



CPM<sup>ZfW</sup>

ComplianceProgramMonitor<sup>ZfW</sup>



## Inhalt

VORWORT	3
A. ZWECK DES LEITFADENS UND DEFINITIONEN	4
B. INTERNATIONALE GESETZE UND STANDARDS IM BEREICH BUSINESS CONDUCT COMPLIANCE	5
C. ELEMENTE EINES BUSINESS CONDUCT COMPLIANCE-PROGRAMMS	6
I. Leadership & Corporate Culture	7
II. Verhaltensgrundsätze und Verhaltensrichtlinien	8
III. Implementierung	9
IV. Verantwortung und Organisation	9
V. Kommunikation und Schulung	10
VI. Risikobeurteilung und Kontrolle	11
VII. Integration in HR-Prozesse	12
VIII. Vertreter, Agenten und Subunternehmer	13
IX. Transparenz und Dokumentation	14
D. COMPLIANCE MONITORING	15
I. Compliance-Monitoring und Compliance-Audit	15
II. Umfang und Dauer	16
III. Prüfungsziel und Prüfungsgegenstand	17
IV. Prüfungsmethoden und Beurteilung	25

## Vorwort

Integritäts- und Redlichkeitsmanagement und die Einhaltung der gesetzlichen Rahmenbedingungen für die Führung der Geschäfte gewinnen unter dem Stichwort Compliance zunehmend an Gewicht. Mit seiner wachsenden Bedeutung wandelt sich der Begriff auch außerhalb der Finanzdienstleistungsbranche zur konkreten Anforderung an die Regeln und Instrumente der Geschäftsführung.

Damit gewinnt die Frage an Gewicht, was mit Compliance eigentlich gemeint ist. Welche Rückwirkungen ergeben sich auf traditionelle Funktionen, wie etwa Rechtsabteilung, Interne Revision, Unternehmenssicherheit, Umweltschutz oder Personal? Welche funktionalen und organisatorischen Konzepte liefern angemessene Lösungen für die Umsetzung der rechtlichen und ethischen Zielsetzungen des Compliance Managements in einem Unternehmen? Welche Bedeutung hat Compliance für die gesamten Managementsysteme wie beispielsweise Führungs- und Kompensationsverfahren, Trainingsprogramme und das Interne Kontrollsystem, und wie soll die Einhaltung der Maßnahmen überwacht werden? Gehören Sozial- und Umweltstandards oder Anforderungen an die „Social Responsibility“ der Unternehmen in das Feld der Compliance?

Auf alle diese Fragen gibt es derzeit noch keine end- und allgemeingültigen Antworten, die Diskussion hierzu ist im Gange. Es werden von Branche zu Branche, Unternehmen zu Unternehmen und in den verschiedenen Kulturkreisen unterschiedliche Lösungen getestet und Antworten gegeben, ohne dass sich bereits ein vorherrschendes Verständnis oder allgemein anerkannte „Blue Prints“ für die „richtige“ Compliance-Lösung ausgebildet hätten.

Das nachstehende Konzept für ein Compliance Monitoring ist ein Beitrag zu dieser global geführten Diskussion; in ihm kommen viele Jahre praktische Erfahrung der im AfW-Anwenderrat für Wertemanagement<sup>ZfW 1</sup> zusammengeschlossenen Unternehmen zum Tragen. Der hier vorgelegte Leitfaden konzentriert sich bewusst auf den Bereich der „Business Conduct Compliance“, also auf die Frage, wie die redliche und regelgetreue Führung der Geschäfte eines Unternehmens entwickelt und unterstützt werden kann. In den vorgeschlagenen Maßnahmen findet auch die Frage nach den angemessenen Kontrollen und dem Monitoring der in einem Unternehmen beschlossenen Compliance-Maßnahmen ihre Antwort.

Wir wollen Leitplanken setzen, die einerseits dafür sorgen, dass Compliance nicht bei der gut gemeinten Absicht stehen bleibt, sondern zu greifbaren und wirksamen Maßnahmen führt, die die Redlichkeit und Regeltreue des Unternehmens stärken. Andererseits wollen wir mit diesem Leitfaden vorhandenen Bestrebungen entgegenwirken, die die klassische Systematik interner Kontrollsysteme auf Compliance übertragen wollen und damit in der Gefahr stehen, ein proaktives werte- und problemorientiertes Redlichkeitsmanagement durch vielfältige Kontrollschritte zu ersticken.

Hierbei beansprucht der dargestellte Lösungsansatz für ein Compliance Monitoring keineswegs Ausschließlichkeit, sondern lässt ganz bewusst andere und neue Entwicklungen für ein Compliance System zu. Compliance Management heute ist „work in progress“ und benötigt noch viele innovative Entwicklungen. Es kann nicht die Aufgabe eines Compliance Monitorings sein, diese im Ansatz zu verhindern. Wie Fälle aus der Vergangenheit zeigen, wird die Redlichkeit und Regeltreue eines Unternehmens letztlich weniger von der Ausprägung seiner internen Kontrollsysteme als von der klaren Fokussierung auf die eigentlichen Verhaltenstreiber, wie die gelebte Integrität und Regeltreue seines Senior Managements, den Kompensations- und Anreizsystemen sowie einer betrieblichen Kultur der offenen Aussprache bestimmt. Letztendlich geht es um eine Unternehmens- und Führungskultur, die eindeutig und konsequent die Integrität unternehmerischen Handelns einfordert. Wenn wir mit diesem Leitfaden dazu einen Beitrag leisten, hat er seine Aufgabe erfüllt.<sup>2</sup>

<sup>1</sup> „AfW“ siehe Seite 24

<sup>2</sup> Dieses Dokument, CPM Compliance ProgramMonitor, ist im Internet abrufbar unter:  
<http://www.dnwe.de/complianceprogrammonitor.html>

## A. ZWECK DES LEITFADENS UND DEFINITIONEN

### Zweck des Leitfadens

Zweck des Leitfadens ist die Bereitstellung von Prinzipien und Anleitungen für eine überwachende und steuernde Begleitung und Überprüfung (Monitoring) der Entwicklung, Implementierung, Aufrechterhaltung und Verbesserung eines effektiven Compliance-Programms in privaten und öffentlichen Organisationen.

Der Leitfaden ist hierzu an einschlägigen internationalen Leading-Practice-Standards im Bereich Business Conduct Compliance orientiert, die in Abschnitt B dargestellt sind.

Die essenziellen Elemente eines effektiven Business Conduct Compliance-Programms werden in Abschnitt C beschreiben. Die Ausführungen zu den einzelnen Elementen stellen keine zwingenden Anforderungen an Unternehmen und andere Organisationen für das Compliance Management dar. Vielmehr sind sie als Einführung in die Thematik sowie als mögliche Beschreibungen von Compliance-Elementen zu verstehen. Die konkreten Anforderungen an die Compliance-Elemente müssen für die jeweilige Organisation festgelegt und beschrieben werden.

Das Compliance Program Monitoring selbst fokussiert die überwachende und steuernde Begleitung und Überprüfung der Ausgestaltung, Implementierung und Umsetzung von Business Conduct Compliance-Programmen im Geschäftsalltag und wird in Abschnitt D beschrieben. Darin enthalten ist auch eine Compliance-Programm-Checkliste, anhand derer das Compliance Monitoring durchgeführt werden kann.

### Definitionen

Der Fachbegriff *Compliance* bedeutet im Unternehmens- und Organisationsbereich die Befolgung der Gesetze und regulatorischen Anforderungen, der Organisationsgrundsätze, interner Kodizes und Richtlinien, der Prinzipien einer guten Unternehmens- bzw. Organisationsführung (Good Governance) sowie allgemein akzeptierter ethischer Normen.

Das auf diesen umfassenden Begriff bezogene *Compliance Management* (Sicherstellung der Compliance durch geeignete Maßnahmen) schließt neben den in der öffentlichen Debatte häufig im Mittelpunkt stehenden Themen der Korruptionsbekämpfung und Fairness im Wettbewerb auch die Bereiche Umwelt, Menschenrechte, Arbeits- und Sozialstandards sowie weitere, auch branchenbezogene Themen ein.

*Compliance-Programme* beschreiben das Maßnahmenbündel im Rahmen des gesamthafter Compliance Managements eines Unternehmens oder einer anderen Organisation bezogen auf einzelne (rechtliche) Themengebiete. Demnach ist ein Umwelt-Management-System (z.B. nach EMAS / ISO 14001) als ein (Bestandteil eines) Umwelt-Compliance-Programm(s) zu verstehen, ein Social Supply Chain-Programm (z.B. nach SA 8000) als ein (Bestandteil eines) Compliance-Programm(s) für die Sicherstellung der Wahrung von Menschenrechten, Arbeits- und Sozialstandards und ein Anti-Bribery-Compliance-Programm als (ein Bestandteil) eines Compliance-Programm(s) zur Sicherstellung des Wohlverhaltens im Geschäftsverkehr (Business Conduct Compliance-Programm).

Diese vorgenommene Abgrenzung von Compliance-Programmen innerhalb des unternehmens- bzw. organisationsbezogenen Compliance Managements stellt lediglich eine Möglichkeit dar. In der Praxis wird die Abgrenzung selbstverständlich häufig anders und entlang organisationspezifischer Erfordernisse gezogen. Darüber hinaus sind einzelne Elemente von Compliance-Programmen, wie z.B. der notwendige „Tone from the Top“ (Commitment, Vorbildverhalten etc. des Managements) und andere Elemente im Bereich der Führung und Organisation themenübergreifend organisiert.

Der *ComplianceProgramMonitor<sup>ZfW</sup>* bezieht sich ausschließlich auf das Feld der Business Conduct Compliance.

Wesentliche Internationale  
Compliance Management Standards

Die im Folgenden aufgeführten Gesetze, Konventionen und Standards sollen eine Orientierung dafür liefern, welche materiellen und prozessualen Normen, i.S. verpflichtender gesetzlicher Regelungen und freiwilliger Best-Practice-Standards im Bereich Business Conduct Compliance, für ein Unternehmen bestehen können. Die Aufzählung ist nicht abschließend; weitere Gesetze, Branchenstandards und andere freiwillige Maßstäbe können maßgebend sein, so z.B. stets die spezifischen Gesetze zur Bekämpfung von Korruption und kartellrechtswidrigen Absprachen in den Ländern, in denen ein Unternehmen tätig ist. Andererseits sind nicht zwingend alle genannten Gesetze, Konventionen und Standards für ein bestimmtes Unternehmen relevant. Insofern ist sowohl für die Entwicklung als auch für die interne oder externe Überprüfung eines Compliance-Programms im Bereich Business Conduct immer eine Analyse der anwendbaren gesetzlichen und freiwilligen Standards durchzuführen.

Gesetze und Konventionen (Auszug)

- Korruptionsgesetze
- Einschlägige Strafbestimmungen (Betrug einschließlich Ausschreibungsbetrug, Erpressung, Insiderhandelsverbot, Geldwäsche, Untreue, Urkundenfälschung, Geheimnisverrat etc.)
- EU-Bestechungsgesetz (EuBestG)
- OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions
- Foreign Corrupt Practices Act (FCPA)
- UN-Konvention gegen Korruption (UNCAC)
- Gesetz gegen Wettbewerbsbeschränkungen
- Deutscher Corporate Governance Kodex
- OECD-Leitsätze für multinationale Unternehmen
- UN Global Compact
- ICC Rules of Conduct and Recommendations on Combating Extortion and Bribery
- World Economic Forum, Partnering Against Corruption Initiative (PACI): Principles for Countering Bribery
- Transparency International/Social Accountability International: Business Principles for Countering Bribery
- Transparency International. A-B-C der Korruptionsprävention und Checkliste für „Self-Audits“ zur Korruptionsprävention in Unternehmen
- World Bank, Department of Institutional Integrity: Voluntary Disclosure Program, Protocol 7, II. „Guidance in Revising and Improving the Compliance Program“
- European Bank for Reconstruction and Development (EBRD): „Fraud and corruption – definitions and guidelines for private sector operations“
- United States Sentencing Guidelines, § 8B2.1 „Effective Compliance and Ethics Program“
- Open Compliance and Ethics Group (OCEG): OCEG-Guidelines „Red Book“
- Committee of Sponsoring Organizations of the Treadway Commission (COSO): COSO Enterprise Risk Management Framework
- Australian Standard (AS) 8002-2003 – Organizational Codes of Conduct und Australian Standard (AS) 2860-2006 – Compliance Programs
- WerteManagementSystem<sup>ZfW</sup> des AfW – Anwenderrat für Wertemanagement
- EMB-Wertemanagement Bau

## C. ELEMENTE EINES BUSINESS CONDUCT COMPLIANCE-PROGRAMMS

Die folgenden Ausführungen sind an den o. g. Normen und Standards, dem WerteManagementSystem<sup>zfw</sup><sup>3</sup> sowie an der einschlägigen deutschen und internationalen Literatur zum Thema Business Conduct Compliance orientiert. Ihr Zweck ist die zusammenfassende Darstellung zu möglichen praktischen Anforderungen für die Implementierung und Umsetzung eines Business Conduct Compliance-Programms.

