Universal-Standard

des International Institute for
Governance, Management, Risk & Compliance der
Technischen Hochschule Deggendorf

Compliance-Managementsystem

in Anlehnung an
ISO 19600:2014
COSO I:2013
IDW PS 980:2011

Stand: 08/2016

Universal-Standard

des International Institut for
Governance, Management, Risk & Compliance der
Technischen Hochschule Deggendorf

Compliance-Managementsystem

in Anlehnung an
ISO 19600:2014
COSO I:2013
IDW PS 980:2011

Herausgeber:

International Institute for Governance,
Management, Risk & Compliance
der Technischen Hochschule Deggendorf
Edlmairstraße 6 und 8
94469 Deggendorf

GMRC-Verlag

GMRC-Verlag-GbR
Verlag für Governance, Management, Risk & Compliance

Mitglieder des Direktoriums:

Prof. Dr. jur. Josef Scherer
Professor für Unternehmensrecht,
Risiko- und Krisenmanagement
Leiter des Internationalen Instituts für
Governance, Management, Risk & Compliance
der Technischen Hochschule Deggendorf
Richter am Landgericht a.D.
Rechtsanwalt

RiAG Klaus Fruth
Vorsitzender Richter des Schöffengerichts
Lehrbeauftragter an der Technischen Hochschule Deggendorf

Frank Romeike
Geschäftsführer RiskNET GmbH
Lehrbeauftragter der Technischen Hochschule Deggendorf
Inhaber des Risikomanagement-Internet-Portals www.RiskNET.de

Prof. Dr. Bruno Brühwiler
Professor für Risikomanagement an der Technischen Hochschule Deggendorf
Vorsitzender ISO TC 262, Working Group „Core Risk Management Standards"
Geschäftsführer der Euro Risk Limited, Zürich

Deggendorf 2016

ISBN: 978-3-00-052446-2

Bibliografische Information der Deutschen Nationalbibliothek:

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Vorwort

Die Ausgestaltung des Compliance-Managementsystems als eigenständiges System ist möglich. Dieser Standard stellt jedoch wahlweise einen neuen Ansatz eines integrierbaren („GRC“) Compliance-Managementsystems dar. Dies erwies sich in Theorie und Praxis als schlüssig und geeignet, die vielen Unternehmensfunktionen, wie Governance, Risiko-, Compliancemanagement, Internes Steuerungs- und Überwachungssystem, Revision, etc., zu vernetzen, dadurch Redundanzen und Insellösungen zu vermeiden und erhebliche Synergien zu gewinnen.

Da sich weltweit Unternehmen bei der Implementierung eines Compliance-Managementsystems an diversen populären (internationalen) Standards / Codices (ISO / COSO / IDW / etc.) orientieren, dienen diese auch als Referenz für dieses Werk.

In der Praxis ist derzeit zu beobachten, dass Unternehmen von ihren Geschäftspartnern die Zusicherung einfordern, unterschiedlichste (Compliance-) Standards oder Codices einzuhalten. Dies führt aufgrund der wachsenden Vielfalt existierender Standards bei den Betroffenen zu Verunsicherung und der Sorge vor erheblichem – bürokratischen – Mehraufwand.

Daher wird mithilfe des vorliegenden „Universal“-Standards versucht, aufzuzeigen, dass die meisten Standardwerke auf einem „gemeinsamen Nenner“ beruhen, wenngleich sie auch in Aufbau oder Formulierungen differieren mögen.

Eine entsprechende Synopse, die jederzeit erweiterbar ist, hilft zu zeigen, dass die Anforderungen unterschiedlichster gängiger Standards Berücksichtigung finden.

Im Februar 2016

Prof. Dr. jur. Josef Scherer

Professor für Unternehmensrecht,
Risiko- und Krisenmanagement
Leiter des International Institute
for Governance, Management, Risk & Compliance
der Technischen Hochschule Deggendorf
Richter am Landgericht a.D.
Rechtsanwalt

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einführung: Governance- und Compliance-Managementsystem: Standardorientiertes, integriertes Management: „Das Richtige *richtig* tun“ („Block 1“)

Synopse[1]

(Corporate) Governance heißt ordnungsgemäße (pflichtgemäße) Unternehmensführung und -überwachung.

Compliance bedeutet pflichtgemäßes Verhalten in Hinblick auf allgemein verbindliche Regeln (Gesetze, Rechtsprechung), aber auch in Hinblick auf für verbindlich erklärte (interne) Vorgaben (z.B. Regelungen aus dem „Code of Conduct“ (unternehmensspezifische Verhaltensregelungen) oder Anstellungsvertrag).

Hinweis: In der Praxis wird z. T. eine enge Auslegung vertreten, dass Compliancemanagement nur straf- und bußgeldbewährte Pflichtverstöße verhindern soll.

Dies entspricht nicht der herrschenden Meinung und Rechtsprechung, die ex- und interne Pflichtenerfüllung als Ziel sieht.

Idealerweise deckt sich pflichtgemäßes Verhalten mit „vernünftigem Verhalten“.

Governance, Risk und Compliance soll zum einen helfen, durch Prophylaxe den Eintritt von Pflichtverletzungen, Schadens- und Haftungsfällen zu vermeiden. Zum anderen sollen eingetretene Pflichtverstöße frühzeitig erkannt und bewertet und es muss angemessen darauf reagiert werden.

Das Compliance-Managementsystem behandelt idealerweise *alle* relevanten (Prozess-) Themenfelder eines Unternehmens / einer Organisation.

Sollten (zunächst) vom Compliance-Managementsystem in einem Unternehmen nur bestimmte (Prozess-) Themenfelder (z.B. Vertrieb / Einkauf / etc.) oder Rechtsgebiete (z.B. Antikorruption / Kartellrecht / etc.) behandelt werden, **muss** dies deutlich gemacht werden.

Dabei ist zu beachten: Legalitätspflicht sowie gesetzliche, behördliche oder sonstige zwingende Anforderungen an Unternehmen, Management oder Mitarbeiter **müssen** jedoch generell erfüllt werden.

[1] Synopse:
ISO 19600:2014: Introduction
IDW PS 980:2011: 1. Vorbemerkung
COSO I:2013: Foreword
ISO 9001:2015: Einleitung 0.1 Allgemeines

Übersicht

Überblick **Integriertes, standardorientiertes Compliance-Managementsystem in 4 Blöcken**		
Block 1		**Einführung in Compliance-Management**
1.1		**Governance, Risk und Compliance (GRC) als Klammer um die zahlreichen "Managementsystem-Inseln" und "Managementsystem-Standards"**
1.1.1		Die "gesuchte Klammer" um (Prozess-) Themenfelder und Unternehmensfunktionen
1.1.2		Ziele
1.1.3		Standardorientierung - Anwendungsbereich des *Standards*
1.2		**Allgemeines**
1.2.1		Begriffserklärung "Compliance-Managementsystem"
1.2.2		Definitionen *im* Compliance-Management
1.2.3		Rechtliche Rahmenbedingungen für ein Compliance-Management
1.2.4		Standards im Bereich Compliance-Managementsysteme
1.2.5		Tools und Methoden im Compliance-Management
1.3		**Die Konzeptionierung, Umsetzung, Überwachung und (kontinuierliche) Verbesserung (Plan / Do / Check / Act) eines ganzheitlichen, standardorientierten Compliance-Managementsystems**
1.3.1	*PLAN*	Konzeptionierung von Aufbau und Inhalt des Compliance-Managementsystems (Plan): Darstellung von Zielen und Wertbeitrag, des Soll-Zustandes, Soll-Ist-Abgleich, Bewertung von alternativen Strategien, Entscheidung, Projektierung
1.3.2		Konzeptionierung der Umsetzung (Do) (Implementierung und Wirksamkeit), Überwachung (Check) und Verbesserung (Act) des ganzheitlichen Compliance-Managementsystems
1.3.3	*DO / CHECK / ACT*	Ausführung: Umsetzung (Do), Überwachung (Check), Verbesserung (Act)

Abbildung 1: Integriertes, standardorientiertes Compliance-Managementsystem in 4 Blöcken - Block 1: Einführung.

1.1 Governance, Risk und Compliance (GRC) als „Klammer" um die zahlreichen „Management-Inseln" und „Managementsystem-Standards"

Da die Einhaltung der Grundsätze ordnungsgemäßer Unternehmensführung (GoU) und -überwachung (GoÜ) die Aufgaben der Geschäftsleitung umfassend beinhaltet, kann Governance, angereichert mit den modernen Methoden von Risiko- und Compliancemanagement, als „GRC"-Funktion eine effektive und effiziente Klammerwirkung um *sämtliche* Unternehmensfunktionen erzielen:

1.1.1 Die „gesuchte Klammer" um (Prozess-) Themenfelder und Unternehmensfunktionen

Synopse[2]

Das Compliance-Managementsystem kann – ebenso wie ein Umwelt-, Arbeitssicherheits-, Risiko-, Qualitäts-, etc.-Managementsystem – grundsätzlich aufgrund der entsprechenden Erwähnung in Standards als isoliertes Inselsystem implementiert werden.

Es kann aber auch *ein* führendes Integriertes Managementsystem (IMS) verschiedene Bereiche wie Compliancemanagement, Qualitätsmanagement, Risikomanagement, etc. verbinden.

Die diversen (Prozess-) Themenfelder eines Unternehmens (Führungs-, Kern- und Unterstützungsthemenfelder) lassen sich bildhaft mit einem „Unternehmensschiff" darstellen:

[2] Synopse:
ISO 19600:2014: Introduction
IDW PS 980:2011: 1. Vorbemerkung
COSO I:2013: Foreword
ISO 9001:2015: Einleitung 0.4 Zusammenhang mit anderen Normen zu Managementsystemen

Nicht der Wind bestimmt den Kurs, sondern das Segel!

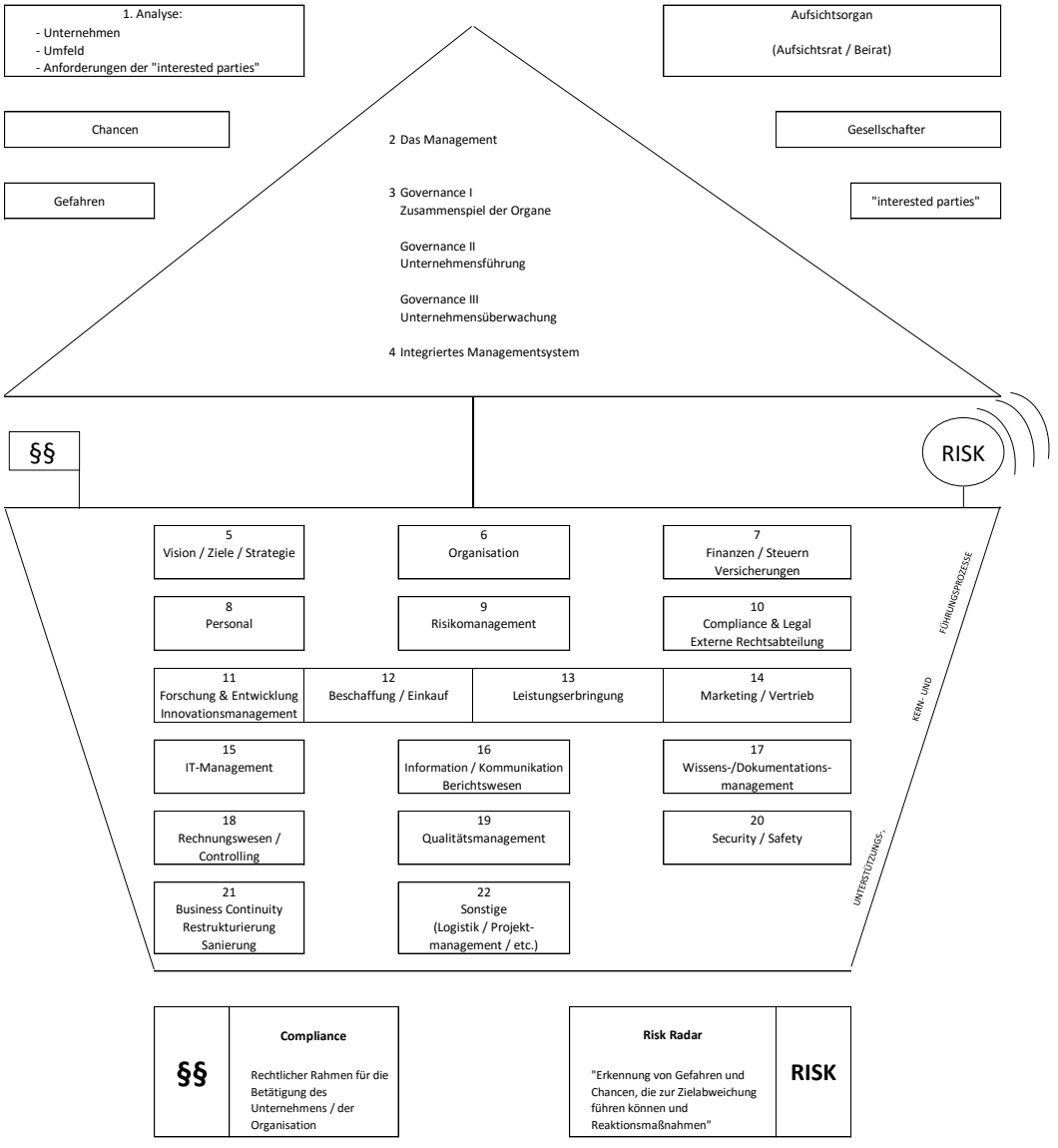

Abbildung 2: Das „Unternehmensschiff“.

1.1.2 Ziele

Ziele und Planung	
Zwingende Ziele:	Planung der Ziel*erreichung*
Freiwillige Ziele:	Entscheidung über Ziel*setzung* und Planung der Ziel*erreichung*

Abbildung 3: Ziele und Planung.

Schwerpunkt des *unternehmerischen* Handelns ist das Erreichen von Zielen.

Dabei ist zu „differenzieren“: Es gibt aufgrund der Legalitätspflicht (Teil von Compliance) zwingende Ziele ohne Ermessens- bzw. Entscheidungsspielräume. Diesbezüglich **muss** nur geplant werden, *wie* diese Ziele unter Beachtung von Ressourcen (Zeit, Geld, Fähigkeiten, etc.) angemessen zu erreichen sind. Über die Zielsetzung selbst ist mangels Spielraum nicht zu entscheiden.

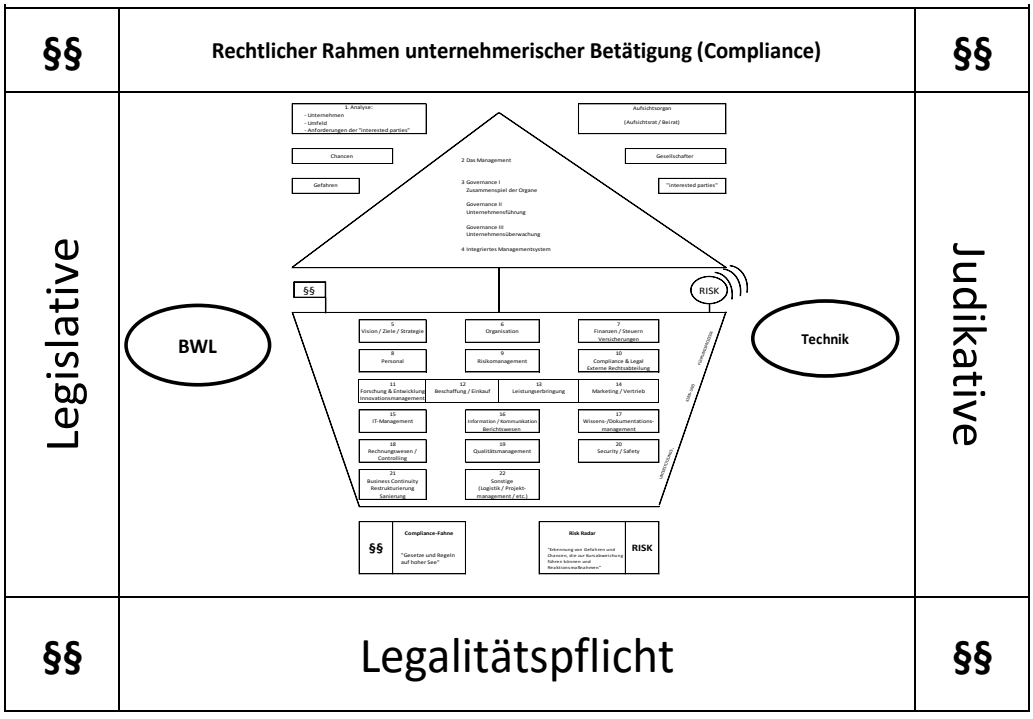

Abbildung 4: Der rechtliche Rahmen bei unternehmerischer Tätigkeit.

Bzgl. der Themen *mit* Entscheidungsspielräumen[3] **muss** zum einen (unter Beachtung der Business Judgment Rule) über die Setzung der Ziele entschieden und die Erreichung der (möglichen) Ziele geplant werden.

