebsablauf, sondern können auch zu einer Misstrauenskultur bei den Mitarbeitern führen mit der Folge, dass die Motivation und Arbeitsleistung der Mitarbeiter darunter leidet und sich letztendlich ökonomisch nachteilig auf das Unternehmen auswirken kann. Andererseits sind Kontroll- und Überwachungsmaßnahmen zwingend erforderlich, um glaubwürdig den Beschäftigten zu vermitteln, dass die Unternehmensleitung kompromisslos die Einhaltung von Compliance erwartet.

Umfang und Intensität der Aufsichts- und Überwachungsmaßnahmen

»Die Anforderungen an den Vorstand und die von ihm zu treffenden Aufsichtsmaßnahmen sind umso höher anzusetzen, je öfter sich im Unternehmen Mitarbeiter dem Vorwurf der Beteiligung an Submissionsabsprachen ausgesetzt sehen.«
OLG Frankfurt, Beschluss vom 21.09.1992 - 6 Ws (Kart) 12/91

Nach der Rechtsprechung des BGH sind von derUnternehmensleitung auch *»... stichprobenartige, überraschende Prüfungen erforderlich und regelmäßig auch ausreichend, um vorsätzliche Zuwiderhandlungen gegen gesetzliche Vorschriften und Anweisungen der Betriebsleitung zu verhindern. Sie halten den Betriebsangehörigen nämlich vor Augen, daß Verstöße entdeckt und gegebenenfalls geahndet werden können ...«*. Der BGH weist in seiner Entscheidung darauf hin, dass regelmäßig derartige Prüfungsmaßnahmen auch ausreichend seien, führt aber im Weiteren aus, dass wenn abzusehen sei, *»... daß stichprobenartige Kontrollen nicht ausreichen, um die genannte Wirkung zu erzielen, weil z.B. die Überprüfung von nur einzelnen Vorgängen etwaige Verstöße nicht aufdecken könnte, so ist der Unternehmer zu anderen geeigneten Aufsichtsmaßnahmen verpflichtet. In solchen Fällen kann es geboten sein, überraschend umfassendere Geschäftsprüfungen durchzuführen.«*
BGH, Beschluss vom 25.06.1985 - KRB 2/85 (KG) in NStZ 1986,34

Stichprobenartige, überraschende Prüfungen

Letztendlich ist eine allgemeinverbindliche Aussage zum erforderlichen Umfang der Kontrollmaßnahmen nicht möglich, sondern hängt vielmehr von den gesamten Umständen des Einzelfalles ab.[46] Im Hinblick auf die von der Rechtsprechung festgelegten Anforderungen haben Unternehmen in Abhängigkeit ihrer Unternehmensgröße und Komplexität ihre Kontroll- und Überwachungsmaßnamen so einzurichten, dass Fehlverhalten im Unternehmen sowie seinen Beteiligungen wesentlich erschwert wird.

Umfang der Kontrollmaßnahmen

»Das Vorstandsmitglied einer Aktiengesellschaft muß die Revisionsabteilung so organisieren, daß sie in der Lage ist, in allen Verkaufsbüros wenigstens stichprobenartige überraschende Prüfungen durchzuführen.«
BGH, Beschl. vom 24.03.1981 - KRB 4/80 in LMRR 1981, 17

45 Vgl. KG, Beschluss vom 22.08.1995 - 2 Ss 102/95 - 5 Ws (B) 234/95 in LMRR 1995,77.

46 Wie vor. Das Bayrische Oberlandesgericht hält beispielsweise auch bei einfachen Vorschriften, zuverlässigem Personal und bei durchschnittlicher Gefahr von Verstößen mindestens eine monatliche Kontrolle für erforderlich, die sich bei Häufung von Pflichtverstößen sogar noch weiter verdichte (vgl. BayObLG, Beschluss vom 10. 8. 2001 - 3 ObOWi 51/2001 in NJW 2002, 766).

Monitoring & Review

Im Rahmen von Monitoring und Review haben Unternehmen turnusmäßig durch geeignete interne Stellen zu prüfen und zu beurteilen, ob das CMS angemessen ausgestaltet und funktionsfähig ist. Eine entsprechende Prüfung und Beurteilung sollte mindestens alle drei Jahre erfolgen, um sicherzustellen, dass eingetretene wesentliche Änderungen (z.B. gesetzliche Anforderungen, Änderungen des Geschäftsmodells und/oder der Geschäftspartnerstruktur) im CMS des Unternehmens angemessen berücksichtigt wurden, daraus abgeleitete erforderliche Compliance-Maßnahmen im Unternehmen umgesetzt worden sind und auch tatsächlich funktionieren.

Funktionsfähigkeitsprüfung des CMS (Monitoring & Review)

Kleinere Unternehmen werden überwiegend schlanke Strukturen und Prozesse implementiert und ein weniger formalisiertes CMS eingerichtet haben. Eine Bewertung, inwieweit die implementierten Maßnahmen angemessen sind und funktionieren, kann von der Unternehmensleitung gegebenenfalls selbst vorgenommen werden. Als Basis für die Bewertung und Beurteilung können mit den Mitarbeitern durchgeführte Interviews oder Checklisten bzw. Fragebögen dienen, in denen die Mitarbeiter die implementierten Compliance-Maßnahmen im Wege einer Selbstbewertung auf Angemessenheit und Funktionsfähigkeit beurteilt haben. Weitere Unterstützung für die Bewertung der Angemessenheit des CMS bieten verschiedene Compliance-Standards, die zur Orientierung herangezogen werden können (vgl. hierzu auch die in → KAPITEL V zusammenfassende Übersicht zu den einschlägigen Standards im Bereich Compliance und Integrity). Mit zunehmender Unternehmensgröße und Komplexität des Geschäfts sind für die Bewertung und Beurteilung des CMS entsprechende Fachkenntnisse erforderlich. In kleineren Unternehmen könnte u.U. ein extern durchgeführter Auditierungsprozess des Qualitätsmanagementsystems nach DIN ISO 9001 in Grenzen Aufschlüsse über die Funktionalität bestimmter implementierter Compliance-Prozesse liefern. Große Unternehmen hingegen haben aufgrund der komplexeren Geschäftstätigkeit und des zunehmenden Internationalisierungsgrades eine auf die Bewertung von Angemessenheit und Funktionalität des CMS spezialisierte Prüfungsinstanz zu beauftragen. Dabei ist die Überprüfung des CMS durch eine ›unbefangene neutrale Stelle‹ durchzuführen. Dies kann sowohl eine interne, unabhängige Abteilung wie die Interne Revision, als auch eine extern beauftragte Prüfungsinstanz sein. Stehen dem Unternehmen intern nicht genügend Ressourcen für die Durchführung der Angemessenheits- und Funktionsprüfung zur Verfügung oder fehlt intern entsprechende Fachexpertise, so hat das Unternehmen auf externe spezialisierte Berater zurückzugreifen. In großen Unternehmen ist die Überprüfung der Compliance-Prozesse in regelmäßigen Abständen durch interne Funktionen im Wege von Regelaudits als auch anlassbezogenen unangekündigten Audits durchzuführen. Gründe für eine anlassbezogene Prüfung können z.B. Hinweise oder

Durchführung von Funktionsfähigkeitsprüfungen

Prüfung durch interne Revision oder externe Berater

Regelaudits und anlassbezogene Audits

das Bekanntwerden von Compliance-Verstößen oder eine Veränderung wesentlicher Faktoren (Änderung von Gesetzen, Änderung der Risikolage im Unternehmen etc.) sein.