Die folgenden Ausführungen stellen keinen Mindeststandard dar. Das heißt, der Text dient nur der Einführung ins Thema und als „Guidance“ bei der Entwicklung, Implementierung und Umsetzung eines Compliance Systems. Gleichwohl sind die einzelnen Elemente (siehe Überschriften I bis IX dieses Abschnitts) notwendige Bestandteile.

<sup>3</sup> WerteManagementSystem<sup>zfw</sup> ist abrufbar unter [www.zfw-online.de](http://www.zfw-online.de).

## I. Leadership & Corporate Culture

Die Verantwortung für ein Business Conduct Compliance-Programm liegt bei der Unternehmensleitung. Sie ist insbesondere verantwortlich für eine kontinuierliche Kommunikation der Grundwerte des Unternehmens sowie der Verhaltensgrundsätze und -richtlinien (siehe II.) nach innen und nach außen, für das demonstrative Handeln entlang der kommunizierten Standards sowie für die Überwachung der Implementierung und Umsetzung des Business Conduct Compliance-Programms.

Die Ernsthaftigkeit und Glaubwürdigkeit eines Business Conduct Compliance-Programms kann nur erreicht werden, wenn die Implementierung, Umsetzung und öffentliche Kommunikation zur „Chefsache“ gemacht wird. Die kontinuierliche Selbstverpflichtung der Unternehmensleitung auf die Grundwerte des Unternehmens und das Business Conduct Compliance-Programm belegen erst deren Ernsthaftigkeit und erzeugen dadurch Handlungsfähigkeit und Erwartungssicherheit bei den Mitarbeitern. Hierbei ist entscheidend, unmissverständlich klarzustellen, dass die Beachtung der Grundwerte und des Business Conduct Compliance-Programms Firmenpolitik ist und abweichendes Verhalten weder stillschweigend erwartet noch geduldet wird. Die Überwachung der Implementierung und Umsetzung trägt darüber hinaus zur Glaubwürdigkeit des Business Conduct Compliance-Programms bei den Geschäftspartnern und weiteren Stakeholdern des Unternehmens bei.

Leadership und Corporate Culture dienen im Rahmen eines Business Conduct Compliance-Programms auch der Entwicklung und Förderung einer spezifischen Unternehmensidentität und erzeugen für alle Beschäftigten erst die notwendige Handlungsorientierung und -sicherheit für schwierige Entscheidungen im unternehmerischen Alltag. Dieser hohe Anspruch kann praktisch dann eingelöst werden, wenn moralische Werte (z.B. Integrität, Fairness, Ehrlichkeit, Vertragstreue, Verantwortung), Kooperationswerte (z.B. Loyalität, Teamgeist, Konfliktfähigkeit, Offenheit), Leistungswerte (z.B. Nutzen, Kompetenz, Leistungsbereitschaft, Flexibilität, Kreativität, Innovationsorientierung, Qualität) und Kommunikationswerte (z.B. Achtung, Zugehörigkeit, Offenheit, Transparenz, Verständigung) konsistent aufeinander abgestimmt sind und sich an der Unternehmensrealität orientieren. Die Un-

ternehmenswerte dürfen sich weder wechselseitig widersprechen, noch dürfen den Stakeholdern damit – sozusagen an der Realität des Geschäftsalltags vorbei – nicht einlösbare Versprechen gegeben werden. So können die Grundwerte eines Unternehmens Führungskräften, Mitarbeitern und unternehmensexternen Stakeholdern gegenüber glaubwürdig kommuniziert werden.

Im Rahmen der Entwicklung einer von Integrität geprägten Unternehmenskultur müssen Führungskräfte und Mitarbeiter die Kompetenz entwickeln, wertesensible Problemstellungen selbst zu erkennen und abzuarbeiten. Die beteiligten Personen müssen hierfür gewonnen werden, ihr Verhalten und das ihrer jeweiligen Unternehmenseinheit dauerhaft compliancegerecht auszurichten. Denn die nachhaltige Wirksamkeit des Business Conduct Compliance-Programms kann nur durch die verbindliche Verpflichtung des Top-Managements, der Führungskräfte und Mitarbeiter gelingen. Ein Business Conduct Compliance-Programm muss ein Prozess des Unternehmens sein, der hohe Priorität und permanente Aufmerksamkeit in der Organisation genießt. Dies erfordert etwa, dass bei einer internen oder externen Implementierungsunterstützung auf das Konzept des Coachings zurückgegriffen wird, um bei allen Mitarbeitern und ihren jeweiligen Unternehmenseinheiten korrektes Verhalten zu gewährleisten bzw. hierauf gerichtete Verhaltensänderungen entlang der Grundwerte und der Verhaltensgrundsätze und -richtlinien zu erzeugen. Nur so ist eine nachhaltige Wirksamkeit zu erzeugen und abzugrenzen gegen kurzfristigen Aktionismus oder Delegation in professionelle Kontexte.

Persönliches Vorbildverhalten und Engagement auf allen Ebenen der Führung einer Organisation sind Voraussetzung für den Erfolg eines Business Conduct Compliance-Programms. Gleiches gilt für die Befähigung und Sicherstellung autonomer Entscheidungskompetenz von Mitarbeitern in ethischen Konfliktsituationen, zu denen keine expliziten Verhaltensgrundsätze und -richtlinien existieren. Dies trägt dem Umstand Rechnung, dass es nicht für jede denkbare Situation im Organisationsalltag konkrete Verhaltens- und Verfahrensgrundsätze geben kann.

## II. Verhaltensgrundsätze und Verhaltensrichtlinien

Das Unternehmen muss schriftlich niedergelegte Verhaltensgrundsätze und Verhaltensrichtlinien schaffen, die Unternehmenswerte definieren und die gewünschte Geschäftsethik festlegen. Ziel solcher Verhaltensgrundsätze und Verhaltensrichtlinien ist in erster Linie, kriminelle und unethische Handlungen im Geschäftsverkehr, insbesondere die Verletzung von Wettbewerbs- und Anti-Korruptionsgesetzen, zu vermeiden. Über die eindeutige Untersagung von unethischen oder dolosen Handlungen hinaus können Verhaltensgrundsätze jedoch auch Erwartungen hinsichtlich positiver Handlungsweisen der Mitarbeiter formulieren (beispielsweise bezüglich Innovation). Die Schaffung von Verhaltensgrundsätzen und Verhaltensrichtlinien bedeutet, dass das Unternehmen eine Grundwerteerklärung, einen Code of Ethics o. ä. erstellen soll. Die Kodifizierung soll die leitenden Werte des Unternehmens in Bezug auf die wichtigsten Interessengruppen fixieren. Dieses Wertemanagement ist sodann in die spezifische Geschäftsstrategie des Unternehmens einzubetten. Die Geschäftsgrundsätze und Verhaltensregeln müssen für alle Mitarbeiter und Geschäftspartner dauerhaft zugänglich sein. Darüber hinaus sollen die Angestellten auf die Einhaltung der Gesetze gesondert und explizit hingewiesen werden. Dies gilt umso mehr, da nicht jeder Mitarbeiter die aktuelle Gesetzeslage kennt und dieser dementsprechend konform handeln kann.

Die Art und Weise der textlichen Niederlegung von Compliance-Regeln ist nicht bestimmt. Möglich sind Arbeitsanweisungen, Richtlinien, Leitfäden, Merkblätter oder Handbücher. Im Rahmen der textlichen Niederlegung muss jedoch sichergestellt sein, dass die Compliance-Regeln den Mitarbeitern bekannt sind. Das bloße Einstellen der Regeln, Verhaltensgrundsätze und Verhaltensrichtlinien in eine Datenbank im Intranet des Unternehmens o. ä. ist demnach nur ausreichend, wenn hierauf unternehmensweit und nachhaltig hingewiesen wird.

Für Business Conduct Compliance-Programme sind regelmäßig die folgenden Gegenstandsbereiche typisch, die im Rahmen der Verhaltensgrundsätze (Code of Conduct) und/oder in Verhaltensrichtlinien, Arbeits- und Geschäftsprozessanweisungen o. ä. geregelt werden:

- Einhaltung der Gesetze, Rechtstreue,
- Korruptionsverbot und Verbot kartellrechtswidriger Absprachen,
- Einhaltung der Menschenrechte, Arbeits- und Sozialstandards sowie Verbot von Diskriminierung, Belästigung am Arbeitsplatz etc.,
- Sicherstellung der Einhaltung der Gesetze und der Geschäftsethik im Umgang mit Auftraggebern und Vertriebsintermediären,
- Sicherstellung der Einhaltung der Gesetze und der Geschäftsethik im Umgang mit Lieferanten und Subunternehmen,
- Annahme und Vergabe von Geschenken, Einladungen zu Bewirtungen und sonstiger Vorteile,
- Umgang mit Interessenkonflikten (Sicherstellung der Trennung und dem Vorrang der Unternehmensinteressen von/vor privaten Interessen),
- Umgang mit Spenden, gemeinnützigem Engagement und Sponsoring,
- Verbot von Insiderhandel,
- Vermögensschutz des Unternehmens (einschließlich Umgang mit Informationen und Schutz von Intellectual Property), Nebentätigkeiten, Schutz des Vermögens von Geschäftspartnern.

### III. Implementierung

Das Unternehmen soll die Zielgruppe einer jeden Richtlinie und Maßnahme bestimmen. Es soll – wenn nötig über Pilot-Tests und ähnliche Maßnahmen – sicherstellen, dass diese verständlich und anwendbar sind. Die richtige Anwendung der Verhaltensgrundsätze und -richtlinien, der Implementierung in die Managementprozesse sowie der zugehörigen Prozesskontrollen sollte fortlaufend belegt werden können. Ebenso sollen Bestätigungen von relevanten Unternehmenseinheiten (Management) und Mitarbeitern eingeholt werden hinsichtlich Erhalt und Verständnis der Richtlinien, Maßnahmen und Kontrollen sowie eine Beratungsstelle für etwaige Rückfragen zu ihrer praktischen Anwendung eingerichtet werden.

Darüber hinaus sollen Maßnahmen ergriffen werden, die wertekonformes und vorbildliches Verhalten anerkennen und fördern sowie werteverletzendes Handeln, insbesondere schwerwiegendes Fehlverhalten im Geschäftsverkehr sanktionieren. Dies kann durch Dienstanweisungen bzw. Führungskräfte- und Mitarbeiterbeurteilungssysteme sowie wertesensible Anreiz- und Kompensationssysteme erfolgen.

Das Unternehmen soll klar definierte, transparente Kriterien und Verfahren bei Rekrutierung, Stellenbesetzung und Beförderung nutzen. Es dürfen keine Personen in Schlüsselfunktionen eingestellt werden, die bereits kriminelle Handlungen vorgenommen haben oder wegen schwerwiegenden Fehlverhaltens aufgefallen sind. Das Unternehmen soll ferner die Einhaltung der Grundwerte und der Verhaltensstandards als eine Bewertungsgrundlage in die Leistungsbewertung, Kompensationssysteme und Boni-Regelungen integrieren oder diese an die Compliance-Ziele anpassen. Damit kann verhindert werden, dass Unternehmenseinheiten (Management) und Mitarbeiter Umsatz- und Gewinnziele mit nicht regel- bzw. rechtskonformen Mitteln erstreben bzw. erlangen.

Des Weiteren sollte in Arbeitsverträgen die Verpflichtung zur Einhaltung von Gesetzen und insbesondere ein Korruptionsverbot enthalten sein. Außerdem empfiehlt es sich, eine Regelung für Nebentätigkeiten und Interessenkonflikte im Arbeitsvertrag zu treffen.