1.1.3 Standardorientierung – Anwendungsbereich des *Standards*

Synopse[4]

Zur Rechtsnatur eines Standards:

Ein Standard stellt in der Regel keine verbindliche (Rechts-)Norm dar (Ausnahme, falls ein Gesetz / Rechtsverordnung die Anwendung eines Standards für verbindlich erklärt[5]), sondern kann unter Umständen wie ein „antizipiertes Sachverständigengutachten" wirken und die Vermutung auslösen, einen derzeitigen Entwicklungsstand („Stand von Wissenschaft und Praxis", „Allgemein anerkannte Regeln der Technik"), widerzuspiegeln.[6]

Sofern Gesetze oder Rechtsprechung einen bestimmten Entwicklungsstand fordern *und* der betreffende Standard diesen tatsächlich widerspiegelt, kann der Standard mittelbar als verpflichtend bezeichnet werden.

Auch vertraglich lässt sich die Einhaltung von zu bezeichnenden Standards verbindlich vereinbaren.

[3] Vgl. z.B. unternehmensstrategische Maßnahmen wie Gründung einer Auslandsniederlassung oder *Zertifizierung* eines Compliance- oder Qualitäts-Managementsystems.

[4] Synopse:
ISO 19600:2014: 1 Scope
IDW PS 980:2011: 1. Vorbemerkung
COSO I:2013: F. Summary of Changes to the COSO Internal Control … (1992)
ISO 9001:2015: Einleitung 0.4 Zusammenhang mit anderen Normen zu Managementsystemen / 1 Anwendungsbereich

[5] Vgl. z. B. § 315a HGB und die „IAS-Verordnung der EU".

[6] Vgl. hierzu ausführlich: *Scherer / Fruth,* Der Einfluss von Standards, Technikklauseln und des „Anerkannten Standes von Wissenschaft und Praxis" auf Organhaftung und Corporate Governance - am Beispiel der ISO 19600 (2014) Compliance-Managementsystem, in Corporate Compliance Zeitschrift (CCZ), 2015, S. 9 -17 mit Kommentierung von *Withus*, Die Angemessenheit eines CMS - eine rein juristische Bewertung oder anerkannter Stand von betriebswirtschaftlichen Grundsätzen?, in Corporate Compliance Zeitschrift (CCZ) 2015, S. 139 ff.

Anwendungsbereich dieses hier dargestellten Universal-Standards für ein Compliance-Managementsystem:

Die Vorgaben / Anforderungen dieses Standards sind auf alle Arten von Unternehmen oder Organisationen (öffentlich-rechtlich, privatrechtlich, profit- / non-profit-Organisationen) unabhängig von Größe, Struktur, Natur und Komplexität anwendbar.

Dieser Standard orientiert sich an Anforderungen von Gesetzgebung und Rechtsprechung an Compliance-Managementsysteme und an (international) anerkannten und angewendeten Standards und damit i.d.R. an dem *„Anerkannten Stand von Wissenschaft und Praxis".*[7]

Die ISO (Internationale Organisation für Standardisierung) ist eine weltweite Vereinigung nationaler Standardisierungsorganisationen und erließ diverse Standards, die u.a. auch das Thema Compliance-Managementsystem betreffen: ISO 19600:2014.

Das Institut der Wirtschaftsprüfer in Deutschland (IDW) erließ den *Prüfungs*standard IDW PS 980:2011 für Compliance-Managementsysteme, um einheitlich zu regeln, *wie und was ein Wirtschaftsprüfer* in Bezug auf ein Compliance-Managementsystem zu prüfen hat. Dieser Prüfstandard verlangt, dass sich das Unternehmen an einem angemessenen allgemeinen oder selbst geschaffenen Standard (*„Rahmenkonzepte […] oder […] selbst entwickelte Grundsätze […]")* orientiert.

Für viele Unternehmen werden COSO I (Internal Control) und COSO II (Enterprise Risk Management) eine große Rolle spielen. Gerade die aktuell überarbeitete Version von COSO I:2013 soll nicht mehr nur finanzbezogene Themen, sondern auch die übrigen unternehmensrelevanten Bereiche im Focus haben, weshalb auch dieser Standard Berücksichtigung findet.

Vergleicht man nun die diversen, vielzähligen Standards, so lässt sich ein ähnlicher Aufbau mit sehr ähnlichen inhaltlichen Modulen erkennen. Es existiert also bereits eine Art „mainstream" bzw. *„Anerkannter Stand".* Dies ist als Beitrag zur internationalen Harmonisierung und für das Ziel einer einheitlichen Architektur, die die Kommunikation und Vernetzung diverser Systeme („Industrie 4.0") ermöglicht, sehr zu begrüßen.

Auch die neue Version der DIN ISO 9001:2015 (Qualitätsmanagementsystem) bestätigt den Trend zur Harmonisierung *(„high-level-structure"* und harmonisierte Definitionen) und enthält an zahlreichen Stellen die Forderung nach Compliance *(„Erfüllung gesetzlicher oder behördlicher Anforderungen"*) und Risikomanagement („*risikobasierter Ansatz*"). Da Compliance-Risiken einen erheblichen Teil der Unternehmensrisiken darstellen, **muss** ein „risikobasierter Ansatz" konsequenterweise ebenfalls auch Compliancethemen behandeln.

[7] Da sich der hier vorgestellte Standard überwiegend an zwingenden Vorgaben (Gesetze und Rechtsprechung) und bzgl. der sonstigen Anforderungen an gängige ISO- / COSO- / IDW- / etc.-Standards anlehnt, ist bzgl. der Vorgaben an das ordnungsgemäße Entstehen eines Standards auf die jeweiligen Verfahrensweisen der dort standardsetzenden Organisation zu verweisen.

Die Harmonisierung und Integration diverser „Managementsysteme" versuchte bereits auch der britische Standard PAS 99:2012 als Vorgabe für ein integriertes Management-System.

Das Verständnis der in Standards wiedergegebenen Anforderungen und das Erkennen einer Systematik ist für die Adressaten erforderlich, um die Vorgaben in der täglichen Arbeit leben zu können („Wirksamkeit") und gegebenenfalls Audit-Fragen unterschiedlichster interessierter Gruppen (z.B. Kunden/Behörden/Versicherer/Kreditinstitute [Rating]/Zertifizierer/etc.) beantworten zu können. Deshalb wird für den Standard eine einfache, klare und verständliche Sprache gewählt. Grafiken sollen das Verständnis der Anforderungen des Standards erleichtern.

Im Gegensatz zu einigen *nicht zertifizierbaren* Standards, wie ISO 19600:2014 (Compliance-Managementsystem), ISO 31000:2009 (Risiko-Managementsystem), IDW PS 980:2011 (Compliance-Managementsystem) sieht dieser Standard verbindliche und damit zertifizierbare Anforderungen vor, die sich in den (fett gedruckten) „**muss**"-Formulierungen – in Abgrenzung zu *„soll"* und *„sollte/kann"* widerspiegeln.

1.2 Allgemeines

1.2.1 Begriffserklärung „Compliance-Managementsystem"

Für Managementsysteme finden sich, da keine gesetzlich vorgegebenen Definitionen (Legaldefinitionen) existieren, unterschiedliche Bezeichnungen und Erklärungen: ERP (Enterprise Resources Planning)-System, IMS (Integriertes Management System), Führungssystem, etc.

Definition von Compliance-Managementsystem

Zunächst der *Vorschlag* einer Definition von *Managementsystem*:

Ein Managementsystem besteht aus formell vorgegebenen (idealerweise vernetzten und interagierenden) überwiegend standardisierten Grundsätzen und Komponenten, wie Aufbau- und Ablauforganisation,[8] *mit dem Zweck, eine Organisation bei Zielsetzung und Planung, Steuerung und Überwachung zur Erreichung zwingender und fakultativ gesetzter Ziele zu unterstützen.*

Bzgl. eines *Compliance*-Managementsystems ließe sich darauf aufbauend definieren:[9]

„Aufbau- und Ablauforganisation einer Institution mit interagierenden Komponenten (z. B. Prozessabläufe / Zuständigkeiten, etc.) mit dem Ziel der Sicherstellung von Pflichtenkonformität im Hinblick auf externe und interne verbindliche Vorgaben."

[8] Zuständigkeiten, Aufgaben- und Verantwortungsbereiche, beispielsweise abgebildet in Organigrammen, Stellenbeschreibungen, etc. sowie Prozessabläufe, Delegationen und Interaktionen.
[9] Auch hier gibt es bisher noch keine Legaldefinition, so dass die Definitionsfreiheit viele Vorschläge ermöglicht.

Wie viele Managementsysteme gibt es im Unternehmen?

In der Praxis besteht zum Teil die Ansicht, es gäbe im Unternehmen Raum für eine beliebige Vielzahl von Management*systemen*. Auch in diversen ISO-Standards wird bei der Definition von „Managementsystem" festgestellt, dass es sich auf alle oder einzelne Themenbereiche (z.B. Compliance, QM, Umwelt, etc.) beziehen kann.

Genährt wird dieser viele Manager und Mitarbeiter verunsichernde Gedanke durch die Verabschiedung ständig neuer „*Managementsysteme*" bzw. Standards:

Risikomanagement: ISO 31000:2009, ONR 49000:2014, COSO II:2004, IDW PS 340:2000 (Risikofrüherkennungssystem),
Compliancemanagement: IDW PS 980:2011, ISO 19600:2014, ONR 192050:2013, US Sentencing Guidelines:2010, ISO 37001:2014 (Draft) (Anti-Korruptions-Management) oder andere,
Internes Steuerungs- und Überwachungssystem (ISÜS): COSO I:2013 (Internal Control-Integrated Framework),
Integriertes Managementsystem: PAS 99:2012

und viele mehr.

Die relevanten Anforderungen der Standards (Qualitätsmanagement, Umwelt, Arbeitssicherheit, Risiko- und Compliance, etc.) müssen nicht in einzelnen „Insel-Managementsystemen" behandelt, sondern können durchaus als Komponenten in die Bestandteile der rechtssicheren Organisation (Aufbau- und Ablauforganisation) eingefügt werden.

Abgrenzung von Governance, Management, Risiko und Compliancemanagement

(Corporate) Governance	Ordnungsgemäße Unternehmensführung und -überwachung und ordnungsgemäßes Zusammenspiel der Organe.
Management	Ordnungsgemäße Entscheidungsfindung und Unternehmensführung unter Berücksichtigung relevanter Vorgaben und Anforderungen: Planung, Umsetzung, Bewertung und Verbesserung/Anpassung (P / D / C / A) von Pflicht-Aufgaben und Themen mit Entscheidungsspielraum unter Beachtung der Business Judgment Rule und des *"Anerkannten Standes von Wissenschaft und Praxis"*
Risiko-management	Bewertung der Unsicherheit auf die Erreichung von Zielen und Steuerung bei der Möglichkeit von positiven (Chancen) und negativen (Gefahren) Planabweichungen, um Ziele bestmöglich zu erreichen.
Compliance-management	Planung, Umsetzung, Überprüfung und Verbesserung einer Organisation, um pflichtgemäßes Verhalten und entsprechende Reaktion bei Verstößen zu gewährleisten.

Abbildung 5: Abgrenzung von Governance, Management, Risk und Compliance.

1.2.2 Definitionen *im* Compliance-Management

Synopse[10]

Die für ein Compliance-Managementsystem benötigten Begriffe **müssen** gesammelt und die betroffenen Mitarbeiter entsprechend geschult sein.

Die Begriffe werden unterteilt in:

- „Grundlagenbegriffe“, die auf *jeden* (Prozess-) Themenbereich Anwendung finden, wie z.B. „Organisation“, „Prozessbeschreibung“, „Managementsystem“

Diese sind bzgl. *aller betroffenen Themenbereiche* vor die Klammer zu ziehen und einheitlich und verständlich zu definieren.

- Spezielle Begriffe zu den jeweiligen Themenbereichen, wie z.B. „whistle-blowing“, „Ombudsmann“ oder „Hinweisgeber-System“ bei Compliancemanagement

Die Begriffe sollten im Unternehmen auch (prozess-) themenbezogen dargestellt und geschult werden.

1.2.3 Rechtliche Rahmenbedingungen für ein Compliance-Managementsystem

Aufgrund der „Legalitätspflicht“ der Geschäftsleitung und der Anforderungen an einen „gewissenhaften“ Geschäftsführer, Vorstand, Aufsichtsrat, Kaufmann (§§ 43 GmbHG, 93, 116 AktG, 347 HGB), etc., sowie der Pflicht nach § 130 OWiG, Vorsorge gegen Pflichtverstöße im Unternehmen zu treffen, **muss** eine entsprechende, angemessene, rechtssichere Organisation, die ein funktionierendes Compliance-Managementsystem ermöglicht, vorgehalten werden.

Für das Thema „Compliance-Managementsystem“ *s*ollte eine Art (prozess-) themenfeldbezogenes (Einkauf / Vertrieb / Personal / etc.) „*Rechtskataster*“ angelegt und gepflegt werden; dieses stellt den für jedes Themenfeld maßgeblichen rechtlichen Rahmen dar. Idealerweise werden diese Regelungen in eine verständliche Sprache übersetzt und in Aufbau- und Ablauforganisation implementiert.

[10] Synopse:
ISO 19600:2014: 3 Terms and definition
IDW PS 980:2011: 2. Begriffsbestimmungen
COSO I:2013: 1. Definition of Internal Control; Appendices A. Glossary
ISO 9001:2015: 3 Begriffe

1.2.4 Standards im Bereich Compliance-Managementsysteme

Synopse[11]

Geschäftsleitung und sonstige Verantwortliche **müssen** die jeweiligen von ihr betreuten (Prozess-) Themenfelder / Bereiche an aktuellen Anforderungen aus Gesetzgebung und Rechtsprechung sowie dem *„Anerkannten Stand von Wissenschaft und Praxis“* ausrichten. Diesbezüglich kann es nützlich sein, sich an gängigen aktuellen Standards zu orientieren, um den Versuch der Einhaltung des „*Anerkannten Standes von Wissenschaft und Praxis*“ zu dokumentieren; auch, um auf Audits, Abschlussprüfung oder Zertifizierung gut vorbereitet zu sein.

Der hier vorliegende Standard nimmt primär auf ISO 19600:2014, IDW PS 980:2011, COSO I:2013 Bezug.

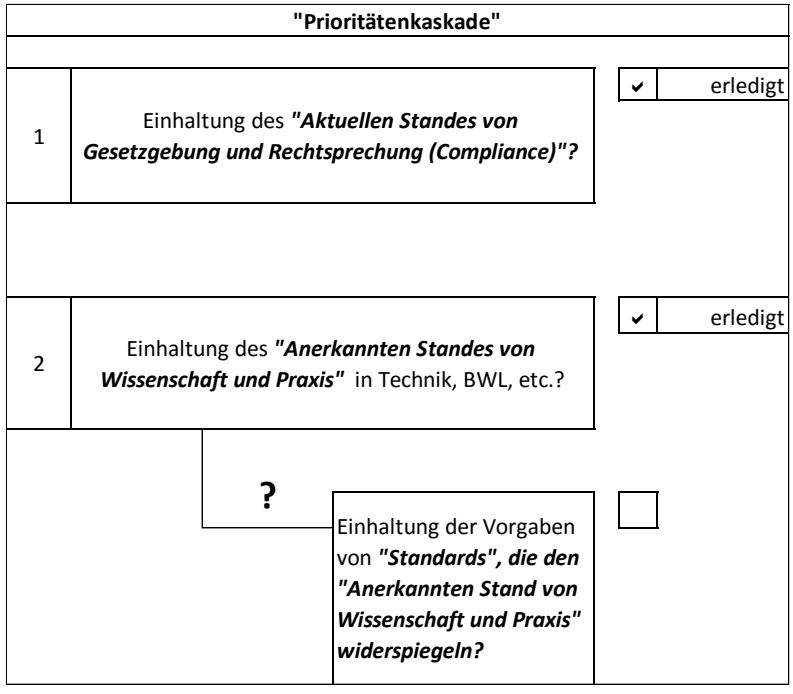

Abbildung 6: Prioritätenkaskade.

[11] Synopse:
ISO 19600:2014: 2 Normative References
IDW PS 980:2011: 6. Anwendungshinweise und Erläuterungen / Konzeption des CMS [Tz. 41 f.] / A30
COSO I:2013: G. Comparison with COSO Enterprise Risk Management - Integrated Framework
ISO 9001:2015: 2 Normative Verweisungen

1.2.5 Tools und Methoden im Bereich Compliance-Management

Die relevanten Tools (Werkzeuge / Arbeitshilfen) und Methoden nach *„Anerkanntem Stand von Wissenschaft und Praxis*" **müssen** bekannt sein und angemessen zur Anwendung gebracht werden.

Für den Bereich Compliance-Management empfiehlt sich eine Matrix, die die jeweils nach *„Anerkanntem Stand von Wissenschaft und Praxis"* relevanten / angemessenen Tools und Methoden (z.B.: Hinweisgebersystem, Compliance-Risikobewertungsmethoden, etc.) auflistet, so dass Vorstand / Geschäftsführung oder die entsprechenden verantwortlichen Delegationsempfänger in ihren Bereichen angemessen über deren sachgerechten Einsatz entscheiden können (Business Judgment Rule).

Zu wichtigen Tools und Methoden allgemein und speziell im Bereich Compliancemanagement gehören (nicht abschließend):

Plan/Do/Check/Act-Methode (P/D/C/A)

vgl. hierzu unten Punkt 1.3

Synopse[12]

Prozessmanagement-Methode:

Synopse[13]

Jedes der ca. 22 (Prozess-) Themenfelder eines Unternehmens stellt ein Hauptprozessfeld als Bestandteil der unternehmensweiten Prozesslandschaft dar, z.B. der Vertriebsprozess, welcher mit den übrigen Prozessfeldern vernetzt sein sollte.