Darüber hinaus kann es sich für das Unternehmen empfehlen, ggf. in definierten Hochrisikogeschäftsbereichen die Geschäftsprozesse auf ihre Anfälligkeit für dolose Handlungen hin im Wege sog. Walkthroughs entlang der Prozesskette zu prüfen, um festzustellen, welche Kontrollen wenig effektiv sind bzw. welche generell fehlen. Dies kann insbesondere für die dem Sarbanes Oxley Act (zum Sarbanes Oxley Act vgl. → ABSCHNITT I.2 des ANNEX) unterfallenden Unternehmen erforderlich sein.

Geschäftsprozessprüfung/ Walkthroughs

Große Unternehmen haben zur Erfüllung ihrer gesellschaftsrechtlichen Sorgfaltspflichten die jährliche Bewertung der Wirksamkeit des IKS in die Beurteilung zur Funktionsfähigkeit des CMS mit einzubeziehen. Handelt es sich bei dem Unternehmen um eine Aktiengesellschaft, so hat die Unternehmensleitung die Erkenntnisse des Abschlussprüfers zu Compliance-relevanten Feststellungen im Rahmen der Abschlussprüfung zum Risikofrüherkennungssystem in die Beurteilung zur Funktionsfähigkeit des CMS mit einzubeziehen.

Auswertung der Berichterstattung zum IKS

Und schließlich kann es für Unternehmen verschiedene Anlässe geben, das eigene CMS oder bestimmte Teilbereiche davon einer externen Prüfung/Zertifizierung zu unterziehen (ausführlicher hierzu vgl. → ABSCHNITT II.3).

Zertifizierung des CMS

Dokumentation

Die Unternehmensleitung ist für eine umfassende und vollständige schriftliche Dokumentation sämtlicher durchgeführten Kontroll- und Prüfungsmaßnahmen verantwortlich. Der Detaillierungsgrad und die Tiefe der Dokumentation hängen dabei primär von der Unternehmenskomplexität und den damit verbunden Compliance-Anforderungen im Unternehmen ab.

Schriftliche Dokumentation der Überwachungs- und Kontrollmaßnahmen

Führung und Unternehmenskultur

Welche Rolle nehmen Unternehmensleitung und Führungskräfte bei der Umsetzung von Compliance im Unternehmen ein?

Welche Rolle spielt die Unternehmenskultur (Corporate Culture) bei der Sicherstellung von Compliance im Unternehmen?

Welche Rolle spielen Unternehmenswerte für die Unternehmens- und Führungskultur?

Warum ist das Vorbildverhalten der Führungskräfte für die Sicherstellung von Compliance im Unternehmen wichtig? Welche Rolle spielen in diesem Zusammenhang der ›Tone from the Top‹ und der ›Tone from the Middle‹?

Welche Maßnahmen können zur Herausbildung einer werteorientierten Unternehmenskultur beitragen?

Welche Maßnahmen und Umstände wirken sich positiv auf die Herstellung einer werteorientierten und auf Integrität basierenden Führungs- und Unternehmenskultur aus?

Wie können Führungskräfte ihre Funktion als ›Compliance-Botschafter‹ oder ›Compliance-Multiplikator‹ erfüllen?

8

Zielsetzung

Der Führungsstil und das Führungsverhalten (*Leadership*) sowie die Kultur eines Unternehmens (*Corporate Culture*) bilden den Rahmen und gleichzeitig das Fundament eines nachhaltigen und funktionsfähigen CMS. Ohne sichtbares Engagement und klares Eintreten der Unternehmensleitung und der Führungskräfte für Compliance und Integrität im Unternehmen werden das CMS und die Bemühungen darum die Ziele nicht erreichen können. Dem CMS-Element *Führung und Unternehmenskultur* kommt damit die größte Bedeutung zu, weil es die Funktionsfähigkeit und Wirksamkeit der weiteren CMS-Elemente ganz entscheidend beeinflusst.

Commitment des Topmanagements

Vorbildfunktion der Unternehmensleitung und Führungskräfte

Tone from the Top

Tone from the Middle

Das Engagement der Unternehmensleitung (*Commitment*) zeigt sich zum einen in einem klaren Bekenntnis zu Compliance und Integrität im Geschäft und der eindeutigen Kommunikation darüber, wie Geschäfte gemacht werden sollen und wie nicht, und zum anderen im Verhalten der Unternehmensleitung, dem eine Vorbildfunktion für alle Mitarbeiter zukommt. Nicht minder wichtig ist neben dem *Tone from the Top* (Führungsverantwortung und Vorbildrolle des Topmanagements) der *Tone from the Middle*, d.h. das Führungsverhalten und die Vorbildfunktion der Führungskräfte auf allen Unternehmensebenen. Die Führungskräfte tragen in ihrer täglichen Arbeit und der Zusammenarbeit mit den Mitarbeitern als Multiplikatoren die Botschaft der Unternehmensleitung zu einem integren Geschäftsgebaren in die Organisation hinein und füllen so das CMS mit Leben. Unternehmensleitung und Führungskräfte nehmen durch ihr Verhalten und ihre Entscheidungen entscheidenden Einfluss darauf, wie das CMS und die Umsetzung der Compliance-Maßnahmen im Unternehmen wahrgenommen werden. Zielsetzung der Compliance-Kultur im Unternehmen sollte sein, dass Compliance nicht als regelgetrieben, verbietend und einschränkend (und die Compliance-Abteilung als Unternehmenspolizei) wahrgenommen wird, sondern als handlungsermöglichende, handlungsleitende und unterstützende Funktion, die Orientierung und Hilfestellung in der täglichen Arbeit gibt, wie gute Geschäfte (im Sinne von legal, integer und nachhaltig erfolgreich) gemacht werden können. Das Engagement und die eindeutige Kommunikation zu Compliance und Integrität von Topmanagement und Führungskräften nehmen bedeutenden Einfluss auf die Unternehmenskultur. Ein klares Bekenntnis der Führungspersonen zu Compliance und Integrität und die konsequente Um- und Durchsetzung dessen bilden die Basis und Voraussetzung für die Entwicklung einer an moralischen Werten orientierten Unternehmenskultur.

Wahrnehmung von Compliance im Unternehmen

Unternehmenskultur

Glaubwürdigkeit des CMS

Das CMS-Element *Führung und Unternehmenskultur* zielt in erster Linie darauf, das CMS mit Glaubwürdigkeit auszustatten und die Bedeutung von Compliance und Integrity für den Geschäftserfolg zu kommunizieren, sowohl gegenüber internen als auch gegenüber externen Interessengruppen. Durch ihr Engagement und Vorbildverhalten demonstriert die Unternehmensleitung, wie ernst es ihr mit dem CMS ist und auf welche Art und Weise sie Geschäfte machen will. Diese Positionierung und das Engagement der Unternehmensleitung und Führungskräfte bilden das Fundament für eine integritätsbasierte und wertegetriebene Kultur im Unternehmen. Vor allem die eindeutige Botschaft zu Compliance und Integrität als auch das Vorbildverhalten von Topmanagement und Führungskräften bewirken eine Sensibilisierung der Mitarbeiter für Compliance im Geschäft und beeinflussen die Motivation zu integrem Handeln im Geschäftsalltag. Gegenüber externen Interessengruppen wie Kunden, Lieferanten und Öffentlichkeit tragen Führungsverhalten und Unternehmenskultur ganz wesentlich dazu bei, die Vertrauenswürdigkeit des Unternehmens zu stärken und die Kooperationsbeziehungen langfristig zu sichern.