### IV. Verantwortung und Organisation

Persönliches Vorbildverhalten und Engagement für das Thema Compliance auf allen Ebenen der Führung eines Unternehmens sind Voraussetzung für den Erfolg ethischer Verhaltensgrundsätze und -richtlinien. Die Verantwortung für Compliance trägt das Management des Unternehmens. Das Unternehmen soll Personen bestimmen, die die Verantwortung für die Entwicklung und Gestaltung des Compliance-Programms übernehmen und das Management bei der Implementierung und Durchsetzung der Unternehmensstandards unterstützen. Hierfür sollen sie mit adäquaten Ressourcen und angemessenen Befugnissen ausgestattet werden. Bei mehrköpfigen Unternehmensleitungen kann es zweckmäßig sein, die Verantwortung für das Compliance-Programm einem Ressort zuzuweisen. Das zuständige Mitglied der Unternehmensleitung kann die vorgenannte Verantwortung für die Gestaltung und Begleitung eines Compliance-Programms delegieren, sowohl an eine bereits vorhandene Stelle als auch an einen oder mehrere dafür benannte Compliance-Beauftragte. Darüber hinaus hat sich in größeren Unternehmen bewährt, diejenigen Funktionen in einem Lenkungskreis Compliance zu involvieren, die für wichtige Aktivitäten und Prozesse im Rahmen eines Compliance-Programms Verantwortung tragen (z.B. Compliance, Recht, Revision, HR, Controlling, Vertrieb, Einkauf, Sicherheit). Dieser Lenkungskreis kann u. a. die Aufgabe haben, das Management bei der umfassenden und widerspruchsfreien Umsetzung des Compliance-Programms zu unterstützen und bei Verdachtsfällen von Compliance- Verstößen tätig zu werden. Über die Bestellung von Verantwortlichen hinaus sollte es im Unternehmen Regelungen geben, wie Mitarbeiter als „Hinweisgeber“ bei entdeckten oder vermuteten Verstößen gegen gesetzliche und/oder betriebsinterne Regeln aktiv werden können (z.B. anonyme Hotline, Ombudsleute). Es muss dabei sichergestellt werden, dass die Mitarbeiter wissen, wie und wo sie Fehlverhalten melden können. Ebenso muss dabei sichergestellt sein, dass Mitarbeiter, ohne Furcht vor negativen Folgen und ohne auf den hierarchischen Kommunikationsweg angewiesen zu sein, den Verdacht krimineller Handlungen melden können. Darüber hinaus können vorhandene institutionalisierte Unternehmensfunktionen für Mitarbeiter (z.B. Rechts- oder Personalabteilung) in ethischen Dilemmasituationen zur Nutzung (ggf. anonym) angeboten werden.

## V. Kommunikation und Schulung

Das Unternehmen muss angemessene Maßnahmen ergreifen, um regelmäßig seine Verhaltensstandards und Verhaltensrichtlinien in Schulungen zu vermitteln. Schulungsmaßnahmen sind eine der wesentlichsten Einrichtungen eines funktionierenden Compliance-Programms.

Das Unternehmen muss dafür Sorge tragen, dass die relevante Zielgruppe an den Schulungen teilnimmt und die vorgesehenen Lernziele praxisgerecht vermittelt werden, so dass die Mitarbeiter das erlangte Wissen anschließend auf ihre Tätigkeiten anzuwenden vermögen. Solche Verhaltenstrainings können insbesondere auch Fallstudien einbeziehen, die etwa auf ethischen Dilemmasituationen aus dem Geschäftsalltag aufbauen. Die Schulungen sind für die Angestellten in sensiblen Funktionen (z.B. Vertrieb, Einkauf) besonders wichtig, sollten aber – zumindest nach und nach – auf alle Unternehmensangehörigen (einschließlich der Unternehmensleitung) ausgedehnt werden. Darüber hinaus ist es für bestimmte Unternehmen sinnvoll bzw. notwendig, auch Handelsvertreter, Vertriebsagenten sowie Berater und Subunternehmer über die Compliance-Regeln zu informieren bzw. Informations- oder Schulungsveranstaltungen durchzuführen.

Für die interne Kommunikation ist es eine bewährte Maßnahme, die Kenntnisnahme der Compliance-Regeln durch die entsprechende schriftliche Erklärung von den relevanten Mitarbeitern (Unternehmensleitung, Führungskräfte und Angestellten in compliancesensiblen Funktionen) bestätigen zu lassen („Compliance-Erklärung“). Für die Auswahl der „relevanten Mitarbeiter“ sind alle Unternehmensstandorte einzubeziehen.

Darüber hinaus ist sicherzustellen, dass die interne Kommunikation von Seiten der Unternehmensleitung und der Compliance-Abteilung bzw. des Compliance-Beauftragten kontinuierlich und fortlaufend, d. h. nicht nur über die Phase der Einführung eines Compliance-Programms, erfolgt. Dazu können neben den regelmäßigen schriftlichen Erklärungen über die Kenntnisnahme und Einhaltung der Compliance-Regeln sowie den Compliance-Schulungen auch z.B. Mitarbeiterbefragungen genutzt werden, mittels derer die Wahrnehmung der Belegschaft über den Stand und die Entwicklung der Corporate Compliance/ Corporate Integrity erhoben werden kann. Aus diesen Erhebungen können ggf. weitere Maßnahmen zur Verbesserung des Compliance-Programms abgeleitet werden.

## VI. Risikobeurteilung und Kontrolle

In den Best-Practice-Standards und der einschlägigen Literatur zur Business Conduct Compliance besteht Einigkeit darin, dass in unregelmäßigen Abständen Kontrollen stattfinden müssen. Eine Aussage darüber, wie die Kontrollen auszugestaltet sind und welche Kontrollmaßnahmen notwendig, ausreichend und zumutbar sind, wurde gerichtlich bislang nicht getroffen. Dies bietet den Vorteil, flexibel auf die Erfordernisse des Unternehmens und seines Geschäftes eingehen zu können. Kontrollen erfüllen hierbei immer eine präventive und eine aufdeckende Funktion. Ihre Ankündigung und Durchführung erhöht die Wahrscheinlichkeit der Entdeckung von Compliance-Verstößen und soll hierdurch gleichzeitig abschreckend, d.h. präventiv, wirken.

Das Unternehmen muss hierzu die relevanten bestehenden Geschäftsprozesse, etwa in Vertrieb und Beschaffung, sowie entsprechende Kontrollen, wie beispielsweise bestehende Unterschriftenregelungen, im Hinblick darauf überprüfen, ob sie regelkonformes Verhalten fördern oder aber Übertretungen Vorschub leisten bzw. erleichtern und ob eingerichtete Kontrollen auch tatsächlich wirksam sind. Wichtig erscheinen regelmäßige Risikobeurteilungen in allen Geschäftsbereichen und relevanten zentralen Abteilungen hinsichtlich möglicher Korruptionsstraftaten, kartellrechtswidriger Absprachen und anderer für das Unternehmen bedeutsamer Gegenstandsbereiche der Compliance (z.B. Arbeits- und Sozialstandards in der Wertschöpfungskette). Die EDV-Systeme des Unternehmens haben sicherzustellen, dass ein Zugriff unberechtigter Dritter ausgeschlossen werden kann und eine mögliche Datenmanipulation jederzeit nachvollziehbar ist (durch Logfiles, Protokollierung und Kontrolle aller Transaktionen – insbesondere in der Finanzbuchhaltung). Es soll eine systematische Anwendung des Vier-Augen-Prinzips bei der Durchführung sensibler Funktionen z.B. bei Zahlungsfreigabe (oder alternative Kontrollen) erfolgen. Das Unternehmen soll eine regelmäßige Kontrolle mit dem Ziel durchführen, dass alle am Geldverkehr beteiligten Mitarbeiter nach den gültigen Grundsätzen ordnungsgemäßer Buchführung (GoB) verfahren.

Das Führungsgremium eines Unternehmens hat zusätzlich zur pflichtmäßigen Sicherstellung der Funktionsfähigkeit der geschäftsprozessorientierten Compliance-Kontrollen die Aufgabe, das Compliance-Programm einer regelmäßigen Bewertung mit Blick auf seine Effektivität und Effizienz zu unterziehen. Dies dient der Qualitätssicherung und der Sicherstellung der Anpassungsfähigkeit an veränderte Rahmenbedingungen (z.B. Mergers & Acquisitions). Diese Bewertung sollte jährlich erfolgen. Ferner sollte das Unternehmen mindestens einmal in fünf Jahren das Compliance-Programm überprüfen. Hierbei sind auch die Vereinbarungen und Verträge mit Agenten, Handelsvertretern, Sub- und Tochterunternehmen in die Prüfung mit einzubeziehen.

## VII. Integration in HR-Prozesse

Das Unternehmen muss sicherstellen, dass es keine Personen, die in der Vergangenheit innerhalb oder außerhalb des Unternehmens durch kriminelle Handlungen oder sonstige Verstöße gegen Compliance-Programme aufgefallen sind, in verantwortungsvolle Positionen befördert oder einstellt. Es muss sicherstellen, dass keine Ermessensentscheidungen an Personen delegiert werden, bei denen die Begehung von dolosen Handlungen bekannt ist. Im Falle der Aufdeckung von kriminellen Handlungen hat das Unternehmen angemessen zu reagieren. Beim Vorliegen von Verstößen gegen Gesetze oder gegen das Compliance-Programm müssen angemessene Disziplinarmaßnahmen ergriffen werden. Dies umfasst auch Disziplinarmaßnahmen gegen Mitarbeiter, die für die Nicht-Aufdeckung von Verstößen verantwortlich sind. Möglich sind Maßnahmen, die von der Ermahnung bis zur außerordentlichen Kündigung reichen. Wichtig ist aber, die Ernsthaftigkeit und den Willen zur Umsetzung eines Compliance-Programms zu zeigen. Das Unternehmen wird auch nach den unternommenen Schritten im Falle eines Verstoßes beurteilt.

Wenige Unternehmen haben bislang für Mitarbeiter (nicht für Angehörige der Unternehmensleitung) so genannte „Amnestie-Programme“ (Kronzeugenregelung) aufgelegt. Dabei verzichtet das Unternehmen auf Schadensersatzansprüche und die Kündigung des Arbeitsverhältnisses, wenn Mitarbeiter, die gegen Compliance-Regeln verstoßen haben, sich selbst anzeigen. Die Sinnhaftigkeit eines solchen Programms kann nur anhand der Gegebenheiten des Einzelfalls beurteilt werden.

Darüber hinaus sollten auch positive Anreize für die Einhaltung des Business Conduct Compliance-Programms bzw. für dessen erfolgreiche Implementierung im Verantwortungs- und Einflussbereich von Managern gesetzt werden. Im Rahmen des Zielvereinbarungs- und Leistungsbewertungsprozesses von Führungskräften sollten Ziele enthalten sein, die sich auf die Grundwerte des Unternehmens und das Business Conduct Compliance-Programm beziehen. Das Unternehmen soll ferner die Einhaltung der Grundwerte und der Verhaltensstandards als eine Bewertungsgrundlage in die Leistungsbewertung und die Kompensationssysteme integrieren.

## VIII. Vertreter, Agenten und Subunternehmer

Die Einschaltung von Agenten, Beratern und Handelsvertretern, die Geschäfte (insbesondere im Ausland) entwickeln und dort Lobbyarbeit vornehmen, muss detailliert geprüft werden (so genannte „Third-Party Due Diligence“). Das Gleiche gilt für die Einschaltung von Subunternehmern. Dabei ist auch die Einhaltung der Gesetze und des Compliance-Programms sowie die Angemessenheit der Auswahl der einzelnen Geschäftspartner im Ausland zu beurteilen. Bei Abschluss von Verträgen ist darauf zu achten, dass sie Erklärungen beinhalten, wonach die Vertragspartner keine Amtsträger oder ähnliche Personen zur Erlangung irgendwelcher Vorteile geschäftlicher oder finanzieller Natur bestochen haben oder bestochen werden. Eine entsprechende Erklärung ist auch bei dem Eingehen von Joint-Ventures notwendig. Die Einhaltung des Verbots ist zu überprüfen.

Es müssen Maßnahmen getroffen werden, die sicherstellen, dass das Compliance-Programm allen Vertretern und Agenten bekannt ist, und es muss klargestellt werden, dass das Unternehmen erwartet, dass alle Handlungen, die in seinem Namen vorgenommen werden, mit dem bestehenden Compliance-Programm vereinbar sind.

Das Unternehmen soll die Vergütungen und Provisionen an Vertreter oder Agenten ihrer Gesellschaften im Inland- und Ausland dahingehend überprüfen, ob diese angemessen und vertretbar sind. Auch die Vertreter und Agenten sollen auf die Einhaltung der hausinternen Richtlinien und Verhaltensregeln verpflichtet und kontrolliert werden.

Nebentätigkeiten von Mitarbeitern sind geregelt und genehmigungspflichtig (insbesondere in Unternehmen, die für sie Wettbewerber, Kunden oder Lieferanten darstellen). Organtätigkeiten sind ausdrücklich verboten bzw. geregelt und genehmigungspflichtig. Der Erwerb von eigenen Unternehmensanteilen/-optionsscheinen zu besonderen Konditionen sowie die Gewährung und Vergabe von Krediten an Mitarbeiter, Geschäftspartner und Tochter- und Beteiligungsunternehmen sind klar geregelt.

Jegliche organisatorische und/oder finanzielle Neugründung, Änderung oder Löschung von Tochter-, Beteiligungs- oder Treuhandgesellschaften im In- und Ausland ist unternehmensweit klar geregelt und genehmigungspflichtig (Geschäftszweck, Geschäftsführung, Aufsichtsorgane, Kapitalausstattung, Eigentumsverhältnisse, etc.). Aktivitäten in Ländern, die als besonders korruptionsanfällig gelten (beispielsweise gemäß TI-Ranking zum Corruption Perceptions Index) unterliegen einer besonderen Aufsicht und Kontrolle.

Das Unternehmen hat seine Beschaffungsprozesse (mit Erstellung von Leistungsverzeichnissen, Ausschreibungen, Vergaben, Reklamationen und Zahlungsabwicklung) transparent und jederzeit nachvollziehbar zu regeln, auch für sachkundige Dritte.