Dieses Hauptprozessfeld kann als Flussdiagramm mit zugehöriger Beschreibung von Prozessschritten, Prozesseignern, mitgeltenden Dokumenten, Compliance-Anforderungen und Risiken, input/output, Kontrollpunkten, etc. dargestellt werden und besteht aus weiteren Unter- / Teil-

[12] Synopse:
ISO 19600:2014: Introduction
IDW PS 980:2011: 3. Rn. 15: „Prozess der Entwicklung und Einführung"
COSO I:2013: 2. Objectives, Components and Principles / Internal Control and the Management Process
ISO 9001:2015: Einleitung 0.3.2 „Planen-Durchführen-Prüfen-Handeln"-Zyklus

[13] Synopse:
ISO 19600:2014: 4.4 Compliance management system and principles of good governance / 8 Operation / 8.1 Operational planning and control / 8.2 Establishing controls and procedures
IDW PS 980:2011: 4. Rn. 23: … „in die Geschäftsabläufe eingebunden" …/… „konkreten Prozessabläufe …"
COSO I:2013: 9. Monitoring Activities / Principle 16 / Point of Focus 72: Integrates with Business Processes
ISO 9001:2015: Einleitung 0.3 Prozessorientierter Ansatz / 4.4 Qualitätsmanagementsystem und seine Prozesse

Prozessfeldern, z.B. Marketing/Akquise, Anfragemanagement, Kundenprüfung, etc., bis hin zu After sales, Produktbeobachtung und Reklamationsmanagement.

Der prozessorientierte Ansatz wird von aktuellen Standards gefordert.

Risikomanagement-Methode:

Synopse[14]

Es gibt für Risikoidentifikation und -bewertung Standard-Methoden, vgl. z.B. ISO 31010 („Riskassessment")

Da auch *Compliance*-Risiken mit Tools und Methoden des Risikomanagements eruiert und bewertet werden, **muss** für Kenntnis und sachgerechte Anwendung auch hier gesorgt werden.

Delegations-Methode: Erfüllung der Anforderungen bei Auslagerungen / Outsourcing (Delegation / Überwachung)

Synopse[15]

Bei Outsourcing / Auslagerungen oder internen / externen Delegationen **muss** darauf geachtet werden, dass der Delegierende die Gesamtverantwortung selbst bei ordnungsgemäßer Delegation in Form einer Überwachungsverantwortung behält und den Delegationsempfänger dazu anhält, sich seinerseits pflichtgemäß zu verhalten.

Die Anforderungen an eine rechtssichere Delegation **müssen** beachtet werden.

Sie bestehen in der Auswahl von geeigneten Delegationsempfängern, in einer entsprechenden Instruktion und einer Überwachung, dass die Leistungen der Delegationsempfänger die Anforderungen: Effektivität, Sicherheit, Rechtssicherheit, Qualität, Termintreue, etc. erfüllen.

---

[14] Synopse:
ISO 19600:2014: 4.6 Identification, analysis and evaluation of compliance risks
IDW PS 980:2011: A 16: Compliance-Risiken; 4. Rn. 23: Compliance-Risiken, A 28: Prozess zur systematischen Erfassung von Compliance-Risiken
COSO I:2013: 6. Risk Assessment / Principles 6 - 9
ISO 9001:2015: Einleitung 0.3.3 Risikobasiertes Denken / A.4 Risikobasiertes Denken / 6.1 Maßnahmen zum Umgang mit Risiken und Chancen

[15] Synopse:
ISO 19600:2014: 8.3 Outsourced processes
IDW PS 980:2011: ./.
COSO I:2013: Appendices / B. Roles and Responsibilities / External parties /
Outsourced Service Providers
ISO 9001:2015: 8.4 Steuerung von extern bereitgestellten Prozessen, Produkten und Dienstleistungen

1.3 Die Konzeptionierung, Umsetzung, Überwachung und (kontinuierliche) Verbesserung (Plan/Do/Check/Act) eines integrierten, standardorientierten Compliance-Managementsystems

Synopse[16]

Die Plan/Do/Check/Act-Methode: Ziele und Planung, Steuerung und Überwachung

Zunächst werden Ziele und der zu erzielende Wertbeitrag des unternehmerischen Handelns definiert, die Strategie festgelegt und die Vorgehensweise geplant. Dies lässt sich auch mit strategischer „Planungsphase" umschreiben und entspricht der Phase „Plan".

Die Steuerung und Überwachung sorgt mit Identifikation der Ziele, deren Anforderungen und durchzuführenden Maßnahmen, um diese Ziele zu erreichen, sowie mit Aufgabenverwaltung (to-do-Verwaltung), Projektmanagement, etc. für eine plangerechte Umsetzung und stellt z.B. durch Soll-Ist-Vergleiche fest, ob Planabweichungen oder Veränderungen in Umfeld oder Organisation Korrekturmaßnahmen erfordern (welche wiederum geplant und gesteuert werden): Do, Check, Act.

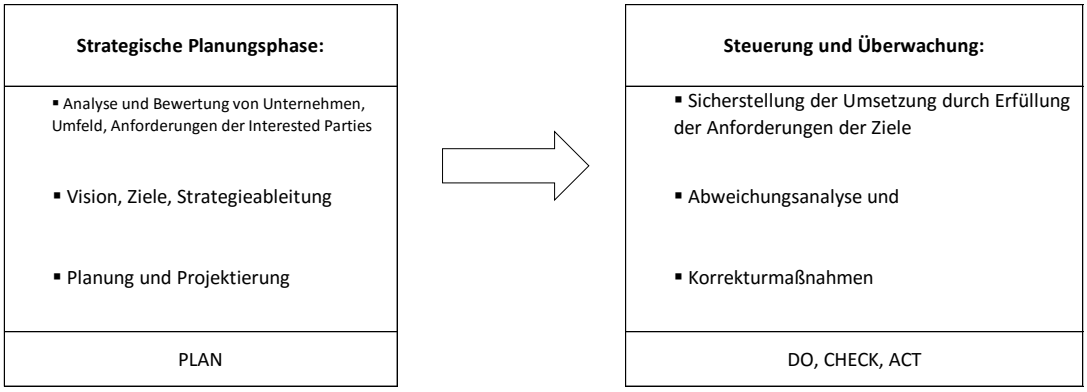

Abbildung 7: Ziele und Planung, Steuerung und Überwachung.

[16] Synopse:
ISO 19600:2014: Introduction / 8 Operation / 8.1 Operational planning and control / 8.2 Establishing controls and procedures
IDW PS 980:2011: 3. Rn. 15: … „Prozess der Entwicklung und Einführung" …
COSO I:2013: 2. Objectives, Components, and Principles / Introduction / An organization adopts a mission and vision, sets strategies, establishes objectives it wants to achieve, and formulates plans for achieving them …
ISO 9001:2015: Einleitung 0.3.2 „Planen-Durchführen-Prüfen-Handeln"-Zyklus / 8 Betrieb / 8.1 Betriebliche Planung und Steuerung

1.3.1 Konzeptionierung von Aufbau und Inhalt des Compliance-Managementsystems (Plan): Darstellung von Zielen und Wertbeitrag, des Soll-Zustandes, Soll-Ist-Abgleich, Bewertung von alternativen Strategien, Entscheidung, Projektierung

Synopse[17]

Der vom Unternehmen dargestellte Soll-Zustand des Compliance-Managementsystems im Konzept **muss** ebenso, wie der zu erreichende Ist-Zustand, *angemessen* sein, d.h. geeignet, die Ziele des Compliance-Managementsystems zu erreichen. Eine Auswahl erforderlicher Komponenten eines Compliance-Managementsystems findet sich in diesem Standard.

Das Ergebnis des Soll-Ist-Abgleichs **muss** zutreffend dargestellt werden. Es kann zugleich – ebenso wie ein Handbuch – die Compliance-Managementsystem-*Beschreibung* darstellen und darf keine wesentlichen Lücken oder Schwachstellen aufweisen.

1.3.2 *Konzeptionierung* der Umsetzung (Do) (Implementierung und Wirksamkeit), Überwachung (Check) und Verbesserung (Act) des Compliance-Managementsystems

Synopse[18]

Konzeptionierung der Umsetzung (Do)

Die Umsetzung besteht aus Implementierung und Herbeiführung der Wirksamkeit: Auch dies **muss** – unter Berücksichtigung des notwendigen inputs (Anforderungen und benötigte Ressourcen) – konzeptioniert / geplant werden.

---

[17] Synopse:
ISO 19600:2014: 4 Context of the organization / 6 Planning / 6.1 Actions to address compliance risks / 6.2 Compliance objectives and planning to achieve them
IDW PS 980:2011: 5.4 Prüfungsdurchführung / 5.4.1.2 Konzeption des CMS
COSO I:2013: 2. Objectives, Components, and Principles / Introduction / An organization adopts a mission and vision, sets strategies, establishes objectives it wants to achieve, and formulates plans for achieving them …
ISO 9001:2015: 4 Kontext der Organisation / 6 Planung / 6.1 Maßnahmen zum Umgang mit Risiken und Chancen / 6.2 Qualitätsziele und Planung zu deren Erreichung / 6.3 Planung von Änderungen

[18] Synopse:
ISO 19600:2014: 6 Planning
IDW PS 980:2011: 3. Gegenstand, Ziel und Umfang der Prüfung: Rn. 20/21; 5.4 Prüfungsdurchführung / 5.4.1.2 Konzeption des CMS
COSO I:2013: 2. Objectives, Components, and Principles / Introduction / An organization adopts a mission and vision, sets strategies, establishes objectives it wants to achieve, and formulates plans for achieving them …
ISO 9001:2015: 6 Planung für das Qualitätsmanagementsystem / 6.3 Planung von Änderungen

Konzeptionierung der Implementierung (Anreicherung der Aufbau- und Ablauforganisation)

Die Anreicherung der Geschäftsprozesse mit Schritten zur Erfüllung der Compliance-Anforderungen **muss** frühzeitig geplant und projektiert werden. Hierzu gehört z.B. die rechtzeitige Klärung der Frage, wie Prozessabläufe einheitlich visualisiert, beschrieben und dokumentiert werden.

Konzeptionierung der Herbeiführung der Wirksamkeit („Gelebt werden")

In einem Konzept / Projektplan ist an dieser Stelle beispielsweise festzuhalten, welche Kompetenzen (Wissen / Wollen / Können) schon vorhanden oder noch zu erwerben sind, wann wer wie von wem in welchen Inhalten geschult / gecoacht / trainiert wird, wann Compliance-Themen wie in Zielvereinbarungen aufgenommen werden, etc.

Dabei **müssen** auch interne (z.B. neue Mitarbeiter) und externe (z.B. neue Gesetze / Rechtsprechung) Veränderungen berücksichtigt werden.

Konzeptionierung der Überwachung / Bewertung (Check) mit Wertbeitragsmessung (Performance Evaluation)

Vgl. unten Pkt. 3.12: Dort werden die Bestandteile eines „Internen Steuerungs- und Überwachungssystems in Bezug auf das Compliance-Managementsystem" dargestellt.

Die *Umsetzung* auch dieser System-Überwachungs- und Bewertungsmaßnahmen **muss** ebenfalls geplant werden.

Konzeptionierung der (kontinuierlichen) Verbesserung / Anpassung (Act)

Synopse[19]

Bereits bei der Konzeption des Compliance-Managementsystems **muss** mit geplant werden, wie der (kontinuierliche) Verbesserungsprozess und Anpassungsprozess bei Veränderungen in Bezug auf das Compliance-Managementsystem gestaltet und gelebt werden kann.

[19] Synopse:
ISO 19600:2014: 7 Support / 8 Operation / 9 Performance evaluation / 10 Improvement
IDW PS 980:2011: A11 und A 20: Compliance-Überwachung und Verbesserung
COSO I:2013: 2. Objectives, Components, and Principles / Introduction / An organization adopts a mission and vision, sets strategies, establishes objectives it wants to achieve, and formulates plans for achieving them …
ISO 9001:2015: 7 Unterstützung / 8 Betrieb / 9 Bewertung der Leistung / 10 Verbesserung

1.3.3 *Ausführung:* Umsetzung (Do), Überwachung (Check), Verbesserung (Act)

Hier geht es um das tatsächliche Doing:

All das, was konzeptioniert und projektiert wurde, **muss** nun in die Tat umgesetzt werden. Die Erreichung der in der Konzeptionierung festgelegten Ziele stellt ein effektives Steuerungs- und Überwachungssystem sicher.

2 Analyse von Unternehmen, Umfeld, etc. und Ableitung des Unternehmensrahmens („Block 2“)

Der aus der Analyse von Unternehmen, Umfeld und Anforderungen der „interested parties“ abgeleitete Unternehmensrahmen (mit Unternehmensstrategie, -politik, -organisation, -kommunikation, -dokumentation) sichert das integrierte, einheitliche Vorgehen in den diversen Themengebieten des Unternehmens.

2.1 Analyse von Unternehmen, Umfeld und Anforderungen der „Interested parties“

Block 2.1: Analyseprozesse

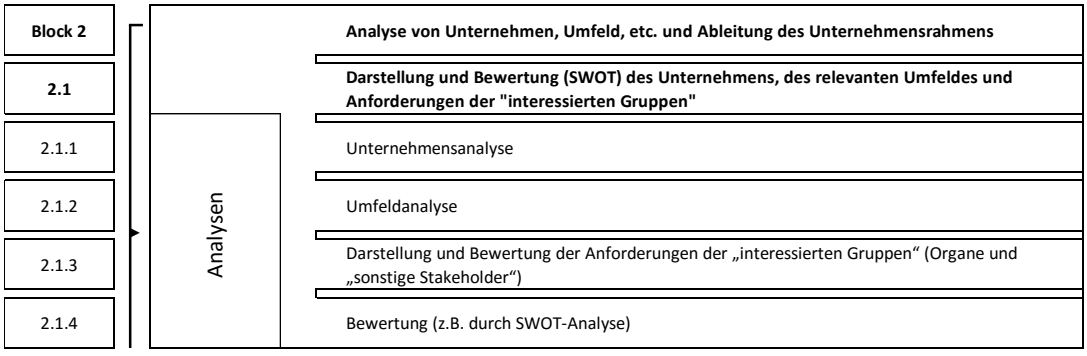

Abbildung 8: Integriertes, standardorientiertes Compliance-Managementsystem in 4 Blöcken - Block 2.1: Analysen.

Block 2.2: Ableitung des Unternehmensrahmens

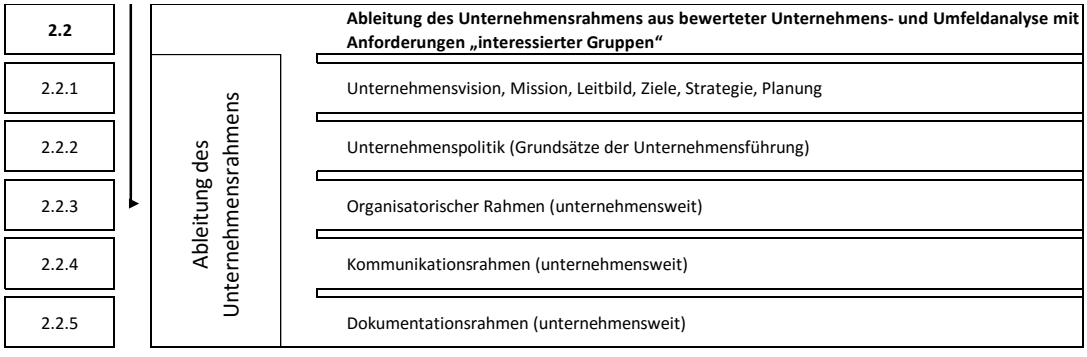

Abbildung 9: Integriertes, standardorientiertes Compliance-Managementsystem in 4 Blöcken - Block 2.2: Unternehmensrahmen.

Der „Block 2“ (2.1 und 2.2) ist im Unternehmen – unabhängig von der Frage, wie viele Themenbereiche (Qualitätsmanagement, Compliance, Personal, Risk, etc.) über das ganzheitliche, integrierte Managementsystem behandelt werden – nur *ein einziges Mal* zu installieren.

2.1.1 Unternehmensanalyse

Synopse[20]

Es **muss** eine Analyse der Unternehmenscharakteristika durchgeführt und dokumentiert werden, um eine Art „Steckbrief des Unternehmens" zu erstellen. Dies sollte der erste Schritt sein und erst danach folgt die Umfeldanalyse, da erst *nach* Charakterisierung des Unternehmens klar wird, welche der vielfachen Umfeldentwicklungen für das konkrete Unternehmen relevant sind.

Es empfiehlt sich eine Kurzdarstellung des Geschäftsmodells („Business-Plan" light) und aller Unternehmensbereiche und Durchleuchtung mittels SWOT-Analysen oder sonstiger angemessener Bewertungsmethoden – auch in Hinblick auf Veränderungen:

Von der Rechtsform, dem Geschäftsmodell, der Managementqualifikation über Strategie, Organisation, Finanzen, Personal, Governance mit Risiko- und Compliance-Management zu Forschung und Entwicklung, Beschaffung, Leistungserbringung, Marketing und Vertrieb.

Auch die unterstützenden Bereiche wie IT, Controlling, Wissens- und Informationsmanagement sowie das (Qualitäts-) Managementsystem sollten beleuchtet werden.