Reputation für Vertrauenswürdigkeit

Sicherung der Kooperationsbeziehungen

Empfehlungen für die Umsetzung

Tone from the Top und Tone from the Middle

Das klare Bekenntnis der Unternehmensleitung und deren Selbstverpflichtung zu integrem Geschäftsgebaren sind unerlässlich für ein funktionsfähiges CMS und damit notwendiges Kriterium für die Beurteilung dessen Funktionsfähigkeit und Angemessenheit. Die Unternehmensleitung trägt die Verantwortung für Compliance und Integrität im Geschäft und muss die Umsetzung und Sicherstellung von Compliance und Integrität zu ihrem Thema machen. Nur dann kann es ihr gelingen, die Bedeutung von Compliance und Integrität im Geschäftsalltag glaubwürdig an die verschiedenen internen und externen Interessengruppen zu kommunizieren. In größeren Unternehmen, in denen die Unternehmensleitung z.B. aufgrund der Dezentralität der Niederlassungen und Geschäftseinheiten nicht mehr alle Mitarbeiter persönlich erreichen kann, übernimmt der Chief Compliance Officer gemeinsam mit der Compliance-Abteilung, den regionalen Compliance Officers sowie den Führungskräften eine Mittler- und Multiplikationsfunktion für Compliance und Integrity im Unternehmen. Als Botschafter der Unternehmensleitung tragen sie deren Anliegen ins Unternehmen und nehmen durch ihre Führungsaufgabe und das eigene Verhalten in der Zusammenarbeit mit ihren Mitarbeitern wesentlichen Einfluss auf die Wahrnehmung und Umsetzung von Compliance und Integrity im Unternehmen.

Verantwortung der Unternehmensleitung

Kommunikation der Unternehmensleitung

Für das Setzen des richtigen Tone from the Top ist die Kommunikation der Unternehmensleitung zu Compliance und Integrity sowie den damit einhergehenden Verhaltenserwartungen an die Mitarbeiter das wichtigste Instrument. Eine solche Kommunikation kann beispielsweise durch die persönliche Ansprache bei geeigneten

Anlässen (Unternehmenseintritt, Personalversammlung, Betriebsfeier etc.), durch einen Brief oder auch durch eine Videobotschaft erfolgen. Der Tone from the Top wird über den Tone from the Middle, d.h. die regelmäßige Kommunikation der Führungskräfte zu Compliance und Integrity und das Engagement und Eintreten der Führungskräfte für die Umsetzung des CMS im eigenen Verantwortungsbereich, in das Unternehmen hinein getragen und in der direkten Zusammenarbeit zwischen Vorgesetzten und Mitarbeitern mit Leben gefüllt (aufgaben- und funktionsbezogende Spezifizierung der Verhaltenserwartungen). Darüber hinaus ist es ganz wesentlich, dass sich die Unternehmensleitung sowie die oberen Führungskräfte klar zu integrem Verhalten und zu risikobehafteten Entscheidungssituationen im Geschäftsverkehr positionieren. Dazu gehört z.B., gegenüber den Mitarbeitern klar zu kommunizieren, dass integres Verhalten in manchen Entscheidungspositionen auch den Verlust eines Auftrages oder den Rückzug aus einem Geschäft bedeuten kann bzw. muss, und gemeinsam mit den Mitarbeitern Strategien und Handlungsoptionen zu entwickeln und einzuüben, mit denen schwierige Situationen im eigenen Verantwortungs- bzw. Arbeitsbereich gemeistert werden können. Eine sorgfältige Auseinandersetzung des Topmanagements mit den Compliance-Risiken im eigenen Verantwortungsbereich bildet hierfür die notwendige Voraussetzung.

Regelmäßige Kommunikation der Führungskräfte zu Compliance und Integrity

Klare Positionierung des Topmanagements zu integrem Verhalten

Auseinandersetzung mit den Compliance-Risiken

Tone from the Top und Vorbildverhalten
Mangelndes Engagement und Vorbildverhalten der Unternehmensleitung kann dazu führen, dass bei Auftreten von Compliance-Verstößen übliche Konsequenzen rechtlich nicht durchsetzbar sind. So hält das Bundesarbeitsgericht eine fristlose Kündigung eines Arbeitnehmers wegen des Verdachts eines Compliance-Verstoßes für unwirksam, wenn der Arbeitnehmer aus vertretbaren Gründen annehmen durfte, dass der Arbeitgeber sein Verhalten und das Abweichen von einer Compliance-Richtlinie billige. In diesem Falle fehle es an einer eine fristlose Kündigung rechtfertigenden schuldhaften Pflichtverletzung des Arbeitnehmers.
Vgl. BAG, Urteil vom 21.06.2012 - 2 AZR 694/11 abrufbar unter http://juris.bundesarbeitsgericht.de/cgi-bin/rechtsprechung/document.py?Gericht=bag&Art=en&Datum=2012-6&nr=16361&pos=14&anz=51 (16.04.2014)

Die Glaubwürdigkeit des Tone from the Top und des Tone from the Middle hängt maßgeblich davon ab, dass sich Unternehmensleitung als auch Führungskräfte selbst an die kommunizierten Verhaltenserwartungen halten und für ihr Verhalten dieselben Maßstäbe für ethisches Handeln anlegen wie bei den Mitarbeitern. Unternehmensleitung und Führungskräfte tragen die Verantwortung für Compliance, d.h. sie müssen durch ihr Handeln und im Umgang mit den Mitarbeitern die Verantwortung für integre Entscheidungen und Handlungen in Geschäftstransaktionen wahrnehmen und dafür einstehen. Trotz der großen Wirkung einer auf Integrität basierenden Führungs- und Unternehmenskultur auf externe Interessengruppen (Glaubwürdigkeit, Vertrauenswürdigkeit) sind für die Umsetzung des Elements *Führung und Unternehmenskultur* in erster Linie die unternehmensinternen Maßnahmen, die sich an die Belegschaft richten, relevant. Gelingt es der Unternehmensleitung, eine integritätsbasierte Unternehmenskultur zu schaffen, wirkt sich dies positiv auf die Präventionswirkung des CMS insgesamt und in der Folge auch auf die Wahrnehmung des Unternehmens bei Lieferanten, Kunden, der Öffentlichkeit und weiteren externen Interessengruppen aus.