## IX. Transparenz und Dokumentation

Zahlungsvorgänge insbesondere für Geschenke, Bewirtungen, Spenden, Bareinkäufe, Provisionen sowie Berater- und Treuhandleistungen sollten grundsätzlich einer besonderen inhaltlichen Kontrolle unterliegen. Darüber hinaus sollten die Dokumentationsanforderungen für die Geschäftsvorfälle und Zahlungen festgelegt sein und deren Einhaltung regelmäßig, z.B. im Rahmen interner Revisionen, überprüft werden. Spenden für politische oder gemeinnützige Zwecke und Sponsoring-Leistungen jeder Art sollten sorgfältig geprüft werden, einem Freigabeprozess unterliegen und ebenfalls angemessen dokumentiert werden. Zur Gewährung und Annahme von Geschenken, Bewirtungen und sonstigen Vorteilen für alle Mitarbeiter im In- und Ausland existieren klare Regeln. Interne Kostenbudgets für allgemeine soziale/gesellschaftliche Zwecke werden regelmäßig überprüft (z.B. Betriebssportverein, Fördervereine, Stiftungen, Betriebsrat).

### I. Compliance-Monitoring und Compliance-Audit

Ein Compliance Audit, hier die Überprüfung der Funktionsfähigkeit des Business Conduct Compliance-Programms, kann sowohl intern (z.B. durch die interne Revision) als auch extern (z.B. durch geeignete Beratungs- oder Wirtschaftsprüfungsgesellschaften) erfolgen. Der Begriff Audit soll im Rahmen dieses Leitfadens für die Fälle reserviert sein, in denen ein Compliance-Programm bereits vorhanden ist, d. h. eine Implementierung abgeschlossen ist. Das bedeutet nicht, dass bereits alle Compliance-Maßnahmen implementiert und umgesetzt sein müssen, die unter den Gesichtspunkten von Best-Practice und Angemessenheit für das Unternehmen notwendig sind. Es bedeutet lediglich, dass der interne oder externe Auditor bzw. das interne oder externe Audit-Team seine Aufgabe nach einem erfolgten Implementierungsprozess ausführt.

Dahingegen soll mit Compliance Monitoring gemeint sein, dass der externe, unabhängige und objektive Compliance Monitor seine Aufgabe im Zuge der Implementierung des Compliance-Programms im Sinne einer prozessbegleitenden Prüfung wahrnimmt. Er agiert in diesem Zusammenhang ausdrücklich nicht als Berater oder Trainer, d. h. er trifft keine Entscheidungen hinsichtlich notwendiger Compliance-Maßnahmen oder gestaltet deren Implementierung und Umsetzung. Dagegen coacht er die Unternehmensleitung, die internen Compliance-Verantwortlichen (Compliance-Beauftragter, Compliance Committee etc.) und etwaige interne und externe Berater entlang von Best-Practice-Standards. Ein Best-Practice-Standard stellt beispielsweise die Gesamtheit der in der Compliance Checkliste (siehe D. III.) genannten Anforderungen dar.

Compliance Monitoring kommt u. a. dann zur Anwendung, wenn private und insbesondere öffentliche Auftraggeber oder Finanzierungsinstitute (z.B. Weltbank, Europäische Bank für Wiederaufbau und Entwicklung) die Einrichtung oder Erneuerung/ Verbesserung eines Compliance Systems von einem Unternehmen verlangen. Der unabhängige Compliance Monitor berichtet in diesem Falle während der Entwicklung und Implementierung über die Fortschritte und den Status und erstellt einen Abschlussbericht nach erfolgter Einrichtung des Compliance Systems.

In den folgenden Abschnitten wird der Begriff Compliance Monitoring auch für eine Compliance-Programm-Implementierung nachgelagerte Überprüfungsverfahren des Compliance Audits verwendet. Dies soll der besseren Lesbarkeit dienen.

Umfang und Dauer eines Compliance Monitorings können nicht allgemeingültig definiert, sondern nur für den Einzelfall vom Compliance Monitor festgelegt werden. In jedem Falle sind die Unternehmensgröße (Umsatz, Anzahl der Mitarbeiter), die Komplexität der Organisation und das Geschäftsmodell wesentliche Kriterien für die Festlegung des Umfangs und der Dauer des Compliance Monitorings. Hinzu kommen ggf. Vorgaben externer Standards, die für das Compliance System zu beachten sind.

## II. Umfang und Dauer

Grundsätzlich sind die folgenden Kriterien in die Planung des Umfangs und der Dauer des Compliance Monitorings einzubeziehen (nicht abschließende Aufzählung):

- Umsatz
- Anzahl der Mitarbeiter; Anzahl der vom Compliance System direkt betroffenen Mitarbeiter (z.B. Mitarbeiter in sensiblen Unternehmensbereichen bzw. Funktionen)
- Branche
- Geschäftsmodell, z.B. bzgl. Vertriebswegen
- Grad der Internationalisierung/Anteil Auslandsgeschäft/Geschäftstätigkeit in Ländern mit erhöhtem Risiko zur Non-Compliance
- Generische Risikoexposition hinsichtlich Compliance-Verstößen (z.B. Korruptionsrisiko)
- Komplexität der Organisationsstruktur
- Dezentrale Entscheidungsbefugnisse/Möglichkeiten zentraler Kontrolle
- Fehlverhalten/Straftaten in der Vergangenheit
- Aussage des Compliance Monitors („reasonable Assurance“ oder „negative Assurance“)

### III. Prüfungsziel und Prüfungsgegenstand

Ein grundlegendes Ziel des Compliance Monitorings ist die Feststellung, ob das Compliance-Programm eines Unternehmens (oder einer anderen Organisation) die Elemente aufweist, die allgemein für erforderlich gehalten werden, um das Unternehmen oder die Organisation angemessen vor Gesetzesverstößen durch Manager, Mitarbeitende oder Geschäftspartner zu schützen.

Voraussetzung hierfür ist die Feststellung, dass die für das jeweilige Unternehmen (die jeweilige Organisation) erforderlichen Compliance-Maßnahmen getroffen sind, das Compliance-Programm insgesamt in die Prozesse des Geschäftsalltags integriert ist sowie das Leben der Unternehmenswerte und Unternehmenskultur unterstützt und damit geeignet ist, Straftaten zu vermeiden, aufzudecken oder zu erschweren.

Gegenstand des Compliance Monitorings ist grundsätzlich die Überprüfung, ob das Unternehmen ein Business Conduct Compliance-Programm entwickelt und angemessen gestaltet hat (i.), funktionsfähig implementiert hat (ii.) sowie im Unternehmensalltag umsetzt bzw. anwendet (iii.).

i. Hinsichtlich der **Ausgestaltung des Compliance-Programms** wird überprüft, ob

— alle für das Unternehmen relevanten **Referenzstandards berücksichtigt** wurden und

— die getroffenen **Compliance-Maßnahmen** für die Organisation **angemessen ausgestaltet** sind (Design Check). Die Angemessenheit bemisst sich an den ggf. weiteren vom Monitor festzulegenden Kriterien („Professional Judgment“).

ii. Bezüglich der **Implementierung bzw. Einrichtung des Compliance-Programms** wird überprüft, ob

— die zur Erfüllung der Angemessenheit notwendigen **Elemente des Compliance Management Systems** grundsätzlich **funktionsfähig** sind (Functionality Check). Das heißt, eine Compliance-Maßnahme muss zur Erfüllung des Status „implementiert“ verabschiedet und in Kraft getreten sein, alle zugehörigen Instrumente (Formulare, technischen Systeme etc.) müssen vorhanden sein, und die Compliance-Maßnahme muss den ihr zgedachten Zweck, das definierte Ziel erfüllen können.

Während die Prüfung der Ausgestaltung des Compliance Systems auf die Struktur abzielt, ist die Implementierungsprüfung somit auf die Realisierbarkeit und Funktionsfähigkeit dieses Programms gerichtet.

iii. Bezüglich der **Umsetzung des Compliance Systems** wird überprüft, ob

— die **Elemente des Compliance Management Systems** im Geschäftsalltag angewendet werden (Effectiveness Check). Dazu muss die geprüfte Compliance-Maßnahme bereits (mindestens einmal) ausgeführt worden sein.

Bei der Prüfung der wirksamen Umsetzung kommt es also darauf an, ob die Compliance-Maßnahme tatsächlich im Unternehmensalltag „gelebt“ wird.

Nicht für alle Compliance-Maßnahmen ist diese Umsetzungsprüfung möglich. Dann sollte dies mit „not applicable“ (n/a) in der Checkliste vermerkt werden. Zum Beispiel ist ein Code of Conduct nur hinsichtlich i. und ii. zu überprüfen, da im Rahmen eines Compliance Monitorings nicht überprüft werden kann und soll, ob sich Mitarbeiter an die inhaltlichen Vorgaben des Kodex halten. Demgegenüber ist die Integration von Compliance in Zielvereinbarungen und Leistungsbewertungen erst dann „effektiv“, wenn dieses Instrument einmal angewendet wurde, nicht, wenn dessen Planung abgeschlossen und das Prozedere vollständig beschrieben ist.

Compliance-Program-Checkliste  
(Business Conduct)

Compliance-Element	Phase	Compliance-Maßnahme	Ergebnis der Relevanzprüfung		Maßnahme ist:		
			relevant	nicht relevant	angemessen entwickelt	funktionsfähig	effektiv
I Verhaltensgrundsätze (Code of Ethics)	Entwicklung	1 Definition der Unternehmensziele und Unternehmenswerte	r	n	a	f	e
		2 Definition der Prinzipien der Geschäftsethik	r	n	a	f	e
		3 Benennung der wesentlichen Stakeholder	r	n	a	f	e
II Verhaltensrichtlinie (Code of Conduct)	Entwicklung	4 Identifikation der anzuwendenden Referenzstandards	r	n	a	f	e
		5 Einhaltung der Gesetze, Rechtstreue	r	n	a	f	e
		6 Korruptionsverbot (zero tolerance), Verbot kartellrechtlicher Absprachen	r	n	a	f	e
		7 Sicherstellung der Einhaltung der Gesetze und der Geschäftsethik im Umgang mit Auftraggebern und Vertriebsintermediären	r	n	a	f	e
		8 Sicherstellung der Einhaltung der Gesetze und der Geschäftsethik im Umgang mit Lieferanten und Subunternehmen	r	n	a	f	e

Compliance-Element	Phase	Compliance-Maßnahme	Ergebnis der Relevanzprüfung		Maßnahme ist:		
			relevant	nicht relevant	angemessen entwickelt	funktionsfähig	effektiv
		9 Annahme und Vergabe von Geschenken, Einladungen zu Bewirtungen und sonstiger Vorteile	r	n	a	f	e
		10 Umgang mit Interessenkonflikten (Sicherstellung der Trennung und dem Vorrang der Unternehmensinteressen vor privaten Interessen)	r	n	a	f	e
		11 Umgang mit Spenden, gemeinnützigem Engagement und Sponsoring	r	n	a	f	e
		12 Vermögensschutz des Unternehmens, Nebentätigkeiten, Schutz des Vermögens von Geschäftspartnern	r	n	a	f	e

Compliance-Element	Phase	Compliance-Maßnahme	Ergebnis der Relevanzprüfung		Maßnahme ist:		
			relevant	nicht relevant	angemessen entwickelt	funktionsfähig	effektiv
III Policies & Procedures	Entwicklung	13 Annahme und Vergabe von Geschenken	r	n	a	f	e
		14 Compliance-Erklärung für Führungskräfte, Mitarbeiter	r	n	a	f	e
		15 Compliance-Prüfung für Third Parties (Agenten, Berater, Handelsbeauftragte) in sensiblen Geschäftsfeldern und Ländern vor Beauftragung	r	n	a	f	e
		16 Compliance Agreement für Third Parties (Compliance-Erklärung, Lieferantenprüfung, Lieferantenbewertung)	r	n	a	f	e
		17 Lieferanten Compliance (z.B. Compliance-Erklärung, Lieferantenprüfung, Lieferantenbewertung)	r	n	a	f	e
		18 Sanktionen bei Complianceverstößen	r	n	a	f	e
IV Transparenz	Entwicklung	19 Risiko-Screening für sensible Geschäftsbereiche	r	n	a	f	e
		20 Kontrolle des Risikomanagements in sensiblen Geschäftsbereichen	r	n	a	f	e