2.1.2 Umfeldanalyse

Synopse[21]

Im Rahmen der zukunftsorientierten Strategieentwicklung **muss** regelmäßig eine Umfeldanalyse durchgeführt werden. Sie nimmt idealerweise Stellung zu: Markt (Bedürfnisse, Verhalten, etc.), Branche, Wettbewerb, gesamtwirtschaftlichen, rechtlich-politischen, gesellschaftlichen und wissenschaftlich-technischen und sonstigen relevanten Gegebenheiten und Entwicklungen.

[20] Synopse:
ISO 19600:2014: 4 Context of the organization / 4.1 Understanding the organization and its context
IDW PS 980:2011: 5.4.1. Prüfungshandlungen zur Risikobeurteilung / 5.4.1.1 Kenntnisse über das rechtliche und wirtschaftliche Umfeld des Unternehmens, Rn. 40 und Tz. A29
COSO I:2013: Komponente (2): Risikobeurteilung (Risk Assessment) / Prinzip 9 / Fokuspunkt 36
ISO 9001:2015: 4 Kontext der Organisation / 4.1 Verstehen der Organisation und ihres Kontextes

[21] Synopse:
ISO 19600:2014: 4 Context of the organization / 4.1 Understanding the organization and its context
IDW PS 980:2011: 5.4.1.1 Kenntnisse über das rechtliche und wirtschaftliche Umfeld des Unternehmens / Tz. A29
COSO I:2013: Komponente (2): Risikobeurteilung (Risk Assessment) / Prinzip 9 / Fokuspunkt 35
ISO 9001:2015: Kontext der Organisation / 4.1 Verstehen der Organisation und ihres Kontextes

2.1.3 Darstellung und Bewertung der Anforderungen der „interessierten Gruppen“ (Organe und „sonstige Stakeholder“)

Synopse[22]

Das Unternehmen (die Organisation) **muss** die – auch für das Compliance-Managementsystem – relevanten interessierten Gruppen und deren Anforderungen bestimmen.

Interessierte Gruppen sind z. B. Organe, wie Geschäftsführung, Gesellschafterversammlung, Aufsichtsorgan oder Sonstige, wie z. B. Arbeitnehmer, Betriebsrat, Kunden, Lieferanten, Behörden (z. B. Gewerbeaufsichtsamt, Zoll, Finanzamt, etc.), Medien.

Mögliche Anforderungen mehrerer unterschiedlicher Gruppen sind z. B. funktionierendes Compliance-Management (Pflichtenbefolgung) oder Transparenz. Die Anforderungen **müssen** bewertet und sich daraus ergebende erforderliche Maßnahmen (z.B. für das Compliance-Managementsystem) umgesetzt werden.

2.1.4 Bewertung (z.B. durch SWOT-Analyse)

Bei der Bewertung (mit angemessenen Methoden, z.B. durch SWOT-Analyse) der Feststellungen oben aufgeführter Analysen und Anforderungen **muss** darauf geachtet werden, dass die Analyse auf *möglichst* umfassender und vollständiger Information beruht und die Bewertung so exakt wie möglich dargestellt wird.

Aus dem Ergebnis der Analyse **müssen** schließlich Handlungsempfehlungen abgeleitet werden, hier nachfolgend insbesondere die Ausgestaltung des „Unternehmensrahmens“.

2.2 Ableitung des *Unternehmensrahmens* aus bewerteter Unternehmens- und Umfeldanalyse mit Anforderungen „interessierter Gruppen“

Der aus bewerteter Analyse abgeleitete Unternehmensrahmen besteht – für das gesamte Unternehmen – aus Unternehmensvision/ -zielen/ -strategie, Unternehmenspolitik und unternehmensweit vereinheitlichten Organisations-, Kommunikations- und Dokumentationsvorgaben.

[22] Synopse:
ISO 19600:2014: 4 Context of the organization / 4.2 Understanding the needs and expectations of interested parties
IDW PS 980:2011: 5.4.1. Prüfungshandlungen zur Risikobeurteilung
COSO I:2013: Komponente (2): Risikobeurteilung (Risk Assessment) / Prinzip 9 / Fokuspunkt 35 / Komponente (4): Information und Kommunikation (Information and Communication) / Prinzip 15 / Fokuspunkte 63-67
ISO 9001:2015: 4 Kontext der Organisation / 4.2 Verstehen der Erfordernisse und Erwartungen der interessierten Parteien / A.3 Verstehen der Erfordernisse und Erwartungen interessierter Parteien

2.2.1 Unternehmensvision, Mission, Leitbild, Ziele, Strategie, Planung

Den ersten Teil des Unternehmensrahmens bilden Unternehmensvision, -mission, -leitbild, -ziele,
-strategie und -planung.

Die zwingende Verpflichtung der Geschäftsleitung zur kurz-, mittel- und langfristigen Planung **muss** beachtet werden.

2.2.2 Unternehmenspolitik *(Grundsätze der Unternehmensführung)*

Unternehmenspolitik ist z.T. schwer von Vision, Leitbild oder Strategie abzugrenzen. Sie könnte folgendermaßen definiert werden:

„Grundsätzliche Aussagen zur Ausgestaltung eines wesentlichen Unternehmensthemas, soweit unternehmerisches Ermessen diesbezüglich vorhanden ist".

All das, was ein *gewissenhafter* Geschäftsführer / Vorstand / Unternehmer / Kaufmann etc. *zwingend* nach *„Anerkanntem Stand von Wissenschaft und Praxis"* machen würde, unterliegt nicht seinem Ermessen und ist damit keine „politische" Entscheidung.

Entsprechend sollte die Unternehmenspolitik also vor allem *grundlegende Entscheidungen* in Bezug auf die Unternehmensausrichtung dokumentieren und kommunizieren, z.B. Innovationsführerschaft, „best in class", starke Ausrichtung auf ökonomische, soziale, ökologische Nachhaltigkeit, etc.

2.2.3 Organisatorischer Rahmen (unternehmensweit)

An dieser Stelle wird *unternehmensweit* einheitlich vorgegeben, wie die Unternehmensorganisation im konkreten Unternehmen ausgeführt wird:

Beispielsweise sollten Stellenbeschreibungen in einem einheitlichen, unternehmensweit geltenden Muster mit allen (rechtlich) erforderlichen Bestandteilen ausgeführt, Prozessbeschreibungen in einer einheitlich festgelegten Darstellungs- und Visualisierungsform, die Delegation einheitlich und auf rechtsicheren Vorgaben beruhend vorgenommen werden.

Relevante Bestandteile eines Konzepts für rechtssichere Unternehmensorganisation **müssen** angemessen vorgehalten werden:

Das Organisationskonzept sollte – nicht abschließend – folgende Komponenten beinhalten, die jede für sich den Anforderungen der Gesetze und Rechtsprechung genügen **muss**:

1. (Den rechtlichen Anforderungen genügende) gesellschaftsrechtlich angemessene Unternehmensstruktur (gegebenenfalls auch Holding-Konzernstruktur)
2. Rechtssichere Organigramme (Konzern-, Unternehmens-, Bereichsorganigramme)
3. Schnittstellenmanagement (Kommunikation und Kooperation der notwendigen Schnittstellen zwischen den einzelnen (Prozess-) Themenbereichen und gegebenenfalls auch zu „Sonstigen" („interested parties", vgl. „Industrie 4.0"))
4. Rechtssichere Stellenbeschreibungen

5. Rechtssicheres Interaktionsmanagement (rechtssichere Regelung, wie die Organe, Gesellschaften (falls Konzernstruktur gegeben), Abteilungen, etc. interagieren u.a. in Hinblick auf: Aufgaben- und Verantwortungsbereiche / Vertretung / Stellvertretung / Aufsicht / Weisung / Kommunikation / etc.)
6. Rechtssichere Delegation (durch Auswahl geeigneter Delegationsempfänger, Instruktion und Überwachung – auch Externer)
7. Rechtssichere Prozessbeschreibungen (Verfahrensanweisungen)
8. Wirksame Aufsichts- bzw. Kontrollmechanismen (auch in Hinblick auf Compliance) – auch, falls Leistungen von Externen erbracht werden (z.B. im Rahmen von outsourcing, z. B. bei Auslagerungen/Belieferung oder Delegation)
9. Implementiertes und wirksames Informations- und Kommunikationsmanagement
10. Implementiertes und wirksames Dokumentationsmanagement
11. Unterstützendes (integriertes) Managementsystem
12. Angemessene Personalressourcen (in Quantität und Qualität (Kompetenzen))

    – In vielen Fällen werden von Gesetzgebung oder Rechtsprechung fehlende Dokumentation und / oder unzureichende Personalressourcen als *grobe* Organisationspflichtverletzung mit verschärften Sanktionen (z.B. Beweislastumkehr, sogar bzgl. Ursächlichkeit der Pflichtverletzung für den Schaden) gewertet.

2.2.4 Kommunikationsrahmen (unternehmensweit)

Synopse[23]

Ein einheitlicher *unternehmensweit* geltender Kommunikationsrahmen **muss** Aussagen treffen, wer? was? wie? wann? und an wen? („5xW“) kommuniziert.

Bei der Kommunikation **muss** interne und externe Kommunikation unterschieden und gesteuert werden.

[23] Synopse:
ISO 19600:2014: 7 Support / 7.4 Communication
IDW PS 980:2011: 4. Grundelemente eines CMS / „Compliance-Kommunikation“ / 6. Anwendungshinweise und Erläuterungen / Grundelemente eines CMS [Tz. 23], A19 „Compliance-Kommunikation“
COSO I:2013: Komponente (4): Information und Kommunikation (Information and Communication) / Prinzip 13 / Fokuspunkte 54-58 / Prinzip 14 / Fokuspunkte 59-62 / Prinzip 15 / Fokuspunkte 63-67
ISO 9001:2015: 7 Unterstützung / 7.4 Kommunikation

2.2.5 Dokumentationsrahmen (unternehmensweit)

Synopse[24]

Die Lenkung (Erstellung und weitere Behandlung) von Dokumenten (einheitlichen Formularen / Mustern wie z.B. Muster-Stellenbeschreibung, etc.) und Aufzeichnungen (individuelle Schriftstücke, wie z.B. ein ausgefülltes Formular oder ein Vertrag) **muss** nach den allgemeinen *unternehmensweit* geltenden, den rechtlichen Anforderungen genügenden, Grundsätzen erfolgen.[25]

Die Dokumente und Aufzeichnungen sind idealerweise je nach Art unternehmensweit einheitlich gestaltet und auch die Frage, wer? was? wie? wann? rechtssicher dokumentiert und archiviert, sollte einheitlich unternehmensweit geregelt sein.

2.2.6 Exkurs: Integriertes Managementsystem (IMS)

An dieser Stelle ist zu unterscheiden, ob ein

Integriertes Managementsystem (*ein einziges* Managementsystem, das die Anforderungen diverser Themen / Standards (z.B. QM, Umwelt, Arbeitssicherheit, Risikomanagement, Compliancemanagement, etc. behandelt), gewollt ist, oder das

Compliance-Managementsystem als „isoliertes" Managementsystem („Insellösung") betrieben wird.

Falls ein Integriertes Managementsystem oder „GRC-System" gewünscht ist, sollte dieses als solches ebenfalls konzipiert und umgesetzt werden, *bevor* einzelne spezielle Themenbereiche, wie z.B. „Compliance-Managementsystem" behandelt werden, da letzteres ja in das IMS integriert wird.

[24] Synopse:
ISO 19600:2014: 7.5 Documented information
IDW PS 980:2011: 3. Rn. 13 Dokumentation des CMS; 4. Rn. 23: … „Voraussetzung ist … ausreichende Dokumentation des CMS …"
COSO I:2013: 4. Additional Considerations / Documentation
ISO 9001:2015: 7.5 Dokumentierte Information / 7.5.1 Allgemeines / 7.5.2 Erstellen und Aktualisieren / 7.5.3 Lenkung dokumentierter Informationen

[25] Vgl. die Vorgaben aus dem Qualitätsmanagement ISO 9001:2015 und unten Punkt 3.8.3.

3 Allgemeine Regelungen des Compliance-Managementsystems („Block 3“)

Die Geschäftsleitung **muss für das Compliance-Managementsystem** *allgemeine Regelungen* vorgeben und für deren Beachtung sorgen:

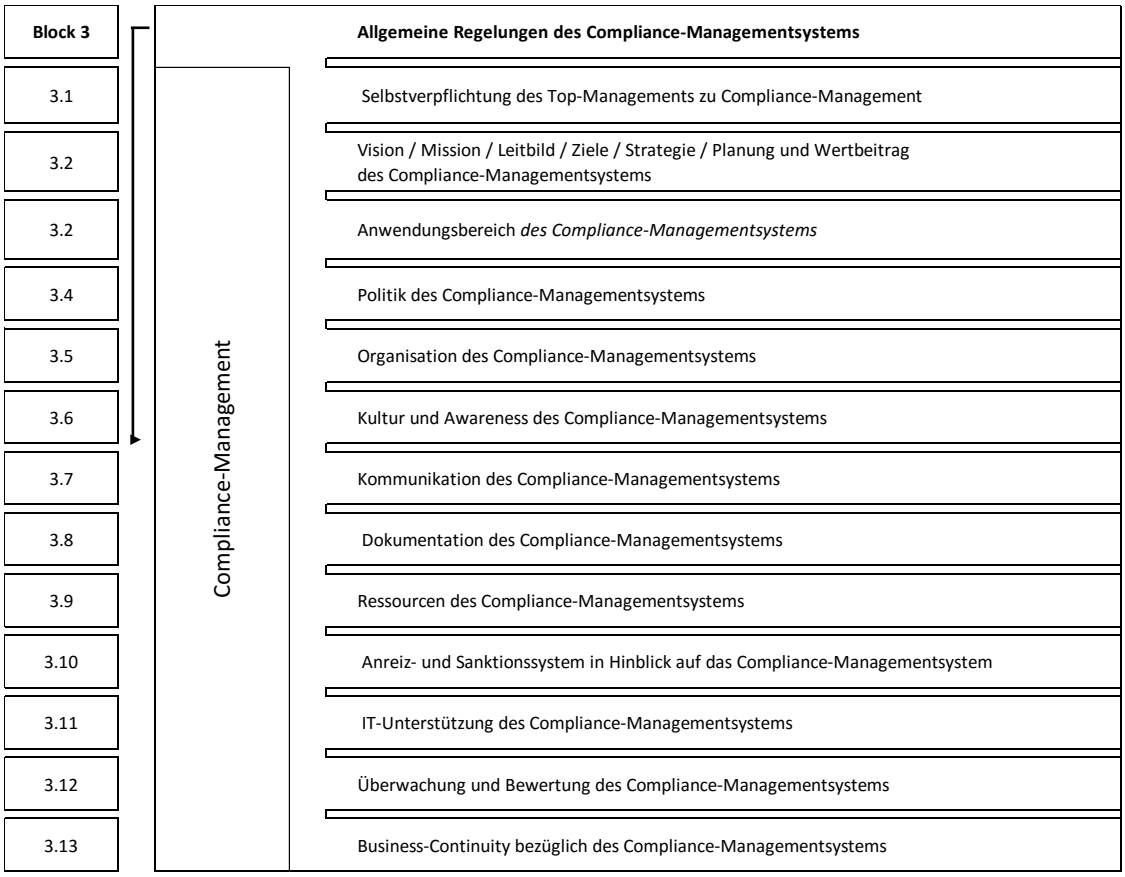

Abbildung 10: Integriertes, standardorientiertes Compliance-Managementsystem in 4 Blöcken - Block 3: Allgemeine Regelungen.

3.1 Selbstverpflichtung des Top-Managements zu Compliance-Managementsystem

Synopse[26]

Das Top Management (Geschäftsführung / Vorstand, etc.) **muss** mit Vorbildcharakter das Compliance-Managementsystem fördern:

Es **muss** die in diesem Standard dargestellten Komponenten des Compliance-Managementsystems transparent machen, konzeptionieren, in Aufbau- und Ablauforganisation implementieren, für Wirksamkeit (gelebt werden), Bewertung und Überwachung, kontinuierliche Anpassung bei internen und externen Veränderungen und Verbesserung des Reifegrades sorgen, sowie intern und extern kommunizieren.

Das Top Management **muss** die Grundzüge des Compliance-Managementsystems verstehen und über den sachgemäßen Einsatz angemessener Tools und Methoden entscheiden können.

Das Bekenntnis zu Compliancemanagement darf bei Vorgesetzten nicht nur ein „Lippenbekenntnis" sein, sondern **muss** vorgelebt werden.

3.2 Vision, Mission, Leitbild, Ziele, Strategie, Planung und Wertbeitrag des Compliance-Managementsystems

Synopse[27]

Heruntergebrochen von *unternehmensweiter* Vision, Mission, Leitbild, Zielsetzung, Unternehmens-Strategie und Planung auf den Bereich Compliance-Management **müssen** verpflichtende und freiwillig beschlossene Compliancemanagement-Ziele und -strategie messbar/nach-prüfbar (SMART) dokumentiert, geplant und kommuniziert werden.

Die Vision für das Compliance-Managementsystem könnte z.B. die Erreichung eines sehr hohen Reifegrades (z.B. „Stufe 4" oder „5", vgl. unten 3.12.5) sein.