Vorbildverhalten der Unternehmensleitung und Führungskräfte

Unternehmenskultur und Beurteilung von Kultur und Integrität im Unternehmen

Geeignete Maßnahmen zur Festigung einer integritätsbasierten Führungs- und Unternehmenskultur setzen bereits bei der Einstellung neuer Mitarbeiter und Führungskräfte an (vgl. hierzu auch das CMS-Element → 5 COMPLIANCE-KOMMUNIKATION & SCHULUNG). Im Rahmen des Einstiegsgesprächs oder der Orientierungswoche für neue Mitarbeiter ist denkbar, dass die Unternehmensleitung persönlich die Inhalte des Verhaltenskodex sowie die Unternehmenswerte vorstellt und aufzeigt, welche Bedeutung integrem Verhalten im Unternehmen zukommt. Auf diese Weise wird den neuen Mitarbeitern gleich zu Beginn ihres Arbeitsverhältnisses eindeutig kommuniziert, auf welche Art das Unternehmen Geschäfte machen will und welche Erwartungen an das Verhalten der Mitarbeiter gestellt werden. Ab einer gewissen Unternehmensgröße, in der es der Unternehmensleitung nicht mehr möglich ist, jeden neueingestellten Mitarbeiter persönlich zu begrüßen und über das CMS zu informieren, übernimmt der jeweilige Vorgesetzte die persönliche Compliance-Kommunikation. In diesem Fall sollte den Mitarbeitern zusätzlich im Rahmen der Einführungsschulung oder der grundlegenden Compliance-Schulung vermittelt werden, dass Compliance und integres Verhalten Anliegen der obersten Unternehmensleitung ist. Zur Unterstützung der persönlichen Ansprache ist zusätzlich jedem Mitarbeiter der Verhaltenskodex in schriftlicher Form auszuhändigen. In größeren Unternehmen sollten der Verhaltenskodex sowie Informationen zum Compliance-Programm feste Bestandteile des Willkommenspakets für neue Mitarbeiter sein.

Integritätsbasierte Führungs- und Unternehmenskultur

Im laufenden Geschäftsalltag geht es darum, dass die Unternehmenswerte sowie die Wichtigkeit integren Geschäftsverhaltens konsistent und regelmäßig an alle Mitarbeiter kommuniziert werden, d.h. die Themen sollten immer wieder gezielt in geeigneten Foren auf die Tagesordnung gesetzt werden, z.B. auf Betriebsversammlungen, Führungskräftemeetings, aber auch in Abteilungs- oder Teammeetings. Um eine Abstumpfung gegenüber dem Thema zu vermeiden, können in der Kommunikation unterschiedliche Schwerpunkte, z.B. aufgrund aktueller Vorfälle, Neuakquisitionen oder Expansionen, gesetzt werden. Wichtig ist dabei, dass das Thema regelmäßig direkt durch die Unternehmensleitung und die Führungskräfte kommuniziert wird, um gegenüber Belegschaft zu zeigen, dass das CMS nicht nur ein ›zahnloser Papiertiger‹ mit vielen Regeln ist, sondern Grundlage der Geschäftstätigkeit, vorangetrieben und vorgelebt durch die Unternehmensleitung und Führungskräfte. Die Compliance-Abteilung unterstützt Unternehmensleitung und Führungskräfte hierbei, indem sie entsprechende Schulungen und Kommunikationsmedien initiiert und gemeinsam mit den Führungskräften entwickelt (hierzu vgl. das CMS-Element → 5 COMPLIANCE-KOMMUNIKATION & SCHULUNG).

Regelmäßige Kommunikation der Führungskräfte zu Compliance und Integrity

Für die Festigung einer integren Unternehmenskultur spielen Unternehmenswerte eine wichtige Rolle. Die Unternehmenswerte beschreiben die Identität und das Selbstverständnis eines Unternehmens und sind für jedes einzelne Unternehmen spezifisch zu entwickeln. Sie bilden die Grundlage für das tägliche Geschäft, geben Handlungsorientierung und kommunizieren Geschäftspartnern und Öffentlichkeit Erwartungssicherheit hinsichtlich Verhalten und Entscheidungen des Unternehmens. Durch die Einbindung von Mitarbeitern und Führungskräften aus verschiedenen Bereichen in die Entwicklung und Festlegung der spezifischen Unternehmenswerte (z.B. im Rahmen von Workshops) kann von Beginn an eine breitere Akzeptanz der Unternehmenswerte erreicht werden.

Unternehmenswerte

Wie bereits erwähnt, kommt den Führungskräften in diesem Zusammenhang eine besondere Verantwortung zu. Als Multiplikatoren und Botschafter der Unternehmenskultur sind sie im täglichen Geschäft im direkten Kontakt mit den Mitarbeitern, ihr (Vorbild-)Verhalten und ihre Haltung zum CMS beeinflusst sowohl die Unternehmenskultur als auch das Verhalten der Mitarbeiter. Aus diesem Grund kommt auch der Auswahl geeigneter Führungskräfte eine wichtige Funktion zu (hierzu vgl. das CMS-Element → 6 INTEGRATION IN HR-PROZESSE). Stellt eine Führungskraft beispielsweise die Sinnhaftigkeit des CMS in Frage oder stellt sie ihr eigenes Verhalten über das CMS, kann dies bei den Mitarbeitern schnell zu Irritationen und Verwirrung führen, darüber welches Verhalten von ihnen erwartet wird und warum sie sich an das CMS halten sollen, wenn es schon ihr Vorgesetzter nicht tut. Die Beförderung von Personen mit fraglicher Integrität oder Auffälligkeiten in Positionen mit Personalverantwortung ist daher zu vermeiden. Neben dem Führungsverhalten wird die Unternehmenskultur von der Arbeitsatmosphäre (Umgang miteinander, faire Personalpolitik etc.) sowie von einer transparenten und verständlichen Kommunikation des CMS, seiner Regelungen und Maßnahmen geprägt (hierzu vgl. das CMS-Element → 5 COMPLIANCE-KOMMUNIKATION & SCHULUNG). Dazu gehört auch, Mitarbeiter zu einer offenen Kommunikation aufzufordern und zu ermuntern, Probleme offen anzusprechen, so dass schwierige oder kritische Situationen möglichst frühzeitig erkannt und entsprechende Gegenmaßnahmen eingeleitet werden können. Die Führungskräfte sind hier in einer Vermittlerrolle, sie müssen die Regeln und Verhaltenserwartungen in den Arbeitsalltag übersetzen und sind Ansprechpartner und Berater. Führungskräfte sollten Fehlverhalten offen ansprechen, angemessen darauf reagieren und ggf. konsequent sanktionieren, aber auch vorbildliches Verhalten – an den richtigen Stellen und im richtigen Maßen – anerkennen (z.B. im Mitarbeitergespräch) (hierzu vgl. CMS-Element → 6 INTEGRATION IN HR-PROZESSE).

Rolle der Führungskräfte

Personal- und Führungskräfteentwicklung

Offene Kommunikationskultur

Schließlich ist es sinnvoll, Feedback zur Unternehmenskultur und -integrität sowie Kritik der Mitarbeiter zum CMS oder einzelnen Maßnahmen im Sinne eines kontinuierlichen Verbesserungsprozesses zuzulassen und ernst zu nehmen. Mittels einiger Fragen im Rahmen einer Mitarbeiterbefragung oder der Auswertung von Indikatoren, wie z.B. der Fluktuationsrate, können Informationen über die Wahrnehmung des CMS sowie die Unternehmenskultur erhoben werden. Sowohl die Unternehmensleitung als auch die Führungskräfte und die Compliance-Abteilung sollten sich aktiv um ein Feedback der Mitarbeiter zur Wahrnehmung und Einstellung bezüglich der Unternehmenskultur und -integrität allgemein sowie zum CMS im Speziellen bemühen. Eine erste Rückmeldung können die einzelnen Vorgesetzten ebenso wie die Compliance Officer z.B. in persönlichen, informellen Gesprächen mit Mitarbeitern gewinnen. Es ist aber auch denkbar, einige Fragen zur Unternehmens- und Führungskultur sowie zu Compliance in eine bestehende, regelmäßig durchgeführte Mitarbeiterbefragung zu integrieren. Umfassendere und tiefer gehende Erhebungen zur Wahrnehmung der Compliance-Kultur und des ethischen Klimas im Unternehmen können mithilfe eines sogenannten Integrity-Barometers (spezifische Mitarbeiterbefragung zu Compliance und Integrity) oder auch im Rahmen von Feedback zum Führungsverhalten von Führungskräften (Einschätzung der Leistung und Kompetenzen einer Führungskraft durch Mitarbeiter, Kollegen, Kunden, Lieferanten etc.) erfolgen.