Compliance-Element	Phase	Compliance-Maßnahme	Ergebnis der Relevanzprüfung		Maßnahme ist:		
			relevant	nicht relevant	angemessen entwickelt	funktionsfähig	effektiv
		21 Dokumentation sensibler Zahlungsvorgänge (z.B. Spenden, Provisionen)	r	n	a	f	e
		22 Sicherung der EDV-Systeme gegen Datenmanipulation	r	n	a	f	e
		23 Vier-Augen-Prinzip bei sensiblen Funktionen	r	n	a	f	e
		24 Kontrolle der Einhaltung der GoB	r	n	a	f	e
V Gelebte Führungs- und Unternehmenskultur	Implementierung	25 Compliance als Nachhaltigkeitsstrategie (legal, ökonomisch, ökologisch, gesellschaftlich)	r	n	a	f	e
		26 Orientierung an ethischen Werten	r	n	a	f	e
		27 Führungsstil: Entschlossenheit, Klarheit, Verbindlichkeit, Verantwortlichkeit, Integrität	r	n	a	f	e
		28 Selbstbindung, Selbstverpflichtung, Legalität	r	n	a	f	e
		29 Vorbildrolle und Führungsverantwortung für Compliance (Tone from the top)	r	n	a	f	e
		30 Proaktive und offensive Kommunikation des CMS durch Leitung und Management	r	n	a	f	e

Compliance-Element	Phase	Compliance-Maßnahme	Ergebnis der Relevanzprüfung		Maßnahme ist:		
			relevant	nicht relevant	angemessen entwickelt	funktionsfähig	effektiv
VI Kommunikation und Training	Implementierung	31 Interne Kommunikation (Meetings, Broschüren, Zeitschriften, Intranet-Plattform)	r	n	a	f	e
		32 Externe Kommunikation (z.B. Geschäftsberichte, Reporting, Broschüren)	r	n	a	f	e
		33 Schriftliche und mündliche Information/Beratung für Agenten, Lieferanten, Berater	r	n	a	f	e
		34 Mitgliedschaft und Engagement in Compliance-Initiativen und Erfahrungsaustausch	r	n	a	f	e
	Implementierung	35 Face to Face Training für obere Führungsebene und Funktionen mit erhöhtem Compliance-Risiko	r	n	a	f	e
		36 Funktions- und Risikogruppenspezifisches (z.B. Einkauf, Vertrieb, Lieferanten) Face to Face Training	r	n	a	f	e
		37 Trainingsinhalt sind Rechtsinformation plus im Schwerpunkt „real cases“	r	n	a	f	e
		38 Web- oder Intranet-basiertes Training für Mitarbeiter	r	n	a	f	e
VII Compliance in HR	Implementierung	39 Integritätsprüfung und Compliance-Erklärung für Mitarbeiter in Bereichen mit hohen Compliance-Risiken	r	n	a	f	e

Compliance-Element	Phase	Compliance-Maßnahme	Ergebnis der Relevanzprüfung		Maßnahme ist:		
			relevant	nicht relevant	angemessen entwickelt	funktionsfähig	effektiv
		40 Integration in Personal-auswahlprozesse	r	n	a	f	e
		41 Karriereplanung für Führung und Management	r	n	a	f	e
		42 Zielvereinbarungen in sensiblen Geschäftsbereichen	r	n	a	f	e
		43 Compliance-Risiken in Vergütungssystemen und Boni	r	n	a	f	e
		44 Angemessene Disziplinarmaßnahmen (Darstellung/ Androhung arbeits-, zivil- und strafrechtlicher Sanktionen)	r	n	a	f	e
VIII Compliance Organisation	Implemen-tierung	45 Top Management Verantwor-tung (Vorstand, Geschäfts-leitung)	r	n	a	f	e
		46 Lenkungskreis Compliance (z.B. Compliance, Recht, Revision, Vertrieb, HR)	r	n	a	f	e
		47 Compliance Office mit angemessenen Ressourcen	r	n	a	f	e
		48 Externer Compliance Monitor	r	n	a	f	e
		49 Hinweisgebersysteme	r	n	a	f	e

Compliance-Element	Phase	Compliance-Maßnahme	Ergebnis der Relevanzprüfung		Maßnahme ist:		
			relevant	nicht relevant	angemessen entwickelt	funktionsfähig	effektiv
IX Audit	Review	50 Interne Revision des CMS in sensiblen Geschäftsbereichen	r	n	a	f	e
		51 Kontrolle sensibler Zahlungsvorgänge (z.B. Spenden, Provisionen)	r	n	a	f	e
		52 Überprüfung der Einhaltung und der Implementierung des CMS in ein gelebtes Alltagsgeschäft	r	n	a	f	e
X Monitoring	Review	53 Regelmäßige Berichterstattung an und Erörterung im Top Management	r	n	a	f	e
		54 Selbstevaluierung von Geschäftsbereichen und Unternehmen	r	n	a	f	e
		55 Externes Monitoring der Entwicklung, Implementierung und Zweckangemessenheit (fit for purpose) des CMS durch Sachverständige und Prüfgesellschaften	r	n	a	f	e

## IV. Prüfungsmethoden und Beurteilung

### **Analyse der Dokumentation**

Im Rahmen des Compliance Monitorings führt der Compliance Monitor eine Analyse der vorhandenen Dokumentation des Compliance Systems durch. Alle für das Compliance System relevanten Compliance-Maßnahmen müssen dokumentiert sein und der Überprüfung unterzogen werden.

### **Durchführung von Interviews**

Der Compliance Monitor führt Interviews mit ausgewählten Personen aus dem Unternehmen durch. Typischerweise zählen hierzu immer Mitglieder der Unternehmensleitung sowie eine vom Monitor vorzunehmende Auswahl von Führungskräften. Darüber hinaus sollten Gespräche mit Mitarbeitern aus sensiblen Funktionsbereichen (z.B. Einkauf, Vertrieb) sowie mit zufällig ausgewählten Mitarbeitern des Unternehmens geführt werden.

### **Beurteilung**

Der Compliance Monitor verfasst einen Bericht und gibt darin eine Beurteilung zum Stand des Compliance Systems des Unternehmens ab. Die Beurteilung erfolgt hinsichtlich der Ausgestaltung, Implementierung und Umsetzung des Compliance Systems. Zu allen drei Dimensionen müssen qualifizierende Beurteilungen vorgenommen werden.

In der Beurteilung sind Aussagen über die thematische Grundausrichtung und die Ziele des Compliance Systems sowie über Stärken und Schwächen des Programms zu treffen. Darüber hinaus muss der Bericht Empfehlungen für die Weiterentwicklung und Verbesserung enthalten und ggf. über Auflagen informieren.

## AfW<sup>ZfW</sup> – Anwenderrat für Wertemanagement<sup>ZfW</sup>

Der AfW<sup>ZfW</sup> ist ein freiwilliger Zusammenschluss von Unternehmen und Verbänden, die Anwender und Multiplikatoren des WerteManagementSystem<sup>ZfW</sup> sind. Er hat sich die Förderung, Weiterentwicklung und Qualitätssicherung des WerteManagementSystem<sup>ZfW</sup> zum Ziel gesetzt. Durch seine Praxiskompetenz ist der Anwendungsbezug des WerteManagementSystem<sup>ZfW</sup> gesichert. Zudem bietet der Anwenderrat für die Mitglieder ein Forum für kontinuierlichen Erfahrungsaustausch und gegenseitige Beratung. Mitglieder im AfW<sup>ZfW</sup> sind derzeit:

- \_\_\_ ABB Deutschland AG,
- \_\_\_ Allianz SE,
- \_\_\_ BASF SE,
- \_\_\_ Bilfinger Berger Industrial Services GmbH,
- \_\_\_ Robert Bosch GmbH,
- \_\_\_ Daimler AG,
- \_\_\_ Deutsches Forum für Kriminalprävention e. V.,
- \_\_\_ Deutsche Post AG,
- \_\_\_ Deutsche Telekom AG,
- \_\_\_ EnBW Energie Baden-Württemberg AG,
- \_\_\_ Ethikmanagement der Bauwirtschaft e. V.,
- \_\_\_ Fraport AG,
- \_\_\_ Lahmeyer International GmbH,
- \_\_\_ Novartis Foundation for Sustainable Development,
- \_\_\_ Siemens AG,
- \_\_\_ Zentrum für Wirtschaftsethik gGmbH.

Weitere Informationen zum AfW sind unter [www.zfw-online.de](http://www.zfw-online.de) abrufbar.

Die vorliegende Schrift wurde im AfW<sup>ZfW</sup> beraten.  
Herausgeber des *ComplianceProgramMonitor<sup>ZfW</sup>* ist allein die Zentrum für Wirtschaftsethik gGmbH, Weingarten.

Das Zentrum für Wirtschaftsethik (ZfW) wurde 1998 durch den Vorstand des Deutschen Netzwerks Wirtschaftsethik – EBEN Deutschland e. V. (DNWE) als dessen zentrales Forschungsinstitut gegründet. In enger Kooperation mit anderen Instituten aus Wissenschaft und Wirtschaft fördert das ZfW in Deutschland und Europa die Theorie- und Anwendungsorientierung der Wirtschafts- und Unternehmensethik. Damit leistet es einen Beitrag zur Lösung gesellschaftlicher und unternehmerischer Probleme, die sich aus der Globalisierung der Wirtschaft ergeben.

**Zentrum für Wirtschaftsethik gGmbH**  
Wissenschaftliches Institut des  
Deutschen Netzwerk Wirtschaftsethik  
– EBEN Deutschland e. V.

---

**Herausgeber**

Zentrum für Wirtschaftsethik gGmbH  
Kirchplatz 7  
88250 Weingarten  
Germany

Telefon +49 (0) 751 56 86-107  
Fax +49 (0) 751 56 86-222  
eMail [zfw@dnwe.de](mailto:zfw@dnwe.de)

[www.zfw-online.de](http://www.zfw-online.de)  
[www.dnwe.de](http://www.dnwe.de)

---

**Wissenschaftlicher Direktor**  
Prof. Dr. Josef Wieland

**Geschäftsführer**  
Dr. Rainer Öhlschläger

**Projektleitung**  
Prof. Dr. Stephan Grüninger

© Zentrum für  
Wirtschaftsethik gGmbH

---

**dn** DEUTSCHES EUROPEAN  
NETZWERK BUSINESS ETHICS  
**we** WIRTSCHAFTS- NETWORK  
ETHIK DEUTSCHLAND E.V.

## Leitfaden für Unternehmen

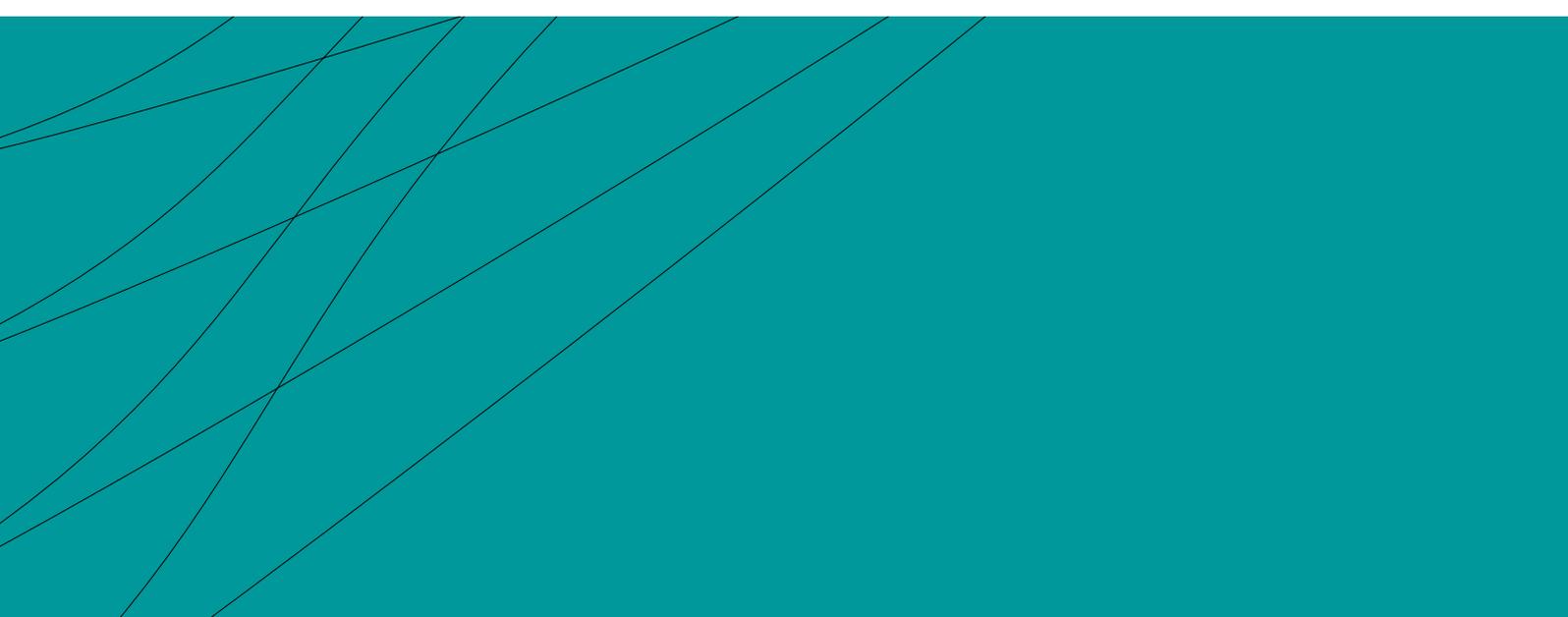
Zweck des Leitfadens ist die Bereitstellung von Prinzipien und Anleitungen für eine überwachende und steuernde Begleitung und Überprüfung (Monitoring) der Entwicklung, Implementierung, Aufrechterhaltung und Verbesserung eines effektiven Compliance-Programms in privaten und öffentlichen Organisationen.