Die Ziele des Compliance-Managementsystems sind (nicht abschließend):

---

[26] Synopse:
ISO 19600:2014: 5 Leadership / 5.1 Leadership and commitment / 7 Support / 7.3.2.2 Role of top management in encouraging compliance
IDW PS 980:2011: 3. Gegenstand, Ziel und Umfang der Prüfung, Rn. 13
COSO I:2013: Komponente (1): Kontrollumfeld (Control Environment) / Prinzip 1 / Fokuspunkte 1-4
ISO 9001:2015: 5 Führung / 5.1 Führung und Verpflichtung / 5.1.1 Allgemeines / 5.1.2 Kundenorientierung / 9. Bewertung der Leistung / 9.3 Managementbewertung

[27] Synopse:
ISO 19600:2014: 6 Planning
IDW PS 980:2011: 4. Grundelemente eines CMS / „Compliance-Ziele"
COSO I:2013: Komponente (2): Risikobeurteilung (Risk Assessment) / Prinzip 6 / Fokuspunkte 21a, 21b, 21c, 21d, 22a, 22b, 22c, 23, 24, 25, 26
ISO 9001:2015: 6 Planung / 6.2 Qualitätsziele und Planung zu deren Erreichung

- die Erzeugung von Transparenz über bestehende, sich ändernde und gerade neu entstehende zwingende externe und interne Anforderungen / Pflichten
- die angemessene Implementierung, Wirksamkeit, Bewertung und Verbesserung einer Aufbau- und Ablauforganisation, die die Einhaltung von Pflichtvorgaben sicherstellt
- im Bereich von Entscheidungsspielräumen die Sicherstellung der Anwendung der sog. Business Judgment Rule
- die Durchführung von Entscheidungen und Planungen sowie die Steuerung und Überwachung erforderlicher Maßnahmen, die das pflichtgemäße Agieren von Unternehmen, Management und Mitarbeitern fördern und sicherstellen.
- das Erkennen, Bewerten und Steuern von Compliance-*Risiken* (Gefahren und Chancen bzw. der Auswirkungen von Unsicherheiten bzgl. pflichtgemäßen Agierens auf das Erreichen der Unternehmensziele) sowie
- Compliance-V*erstöße* (die auch trotz eines funktionierenden Compliance-Managementsystems nicht völlig auszuschließen sind), frühzeitig zu entdecken, zu steuern und als Informationsquelle für Verbesserungsmaßnahmen zu nutzen.

Ein positiver Wertbeitrag des Compliance-Managementsystems (Differenz zwischen Nutzen und Aufwand) hängt stark vom erreichten Reifegrad (vgl. unten 3.12.5) des Compliance-Management-systems ab.

3.3 Anwendungsbereich *des Compliance-Managementsystems*

Synopse[28]

Im Rahmen der Frage des Anwendungsbereiches ist zu klären, ob das Compliance-*Management-system* (nicht: der *Standard,* vgl. dazu oben Pkt. 1.1.3) nur einzelne Funktionen / Bereiche des jeweiligen Rechtssubjekts (Unternehmen oder Körperschaften) behandelt oder alle: z.B. nur Inlandsgesellschaften oder alle Unternehmen einer „Gruppe"; nur Einkauf und Vertrieb oder alle (Prozess-) Themenfelder; nur Anti-Korruption oder Kartellrecht oder *alle* relevanten Anforderungen.

[28] Synopse:
ISO 19600:2014: 4 Context of the organization / 4.3 Determining the scope of the compliance management system
IDW PS 980:2011: 6. Anwendungshinweise und Erläuterungen / Vorbemerkungen [Tz. 1 ff.], A1-A3
COSO I:2013: 2. Objectives, Components, and Principles / Relationship of Objectives, Components, and the Entity / Entity Structure
ISO 9001:2015: 4 Kontext der Organisation / 4.3 Festlegen des Anwendungsbereiches des Qualitätsmanagementsystems

Compliancemanagement **muss** sich aufgrund des Legalitätsprinzips allerdings nicht nur auf einzelne Themenfelder oder Rechtsgebiete, sondern auf alle darunter fallende Anforderungen beziehen.

Natürlich kann bei der Einführung zunächst mit einzelnen Themen begonnen werden. Dass dies in den übrigen Bereichen nicht von der Legalitätspflicht befreit, **muss** klargestellt werden. Die Konzeptionierung sollte jedoch von Anfang an unternehmensweit und umfassend angelegt sein.

Außerdem darf es auch bzgl. der relevanten Rechtsthemen im Rahmen des Legalitätsprinzips keine Bereichsausnahmen geben.

3.4 Politik/Grundsätze des Compliance-Managementsystems

Synopse[29]

Die Politik des Compliance-Managementsystems wird aus der *Unternehmens*-Politik (vgl. oben Pkt. 2.2.2) abgeleitet.

All das, was ein *gewissenhafter* Geschäftsführer / Vorstand / Unternehmer / Kaufmann etc. *zwingend* nach *„Anerkanntem Stand von Wissenschaft und Praxis"* machen würde, unterliegt nicht seinem Ermessen und ist damit keine „politische" Entscheidung.

In Hinblick auf Compliance-Risiken verbietet sich daher aufgrund des Legalitätsprinzips die Festlegung eines „Compliance-Risikoappetits". Vielmehr **muss** in diesem Bereich „Compliance-Risikoaversion" beschlossen und kommuniziert werden.

Viele weitere Pflichtthemen oder an anderen Stellen in Compliance-Managementsystem-*Beschreibung*, -konzept, -oder -handbuch enthaltene Komponenten müssen nicht zwingend in der Compliance-Managementsystem-Politik wiederholt werden.

Entscheidungsspielraum besteht jedoch z.B. bei der Frage, ob Compliancemanagement als „Insel-Managementsystem" implementiert oder in ein (bereits vorhandenes) System integriert (IMS) wird. Jedoch ***müssen*** auch bei einer „Insel-Lösung" zwingend die Schnittstellen zu den anderen (Prozess-) Themenfeldern beachtet werden.

Ob Compliancemanagement zentral oder dezentral implementiert wird, ist ebenfalls Ermessenssache und damit in der „Politik" zu regeln.

Auch ist regelbar, ob das Unternehmen mit Management und Mitarbeitern lediglich dem *„Anerkannten Stand von Wissenschaft und Praxis"* bzgl. des Compliance-Managements entsprechen wollen (weniger wäre nicht erlaubt) oder „best in class" oder auf „höchstem Reifegrad" unter Berücksichtigung des *neuesten* Standes der Wissenschaft zu sein wünschen.

---

[29] Synopse:
ISO 19600:2014: 5 Leadership / 5.2 Compliance policy
IDW PS 980:2011: 4. Rn. 23: Compliance-Ziele; A14: Compliance-Kultur; A15: Compliance-Ziele
COSO I:2013: 2. Objectives, Components, and Principles / Introduction / An organization adopts a mission and vision, sets strategies, establishes objectives it wants to achieve, and formulates plans for achieving them …
ISO 9001:2015: 5 Führung / 5.2 Politik

Auch bei der „Politik“ ist auf eine verständliche, knappe Ausdrucksweise Wert zu legen und alle betroffenen Mitarbeiter sollten die vom Umfang her überschaubaren Grundsatzentscheidungen der Geschäftsleitung bezüglich des Compliance-Managementsystems kennen und verstehen.

3.5 Organisation des Compliance-Managementsystems: Verantwortlichkeiten, Aufgaben, Pflichten und Befugnisse, erforderliche Kompetenzen (persönliche und fachliche Anforderungen), Schnittstellen

Synopse[30]

Die Organisation des Compliance-Managementsystems **muss** sich nach den grundsätzlichen (rechtlichen) Vorgaben der Unternehmensorganisation richten und ist Bestandteil der unternehmensweiten Aufbau- und Ablauforganisation, vgl. oben Pkt. 2.2.3.

Die Verantwortlichkeiten (Aufgaben / Pflichten / Befugnisse) der jeweiligen Managementebene in Bezug auf Compliancemanagement sollten sich auch in (rechtssicheren) Stellen- oder Arbeitsplatzbeschreibungen wiederfinden.

Das Bekenntnis zu Compliancemanagement darf bei Vorgesetzten nicht nur ein „Lippenbekenntnis“ sein, sondern **muss** vorgelebt werden.

Ebenso **müssen** die für die gewissenhafte Wahrnehmung der Funktionen mit Bezug zu Compliancemanagement erforderlichen Kompetenzen und Ressourcen sichergestellt werden. Bezüglich der erforderlichen Kompetenzen – unter Berücksichtigung von internen / externen Veränderungen – **muss** auch auf regelmäßige Schulungen bzw. auf Coaching durch kompetente Trainer geachtet werden.

[30] Synopse:
ISO 19600:2014: 5 Leadership / 5.3 Organizational roles, responsibilities and authorities / 5.3.1 General / 5.3.2 Assigning responsibility for compliance in the organization / 7.2 Competence and training
IDW PS 980:2011: 4. Grundelemente eines CMS / „Compliance-Organisation“ / 6. Anwendungshinweise und Erläuterungen / Grundelemente eines CMS [Tz. 23], A18 „Compliance-Organisation“
COSO I:2013: Komponente (1): Kontrollumfeld (Control Environment) / Prinzip 2 / Fokuspunkte 5-8 / Prinzip 3 / Fokuspunkte 9-11
ISO 9001:2015: 5 Führung / 5.3 Rollen, Verantwortlichkeiten und Befugnisse in der Organisation / 7.2 Kompetenz

3.5.1 Top-Management

Synopse[31]

Die gesetzlichen Vertreter, Top Management und sonstigen Verantwortlichen **müssen** besondere Vorbildfunktion in Bezug auf das „Leben" des Compliance-Managementsystems zeigen, vgl. auch oben Pkt. 3.1.

Hier **müssen** auch grundlegende Kompetenzen vorhanden sein, um rechtssicher delegieren zu können. Die einschlägigen Tools und Methoden **müssen** bekannt sein und sachgerechte Anwendung finden.

3.5.2 Beauftragter für Compliance-Management

Synopse[32]

Hier herrscht in der Praxis – oft verwirrende – Vielfalt bzgl. Aufgabenbereich / Verantwortung und Abgrenzung der diversen Bezeichnungen wie „Beauftragter" oder „Verantwortlicher" für Compliancemanagement, „Compliance-Officer", „Compliance-Manager", etc. Eine Legaldefinition gibt es hier (noch) nicht. Nachfolgend wird von „Compliancemanagement-Beauftragten" gesprochen.

Auf den Compliancemanagement-Beauftragten kommen besondere Aufgaben zu:

Er hat das Thema Compliance-Management(system) in Abstimmung mit der Geschäftsführung zu planen, Ziele zu setzen, zu kommunizieren und zu steuern, zu delegieren und zu überwachen. Er nimmt eine Schnittstellen- und Beratungsfunktion für Compliancethemen zu allen weiteren Themenbereichen des Unternehmens sowie zur Unternehmensleitung wahr.

---

[31] Synopse:
ISO 19600:2014: 5 Leadership / 5.3 Organizational roles, responsibilities and authorities / 5.3.1 General / 5.3.2 Assigning responsibility for compliance in the organization / 5.3.3 Governing body and top management role and responsibility / 7 Support / 7.3.2.2 Role of top management in encouraging compliance
IDW PS 980:2011: 3. Rn. 13: … Verantwortung für CMS … liegt bei den gesetzlichen Vertretern …, 4. Rn. 23: Compliance-Kultur: … „tone at the top" …, Compliance-Ziele: „Die gesetzlichen Vertreter …"
COSO I:2013: Komponente (1): Kontrollumfeld (Control Environment), Prinzip 1 / Fokuspunkt 1: „Tone at the top"
ISO 9001:2015: 5 Führung / 5.3 Rollen, Verantwortlichkeiten und Befugnisse in der Organisation

[32] Synopse:
ISO 19600:2014: 5 Leadership / 5.3 Organizational roles, responsibilities and authorities / 5.3.1 General / 5.3.2 Assigning responsibility for compliance in the organization / 5.3.4 Compliance function
IDW PS 980:2011: A 18: Compliance-Organisation: … "Compliance-Beauftragter"
COSO I:2013: Komponente (1): Kontrollumfeld (Control Environment) / Prinzip 5 / IKS-Verantwortliche
ISO 9001:2015: 5 Führung / 5.3 Rollen, Verantwortlichkeiten und Befugnisse in der Organisation

Der Compliancemanagement-Beauftragte ist nicht alleine für die Umsetzung und das Leben der Compliancemanagement-Anforderungen in den diversen Unternehmensbereichen verantwortlich, da diese Aufgabe vielmehr dem einzelnen Mitarbeiter in seinem jeweiligen Pflichten- und Verantwortungsbereich und im Rahmen der Überwachung dessen Vorgesetzten zukommt.

Falls ein Compliance-Beauftragter eigesetzt wird, **muss** er von der Unternehmensleitung mit den notwendigen Befugnissen und Ressourcen ausgestattet werden.

Die Funktion kann auch von kompetenten Externen („Externer Compliancemanagement-Beauftragter") wahrgenommen werden (vgl. 3.5.6).

3.5.3 Compliance-Komitee

Synopse[33]

Sofern kein Compliancemanagement-Beauftragter vorgesehen ist (oder auch zusätzlich), kann für die Wahrnehmung entsprechender Aufgaben ein Compliance-Komitee, das Mitarbeiter aus verschiedenen (Prozess-) Themenbereichen enthält, eingerichtet werden. Hierdurch wird eine interdisziplinäre Sichtweise und Schnittstellenmanagement gefördert.

3.5.4 Vorgesetzte

Synopse[34]

Die Vorgesetzten in den diversen (Prozess-) Themenbereichen **müssen** u.a. Compliancemanagement-Verantwortung in ihrem jeweiligen Verantwortungsbereich übernehmen, die in den entsprechenden Stellen- und Arbeitsplatzbeschreibungen festgehalten werden sollte.

Auch hier **muss** darauf geachtet werden, dass die erforderlichen Kompetenzen vorliegen, da sonst nicht rechtssicher von der Geschäftsleitung auf diese vorgesetzten Mitarbeiter delegiert werden kann. Dies erfordert u.U. entsprechende Schulungen unter Berücksichtigung von externen / internen Veränderungen.

---

[33] Synopse:
ISO 19600:2014: 5 Leadership / 5.3 Organizational roles, responsibilities and authorities / 5.3.1 General / 5.3.2 Assigning responsibility for compliance in the organization / 5.3.4 Compliance function
IDW PS 980:2011: A 18: Compliance-Organisation: … „Compliance-Gremium"
COSO I:2013: Komponente (1): Kontrollumfeld (Control Environment) / Prinzip 5 / IKS-Verantwortliche
ISO 9001:2015: 5 Führung / 5.3 Rollen, Verantwortlichkeiten und Befugnisse in der Organisation

[34] Synopse:
ISO 19600:2014: 5 Leadership / 5.3 Organizational roles, responsibilities and authorities / 5.3.1 General / 5.3.2 Assigning responsibility for compliance in the organization / 5.3.5 Management responsibilities
IDW PS 980:2011: A 14: … „Verhalten der Mitglieder des Managements auf allen Managementebenen"
COSO I:2013: Komponente (1): Kontrollumfeld (Control Environment), Prinzip 1 / Fokuspunkt 1: „Tone at the top"
ISO 9001:2015: 5 Führung / 5.3 Rollen, Verantwortlichkeiten und Befugnisse in der Organisation

3.5.5 Sonstige Mitarbeiter

Synopse[35]

Jeder Mitarbeiter ist in seinem Verantwortungsbereich auch zugleich „Compliance-Manager" bzw. „Compliance-Risk-Owner", d.h., er **muss** sich pflichtgemäß in seinem Verantwortungsbereich verhalten. Dies **muss** von den Vorgesetzten kommuniziert und überwacht werden.

Auch dies sollte in den jeweiligen Stellenbeschreibungen (Schnittstellen-Verantwortung) und Zielvereinbarungsgesprächen sowie Beurteilungen (auch u.U. im Rahmen des Anreiz- und Sanktionssystems) Einfluss finden.

3.5.6 Outsourcing von Compliancemanagement-Funktionen

Das Unternehmen kann sich auch dafür entscheiden, bestimmte Compliancetätigkeiten und -funktionen im Rahmen einer (rechtssicheren) Delegation auf Unternehmensexterne zu delegieren (Outsourcing).

Hierbei **muss** jedoch ebenso für die Beachtung der entsprechenden Grundsätze zur rechtssicheren Delegation – Auswahl eines kompetenten und zuverlässigen Externen, entsprechende Instruktion und Überwachung – gesorgt werden.

Ein anderes Thema ist die Verpflichtung der Unternehmensleitung zur Sicherstellung der Erfüllung von Compliance-Anforderungen durch die Delegationsempfänger bei Delegationen und outsourcing, vgl. oben Punkt 2.2.3.

3.5.6.1 Externer Compliance-Management-Berater

Für das Unternehmen, insbesondere für Compliancemanagement-Verantwortliche, wie Geschäftsleitung / Aufsichtsgremien, Compliance-Beauftragte oder -komitee, sollte ein fachlich und persönlich versierter Compliance-Management-Berater zur Verfügung stehen, der Unternehmen, Verantwortliche und Beauftragte auf relevante Compliancethemen und (Rechts-) Änderungen hinweist.

Ansonsten **muss** diese Kompetenz unternehmensintern vorhanden und aktiv sein.