Beurteilung der Unternehmenskultur und -integrität

Feedback zur Wahrnehmung der Unternehmenskultur einholen
Die Unternehmensleitung bzw. die Compliance-Abteilung sollte in regelmäßigen Abständen bei den Mitarbeitern ein Feedback zur Wahrnehmung der Unternehmenskultur und zur Wahrnehmung von Compliance im Unternehmen insgesamt einholen.
Das Feedback der Mitarbeiter ist wichtig, um ein Gespür dafür zu bekommen, wie das CMS und die damit verbundenen Erwartungen an die Mitarbeiter wahrgenommen und umgesetzt werden und wo ggf. noch Verbesserungsbedarf besteht.

Integrity-Barometer

Feedback zum Führungsverhalten

Die aktive Einholung von Feedback der Mitarbeiter ist zum einen für die Unternehmensleitung und Compliance-Verantwortlichen von Bedeutung, indem sie Aufschluss gibt über die Funktionsfähigkeit und Wahrnehmung der implementierten CMS-Maßnahmen und Ergänzungs- bzw. Verbesserungsbedarf aufzeigt (z.B. sind die Verhaltensrichtlinien bei den Mitarbeitern bekannt und werden sie akzeptiert? werden die Regelungen im Geschäftsalltag umgesetzt? warum (nicht)?). Die Einholung von Feedback zum Führungsverhalten der Führungskräfte eignet sich vor allem zur Bewertung der Führungskultur im Unternehmen. Zum anderen kann die Unternehmensleitung mit solchen Feedback-Instrumenten nochmals deutlich machen, wie wichtig Integrität und Compliance für die Geschäftstätigkeit sind, und die Ernsthaftigkeit der Compliance-Anstrengungen sichtbar machen, indem Sie den Mitarbeitern durch die Einholung von Rückmeldung deren Einbringen in den kontinuierlichen Verbesserungsprozess des CMS aktiv ermöglicht und wertschätzt.

Instrumente der Implementierung für die verschiedenen Unternehmensgrößenklassen

KAPITEL

IV

Die nachfolgende Matrix gibt einen Überblick über Instrumente für die Implementierung eines angemessenen und funktionsfähigen Compliance-Management-Systems für die verschiedenen Unternehmensgrößenklassen der vier Leitlinien. Darüber hinaus liefert die Matrix für jedes Instrument eine Einschätzung, ob und inwieweit das Instrument für Unternehmen der jeweiligen Unternehmensgrößenklasse geeignet und für die Funktionsfähigkeit des CMS erforderlich ist. Wie in den einführenden Hinweisen in dieser Guidance beschrieben, sind zum einen die Größengrenzen zwischen den einzelnen Leitlinien fließend, d.h. insbesondere Unternehmen, deren Mitarbeiterzahl an einer der Größengrenzen angesiedelt ist, sollten für die Umsetzung eines funktionsfähigen CMS die Empfehlungen beider angrenzenden Leitlinien für ihr Unternehmen in Erwägung ziehen und im Zweifelsfall die höheren Anforderungen beachten. Zum anderen sei auch an dieser Stelle nochmals darauf hingewiesen, dass die Unternehmensgröße hier eine wesentliche, aber nicht die einzige Einflussgröße für die Implementierung geeigneter Compliance-Instrumente ist. Unternehmensspezifische Faktoren, wie eine erhöhte Risikoexposition aufgrund des Geschäftsmodells oder internationaler Tätigkeit, sowie die Zugehörigkeit zu einer bestimmten Branche oder der Einfluss spezifischer regulatorischer Anforderungen, können unter Umständen die Erfüllung höherer Anforderungen bezüglich der Ausgestaltung des CMS und somit eine Einordung in eine höhere Unternehmensgrößenklasse erfordern oder unter Umständen bei bestimmten Instrumenten sogar geringere Anforderungen zulassen.[47]

Darüber hinaus ist zu beachten, dass die Einschätzung der Instrumente bezüglich ihrer Eignung und funktionalen Erforderlichkeit für Unternehmen der einzelnen Leitlinien einen Planungszustand für die Implementierung eines CMS beschreibt bzw. im Falle eines bereits implementierten CMS nur gelten kann, solange dem Unternehmen keine schwerwiegenden Compliance-Verstöße oder schwerwiegende Lücken und Mängel am CMS bekannt geworden sind. Denn in solchen Fällen hat die Unternehmensleitung die Pflicht, bekannt gewordene schwerwiegende Compliance-Verstöße abzustellen bzw. schwerwiegende Mängel oder Lücken im CMS zu beseitigen, was – entgegen den Empfehlungen in der Matrix – in der Regel weitaus umfassendere Maßnahmen erforderlich machen wird (vgl. hierzu insbesondere → ABSCHNITT I.6 ›COMPLIANCE-REMEDIATION NACH ENTDECKTEM SYSTEMATISCHEM FEHLVERHALTEN‹ im ANNEX).

47 Vgl. hierzu auch → FUSSNOTE 23 S.50.

Folgende Kategorien werden den Bewertungen in der Matrix zugrunde gelegt:

1. erwartet
Dieses Instrument ist zur Herstellung der Funktionsfähigkeit des CMS funktional erforderlich. Unternehmen, die davon abweichen, müssen darlegen können, mit welchen anderen Instrumenten sie die Funktionalität des CMS an dieser Stelle sicherstellen.

2. empfohlen
Dieses Instrument wird zur Herstellung einer integren Unternehmensführung empfohlen und ist für Unternehmen der entsprechenden Leitlinie ökonomisch zumutbar.

3. im Ermessen
Dieses Instrument ist nicht zwingend erforderlich und/oder für Unternehmen dieser Compliance-Komplexitätsstufe ökonomisch nicht zumutbar. Diese Bewertung des Instruments impliziert nicht, dass die Implementierung des Instruments keine positiven Beiträge zur Funktionsfähigkeit des CMS leisten könnte. Vielmehr bedeutet diese Bewertung, dass die Implementierung des Instruments in Abhängigkeit von dem entstehenden Mehrwert selbständig durch die verantwortlichen Stellen im Unternehmen erwogen werden soll.

4. alternativ
Mindestens eines der alternativen Instrumente wird zur Herstellung der Funktionsfähigkeit des CMS erwartet.

5. nicht geeignet
Dieses Instrument ist aufgrund der vorliegenden Compliance-Komplexität der Unternehmen dieser Leitlinie nicht sinnvoll umsetzbar.