[www.zfw-online.de](http://www.zfw-online.de)  
[www.dnwe.de](http://www.dnwe.de)



CPM<sup>ZfW</sup>

ComplianceProgramMonitor<sup>ZfW</sup>



## Contents

FOREWORD	3
A. AIM OF THE GUIDELINES AND DEFINITIONS	4
B. INTERNATIONAL LAWS AND STANDARDS IN BUSINESS CONDUCT COMPLIANCE	5
C. ELEMENTS OF A BUSINESS CONDUCT COMPLIANCE PROGRAM	6
I. Leadership & Corporate Culture	7
II. Conduct Principles and Conduct Guidelines	8
III. Implementation	9
IV. Responsibility and Organization	9
V. Communication and Training	10
VI. Risk Assessment and Monitoring	11
VII. Integration into HR Processes	12
VIII. Sales Representatives, Agents and Subcontractors	13
IX. Transparency and Documentation	14
D. COMPLIANCE MONITORING	15
I. Compliance Monitoring and Compliance Audit	15
II. Extent and Duration	16
III. Purpose and Scope of Monitoring	17
IV. Monitoring Methods and Evaluation	25

## Foreword

From the perspective of "compliance," corporate integrity and probity management and legal compliance in the conduct of business are constantly gaining in importance. As a result, the term has come to be used also outside of the financial services industry to denote the specific demands made on the rules and instruments of business management.

This makes it all the more relevant to define what compliance really means. How does it affect traditional company functions such as legal and internal audit, corporate security, environmental protection or human resources? Which functional and organizational concepts provide appropriate solutions for achieving the legal and ethical compliance objectives within a company? What does compliance mean for the management systems as a whole, such as leadership and compensation processes, training programs, and the internal control system, and how should compliance be monitored? Are social, environmental or corporate social responsibility (CSR) standards a part of compliance?

With the debate in progress, there are as yet no definitive and general answers to all of these questions. Different industries, companies and cultures try different solutions and provide different answers, but there has not yet developed a dominant understanding of or generally accepted blueprint for the "right" compliance solution.

The following compliance monitoring program is a contribution to this global debate; it draws on many years of practical experience of the companies that are members of the Users' Board for Values Management (AfW – Anwenderrat für Wertmanagement<sup>ZfW</sup><sup>1</sup>). The guidelines presented here deliberately focus on the area of "business conduct compliance," i.e. the question of how we can develop and promote probity and legal compliance in business management. The measures proposed here also address the question of how to appropriately control and monitor a company's compliance measures.

On the one hand, we want to provide guideposts to ensure that compliance is not just a declaration of good intentions, but leads to tangible and effective measures that strengthen a company's integrity and legal compliance. On the other hand, these guidelines also seek to undermine efforts to apply to compliance the classical methods of internal control systems, whose many checks and controls risk hampering a pro-active values- and problem-oriented integrity management.

The compliance monitoring approach proposed here does not claim to be exclusive, but leaves room for other and new compliance system developments. Compliance management today is a "work in progress" still requiring many innovative approaches. It cannot be the task of a compliance monitoring program to nip these in the bud. As past cases have shown, a company's integrity and legal compliance ultimately is determined less by the characteristics of its internal control systems, but by a clear focus on the real drivers of conduct such as the integrity and legal compliance practiced and lived by its senior management, the company's compensation and incentive systems, and a corporate culture of open debate. In the final analysis, the key is a corporate and leadership culture that unequivocally and consistently insists on the integrity of business conduct. If these guidelines succeed in contributing to this culture, they have accomplished their purpose.

<sup>1</sup> For more information about AfW<sup>ZfW</sup> see p. 26.

## A. AIM OF THE GUIDELINES AND DEFINITIONS

### Aim of the Guidelines

These guidelines aim to make available principles and instructions for supervising and monitoring the development, implementation, maintenance, and improvement of an effective compliance program in both private and public organizations.

To this end, the guidelines follow relevant international leading practice standards in business conduct compliance, which are listed in section B.

The key elements of an effective business conduct compliance program are described in section C. The explanations on the individual elements are not imperative for the compliance management of companies and other organizations. Rather, they should be understood as introductory remarks on the topic and as possible descriptions of compliance elements. The specific demands made on the compliance elements have to be determined and described for every organization on a case-by-case basis.

The Compliance Program Monitoring itself focuses on the monitoring and control of the design, implementation and application of business conduct compliance programs in everyday business and is described in section D. It also includes a Compliance Program Checklist designed to help conduct the compliance monitoring.

### Definitions

In the context of companies and organizations, the term *compliance* means complying with laws and regulations, organizational principles, internal rules and guidelines, the principles of good governance as well as generally accepted ethical norms.

Thus broadly defined, *compliance management* (i.e. ensuring compliance through appropriate measures) encompasses not only issues such as fairness in competition and the fight against corruption – topics that are frequently at the center of the public debate –, but also the environment, human rights, labor and social standards, and other industry-related issues.

*Compliance programs* describe the package of measures in the context of a company's – or organization's – entire compliance management, as they refer to individual (legal) areas. Accordingly, an environmental management system (e.g. in accordance with EMAS/ISO 14001) is to be understood as (an element of) an environmental compliance program, a social supply chain program (e.g. in accordance with SA 8000) as (an element of) a compliance program ensuring adherence to human rights, labor and social standards, and an anti-bribery compliance program as (an element of) a compliance program ensuring probity in the conduct of business (*business conduct compliance program*).

This differentiation of compliance programs within a company's or organization's compliance management is merely one option, of course. In practice, there are frequently other differentiations, depending on the company's, or organization's, specific requirements. Moreover, individual elements of compliance programs, e.g. the necessary "tone from the top" (commitment and exemplary behavior of the management) and other elements related to leadership and organization, cut across themes and are organized accordingly.

The *ComplianceProgramMonitor*<sup>ZfW</sup> applies solely to the field of business conduct compliance.

### Principal International Compliance Management Standards

The laws, conventions and standards listed below shall provide orientation about the material and procedural norms that can exist for a company – in the sense of binding legal rules and regulations and voluntary best practice standards in business conduct compliance. The list is not exhaustive. Additional laws, industry standards and other voluntary standards can be relevant, e.g., at all times, the specific anti-corruption and anti-trust laws in the countries where the company does business. On the other hand, not all the laws, conventions and standards listed here need to be relevant for a certain company. Therefore, it is always necessary to analyze the relevant legal and voluntary standards in order to develop and monitor, both internally and externally, a business conduct compliance program.

#### Selected Laws and Conventions

- Anti-corruption laws
- Relevant criminal law codes (fraud including bidding fraud, extortion, illegal insider trading, money laundering, embezzlement, document forgery, betrayal of secrets, etc.)
- EU Anti-Bribery Law (EUBestG)
- OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions
- Foreign Corrupt Practices Act (FCPA)
- UN Convention Against Corruption (UNCAC)
- Act Against Competition Restraints
- German Corporate Governance Code
- OECD Guidelines for Multinational Enterprises
- UN Global Compact
- ICC Rules of Conduct and Recommendations on Combating Extortion and Bribery
- World Economic Forum, Partnering Against Corruption Initiative (PACI): Principles for Countering Bribery
- Transparency International/Social Accountability International: Business Principles for Countering Bribery
- Transparency International: "A-B-C of Corruption Prevention" and "Checklist for 'Self-audits' to Prevent Corruption in Companies"
- World Bank, Department of Institutional Integrity: Voluntary Disclosure Program, Protocol 7, II. "Guidance in Revising and Improving the Compliance Program"
- European Bank for Reconstruction and Development (EBRD): "Fraud and corruption – definitions and guidelines for private sector operations"
- United States Sentencing Guidelines: "Effective Compliance and Ethics Program" (§8B2.1)
- Open Compliance and Ethics Group (OCEG): OCEG Guidelines "Red Book"
- Committee of Sponsoring Organizations of the Treadway Commission (COSO): COSO Enterprise Risk Management Framework
- Australian Standard (AS) 8002-2003 – Organizational Codes of Conduct, and Australian Standard (AS) 2860-2006 – Compliance Programs
- ValuesManagementSystem ZfW of the Users' Board for Values Management (AfW – Anwenderrat für Wertemanagement).
- EMB Values Management in the Construction Industry

## C. ELEMENTS OF A BUSINESS CONDUCT COMPLIANCE PROGRAM

The following remarks and comments are based on the above-mentioned laws and standards, the ValuesManagementSystem<sup>ZfW</sup><sup>2</sup>, and the relevant German and international literature on the topic of business conduct compliance. They aim to provide a summary of the possible practical requirements for implementing a business conduct compliance program.

The following remarks and comments do not establish a minimum standard. I.e., the text only serves as an introduction to the topic and as guidance for the development and implementation of a compliance system. The individual elements (see subject headings I to IX of this section), however, are necessary components of a business conduct compliance program.

<sup>2</sup> The ValuesManagementSystem<sup>ZfW</sup> is available at [www.zfw-online.de](http://www.zfw-online.de).

## I. Leadership & Corporate Culture

The company management is responsible for the business conduct compliance program. In particular, it is responsible for constantly communicating, both internally and externally, the company's core values, conduct principles and conduct guidelines (see II.), for acting in accordance with the communicated standards, and for monitoring the implementation and application of the business conduct compliance program.

A business conduct compliance program can only achieve sincerity and credibility if its implementation, application, and public communication are given "top-level" priority. Only the management's continual self-commitment to the company's core values and business conduct compliance program proves the sincerity of the program and thus generates both the ability to act and an environment of reliability and trust for the employees. In this context, it is essential to make clear that complying with the core values and the business conduct compliance program is company policy and that any behavior that does not respect and comply with these values and this program will neither be tacitly expected nor condoned. In addition, monitoring the implementation and application of the business conduct compliance program makes the program more credible in the eyes of business partners and other stakeholders of the company.

In the context of a business conduct compliance program, leadership and corporate culture also help to develop and promote a specific corporate identity, and to provide all employees with the orientation and security required for making difficult decisions in everyday business. In order to live up to this high standard in practice, moral values (e.g. integrity, fairness, honesty, loyalty to the contract, responsibility), cooperation values (e.g. loyalty, team spirit, ability to manage conflict, openness), performance values (e.g. gain, expertise, willingness to perform, flexibility, creativity, innovativeness, quality), and communication values (e.g. respect, belonging, openness, transparency, communication) must be consistent with each other and with everyday business realities. The company values must not contradict one another nor must they make promises to the stakeholders that cannot be kept – ignoring the business realities, so to speak. Only then can a company's core values be credibly communicated to its managers, employees and external stakeholders.

When building a corporate culture defined by integrity, both managers and employees have to develop the skills to recognize and solve values-sensitive problems. The persons involved have to make sure that their conduct and that of their business unit is geared towards compliance in a long-term-perspective. The business conduct compliance program can only be effective in the long term if the top management, the unit managers and the employees make a binding commitment to the program. A business conduct compliance program has to be a high-priority company process that receives constant attention within the organization. To this end, the company must, for example, use coaching methods during an internal or external implementation support in order to ensure the proper conduct of all employees and their units and to bring about changes in behavior in line with the company's core values, conduct principles and conduct guidelines. Only then will the program be effective in the long term and different from short-term and short-sighted activities or delegation to professional contexts. A business conduct compliance program can only be successful if the managers live by and commit to this program at every level of the organization. At the same time, it is equally important to enable and safeguard employees' autonomous decision-making competencies in ethical conflict situations for which there are no explicit conduct principles or guidelines. This allows for the fact that there cannot be specific conduct and procedural principles for every conceivable situation that may arise in a company's, or organization's, daily routine.

## II. Conduct Principles and Conduct Guidelines

A company has to have written conduct principles and conduct guidelines, define the company values, and lay down the business ethics it desires. The primary objective of these conduct principles and conduct guidelines is to prevent criminal and unethical business actions, in particular violations of competition and anti-corruption laws. In addition to unequivocally prohibiting unethical or fraudulent actions, conduct guidelines can also articulate expectations about employees' positive actions (e.g. regarding innovation). Establishing conduct principles and conduct guidelines means that the company should draw up a declaration of values, a code of ethics or similar document. This document is to outline the values that guide the company in its relations with its most important interest groups. Furthermore, this values management (see E.) has to be incorporated into the company's specific business strategy. The business principles and rules of conduct have to be available for all employees and business partners at all times. In addition, all employees should be specifically and explicitly informed about legal compliance. This is all the more important since not every employee is up to date on the current legal situation and knows how to act in accordance with the law.