---

[35] Synopse:
ISO 19600:2014: 5 Leadership / 5.3 Organizational roles, responsibilities and authorities / 5.3.1 General / 5.3.2 Assigning responsibility for compliance in the organization / 5.3.6 Employee responsibility
IDW PS 980:2011: A 14: … Anreizsysteme …, Personalpolitik …, werden von den Mitarbeitern beachtet
COSO I:2013: Komponente (1): Kontrollumfeld (Control Environment), Prinzip 4 / Fokuspunkte 12 – 15 / Mitarbeiter
ISO 9001:2015: 5 Führung / 5.3 Rollen, Verantwortlichkeiten und Befugnisse in der Organisation

3.5.6.2 (Externer) Compliancemanagement-Ombudsmann oder Hinweisgebersystem

Durch Einrichtung eines Ombudsmann- oder Hinweisgeber-Systems oder einer ähnlichen Institution sollte intern oder auch Externen die Möglichkeit gegeben werden, unter Sicherstellung der Wahrung gewünschter Anonymität, Fragen zu Compliancethemen („help-desk-Funktion") zu stellen oder Hinweise auf drohende oder begangene Pflichtverstöße geben zu können.

Hier spielt der berufsrechtliche Geheimnisschutz und Beschlagnahme- bzw. Verwertungsverbote bei Ombudsmann oder Hinweisgeberstelle zur effektiven und rechtlich abgesicherten Wahrung der Anonymität der Hinweisgeber eine wichtige Rolle.

3.5.7 Schnittstellenmanagement

Egal, ob Compliancemanagement als eigener Bereich oder als Unterfunktion (z.B. von GRC) installiert wird: Relevante Schnittstellen zu den übrigen (Prozess-) Themenbereichen des Unternehmens **müssen** realisiert und angemessen bedient werden.

3.6 Kultur und Awareness des Compliance-Managementsystems

Synopse[36]

Die Geschäftsleitung und das Aufsichtsgremium **müssen** dafür sorgen, dass im Unternehmen eine positive Compliance-Kultur herrscht, die vor allem auch von den Führungskräften vorgelebt wird.

Entscheidend sind hierfür die gelebten und dokumentierten Unternehmenswerte, Verhaltensgrundsätze und das Verhalten im täglichen strategischen und operativen Geschäft.

Auch Anreiz- und Sanktionssysteme sollten die Förderung proaktiven Verhaltens in Richtung Compliance berücksichtigen.

Der Führungsstil und die Personalpolitik des Unternehmens sowie die transparente Durchführung von Aufsicht und Sanktion bei Fehlverhalten **müssen** eine Compliancemanagement-Kultur unterstützen, die einen offenen, positiven Umgang mit diesem Thema ermöglicht.

[36] Synopse:
ISO 19600:2014: 7 Support / 7.3 Awareness
IDW PS 980:2011: 4. Grundelemente eines CMS / „Compliance-Kultur" / 6. Anwendungshinweise und Erläuterungen / Grundelemente eines CMS [Tz. 23], A14 „Compliance-Kultur"
COSO I:2013: Komponente (1): Kontrollumfeld (Control Environment), Prinzip 1 / Fokuspunkte 1 - 4: „Tone at the top"
ISO 9001:2015: 7 Unterstützung / 7.3 Bewusstsein

3.7 Kommunikation des Compliance-Managementsystems

Synopse[37]

Die Ziele und Bestandteile sowie sonstige relevante Informationen für „interessierte Parteien" des Compliance-Managementsystems **müssen** unternehmensintern und auch extern gegenüber Geschäftspartnern und sonstigen Stakeholdern angemessen kommuniziert werden.

Dies erfordert eine für *jeden* Adressaten verständliche und prägnante Ausdrucksweise.

Die Kommunikation des Compliance-Managementsystems richtet sich nach den grundsätzlichen Vorgaben der Unternehmenskommunikation vgl. oben Pkt. 2.2.4.

3.8 Dokumentation des Compliance-Managementsystems

Synopse[38]

Die Dokumentation des Compliance-Managementsystems **muss** rechtlichen Anforderungen entsprechen und richtet sich nach den grundsätzlichen Vorgaben der Unternehmensdokumentation, vgl. oben Pkt. 2.2.5.

[37] Synopse:
ISO 19600:2014: 7 Support / 7.4 Communication
IDW PS 980:2011: 4. Grundelemente eines CMS / „Compliance-Kommunikation" / 6. Anwendungshinweise und Erläuterungen / Grundelemente eines CMS [Tz. 23], A19 „Compliance-Kommunikation"
COSO I:2013: Komponente (4): Information und Kommunikation (Information and Communication) / Prinzip 13 / Fokuspunkte 54-58 / Prinzip 14 / Fokuspunkte 59-62 / Prinzip 15 / Fokuspunkte 63-67
ISO 9001:2015: 7 Unterstützung / 7.4 Kommunikation

[38] Synopse:
ISO 19600:2014: 7 Support / 7.5 Documented information / 7.5.1 General / 7.5.2 Creating and updating / 7.5.3 Control of documented information
IDW PS 980:2011: 3. Rn. 13 Dokumentation des CMS; 4. Rn. 23: … „Voraussetzung ist … ausreichende Dokumentation des CMS …"
COSO I:2013: 4. Additional Considerations / Documentation
ISO 9001:2015: 7.5 Dokumentierte Information / 7.5.1 Allgemeines / 7.5.2 Erstellen und Aktualisieren / 7.5.3 Lenkung dokumentierter Informationen

3.8.1 Allgemeine Dokumentationsanforderungen

Synopse[39]

Die allgemeinen Anforderungen an Dokumente und Aufzeichnungen **müssen** entsprechend der unternehmensweit geltenden Regelungen und verpflichtenden rechtlichen Anforderungen eingehalten werden. Alle wesentlichen Bestandteile des Compliance-Managementsystems sind grundsätzlich rechtssicher zu dokumentieren und zu archivieren.

3.8.2 Handbuch

Das Compliance-Management-Handbuch[40] sollte dem Compliance-Beauftragten und seinen Mitarbeitern Hilfestellung geben.

Je nach Adressatenkreis, der vom Handbuch angesprochen werden soll, ist auf Verständlichkeit, Umsetzbarkeit und angemessenen Umfang zu achten.

3.8.3 Lenkung von Informationen (Dokumenten und Aufzeichnungen)

Synopse[41]

Die Lenkung (Erstellung und weitere Behandlung) von Dokumenten (einheitlichen Formularen / Mustern, etc.) und Aufzeichnungen (individuelle Schriftstücke, wie z.B. ein ausgefülltes Formular) erfolgt nach den allgemeinen Grundsätzen im Unternehmen.[42]

---

[39] Synopse:
ISO 19600:2014: 7 Support / 7.5 Documented information / 7.5.1 General
IDW PS 980:2011: 3. Rn. 13 Dokumentation des CMS; 4. Rn. 23: … „Voraussetzung ist … ausreichende Dokumentation des CMS …"
COSO I:2013: 4. Additional Considerations / Documentation
ISO 9001:2015: 7.5 Dokumentierte Information / 7.5.1 Allgemeines

[40] In ISO 9001:*2015* Qualitätsmanagementsysteme nicht mehr zwingend vorgeschrieben.

[41] Synopse:
ISO 19600:2014: 7 Support / 7.5 Documented information / 7.5.2 Creating and updating / 7.5.3 Control of documented information
IDW PS 980:2011: 3. Rn. 13 Dokumentation des CMS; 4. Rn. 23: … „Voraussetzung ist … ausreichende Dokumentation des CMS …"
COSO I:2013: 4. Additional Considerations / Documentation
ISO 9001:2015: 7.5 Dokumentierte Information / 7.5.2 Erstellen und Aktualisieren / 7.5.3 Lenkung dokumentierter Informationen

[42] Vgl. z.B. die Vorgaben aus dem Qualitätsmanagement (ISO 9001:2015) und oben den Punkt 2.2.5 Dokumentationsanforderungen.

3.9 Ressourcen des Compliance-Managementsystems

Synopse[43]

Die Geschäftsleitung **muss** die Ressourcen, die für ein angemessenes, gelebtes Compliance-Managementsystem erforderlich sind, zur Verfügung stellen.

3.9.1 Personell

Bezüglich der personellen Ressourcen **muss** für angemessene Quantität und Qualität sowohl in fachlicher sowie persönlicher Hinsicht gesorgt werden.

Schulungen und Coachings spielen hierbei eine wesentliche qualifizierende Rolle.

Ziel der Schulungen ist eine angemessene Compliance-Kompetenz bei Management und Mitarbeitern (positive Einstellung), um pflichtgemäßes Verhalten zu erreichen.

Bzgl. der Thematik „Einstellung / Einstellungsänderung" zu pflichtgemäßem Verhalten ist auf die Komponentenfolge „Transparenz von Zielen / Anforderungen", „Wissen, Verstehen, Können (kognitives Element)", „Wollen (emotionales Element)" als input und „zielorientiertes Handeln / Erfüllung der Anforderungen" als output zu achten.

In Hinblick auf Compliance-Kompetenzen im Unternehmen sollte eine „Wissensbilanz" vorgehalten werden. Diese enthält u.a. die Darstellung von erforderlichem und vorhandenem Wissen und Fertigkeiten im Unternehmen, bei Management, Mitarbeitern und externen Leistungserbringern (z.B. in der Lieferkette oder bei Outsourcing).

Dabei sollte auch betrachtet werden, welches zukünftige Wissen erforderlich sein wird und wie dieses frühzeitig genug aufgebaut werden kann.

3.9.2 Finanziell

Die für das Compliance-Managementsystem erforderlichen finanziellen Ressourcen **müssen** eingeplant und zur Verfügung gestellt werden.

3.9.3 Logistisch

Die erforderlichen angemessen logistischen Ressourcen, wie entsprechende Arbeitsräumlichkeiten oder Werkzeuge, wie EDV-Tools, **müssen** vorgehalten werden.

---

[43] Synopse:
ISO 19600:2014: 7 Support / 7.1 Resources
IDW PS 980:2011: A 18 Compliance-Organisation: … "Bereitstellung von … ausreichenden Ressourcen …", A 28: "Wesentliche Mängel: … Keine ausreichenden Ressourcen…"
COSO I:2013: Komponente (1): Kontrollumfeld (Control Environment) / Prinzip 4 / Fokuspunkte 12-15
ISO 9001:2015: 7 Unterstützung / 7.1 Ressourcen / 7.1.1 Allgemeines / 7.1.2 Personen / 7.1.3 Infrastruktur / 7.1.4 Prozessumgebung / 7.1.5 Ressourcen zur Überwachung und Messung / 7.1.6 Wissen der Organisation

3.10 Anreiz- und Sanktionensystem in Hinblick auf Compliance-Management

Synopse[44]

In Hinblick auf Compliance-Management sollte ein Anreiz- und **muss** ein Sanktionensystem (vgl. 4.2.3) entweder eingeführt oder erweitert werden.

3.11 IT-Unterstützung des Compliance-Managementsystems

Den verantwortlichen Mitarbeitern **müssen** – sofern erforderlich – entsprechende IT-basierte Werkzeuge zur erfolgreichen Bewältigung ihrer Aufgaben zur Verfügung gestellt werden. Schulungen zur Sicherstellung der Kompetenz zum richtigen Umgang mit diesen Hilfen gehören dazu.

3.12 Überwachung und Bewertung des Compliance-Managementsystems

Synopse[45]

Das Compliance-Managementsystem **muss** regelmäßig angemessen überwacht und bewertet werden. Bei Bedarf **müssen** Steuerungsmaßnahmen durchgeführt werden.

Hinweis: In diesem Punkt hier geht es um die Überwachung und Bewertung *des Compliance-Managementsystems* (nicht um die *gesamte* interne und externe *Unternehmens*-Überwachung).

Die Überwachung und Bewertung des Compliance-*Managementsystems* an sich erfolgt ebenfalls primär intern durch diverse idealerweise „gebündelte" Funktionen (Controlling, Compliance, Internes Audit, IKS, Revision (vgl. auch die „Three lines of defense, unten Pkt. 4.2)), kann aber auch Gegenstand externer Überwachung (Aufsichtsrat, Behörden, „second" und „third party"(Zertifizierungs-) Audits, etc.) sein.

---

[44] Synopse:
ISO 19600:2014: 10.1Nonconformity, noncompliance and corrective action
IDW PS 980:2011: Rn. 28: "wenn … Nichtbeachtung des CMS durch die Mitarbeiter keine wirksamen Konsequenzen hat …"
COSO I:2013: Komponente (1): Kontrollumfeld (Control Environment) / Prinzip 5 / Fokuspunkte 16-20
ISO 9001:2015: 10. Verbesserung

[45] Synopse:
ISO 19600:2014: 9 Performance evaluation
IDW PS 980:2011: 2. Rn. 20: … „bereits eingetretene Regelverstöße" …; A 11: „Compliance Überwachung und Verbesserung"; A 20: „Compliance-Überwachung und Verbesserung"
COSO I:2013: Komponente (5): Überwachung (Monitoring) / Prinzip 16 / Fokuspunkte 68-74 / Prinzip 17 / Fokuspunkte 75-77
ISO 9001:2015: 7.1.5 Ressourcen zur Überwachung und Messung / 9 Bewertung der Leistung

3.12.1 Überwachung, Messung, Analyse und Bewertung

Reifegrad, Effektivität (Zielerreichung) und Effizienz (Wirtschaftlichkeit) des Compliance-Managementsystems **müssen** kontinuierlich analysiert, bewertet und von den verantwortlichen Stellen beobachtet werden. Dazu gehört das Sammeln und Auswerten relevanter Informationen und die Entwicklung und Implementierung von (wertorientierten) Kennzahlen, die helfen, die Objekte der „Überwachung" messen zu können.

Hierzu gehört auch die Feststellung der Berücksichtigung von kontinuierlich neu entstehenden Anforderungen an das Compliance-Managementsystem.

3.12.2 Internes Audit

Ein internes Audit („first party audit") durch fachlich und persönlich versierte Compliance-Spezialisten kann Schwachstellen im System aufzeigen und Verbesserungsempfehlungen geben.

3.12.3 Management-Bewertung

Im Rahmen eines regelmäßig stattfindenden Management-Reviews (Bewertung des Compliance-Managementsystems *durch* das Management) **müssen** Reifegrad inklusive Angemessenheit und Wirksamkeit des Compliance-Managementsystems durch das Top-Management bewertet werden. Dabei sollte auch Stellung zu der Frage genommen werden, ob und wie das Top-Management der ihm diesbezüglich zukommenden Verantwortung gerecht geworden ist.

3.12.4 System-Bewertung

Bei der System-Bewertung **muss** geklärt werden, ob das System grundsätzlich und unter Berücksichtigung von Veränderungen in Unternehmen und Umfeld (noch) angemessen (geeignet, die damit verfolgten Ziele zu erreichen) und effektiv ist.[46]

3.12.5 Reifegradmessung

Synopse[47]

Die Überprüfung (performance evaluation) bzw. Reifegrad- bzw. auch Wertbeitragsmessung (vgl. oben Pkt. 3.2) erbringt Hinweise, ob das Compliance-Managementsystem wesentliche Mängel aufweist, die die Erreichung der Ziele des Compliance-Managementsystems gefährden und

[46] Vgl. das *Compliance*-Urteil des *LG München I* vom 10.12. 2013 – Az. 5 HK O 1387/10.

[47] Synopse:
ISO 19600:2014: 9.1.6 Development of indicators
IDW PS 980:2011: 6. Anwendungshinweise und Erläuterungen / Wesentlichkeit [Tz. 37], A26 / A27
COSO I:2013: Komponente (5): Überwachung (Monitoring) / Prinzip 16-17 / Fokuspunkte 68-77
ISO 9001:2015: 9. Bewertung der Leistung

die zur Versagung eines zufriedenstellenden Prüfvermerks / Testat / Auditergebnisses führen würden.

Üblicherweise werden Reifegrade in Stufen von 1 („sehr gering") bis 5 („sehr hoch") abgestuft.

Für die Messung des Reifegrades eines Managementsystems gibt es diverse Methoden / Modelle.[48]

Es ist eine angemessene Methode anzuwenden.

Auch entlang der Phasen Plan: Konzeptionierung (1), Do: Implementierung (2), Wirksamkeit (3), Check: Schwachstellenanalyse / Bewertung (4), Act: Verbesserung / Anpassung, (5) nimmt der Reifegrad zu.

3.12.6 Externes (Zertifizierungs-) Audit

Audit

Der Audit-Prüfbericht für ein Compliance-Managementsystem („third party audit") kann u.a. analog den Ausführungen des IDW-Prüfstandards PS 980:2011 für Compliance-Managementsysteme konzipiert werden:

Der IDW PS 980:2011 sieht abgestufte Prüfungsaufträge vor: eine Konzeptionierungs-, Angemessenheits- und Implementierungsprüfung und – die umfassendste Form – Wirksamkeitsprüfung.

Das Audit soll, entsprechend dem Auftragsinhalt, Aussagen zur Konzeptionierung oder Angemessenheit, Implementierung bzw. Wirksamkeit abgeben. Das Audit stellt eine Systemprüfung dar und zielt nicht auf das Verhindern oder Aufdecken von einzelnen Pflichtverstößen oder das Erlangen von Erkenntnissen über die tatsächliche, konsequente Einhaltung von Regeln ab. Diese Überwachungsverantwortung bleibt selbst bei entsprechender Delegation bei der Geschäftsleitung (und ggf. Aufsichtsrat) und u. U. etwaigen Beauftragten für das Compliance-Managementsystem.