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
Risikoidentifikation und -bewertung	↓	↓	↓	↓
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

Compliance-Organisation und Governance-System				
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

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
	↓	↓	↓	↓
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
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

Verhaltensgrundsätze und -richtlinien

Verhaltenskodex (Code of Ethics/Code of Conduct)	**erwartet**	**erwartet**	**erwartet**	**erwartet**
Schriftliche Fixierung eines Verhaltenskodex und Bekanntmachung an die Mitarbeiter	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
Schriftliche Fixierung und Bekanntmachung von Verhaltensrichtlinien, die die Regelungen des Verhaltenskodex spezifizieren (z.B. Richtlinie zum Umgang mit Geschenken und Zuwendungen, Anti-Korruptionsrichtlinie)	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
Geschäftspartnerprüfung				
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
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

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
Compliance-Kommunikation & Schulung	↓	↓	↓	↓
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

	↓	↓	↓	↓
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

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 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

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

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 in HR-Prozesse	↓	↓	↓	↓
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

	↓	↓	↓	↓
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

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
Überwachungs- und Kontrollmaßnahmen	↓	↓	↓	↓
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

	↓	↓	↓	↓
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

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
Führung und Unternehmenskultur	↓	↓	↓	↓
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
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

Übersicht über Standards, Handlungsempfehlungen und Rahmenkonzepte

KAPITEL

V

Diese Aufstellung stellt lediglich einen Überblick zu verschiedenen bestehenden Standards, Handlungsempfehlungen und Rahmenkonzepte im Bereich ›Compliance & Integrity‹ dar und erhebt keinen Anspruch auf Vollständigkeit.

A **American Institute of CPS's (2004)**:
COSO Enterprise Risk Management – Integrated Framework (2004)
http://www.coso.org/guidance.htm
(Stand: 16.04.2014)

Austrian Standards Institute, Österreichisches Normungsinstitut (ON) (2013):
ONR 192050 – Compliance Management Systeme (CMS) – Anforderungen und Anleitung zur Anwendung
https://www.austrian-standards.at
(Stand: 16.04.2014)

B – D **British Ministry of Justice (2010):**
The Bribery Act 2010 – Guidance about procedures which relevant commercial organisations can put into place to prevent persons associated with them from bribing (section 9 of the Bribery Act 2010)
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/181762/bribery-act-2010-guidance.pdf
(Stand: 16.04.2014)

Bundesministerium des Innern (Initiativkreis Korruptionsprävention – Bundesverwaltung/Wirtschaft - Gemeinsam gegen Korruption) (2013):
Band 2, Praktische Hilfestellungen für Antikorruptionsmaßnahmen
http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2013/praktische-hilfestellungen-antikorruptionsmassnahmen.pdf?__blob=publicationFile
(Stand: 16.04.2014)

Bundesministerium des Innern (Initiativkreis Korruptionsprävention – Wirtschaft/Bundesverwaltung):
Fragen-/ Antwortenkatalog zum Thema Annahme von Belohnungen, Geschenken und sonstigen Vorteilen (Zuwendungen)
http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Korruption_Sponsoring/initiativkreis_korruptionspraevention.pdf?__blob=publicationFile
(Stand: 16.04.2014)

Bundesverband Informationswirtschaft Telekommunikation und neue Medien e. V. (Bitkom) (2012):
Leitfaden Compliance – Rechtliche Anforderungen an ITK-Unternehmen
http://www.bitkom.org/files/documents/BITKOM_Leitfaden_Compliance.pdf
(Stand: 16.04.2014)

Bundesverband Materialwirtschaft, Einkauf und Logistik e.V. (BME-Verband) (2008):
BME-Verhaltensrichtlinie – Code of Conduct
http://www.bme.de/BME-Compliance-Initiative.compliance.0.html
(Stand: 16.04.2014)

E – F **EMB-Wertemanagement Bau e.V. (2007):**
EMB-Wertemanagement Bau
http://www.bauindustrie-bayern.de/fileadmin/docs_pub/emb/docs/emb_broschuere2007.pdf?PHPSESSID=f23a8fc6f7fbf5e5f366d249722af262
(Stand: 16.04.2014)

European Bank for Reconstruction and Development (EBRD):
Fraud and corruption – definitions and guidelines for private sector operations
http://www.ebrd.com/downloads/integrity/FCguidelines.pdf (Stand: 16.04.2014)

G – H **Gesamtverband der Deutschen Versicherungswirtschaft e. V. (GDV) (2012):**
GDV Compliance-Leitfaden
http://www.gdv.de/2012/01/compliance-leitfaden/ (Stand: 16.04.2014)

I – N **ICC Deutschland e. V. (Internationale Handelskammer) u. Deutscher Industrie- und Handelskammertag e. V. (DIHK) (2008):**
Korruption bekämpfen – Ein ICC-Verhaltenskodex für die Wirtschaft
http://www.icc-deutschland.de/fileadmin/ICC_Dokumente/ICC-Verhaltenskodex_Korruption_final.pdf (Stand: 16.04.2014)

IDW Verlag GmbH (2011):
IDW Prüfungsstandard: Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen (IDW PS 980)
http://shop.idw-verlag.de/product.idw;jsessionid=806D40707225EF33AFD66EBF0235027A?product=20205 (Stand: 16.04.2014)

Initiative Corporate Governance der deutschen Immobilienwirtschaft e.V. (2009):
Pflichtenheft zum ComplianceManagement in der Immobilienwirtschaft
http://www.immo-initiative.de/wp-content/uploads/downloads/2011/zertifizierung/pflichtenheft_compliance_management.pdf
(Stand: 16.04.2014)

International Chamber of Commerce (ICC) (2011):
Combating Extortion and Bribery: ICC Rules of Conduct and Recommendations
http://www.iccwbo.org/advocacy-codes-and-rules/document-centre/2011/icc-rules-on-combating-corruption/ (Stand: 16.04.2014)

OECD (2011):
OECD-Leitsätze für multinationale Unternehmen
http://www.oecd-ilibrary.org/governance/oecd-leitsatze-fur-multinationale-unternehmen_9789264122352-de (Stand: 16.04.2014)

Open Compliance and Ethics Group (OECG):
GRC Capability Model (Red Book)
http://www.oceg.org/resources/grc-capability-model-red-book/ (Stand: 16.04.2014)

Standards Australia (2003):
AS 8002-2003, Australien Standard™, Corporate governance – Organizational codes of conduct
http://infostore.saiglobal.com/EMEA/Details.aspx?ProductID=323765 (Stand: 16.04.2014)

Standards Australia (2006):
AS 3806-2006, Australian Standard™, Compliance programs
http://www.saiglobal.com/PDFTemp/Previews/OSH/as/as3000/3800/3806-2006.pdf (Stand: 16.04.2014)

Transparency International – Deutsches Chapter e.V. (2004):
A-B-C der Korruptionsprävention – Leitfaden für Unternehmen
http://www.transparency.de/uploads/media/DOK514_ABC_2004.pdf (Stand: 16.04.2014)

Transparency International (2013):
Business Principles for Countering Bribery
http://www.transparency.org/whatwedo/tools/business_principles_for_countering_bribery/1/ (Stand: 16.04.2014)

Transparency International (2010):
Checkliste für Self-Audits zur Korruptionsprävention in Unternehmen
http://www.transparency.de/Wirtschaft.64.0.html (Stand: 16.04.2014)

TÜV Rheinland (2011):
TR CMS 101:2011 Standard für Compliance Management Systeme (CMS)
http://www.tuv.com/media/germany/60_systeme/compliance/compliance_standard_tr.pdf (Stand: 16.04.2014)

UN Global Compact:
The Ten Principles
http://www.unglobalcompact.org/AboutTheGC/TheTenPrinciples/index.html (Stand: 16.04.2014)