There are no definitive rules as to what the written compliance regulations have to look like. They can be working instructions, guidelines, instruction leaflets, flyers or handbooks. However, by putting the rules in writing, the company must ensure that its employees know the compliance regulations. Simply publishing the rules, conduct principles and conduct guidelines on the company's intranet or similar platforms will not be enough unless all employees are systematically and notified.

Business conduct compliance programs typically address the following areas, which are regulated as part of the conduct principles (Code of Conduct) and/or by conduct guidelines, working instructions and business process instructions:

- legal compliance, law abidance;
- prohibition of corruption and of violations of anti-trust laws;
- respect for human rights, labor and social standards, prohibition of discrimination and workplace harassment, etc.;
- ensuring legal compliance and compliance with business ethics when dealing with clients and sales intermediaries;
- ensuring legal compliance and compliance with business ethics when dealing with suppliers and subcontractors;
- acceptance and giving of gifts, invitation to meals, drinks or other entertainments, other benefits;
- dealing with conflicts of interests (ensuring the separation of company and personal interests and the priority of company interests over personal interests);
- dealing with donations, not-for-profit activities, and sponsoring;
- prohibition of insider trading;
- protection of company assets (including dealing with information and protection of intellectual property), secondary employment, protection of the assets of business partners.

### III. Implementation

The company should define the target group of every guideline and measure. It should make sure – if necessary, by means of pilot tests or similar means – that the guidelines and measures are easy to understand and apply. The correct application of conduct principles and conduct guidelines, the integration into management processes and the corresponding quality control should be continuously documented. The company should also seek confirmation from relevant company units (management) and employees that the guidelines, measures and controls have been received and understood; it should also establish a helpdesk or information office to be able to field questions about their practical application.

In addition, measures should be taken to recognize and promote exemplary conduct that complies with and reflects the company's values and to impose sanctions for violations of values, especially for gross misconduct in business dealings. This can be done through job instructions, management and staff evaluation systems, and values-sensitive incentive and compensation systems.

The company should use clearly defined, transparent criteria and procedures to recruit, hire and promote employees. Key positions must not be held by individuals who have already committed crimes or come to attention because of major misconduct. Moreover, compliance with the company's core values and conduct guidelines should be part of the evaluation criteria of performance evaluations, compensation systems and bonus regulations or adapt the latter in accordance with its compliance objectives. This is to prevent that company units (management) and employees use means that do not comply with the rules and regulations to strive for or achieve sales and profit targets.

In addition, employment contracts should contain a commitment to legal and in particular anti-corruption compliance. Moreover, it is recommended to include regulations regarding secondary employment and conflicts of interest in the employment contract.

### IV. Responsibility and Organization

Conduct principles and conduct guidelines can only be successful if a company's management demonstrates exemplary conduct and commitment to compliance at every level. The Board of Directors is responsible for compliance.

The company should select individuals who take responsibility for developing and designing the compliance program and support the management in implementing and applying the company standards. To this end, they should have the appropriate resources and powers. In the case of multi-headed company managements, it may be expedient to assign the responsibility for the compliance program to a department. The board member in charge can delegate the above-mentioned responsibility for designing and supervising the compliance program either to an already existing position or to one or more appointed compliance representatives. Moreover, in larger companies, it has proven effective to form a compliance steering committee consisting of the functions that are responsible for important activities and processes in the context of a compliance program (e.g. compliance, legal division, audit, HR, controlling, sales, purchasing, safety). Among other things, this steering committee can be tasked with supporting the management in comprehensively and consistently applying the compliance program and with acting in case of suspected compliance violations.

In addition to appointing individuals in charge, the company should have regulations about how employees can act as "whistleblowers" if they discover or suspect violations of legal and/or internal regulations (e.g. anonymous hotline, ombudspersons). Here, it has to be ensured that the employees know where and how to report misconduct. It also has to be ensured that employees can report suspected criminal activities without fear of negative consequences and without having to resort to hierarchical communication structures. Moreover, the company can offer employees the option to report any ethical dilemmas to existing institutionalized company functions (e.g. legal or human resource departments) – if necessary, anonymously.

## V. Communication and Training

The company has to conduct regular trainings to inform and educate about its conduct principles and conduct guidelines.] Trainings are one of the key instruments of a functioning compliance program.

The company has to make sure that the relevant target groups participate in the trainings and that the learning objectives are communicated with a view to practical application, so that the employees are able to apply the knowledge. Such conduct trainings can in particular include case studies based on ethical dilemmas in everyday practice. The trainings are particularly important for employees in sensitive functions (e.g. sales, purchasing), but should be expanded – at least gradually – to include all company staff and employees (including the company management). Moreover, for certain companies it is reasonable and/or necessary to also inform its sales representatives, sales agents as well as consultants and subcontractors about its compliance rules and to conduct information or training sessions for these groups.

For internal communication, it has proven effective to seek confirmation from the relevant employees (board members, managers and employees in compliance-sensitive functions) that they have taken note of the compliance rules by asking them to sign a written declaration ("compliance declaration"). For the selection of the "relevant employees," all company locations should be taken into account.

In addition, it has to be ensured that the company management and the compliance department/ compliance representative communicate the compliance program within the company continually and continuously, i.e. beyond its introduction stage. In addition to compliance trainings and regular written declarations about having taken note of and complying with the compliance rules, employee polls, for example, can be used to gain information about the staff's perceptions of the status and development of corporate compliance/corporate integrity. If necessary, these surveys can be used to implement further measures for improving the compliance program.

## VI. Risk Assessment and Monitoring

Both best practice standards and the literature on business conduct compliance agree that there have to be controls at irregular intervals. There is as yet no judicial pronouncement on how these controls should be organized and which control measures are necessary, sufficient and reasonable. This offers the advantage that it is possible to flexibly respond to the requirements of the company and its business operations. Controls always fulfill a pro-active function and an investigative function. Announcing and performing controls increases the likelihood of discovering compliance violations while, at the same time, serving as a deterrent, i.e. in a preventive manner.

To this end, the company must evaluate the relevant existing business processes (e.g. in sales and purchasing) and relevant regulations such as the existing signature policy as to whether they promote rule-abiding behavior or encourage or facilitate transgressions. It also has to assess whether the implemented controls are really effective. It is important to have regular risk assessments in all business fields and relevant key departments regarding potential violations of anti-corruption and anti-trust laws and other compliance issues (e.g. labor and social standards throughout the value chain). The company's IT systems have to make sure that no unauthorized third party is able to access the system and that data manipulations can be documented at any time (through logfiles, protocols and controls of all transactions – especially in financial accounting). The two-person rule (or other controls) should be systematically applied during the performance of sensitive functions, e.g. for payment authorization. The company should perform regular controls in order to ensure that all employees taking part in money transactions act in accordance with the generally accepted accounting principles (GAAP; in Germany: Grundsätze ordnungsgemäßer Buchführung, GoB).

In addition to having make sure that the compliance controls of its business processes are functional, the company board is responsible for regularly evaluating the compliance program with a view to its effectiveness and efficiency. This is to guarantee both its quality and its adaptability to changing conditions (e.g. mergers & acquisitions). This evaluation should take place once a year. Moreover, the company should review the compliance program at least once every five years. This review should also include agreements and contracts with agents, sales representatives, subcontractors and subsidiaries.

## VII. Integration into HR Processes

The company has to make sure that individuals who have come to attention for criminal actions or other violations of compliance programs within or outside the company in the past are not promoted to or hired for responsible positions. It has to make sure that no discretionary decisions are delegated to individuals known for having committed fraudulent actions. If criminal actions are discovered, the company has to respond in an appropriate fashion. In case of violations of laws or the compliance program, it has to take appropriate disciplinary measures, also against employees who are responsible for covering up infractions. These measures can range from reprimands to dismissals. Most importantly, the company has to demonstrate its sincerity and will to apply its compliance program. The company will also be judged by the steps it takes in case of a compliance violation.

Until now, few companies have adopted so-called "amnesty programs" (leniency programs) for employees (not for members of the executive management). Here, the company waives claims for damages and refrains from terminating the employment contract if employees who have violated compliance rules bring charges against themselves. Whether such a program makes sense can only be determined by reviewing the particulars of every case.

In addition, there should be positive incentives for complying with the business conduct compliance program and for successfully implementing the program. The target agreements and performance evaluations of managers and executives should include targets that refer to the company's core values and business conduct compliance program. Moreover, the company should make compliance with its core values and conduct guidelines an integral part of the evaluation basis for its performance evaluation and compensation systems.

## VIII. Sales Representatives, Agents and Subcontractors

The hiring of agents, consultants and sales representatives who develop business and do lobby work (especially abroad) has to be thoroughly evaluated (so-called "third-party due diligence"). The same applies to the hiring of subcontractors. In this context, one also has to assess the compliance with laws and compliance programs and the suitability of the business partners selected abroad. When signing contracts, one has to make sure that they include declarations to the effect that the contract partners have not and will not bribe office holders or similar persons to gain any professional or financial advantage. Such declaration is also necessary when entering into joint ventures. Compliance with the prohibition has to be monitored.

The company has to take measures to ensure that all representatives and agents know the compliance program; it also has to make clear that it expects all actions undertaken in its name to be consistent with the existing compliance program.

The company should review the fees and commissions of its representatives and agents at home and abroad with a view as to whether they are reasonable and justifiable. Representatives and agents, too, should be bound to comply with the company's guidelines and conduct rules and be subject to controls.

Secondary employments of employees must be subject to regulation and approval (in particular in companies that are competitors, clients or suppliers). Board memberships are expressly prohibited or subject to regulation and approval. There are clear rules for acquiring company shares/warrants on special terms as well as for granting and giving loans to employees, business partners, subsidiary and holding companies.

Any organizational and/or financial establishment, alteration or liquidation of subsidiary, holding or trust companies at home and abroad is regulated company-wide and subject to approval (purpose of business, management, supervisory bodies, capitalization, ownership structure, etc.). Activities in countries that are considered to be particularly prone to corruption (e.g. according to the Transparency International Corruption Perceptions Index) are subject to particular monitoring and control.

The company has to make sure that its buying processes are documented and transparent at all times, also for competent third parties (by recording procurement specifications, calls for tender, awarding of contracts, complaints, and payment handling).

## IX. Transparency and Documentation

As a matter of principle, payment transactions – in particular for gifts, meal invitations, donations, cash purchases, commissions, and consultancy and trustee services – should be subject to particular control. Moreover, documentation requirements for business transactions and payments should be established and compliance with these requirements should be regularly reviewed, e.g. by internal audits. Donations for political or non-profit causes and sponsoring of any kind should be carefully evaluated, subject to approval and properly documented. There are clear rules for giving and accepting gifts as well as for meal invitations and other benefits, which apply to all employees at home and abroad. Internal budgets for general charitable or social purposes (e.g. company sports club, sponsoring associations, foundations, works council) are to be regularly reviewed.

### I. Compliance Monitoring and Compliance Audit

A compliance audit, i.e. a review of the efficiency and effectiveness of the business conduct compliance program, can be performed either by internal auditors (e.g. by internal audit) or external auditors (e.g. by qualified consulting or auditing companies). In these guidelines, the term *audit* is reserved for cases where a compliance program already exists, i.e. where its implementation has been concluded. That does not mean that all compliance measures, which the company needs from the perspective of best practice and suitability, have to be already implemented and realized. It only means that the internal or external auditor/audit team comes into play after the implementation process has been concluded.

On the other hand, *compliance monitoring* means that the external, independent and objective compliance monitor carries out his/her tasks during the implementation of the compliance program, i.e. s/he accompanies the implementation process. In this context, the compliance monitor expressly does not act as a consultant or trainer, i.e. s/he does not make any decisions about necessary compliance measures nor does s/he design their implementation and application. What the compliance monitor does is to coach the company's management board, internal compliance personnel (compliance representative, compliance committee, etc.) as well as any internal and external consultants along best-practice standards. For example, the whole set of requirements listed in the *Compliance Checklist* (see D. III.) is a best-practice standard.

Among other cases, compliance monitoring takes place when private and in particular public clients or funding institutions (World Bank, European Bank for Reconstruction and Development, etc.) ask a company to establish or improve/update a compliance system. In this case, the independent compliance monitor reports on the progress and status of the compliance system during its development and implementation and submits a final report after the compliance system has been put in place.

In the interest of readability, the term *compliance monitoring* will be used in the following paragraphs to also include the compliance audit, which takes place after the compliance program has been implemented..

## II. Extent and Duration

The extent and duration of a compliance monitoring process cannot be generally defined, but have to be established on a case-by-case basis by the compliance monitor. In any event, the size of the company (turnover, number of employees), the complexity of the organization, and the business model are key criteria for determining the extent and duration of the compliance monitoring process. If applicable, there may be additional, external standards that are relevant for the compliance system.