Konzeptionierungs-Audit

Das Compliance-Managementsystem ist hinreichend konzeptioniert, wenn das Konzept angemessen und messbar / nachprüfbar Ziele (und idealerweise auch den angestrebten Wertbeitrag) sowie den Soll-Zustand mit zwingenden und sonstigen gewünschten Komponenten nach *„Anerkanntem Stand von Wissenschaft und Praxis"* nennt, das Ergebnis eines Soll-Ist-Abgleichs und eine bewertete Strategie zur Schließung eventueller Lücken darstellt.

Bzgl. der noch erforderlichen durchzuführenden Maßnahmen muss eine positive und Ressourcen freigebende Managemententscheidung vorliegen, sowie eine Projektierung (Konzeptionierung) der Umsetzung (Implementierung und Herbeiführung der Wirksamkeit (gelebt werden)),

[48] Vgl. COBIT-Reifegradmodell für IT-Systeme, Anlage zu ISO 9004, EDEN-Reifegradmodell, CMMI (Capabilities Maturity Model Integration), BPMM (Business Process Maturity Model), PEMM (Process Enterprise Maturity Model), ISO 15504 (SPICF), QMMG-Quality Management Maturity Grid, 8 Omega / Orca-Methode, etc.

Überprüfung und gegebenenfalls Verbesserung / Korrektur / Anpassung an externe und interne Veränderungen.

Implementierungs-Audit

Das Compliance-Managementsystem ist nach IDW PS 980:2011 angemessen, *„wenn es geeignet ist, mit hinreichender Sicherheit sowohl Risiken für wesentliche Regelverstöße rechtzeitig zu erkennen als auch solche Regelverstöße zu verhindern. [... und], dass bereits eingetretene Verstöße zeitnah an die zuständige Stelle im Unternehmen zu berichten sind, damit die notwendigen Konsequenzen für eine Verbesserung getroffen werden."*

Das Compliance-Managementsystem ist implementiert, wenn die Aufbau- (Organigramme, Stellenbeschreibungen, etc.) und Ablauforganisation (Prozessabläufe, Delegationen, Interaktionen, etc.) mit den relevanten notwendigen Komponenten aus dem Bereich Compliance-Management angemessen angereichert (dokumentiert und „in Kraft gesetzt") wurden.

Wirksamkeits-Audit

Die Wirksamkeit des Compliance-Managementsystems liegt vor, wenn relevante Compliance-Anforderungen (in Aufbau – und Ablauforganisation) inklusive intern oder extern delegierter Abläufe von den davon Betroffenen / Verantwortlichen angemessen verstanden, zu erreichen gewollt und erfüllt werden.

Compliance-Managementsystem-Beschreibung

Bei der Compliance-Managementsystem-*Beschreibung*[49] des zu auditierenden Unternehmens ist zu beachten, dass sie den Ist-Zustand zutreffend wiedergibt und nicht lediglich den (angestrebten) Soll-Zustand – mit den dazugehörigen Komponenten (Ziele und Anforderungen, Verantwortungen, Maßnahmen, Prozessabläufe, Ressourcen, etc.) – beschreibt. Erst nach Erreichung eines angemessenen Reifegrades decken sich Ist-Zustand bzw. System-Beschreibung und (angemessener) Soll-Zustand bzw. Konzeptionierung.

3.13 Business Continuity bzgl. des Compliance-Managementsystems

Bzgl. des Compliance-Managementsystems **muss** auf ein Notfall-, Krisen- und Kontinuitätsmanagement geachtet werden.[50] Dabei sind wesentliche, für die Aufrechterhaltung des Compliance-Managementsystems unverzichtbare Prozessabläufe, Funktionen, Ressourcen, etc. zu ermitteln („Business-Impact-Analyse – BIA") und deren Kontinuität abzusichern. Neben Notfall-, Krisen- und Kontinuitätsunterbrechungsprophylaxe und -früherkennung in Hinblick auf das Compliance-Managementsystem sind auch Notfallpläne vorzuhalten.

[49] Vgl. IDW PS 980:2011: 6 Anwendungshinweise und Erläuterungen / Begriffsbestimmungen [Tz. 5 ff.] A8
[50] Vgl. auch den Standard ISO 22301:2012 (Business Continuity-Managementsystem).

4 Kernbereich / Leistungserbringung des Compliance-Managementsystems (Compliance-Programm) („Block 4“)

Synopse[51]

Übersicht Teil 1

Block 4	Kernbereich / Leistungserbringung des Compliance-Managementsystems (Compliance-Programm)
4.1	Identifikation und Bewertung von Zielen, Anforderungen und Handlungsbedarf für Maßnahmen zur Erreichung der Ziele des Compliance-Managementsystems
4.1.1	Identifikation und Bewertung von Compliancemanagement-Zielen, -Anforderungen und Regelungen in den jeweiligen Unternehmensbereichen / (Prozess-) Themenfelder
4.1.1.1	Compliance-Anforderungen in Aufbau- und Ablauforganisation, bei Management und Mitarbeitern in den jeweiligen Unternehmensbereichen / (Prozess-) Themenfelder (Gesetze / Verordnungen / Allg. Rechtsprechung / etc.)
4.1.1.1.1	Rechtliche Anforderungen in den jeweiligen Unternehmensbereichen / (Prozess-) Themenfelder (Gesetze / Verordnungen / Allg. Rechtsprechung / etc.)
4.1.1.1.2	Anforderungen / Verpflichtungen aus Genehmigungen (Zulassungen / Lizenzen / etc.)
4.1.1.1.3	Anforderungen und Auflagen von Behörden
4.1.1.1.4	Anforderungen aus Urteilen / von Verwaltungsmaßnahmen, die direkt auf das Unternehmen bezogen sind
4.1.1.1.5	Anforderungen aus Abkommen (treaties / conventions / protocols)
4.1.1.1.6	Anforderungen aus einschlägigen Industrie-Standards (ISO / COSO / VDI / VDE / IDW / etc.)
4.1.1.1.7	Anforderungen aus abgeschlossenen Verträgen
4.1.1.1.8	Anforderungen aus zusätzlichen Verpflichtungen, (z.B. aus fakultativen Vereinbarungen mit Gemeinschaften / Organisationen / gegenüber Kunden / freiwillige Standards / etc.)
4.1.1.1.9	etc.
4.1.1.2	Sonstige Anforderungen aus dem *"Anerkannten Stand von Wissenschaft und Praxis"* in den jeweiligen Unternehmensbereichen / (Prozess-) Themenfeldern
4.1.1.2.1	Tools und Methoden nach dem *"Anerkannten Stand von Wissenschaft und Praxis"*
4.1.1.2.2	Prozessabläufe nach *"Anerkannten Stand von Wissenschaft und Praxis"*
4.1.1.2.3	etc.
4.1.2	Identifikation und Bewertung von Handlungsbedarf für Maßnahmen aus den eruierten Anforderungen zur Erreichung der Ziele des Compliance-Managementsystems

Abbildung 11: Integriertes, standardorientiertes Compliance-Managementsystem in 4 Blöcken - Block 4: Kernbereich des CMS - Teil 1.

[51] Synopse:
ISO 19600:2014: 4.4 Compliance management system and principles of good governance / 8 Operation
IDW PS 980:2011: 4 Grundelemente eines CMS / „Compliance-Programm“ / 6 Anwendungshinweise und Erläuterungen / Grundelemente eins CMS [Tz. 23] / „Compliance-Programm“ A17
COSO I:2013: Komponente (3): Kontrollaktivitäten (Control Activities) / Prinzip 10 – 12 / Fokuspunkte 38 - 53
ISO 9001:2015: 4.4 Qualitätsmanagementsystem und seine Prozesse / 8 Betrieb

Übersicht Teil 2

4.2	Allgemeine Prophylaxe- und Reaktionsmaßnahmen
4.2.1	Erlass von fehlenden oder ergänzenden Regelungen / Anforderungen (unter Berücksichtigung von Veränderungen) und Schaffung angemessener Rahmenbedingungen
4.2.2	Installation eines Compliancemanagement-Risiko-Prozesses
4.2.2.1	(Rechtzeitiges) Erkennen von Compliance-Risiken (Gefahren und Chancen) (unter Berücksichtigung von Veränderungen) (Riskassessement)
4.2.2.2	Compliance-Risiken bewerten und priorisieren
4.2.2.3	Steuerung der Compliance-Risiken (Reaktion auf erkannte Risiken)
4.2.2.3.1	Installation von Prophylaxemaßnahmen zur Vermeidung und Früherkennung von Compliance-Verstößen: "Lines of defense"
4.2.2.3.1.1	First Line: Anreicherung der Aufbau- und Ablauforganisation mit Compliance-Prophylaxe-Maßnahmen
4.2.2.3.1.2	Second Line: Internes Compliance-Steuerungs- und Überwachungssystem (Audits / Controlling / Risikomanagement / etc.)
4.2.2.3.1.3	Third Line: Assurance / Revision / Investigation / etc.
4.2.2.3.1.4	"Fourth Line": Überwachung durch "interested parties" (Business Partner / Betriebsrat / externe Aufsichtsorgane / Medien / etc.)
4.2.2.3.2	Installation eines Reaktionssystems auf erkannte Compliance-Risiken (Gefahren und Chancen)
4.2.3	Installation eines Compliancemanagement-Zielabweichungs-(*Verstoß)* -Erkennungs- und Reaktions-Prozesses
4.2.3.1	(Rechtzeitiges) Erkennen von Compliance-Verstößen / "Lines of defense"
4.2.3.2	Sachverhaltsermittlung
4.2.3.3	Bewertung des festgestellten Compliance-Verstoßes
4.2.3.4	Ad-hoc-Maßnahmen
4.2.3.5	Kommunikation des Compliance-Verstoßes
4.2.3.6	Sanktion des Compliance-Verstoßes
4.2.3.7	Ursachenanalyse bzgl. des Compliance-Verstoßes
4.2.3.8	Durchführung von Verbesserungsmaßnahmen (Vermeidung von Wiederholungen)

Abbildung 12: Integriertes, standardorientiertes Compliance-Managementsystem in 4 Blöcken - Block 4: Kernbereich des CMS - Teil 2.

4.1 Identifikation und Bewertung von Zielen, Anforderungen und Handlungsbedarf für Maßnahmen zur Erreichung der Ziele des Compliance-Managementsystems

Synopse[52]

Zunächst **müssen** eruiert / identifiziert und bewertet werden:

- Die diversen unternehmensspezifisch einschlägigen, relevanten und erheblichen Compliance-Managementsystem-Ziele (vgl. oben 3.2), Anforderungen und Regelungen sowie
- der Handlungsbedarf für Maßnahmen aufgrund der aktuell (und in naher Zukunft) existierenden Anforderungen, um die Ziele des Compliance-Managementsystems zu erreichen.

Compliance-Anforderungen in Aufbau- und Ablauforganisation, bei Management und Mitarbeitern **müssen** identifiziert und bewertet werden. Diese können sich – nicht abschließend – ergeben aus Gesetzen, Verordnungen, Rechtsprechung, Lizenzen, behördlichen Auflagen, Urteilen, Abkommen, verpflichtenden Standards, Verträgen sowie sonstigen Verpflichtungen. Auch aus der allgemeinen Pflicht, bei unternehmerischer Betätigung zumindest den *„Anerkannten Stand von Wissenschaft und Praxis"* zu beachten, ergeben sich diverse Anforderungen an eingesetzte Tools und Methoden sowie Prozessabläufe.

[52] Synopse:
ISO 19600:2014: 6 Planning / 6.2 Compliance objectives and planning to achieve them / 8 Operation / 8.1 Operational planning and control / 8.2 Establishing controls and procedures / 8.3 Outsourced processes
IDW PS 980:2011: A 15: Compliance-Ziele; A 17: Compliance-Programm;
COSO I:2013: Komponente (2): Risikobeurteilung (Risk Assessment) / Prinzip 6 / Fokuspunkte 21a, 21b, 21c, 21d, 22a, 22b, 22c, 23, 24, 25, 26 / Prinzip 9 / Fokuspunkte 35-37
ISO 9001:2015: 6 Planung / 6.2 Qualitätsziele und Planung zu deren Erreichung / 8 Betrieb / 8.1 Betriebliche Planung und Steuerung / 8.2 Anforderungen an Produkte und Dienstleistungen

4.1.1 Identifikation und Bewertung von Compliancemanagement-Zielen, -Anforderungen und Regelungen in den jeweiligen Unternehmensbereichen / (Prozess-) Themenfeldern

Synopse[53]

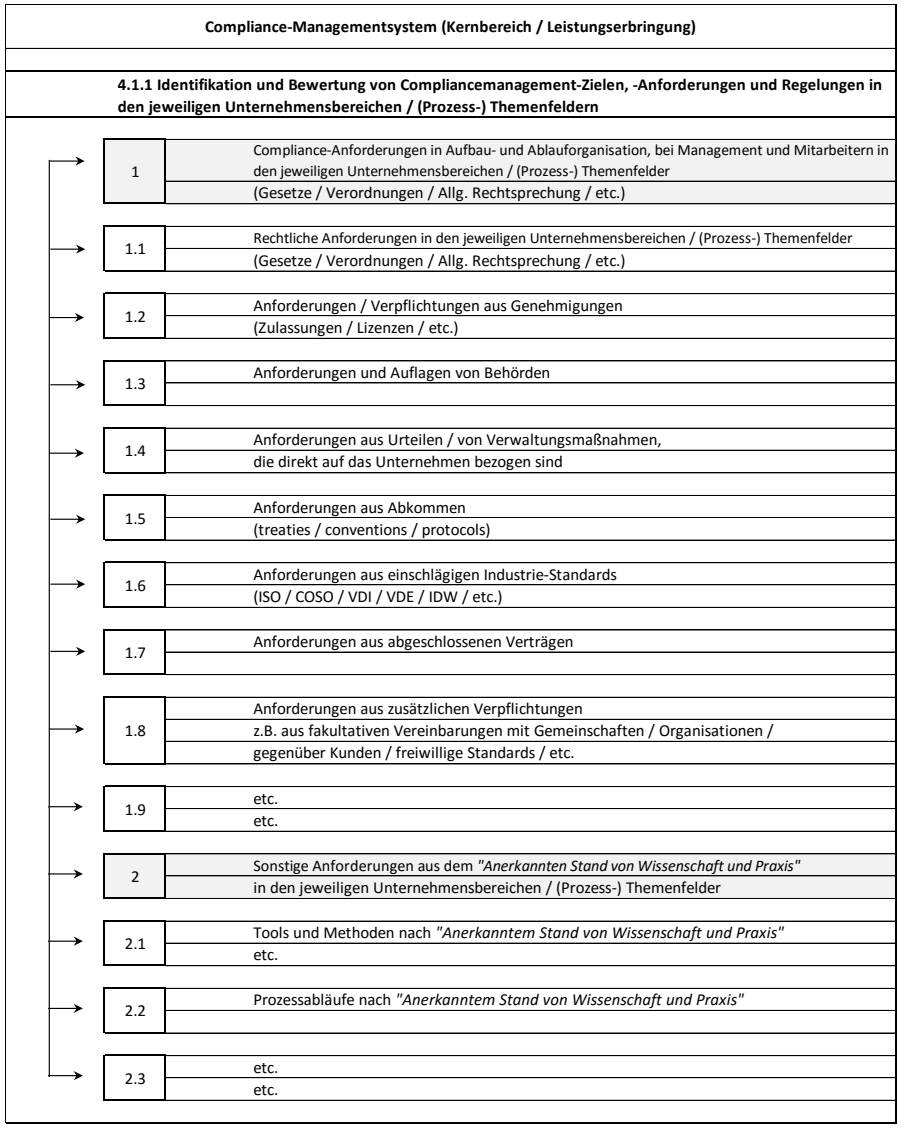

Abbildung 13: Identifikation und Bewertung von Compliancemanagement-Zielen, -Anforderungen und Regelungen.

[53] Synopse:
ISO 19600:2014: 4.5 Compliance obligations / 4.5.1 Identification of compliance obligations
IDW PS 980:2011: A 15: Compliance-Ziele; A 17: Compliance-Programm
COSO I:2013: Komponente (2) Risikobeurteilung (Risk Assessment) / Prinzip 6 / Fokuspunkte 21 - 26
ISO 9001:2015: 8. Betrieb

Anforderungen an Produkte, Leistungen, Prozesse, Systeme…

Ein Produkt, eine (Dienst-)Leistung, ein Prozessablauf, eine Unternehmensabteilung, ein Managementsystem, das Entscheiden und Handeln von Management und Mitarbeitern, etc. **muss** die in folgendem Schaubild dargestellten Anforderungen erfüllen, um einen hohen Reifegrad und zugleich einen hohen Pflichterfüllungsgrad aufzuweisen:

Anforderung:	**Folge bei Fehlern:**
✓ Effektiv (Ziel wird erreicht)	Unmöglichkeit (§§)
✓ Qualitativ	Mängelhaftung (§§)
✓ Fristgerecht	Verzug (§§)
✓ Sicher	Nebenpflichtverletzung § 823 BGB, § 280 BGB (§§)
✓ Rechtssicher (compliant)	Vielfältige Sanktionen (§§)
✓ Dem *„Anerkannten Stand von Wissenschaft und Praxis"* (Standards) entsprechend	Mängelhaftung / Sonstige Haftung bei Schäden / Beweislastumkehr (§§)
✓ Effizient (wirtschaftlich)	Liquiditätsprobleme / Ergebnisprobleme (§§) (Haftung für finanzielle Einbußen, Krisen- und Insolvenzverursachung, etc.)
✓ Gewissenhaft	Fehlende Gewissenhaftigkeit der Geschäftsführung § 43 GmbHG, § 93 AktG.: Pflichtverstoß und persönliche Haftung (§§)

Abbildung 14: Anforderungen an Produkte, Leistungen, Prozesse, Systeme.