United States Sentencing Commission (2012):
2012 Guidelines Manual, §8B2.1 Effective Compliance and Ethics Program
http://www.ussc.gov/Guidelines/2012_Guidelines/Manual_HTML/8b2_1.htm (Stand: 16.04.2014)

World Bank, Department of Institutional Integrity:
Voluntary Disclosure Program Protocol 7, II. Guidance in Revising and Improving the Compliance Program
http://siteresources.worldbank.org/INTVOLDISPRO/Resources/2720448-1300821628018/VDP_Protocol_7.pdf (Stand: 16.04.2014)

World Economic Forum, Partnering Against Corruption Initiative (PACI) (2005):
Principles for Countering Bribery
http://www.weforum.org/issues/partnering-against-corruption-initiative (Stand: 16.04.2014)

World Law Group (2012):
Global Guide to Whistleblowing Programs
http://www.theworldlawgroup.com/?cm=Doc&ce=details&primaryKey=53535 (Stand: 16.04.2014)

Zentrum für Wirtschaftsethik gGmbH (2007):
WerteManagementSystem[ZfW]
Standard & Guidance Document
http://www.dnwe.de/tl_files/ZfW/wms.pdf (Stand: 16.04.2014)

Zentrum für Wirtschaftsethik gGmbH (2009):
ComplianceProgramMonitor[ZfW]
http://www.dnwe.de/complianceprogrammonitor.html?file=tl_files/ZfW/ZfW-CPM.pdf (Stand: 16.04.2014)

Literaturübersicht

KAPITEL

VI

Die Guidance, Leitlinien sowie der Annex wurden auf Basis relevanter Gesetze, der einschlägigen Standards und Empfehlungen im Bereich Compliance & Integrity (vgl. → KAPITEL V dieser GUIDANCE), durch Hinzuziehung von Literatur sowie durch Auswertung der Experteninterviews mit den Kooperationspartnern des Forschungsprojekts erstellt.

Verwendete und vertiefende Literatur

A

AKEIÜ (2010):
Compliance: 10 Thesen für die Unternehmenspraxis.
In: Der Betrieb, 27-28/2010, S. 1509-1518

Annuß, G.; Pelz, C. (2010):
Amnestieprogramme – Fluch oder Segen?
In: BB Special 4, 50/2010, S. 14-20

B

Barth, V.M. (2012):
Compliance-Systeme zur Vermeidung von Korruption.
In: Der Schweizer Treuhänder, Nr. 9/2012, S. 658–664

Behringer, S. (2011):
Aufsichtsrat und Compliance-Management - Aufgaben und Best Practice.
In: Zeitschrift Risk, Fraud & Compliance (ZRFC), 3/11, S. 127-132

Behringer, S. (Hrsg.) (2012):
Compliance für KMU – Praxisleitfaden für den Mittelstand.
Berlin: Erich Schmidt Verlag

Bock, D. (2010):
Strafrechtlich gebotene Unternehmensaufsicht (Criminal Compliance) als Absenkung des Schadenserwartungswerts aus unternehmensbezogenen Straftaten.
In: HRRS, 7-8/2010, S. 316-329

Bock, D. (2011):
Criminal Compliance.
Baden-Baden: Nomos Verlag

Bohnert, J. (Hrsg.) (2010):
Kommentar zum Ordnungswidrigkeitengesetz, 3. Auflage
München: C. H. Beck Verlag

Brand-Noé, C. (2007):
Aufgaben des Personalwesens im Hinblick auf die Prävention von unternehmensschädigendem Verhalten.
In: Zeitschrift Risk, Fraud & Compliance (ZRFC), 2/07, S. 63-70

C – D

Campos Nave, J.; Bonenberger, S. (2008):
Korruptionsaffären, Corporate Compliance und Sofortmaßnahmen für den Krisenfall.
In: BetriebsBerater, 15/2008, S. 734-741

Cohen, J.M.; Holland, M.P. (2008):
Fünf Punkte, die ausländische Unternehmen über den United States Foreign Corrupt Practices Act (FCPA) wissen sollten.
In: Corporate Compliance Zeitschrift (CCZ), 1/08, S. 7-10

E – F

Ethics Resource Center (Hrsg.) (2012):
Ethical Leadership and Executive Compensation: Rewarding Integrity in the C-Suite.
http://www.ethics.org/files/u5/execComp.pdf (Stand: 16.04.2014)

G

Gäbel, J.K. (2012):
Bericht des Komitees zu internationalen Transaktionen der Anwaltskammer der Stadt New York.
In: Corporate Compliance Zeitschrift (CCZ), 6/12, S. 229-236

Geismar, A.-G. (2011):
Der Tatbestand der Aufsichtspflichtverletzung bei der Ahndung von Wirtschaftsdelikten (Kiel, Univ., Diss.).
Baden-Baden: Nomos

Gnändiger, J.-H.; Steßl, A. (2012):
Im Blickpunkt: Akzeptanz von Compliance-Management-Systemen auf Mitarbeiterebene.
In: BetriebsBerater, 37/2012, S. 6-7

Görling, H.; Inderst, C.; Bannenberg, B. (Hrsg.) (2013):
Compliance – Aufbau-Management-Risikobereiche.
Heidelberg: C.F. Müller

Goette, W.; Habersack, M. (Hrsg.) (2008):
Münchener Kommentar zum Aktiengesetz, Band 2, 3. Auflage
München: C. H. Beck Verlag/Franz Vahlen Verlag

Grüninger, S. (2005):
Codes of Conduct – Grundsätze für integres Unternehmensverhalten entwickeln und implementieren.
In: KPMG Audit Committee Quarterly, III/2005, S. 6-13

Grüninger, S.; Fürst, M.; Pforr, S.; Schmiedeknecht, M. (Hrsg.)(2011):
Verantwortung in der globalen Ökonomie gestalten.
Marburg: Metropolis-Verlag

Grüninger, S.; Jantz, M. (2013):
Möglichkeiten und Grenzen der Prüfung von Compliance-Management-Systemen – Gestaltung interner oder externer Wirksamkeits- und Umsetzungsprüfungen.
In: Zeitschrift für Corporate Governance (ZCG), 03/2013, S. 131-136

Grüninger, S.; Jantz, M.; Schweikert, C.; Steinmeyer, R. (2012):
Sorgfaltsbegriff und Komplexitätsstufen im Compliance Management
(KICG-Forschungspapier Nr. 2/2012)

Grüninger, S.; Jantz, M.; Schweikert, C.; Steinmeyer, R. (2012):
Organisationspflichten - eine Synopse zum Begriffsverständnis und den daraus abzuleitenden Anforderungen an Aufsichts- und Sorgfaltspflichten aus juristischer und betriebswirtschaftlicher Perspektive (Studie 2 im Forschungsprojekt Leitlinien für das Management von Organisations- und Aufsichtspflichten)
(KICG-Forschungspapier Nr. 4/2012)

Grüninger, S.; Jantz, M.; Schweikert, C. (2013):
Risk-Governance-Cluster-Cube
(KICG-Forschungspapier Nr. 5/2013)

Grüninger, S.; Jantz, M.; Schweikert, C. (2013):
Begründung für die Festlegung der Größengrenzen zur Einteilung von Unternehmen in die verschiedenen Leitfäden
(KICG-Forschungspapier Nr. 6/2013)

Grüninger, S.; Steinmeyer, R.; Strenger, C. (im Erscheinen):
Compliance und Aufsicht
In: Wieland, J.; Steinmeyer, R.; Grüninger, S. (Hrsg.): Handbuch Compliance-Management, 2. Auflage
Berlin: Erich Schmidt Verlag