Basically, the following criteria have to be taken into consideration when planning the extent and duration of a compliance monitoring process (please note that this list is not exhaustive):

- Business volume
- Number of employees; number of employees directly affected by the compliance system (e.g. employees in sensitive company departments or functions)
- Branch of industry
- Business model, e.g. regarding distribution and sales channels
- Level of internationalization/percentage of foreign business/business activities in countries with an increased risk of non-compliance
- Generic risk exposure regarding compliance violations (e.g. risk of corruption)
- Complexity of organizational structure
- Decentralized decision-making powers/possibilities for central control
- Misconduct/criminal behavior in the past
- Opinion of the compliance monitor ("reasonable assurance" or "negative assurance")

### III. Purpose and Scope of Monitoring

A key goal of compliance monitoring is to determine whether the compliance program of a company (or organization) contains the elements that are generally considered necessary to properly protect the company (or organization) from unlawful actions by managers, employees or business partners.

To this end, it has to be established that the company (or organization) has taken the necessary compliance measures, that the compliance program as a whole is integrated into the day-to-day business processes and makes it possible to support the company's values and culture and is thus suited to preventing, uncovering or thwarting crimes and offenses.

The scope of a compliance monitoring program is basically to review whether a business conduct compliance program has been properly developed and designed (i.), effectively implemented (ii.) and whether it is used and applied (iii.) in a company's (or organization's) everyday business.

#### I. Regarding the **design of the compliance program**, it is reviewed whether

- all **reference standards** relevant for the company **have been taken into account** and whether
- the **compliance measures** are **appropriately designed** for the company (*design check*). The appropriateness is determined by the criteria mentioned in E. II. and, if necessary, by further criteria established by the compliance monitor ("professional judgment").

#### II. Regarding the **implementation or establishment of the compliance program**, it is reviewed whether

- the **elements of the compliance management system** necessary to meet the appropriateness requirements are **functional** (*functionality check*). I.e., in order to achieve the "implemented" status, a compliance measure has to have been adopted and become effective, all accompanying instruments (written forms, technical systems, etc.) have to be available, and the compliance measure has to be able to serve its desired purpose and meet the defined goal.

While monitoring the design focuses on the compliance system's structure, monitoring its implementation focuses on the system's feasibility and ability to function.

#### III. Regarding the **application of the compliance system**, it is reviewed whether

- the **elements of the compliance management system** are applied in day-to-day business practices (*effectiveness check*). To this end, the reviewed compliance measure must have been used already (at least once).

Reviewing the effective application takes on the question of whether the compliance measure is really adhered to and internalized in the company's day-to-day business.

It might not be possible to perform this kind of application monitoring for all compliance measures. Where this is the case, "not applicable (n/a)" should be noted in the checklist. A Code of Conduct, for example, can only be evaluated regarding i. and ii., since it cannot and should not be reviewed in the context of a compliance monitoring program whether the employees follow the guidelines specified in the Code. On the other hand, the integration of compliance into target agreements and performance evaluations is only "effective" once this instrument has been used and not after its planning has been concluded and the process has been fully described.

## Compliance Program Checklist (Business Conduct)

Compliance Element	Stage	Compliance Measure	Relevancy		Measure is ...		
			relevant	irrelevant	appropriately developed	functional	effective
I Conduct Principles (Code of Ethics)	Development	1 Definition of company goals and company values	r	i	a	f	e
		2 Definition of the principles of business ethics	r	i	a	f	e
		3 Naming of key stakeholders	r	i	a	f	e
		4 Identification of the applicable reference standards	r	i	a	f	e
II Conduct Guidelines (Code of Conduct)	Development	5 Legal compliance, law abidance	r	i	a	f	e
		6 Prohibition of corruption (zero tolerance), prohibition of anti-trust law violations	r	i	a	f	e
		7 Ensuring compliance with laws and business ethics in dealing with clients and sales intermediaries	r	i	a	f	e
		8 Ensuring compliance with laws and business ethics in dealing with suppliers and subcontractors	r	i	a	f	e

Compliance Element	Stage	Compliance Measure	Relevancy		Measure is ...		
			relevant	irrelevant	appropriately developed	functional	effective
		9 Acceptance and giving of gifts, meal invitations, and other benefits	r	i	a	f	e
		10 Dealing with conflicts of interests (ensuring the separation between company and personal interests and the priority of company interests over personal interests)	r	i	a	f	e
		11 Dealing with donations, non-profit activities, and sponsoring	r	i	a	f	e
		12 Protection of the assets of the company, secondary employment, protection of the assets of business partners	r	i	a	f	e

Compliance Element	Stage	Compliance Measure	Relevancy		Measure is ...		
			relevant	irrelevant	appropriately developed	functional	effective
III Policies & Procedures	Development	13 Acceptance and giving of gifts	r	i	a	f	e
		14 Compliance declaration for managers, employees	r	i	a	f	e
		15 Compliance review of third parties (agents, consultants, sales representatives) in sensitive business departments and countries before hiring their services	r	i	a	f	e
		16 Compliance agreement for third parties (compliance declaration, review of suppliers, evaluation of suppliers)	r	i	a	f	e
		17 Supplier compliance (e.g. compliance declaration, review of suppliers, evaluation of suppliers)	r	i	a	f	e
		18 Sanctions in case of non-compliance	r	i	a	f	e
IV Transparency	Development	19 Risk screening for sensitive business areas	r	i	a	f	e
		20 Control of risk management in sensitive business areas	r	i	a	f	e

Compliance Element	Stage	Compliance Measure	Relevancy		Measure is ...		
			relevant	irrelevant	appropriately developed	functional	effective
		21 Documentation of sensitive payment transactions (e.g. donations, commissions)	r	i	a	f	e
		22 Protection of IT systems against data manipulation	r	i	a	f	e
		23 Two-person rule in sensitive functions	r	i	a	f	e
		24 Control of compliance with generally accepted accounting principles	r	i	a	f	e
V Leadership and Corporate Culture	Implementation	25 Compliance as a strategy of (legal, economic, ecological, social) sustainability	r	i	a	f	e
		26 Orientation towards ethical values	r	i	a	f	e
		27 Leadership style: determination, clarity, reliability, accountability, integrity	r	i	a	f	e
		28 Self-commitment, legality	r	i	a	f	e
		29 Managers serve as role models and take responsibility for compliance ("tone from the top")	r	i	a	f	e
		30 Pro-active and aggressive communication of CMS by company board and management	r	i	a	f	e

Compliance Element	Stage	Compliance Measure	Relevancy		Measure is ...		
			relevant	irrelevant	appropriately developed	functional	effective
VI Communication and Training	Implement- ation	31 Internal communication (meetings, brochures, newspapers, intranet)	r	i	a	f	e
		32 External communication (e.g. annual reports, reporting, brochures)	r	i	a	f	e
		33 Written and oral information for agents, suppliers, consultants	r	i	a	f	e
		34 Membership and engagement in compliance initiatives and exchange of experiences	r	i	a	f	e
	Implemen- tation	35 Face-to-face training for top-level management and functions with increased compliance risk	r	i	a	f	e
		36 Specific face-to-face training for certain functions and high-risk groups (e.g. purchasing, sales, suppliers)	r	i	a	f	e
		37 Trainings include legal information plus a focus on "real cases"	r	i	a	f	e
		38 Web- or intranet-based training for employees	r	i	a	f	e
VII Compliance in HR	Implement- ation	39 Integrity review and compliance declaration for employees in areas with high compliance risks	r	i	a	f	e

Compliance Element	Stage	Compliance Measure	Relevancy		Measure is ...		
			relevant	irrelevant	appropriately developed	functional	effective
		40 Integration into employee selection and hiring processes	r	i	a	f	e
		41 Career planning for board members and managers	r	i	a	f	e
		42 Target agreements in sensitive business areas	r	i	a	f	e
		43 Compliance risks in salary systems and bonuses	r	i	a	f	e
		44 Appropriate disciplinary measures (presentation/threat of sanctions in line with labor, civil or criminal law)	r	i	a	f	e
VIII Organization	Implementation	45 Responsibility of top management (board, management)	r	i	a	f	e
		46 Compliance steering committee (e.g. compliance, legal, audit, sales, HR)	r	i	a	f	e
		47 Compliance office with appropriate resources	r	i	a	f	e
		48 External compliance monitor	r	i	a	f	e
		49 Whistleblower systems	r	i	a	f	e

Compliance Element	Stage	Compliance Measure	Relevancy		Measure is ...		
			relevant	irrelevant	appropriately developed	functional	effective
IX Audit	Review	50 Internal audit of CMS in sensitive business areas	r	i	a	f	e
		51 Control of sensitive payment transactions (e.g. donations, commissions)	r	i	a	f	e
		52 Control of compliance with and implementation of CMS into everyday business practices	r	i	a	f	e
X Monitoring	Review	53 Regular reports to and discussion in the top management	r	i	a	f	e
		54 Self-evaluation of business areas and companies	r	i	a	f	e
		55 External monitoring of the development, implementation and suitability (fit for purpose) of CMS by experts and auditing companies	r	i	a	f	e

## IV. Monitoring Methods and Evaluation

### **Analysis of the Documentation**

As part of the compliance monitoring program, the compliance monitor examines the existing documentation of the compliance system. All measures relevant for the compliance system have to be documented and reviewed.

### **Conduct of Interviews**

The compliance monitor conducts interviews with selected individuals who work for the company. Typically, these always include members of the company's executive management and a group of department heads selected by the monitor. In addition, interviews should be conducted with employees in sensitive functions (e.g. purchasing, sales) and with randomly selected company employees.

### **Evaluation**

The compliance monitor writes a report in which s/he assesses the status of a company's compliance system. S/he evaluates the design, implementation and application of the compliance systems. On all three points, the evaluations should include qualifying remarks.

The evaluation has to include statements about the basic orientation and the aims of the compliance system as well as the program's strengths and weaknesses. In addition, the report has to contain recommendations for the program's further development and improvement and, if applicable, provide information about conditions that have been imposed on the company.

## AfW<sup>ZfW</sup> – Anwenderrat für Wertemanagement<sup>ZfW</sup>

The AfW<sup>ZfW</sup> is a voluntary association of companies and organizations that use and promote the ValuesManagementSystem<sup>ZfW</sup>. Its goal is to advance, enhance and assure the quality of the ValuesManagementSystem<sup>ZfW</sup>. Its practical expertise ensures that the ValuesManagementSystem<sup>ZfW</sup> is highly application-oriented. In addition, the AfW<sup>ZfW</sup> provides its members with a forum for the continuing exchange of experiences and mutual advice. Current AfW<sup>ZfW</sup> members are: ABB, Allianz, BASF, Bilfinger Berger Industrial Services, Bosch, Daimler AG, Deutsche Post, Deutsche Telekom, German Forum for Crime Prevention (Deutsches Forum für Kriminalprävention, DFK), EnBW, Ethics Management of the German Construction Industry (EthikManagement der Bauwirtschaft e.V.), Fraport, Lahmeyer International, Novartis Foundation for Sustainable Development, Schwarz Pharma, Siemens, The Centre for Business Ethics, ZF Marine. Additional information about the AfW<sup>ZfW</sup> is available at **[www.zfw-online.de](http://www.zfw-online.de)**.

This document was discussed in the AfW<sup>ZfW</sup>. The Centre for Business Ethics, Weingarten, is the sole publisher of the ComplianceProgramMonitor<sup>ZfW</sup>.

The Centre for Business Ethics (Zentrum für Wirtschaftsethik – ZfW gGmbH) was founded in 1998 by the managing board of the German Business Ethics Network (Deutsches Netzwerk Wirtschafts-ethik – DNWE) as its central research institute. Its task is to promote the implementation of business ethics in Germany and Europe in close cooperation with other scientific and economic institutions. At the same time it contributes to the solution of social and entrepreneurial problems that result from economic globalization.

**Zentrum für Wirtschaftsethik gGmbH**  
Wissenschaftliches Institut des  
Deutschen Netzwerk Wirtschaftsethik  
– EBEN Deutschland e. V.

---

**Published by**  
Zentrum für Wirtschaftsethik gGmbH  
Kirchplatz 7  
88250 Weingarten  
Germany

Telefon +49 (0) 751 5686-107  
Fax +49 (0) 751 5686-222  
eMail zfw@dnwe.de

[www.zfw-online.de](http://www.zfw-online.de)  
[www.dnwe.de](http://www.dnwe.de)

---

**Academic Director**  
Prof. Dr. Josef Wieland

**Managing Director**  
Dr. Rainer Öhlschläger

**Project Director**  
Prof. Dr. Stephan Grüninger

**Translation**  
Manuela Thurner, Munich

© Zentrum für  
Wirtschaftsethik gGmbH

---

**dn** DEUTSCHES EUROPEAN  
NETZWERK BUSINESS ETHICS  
**we** WIRTSCHAFTS- NETWORK  
ETHIK DEUTSCHLAND E. V.

## Guidelines for organizations

These guidelines aim to make available principles and instructions for supervising and monitoring the development, implementation, maintenance, and improvement of an effective compliance program in both private and public organizations.