Grützner, T.; Behr, N. (2013):
Effektives Compliance Programm verhindert Bestrafung von Investmentbank wegen Verstößen gegen FCPA.
In: Corporate Compliance Zeitschrift (CCZ), 2/2013, S. 71-74

Grützner, T.; Leisch, F.C. (2012):
§§130, 30 OWiG – Probleme für Unternehmen, Geschäftsleitung und Compliance-Organisation.
In: Der Betrieb, 14/2012, S. 787–794

Günther, E.; Ruter, R.X. (Hrsg.) (2012):
Grundsätze nachhaltiger Unternehmensführung – Erfolg durch verantwortungsvolles Management
Berlin: Erich Schmidt Verlag

H – J

Hauschka, C.E. (2007):
Compliance in der Korruptionsprävention – was müssen, was sollen, was können die Unternehmen tun?
In: BetriebsBerater, 4/07, S. 165-173

Hauschka, C.E. (Hrsg.) (2010):
Corporate Compliance.
München: C.H. Beck Verlag

Hölters, W. (Hrsg.) (2011):
Aktiengesetz – Kommentar
München: C.H. Beck Verlag/Vahlen Verlag

Hüffer, U. (Hrsg.) (2012):
Aktiengesetz, 10. Auflage
München: C.H. Beck Verlag

K – L

Kahlenberg, H.; Schwinn, H. (2012):
Amnestieprogramme bei Compliance-Untersuchungen im Unternehmen.
In: Corporate Compliance Zeitschrift (CCZ), 3/12, S. 81-86

Kaptein, M. (1998):
The Ethics Thermometer: An Audit-Tool for Improving the Corporate Moral Reputation.
In: Corporate Reputation Review, 2/1., S. 10-15

KfW Bankengruppe (Hrsg.) (2013):
KfW-Mittelstandspanel 2013 – Solider Gesamteindruck trotz Sand im Getriebe
https://www.kfw.de/KfW-Konzern/KfW-Research/Economic-Research/Publikationen/KfW-Mittelstandspanel/Aktueller-Ergebnisbericht/index.html
(Stand: 16.04.2014)

KPMG (Hrsg.) (2012):
Wirtschaftskriminalität in Deutschland 2012 – Eine empirische Studie zur Wirtschaftskriminalität im Mittelstand und in den 100 größten Unternehmen.
http://www.kpmg.de/Publikationen/35116.asp
(Stand: 16.04.2014)

Klengel, J.; Dymek S. (2011):
Criminal Compliance in Zeiten des UK Bribery Act – Extraterritoriales Antikorruptionsgesetz als Herausforderung für die Compliance-Strukturen deutscher und international tätiger Unternehmen.
In: HRRS, 1/2011, S. 22-25

Krieger, G. (Hrsg.) (2010):
Handbuch Managerhaftung: Vorstand, Geschäftsführer, Aufsichtsrat, Pflichten und Haftungsfolgen, typische Risikobereiche.
Köln: Dr. Otto Schmidt

M – O

Moosmayer, K. (2012):
Compliance – Praxisleitfaden für Unternehmen.
München: C. H. Beck Verlag

Moosmayer, K. (2012):
Modethema oder Pflichtprogramm guter Unternehmensführung? – Zehn Thesen zu Compliance.
In: Neue Juristische Wochenschrift (NJW), 41/12, S. 3013-3016

Mössner, B., Kerner, M. (2011):
Praxisbeitrag: Einführung konzernweiter Standards für die Geschäftspartner-Prüfung.
In: Corporate Compliance Zeitschrift (CCZ), 5/11, S. 182-184

P – Q

PricewaterhouseCoopers/Martin-Luther-Universität Halle-Wittenberg (Hrsg.) (2010):
Compliance und Unternehmenskultur – Zur aktuellen Situation in deutschen Großunternehmen.
http://www.pwc.de/de/risiko-management/studie-untersucht-den-zusammenhang-zwischen-compliance-und-unternehmenskultur-in-grossunternehmen.jhtml
(Stand: 16.04.2014)

PwC (Hrsg.) (2013):
Wirtschaftskriminalität und Unternehmenskultur 2013.
http://www.pwc.de/wirtschaftskriminalitaet
(Stand: 16.04.2014)

R **Ringleb, H.M.; Kremer, T.; Lutter, M.; v.Werder, A. (Hrsg.) (2010):**
Kommentar zum Deutschen Corporate Governance Kodex, 4. Auflage
München: C. H. Beck Verlag

Rogall, K. (2006):
Vierter Abschnitt. Verletzung der Aufsichtspflicht in Betrieben und Unternehmen.
In: Karlsruher Kommentar zum Gesetz über Ordnungswidrigkeiten, 3. Auflage.
München: C. H. Beck Verlag

S – V **Schimansky, H.; Bunte, H.-J.; Lwowski, H.-J. (Hrsg.) (2011):**
Bankrechts-Handbuch.
München: C. H. Beck Verlag

Schweikert, C.; Jantz, M. (2012):
Corporate Governance in Abhängigkeit von Unternehmensstruktur und Unternehmensgröße – eine betriebswirtschaftlich-juristische Analyse (Studie 1 im Forschungsprojekt Leitlinien für das Management von Organisations- und Aufsichtspflichten)
(KICG-Forschungspapier Nr. 3/2012)

Senge, L. (Hrsg.) (2006):
Karlsruher Kommentar zum Gesetz über Ordnungswidrigkeiten.
München: C. H. Beck Verlag

Spindler, G.; Stilz, E. (Hrsg.) (2010):
Kommentar zum Aktiengesetz, Band 1, 2. Auflage
München: C. H. Beck Verlag

Steßl, A. (2012):
Effektives Compliance Management in Unternehmen.
Wiesbaden: Springer, VS

W – Y **Weber Shandwick (Eds.) (2012):**
The company behind the brand: in reputation we trust.
http://www.webershandwick.eu/home/news/673 (Stand: 16.04.2014)

Wieland, J., Steinmeyer, R., Grüninger, S. (Hrsg.) (2010):
Handbuch Compliance-Management.
Berlin: Erich Schmidt Verlag

Wieland, J.; Steinmeyer, R.; Grüninger, S. (Hrsg.) (im Erscheinen):
Handbuch Compliance-Management, 2. Auflage
Berlin: Erich Schmidt Verlag

Z **Zentrum für Wirtschaftsethik gGmbH (ZfW) (2009):**
ComplianceProgramMonitor^{ZfW}.
http://www.dnwe.de/complianceprogrammonitor.html?file=tl_files/ZfW/ZfW-CPM.pdf (Stand: 16.04.2014)

Projektbeteiligte

KAPITEL VII

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

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

MARK BAU

PAUTHNERDAY

PFISTERER

pwc

rkw

SIEMENS

TaylorWessing

T

The AuditFactory Prüfung. Beratung. Training.

TPA Horwath

WILMERHALE

ZF Lenksysteme

HOCHSCHULE KONSTANZ TECHNIK, WIRTSCHAFT UND GESTALTUNG

KICG

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

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

Stichwortverzeichnis

KAPITEL VIII

Seitenangaben mit dem Zusatz ›Ax‹ (z.B. Ax 41) verweisen auf die entsprechende Seitenzahl im **ANNEX**.

www.kicg.htwg-konstanz.de