Prozessabläufe nach *„Anerkanntem Stand von Wissenschaft und Praxis“*

Hier **muss** eine nach Unternehmensbereichen / (Prozess-) Themenfeldern sortierte Prozesslandkarte bzw. „Prozess-Matrix“ erstellt werden, die dokumentiert, dass die für das jeweilige Unternehmen erforderlichen Prozesse vorhanden sind. Diese Prozesse wiederum **müssen** so angereichert werden, dass sie die Erfüllung diverser Compliance-Anforderungen und die Erreichung der Compliance-Prozessziele gewährleisten.

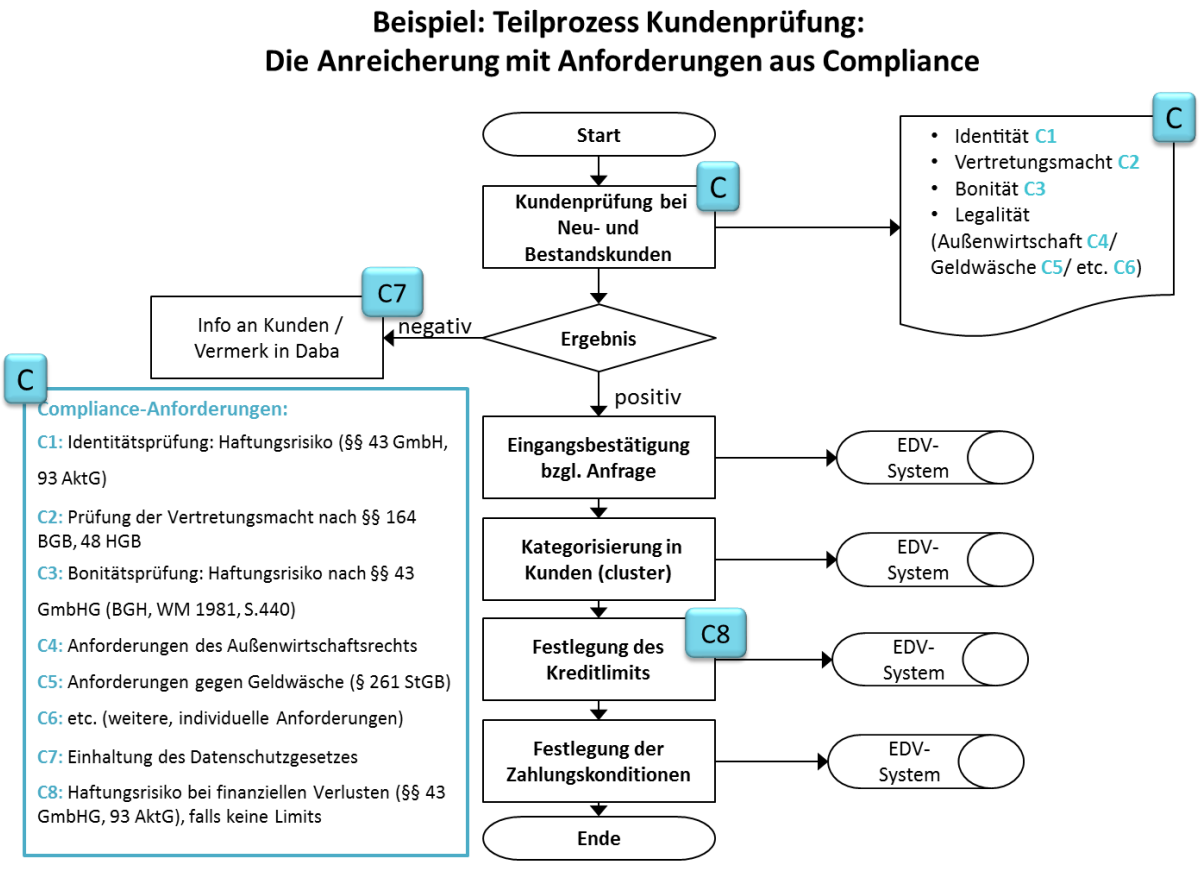

Abbildung 15: Beispiel für Prozessanreicherung mit Compliance-Komponenten.

4.1.2 Identifikation und Bewertung von Handlungsbedarf für Maßnahmen aus den eruierten Anforderungen zur Erreichung der Ziele des Compliance-Managementsystems

Synopse[54]

Durch Soll-Ist-Vergleich, Gap-Analyse, Bewertung (Scoring) und Priorisierung **muss** der Handlungsbedarf (ad hoc und kontinuierlich) ermittelt und über die Abarbeitung entschieden, projektiert und umgesetzt werden.

4.2 Allgemeine Prophylaxe- und Reaktionsmaßnahmen

4.2.1 Erlass von fehlenden oder ergänzenden Regelungen / Anforderungen (unter Berücksichtigung von Veränderungen) und Schaffung angemessener Rahmenbedingungen

Synopse[55]

Es **müssen** erforderliche Rahmenbedingungen vorhanden sein bzw. geschaffen werden:

Dazu gehören ggf. ergänzende Regelungen: Z.B. kann unternehmensintern ein „Code of Conduct" (Verhaltensregelungen) erlassen werden, falls im Unternehmen noch nicht (u.U. auch in anderer Form: Leitbild / Politik / „Tone from / at the top", „Code of Ethics", etc.) vorhanden. Entscheidend ist der Inhalt, nicht die Bezeichnung: Einige Unternehmen regeln darin spezifisch und dezidiert Compliance-Vorgaben, z.B. bis zu welcher Wertgrenze Geschenke angenommen werden dürfen, andere stellen ihre grundsätzlichen Aussagen zu Governance / Risk / Compliance / etc. dar.

---

[54] Synopse:
ISO 19600:2014: 4.5 Compliance obligations / 4.5.2 Maintenance of compliance obligations / 4.6 Identification, analysis and evaluation of compliance risks / 6 Planning / 6.1 Actions to address compliance risks / 6.2 Compliance objectives and planning to achieve them
IDW PS 980:2011: A 15: Compliance-Ziele; A 17: compliance-Programm
COSO I:2013: Komponente (2) Risikobeurteilung (Risk Assessment) / Prinzip 6 / Fokuspunkte 21-26
ISO 9001:2015: 6 Planung / 6.2 Qualitätsziele und Planung zu deren Erreichung

[55] Synopse:
ISO 19600:2014: 7 Support / 7.1 Resources / 7.2 Competence and training / 8.2 Establishing controls and procedures
IDW PS 980:2011: A 18: Compliance-Organisation: … „ausreichende Ressourcen"…; … „organisatorische und technische Hilfsmittel" …
COSO I:2013: Komponente (2) Risikobeurteilung (Risk Assessment) / Prinzip 6 / Fokuspunkte 21-26
ISO 9001:2015: 7 Unterstützung / 7.1 Ressourcen / 7.1.1 Allgemeines / 7.1.2 Personen / 7.1.3 Infrastruktur / 7.1.4 Prozessumgebung / 7.1.5 Ressourcen zur Überwachung und Messung / 7.1.6 Wissen der Organisation / 7.2 Kompetenz

Auch die Neuerstellung von Prozessabläufen aus dem Bereich „Compliancemanagement" (z.B. ein Compliance-Risikomanagement-Prozess) oder Anreicherung bereits bestehender Prozessabläufe (z.B. in Einkauf / Vertrieb / Finanzen / etc.) um Komponenten zur Erfüllung von z.B. Risiko- und Compliancemanagement-Anforderungen gehört hierher.

Ebenso gehört zu den erforderlichen Rahmenbedingungen, dass Arbeitsumgebung, Material und Werkzeuge, Infrastruktur und kompetentes Personal in angemessener Quantität und Qualität zur Verfügung stehen, um die Ziele des Compliance-Managementsystems zu erreichen.

4.2.2 Installation des Compliance-Risikomanagement-Prozesses

Synopse[56]

Der Compliancemanagement-Risiko-Prozess **muss** implementiert und wirksam sein und umfasst das Erkennen, Bewerten und Steuern von Compliance-Risiken (Gefahren und Chancen), die für das Erreichen der Compliancemanagement-Ziele eine Unsicherheit darstellen. Dadurch soll die Zielerreichung abgesichert werden.

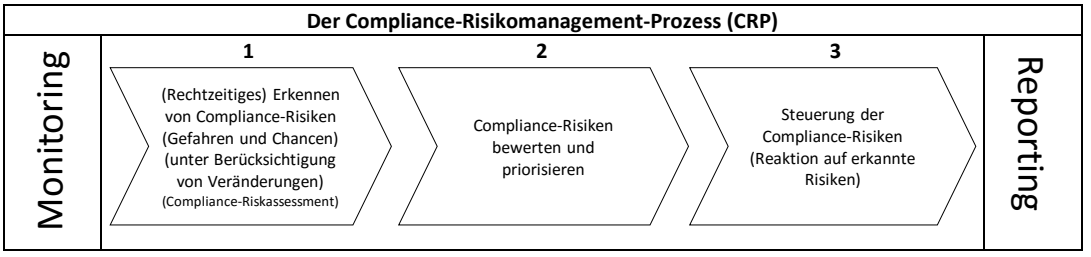

Abbildung 16: Der Compliance-Risikomanagement-Prozess (CRP).

CRP 1. (Rechtzeitiges) Erkennen von Compliance-Risiken (Gefahren und Chancen) (unter Berücksichtigung von Veränderungen) (Compliance-Riskassessment)

Mithilfe eines Riskassessment (z.B. nach ISO 31010) **müssen** Compliance-Risiken ermittelt, bzgl. möglicher Ursachen und Auswirkungen beschrieben, etc. werden. Risiken aus künftigen Entwicklungen sind über ein „Risks-of-changes-Management"[57] zu eruieren.

[56] Synopse:
ISO 19600:2014: 4.5 Compliance obligations / 4.5.2 Maintenance of compliance obligations / 4.6 Identification, analysis and evaluation of compliance risks / 6 Planning / 6.1 Actions to address compliance risks
IDW PS 980:2011: 4 Grundelemente eines CMS / „Compliance-Risiken" / 6 Anwendungshinweise und Erläuterungen / Grundelemente eines CMS [Tz. 23] / „Compliance-Risiken" A16
COSO I:2013: Komponente (2): Risikobeurteilung (Risk Assessment) / Prinzip 6 / Fokuspunkte vgl. oben Punkt 4.1 / Prinzip 7 / Fokuspunkte 27-30 / Prinzip 8 / Fokuspunkte 31-34 / Prinzip 9 / Fokuspunkte 35-37
ISO 9001:2015: 6 Planung / 6.1 Maßnahmen zum Umgang mit Risiken und Chancen

[57] Vgl. *Scherer,* Good Governance und ganzheitliches strategisches und operatives Management: Die Anreicherung des „unternehmerischen Bauchgefühls" mit Risiko-, Chancen- und Compliancemanagement, in: Corporate Compliance Zeitschrift (CCZ), 6/2012, S. 201 – 211.

CRP 2. Compliance-Risiken bewerten und priorisieren

Synopse[58]

Bzgl. der Compliancemanagement-Risiko*bewertung* gibt es zahlreiche qualitative und quantitative Methoden. Beim Einsatz von komplexen Methoden **muss** auf professionelle Auswahl, Anwendung und zusätzlich auf den gesunden Menschenverstand geachtet werden.

CRP 3. Steuerung der Compliance-Risiken (Reaktion auf erkannte Risiken)

Synopse[59]

Die Sicherstellung des pflichtgemäßen Verhaltens (Steuerung) **muss** erfolgen:

- durch Auflistung der Steuerungsmaßnahmen mit Zielvorgaben, Planung und Projektierung (Plan)
- Zu den Steuerungsmaßnahmen gehören
  - CRP 3.1 die Installation von Prophylaxemaßnahmen und Compliance-Risiko-Früherkennung sowie
  - CRP 3.2 ein Reaktionssystem für erkannte Risiken (vgl. hierzu die nächste Abbildung)
- durch Sicherstellung der Durchführung der beschlossenen Maßnahmen (Do) (Aufgaben / Projektmanagement)
- durch Abweichungscontrolling (Feststellung von Abweichungen und Korrekturmaßnahmen) (Check / Act) („Compliancemanagement-Steuerungs- und Überwachungssystem-ISÜS“) und angemessener Reaktion

[58] Synopse:
ISO 19600:2014: 4.6 Identification, analysis and evaluation of compliance risks
IDW PS 980:2011: 6 Anwendungshinweise und Erläuterungen / Grundelemente eines CMS [Tz. 23] / „Compliance-Risiken“ A16
COSO I:2013: Komponente (2): Risikobeurteilung (Risk Assessment) / Prinzip 7 / Fokuspunkte 27-39 / Prinzip 8 / Fokuspunkte 31-34
ISO 9001:2015: 6 Planung / 6.1 Maßnahmen zum Umgang mit Risiken und Chancen

[59] Synopse:
ISO 19600:2014: 6.1 Actions to address compliance risks / 8 Operation
IDW PS 980:2011: 6 Anwendungshinweise und Erläuterungen / Grundelemente eines CMS [Tz. 23] / „Compliance-Risiken“ A16 + A 17: „Compliance-Programm, … „Begrenzung der Compliance-Risiken“ …
COSO I:2013: Komponente (3): Kontrollaktivitäten (Control Activities) / Prinzip 10 / Fokuspunkte 38-43 / Prinzip 11 / Fokuspunkte 44-47 / Prinzip 12 / Fokuspunkte 48-53
ISO 9001:2015: 6 Planung / 6.1 Maßnahmen zum Umgang mit Risiken und Chancen

CRP 3.1 Steuerung: Installation von Prophylaxemaßnahmen zur Vermeidung und Früherkennung von Compliance-Verstößen: „Lines of defense“

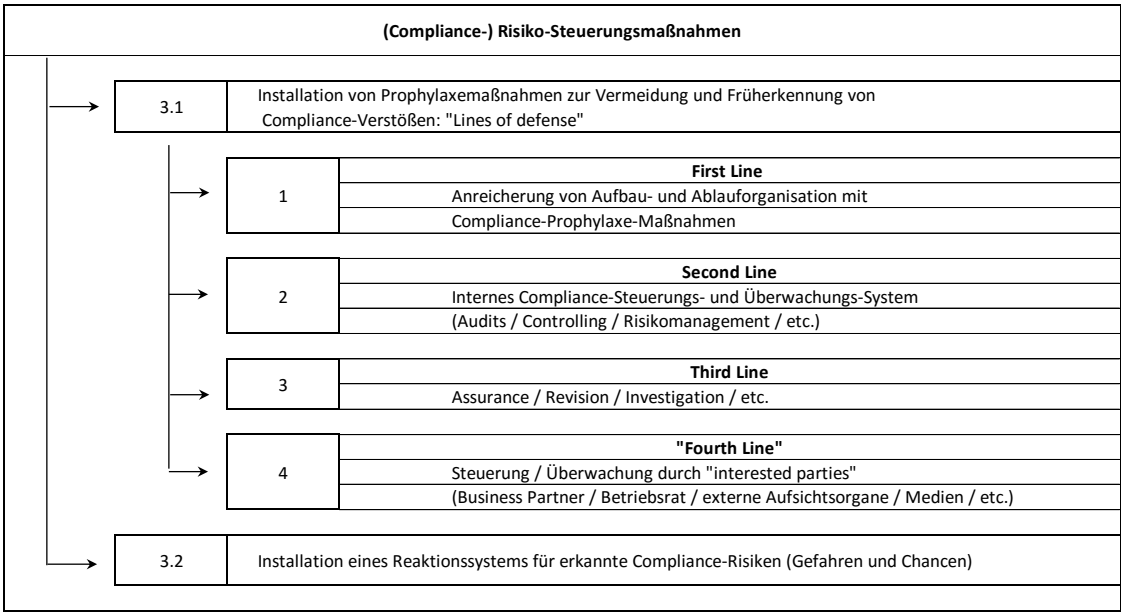

Abbildung 17: (Compliance-) Risiko-Steuerungsmaßnahmen.

Die erste und eigentlich wichtigste Prophylaxe bzw. Abwehrlinie **muss** das (rechts-/Anforderungs-) konforme Verhalten aller Mitarbeiter und Geschäftspartner, etc. im strategischen und operativen Geschäft sein. Ein ganz erheblicher Bereich ist die Anreicherung der wesentlichen Prozesse im Unternehmen mit Komponenten, die die Erfüllung der diversen Compliance-Anforderungen gewährleisten und deren Beachtung (vgl. 4.1.1). Wenn die Sollvorgaben in Aufbauorganisation und den Prozessabläufen zutreffend sind, müssen sich die Adressaten nur noch daran halten, wobei das vernünftige und rechtskonforme Verhalten „in Fleisch und Blut“ übergehen sollte.

CRP 3.1.1 First Line: Anreicherung der Aufbau- und Ablauforganisation mit Compliance-Prophylaxe-Maßnahmen

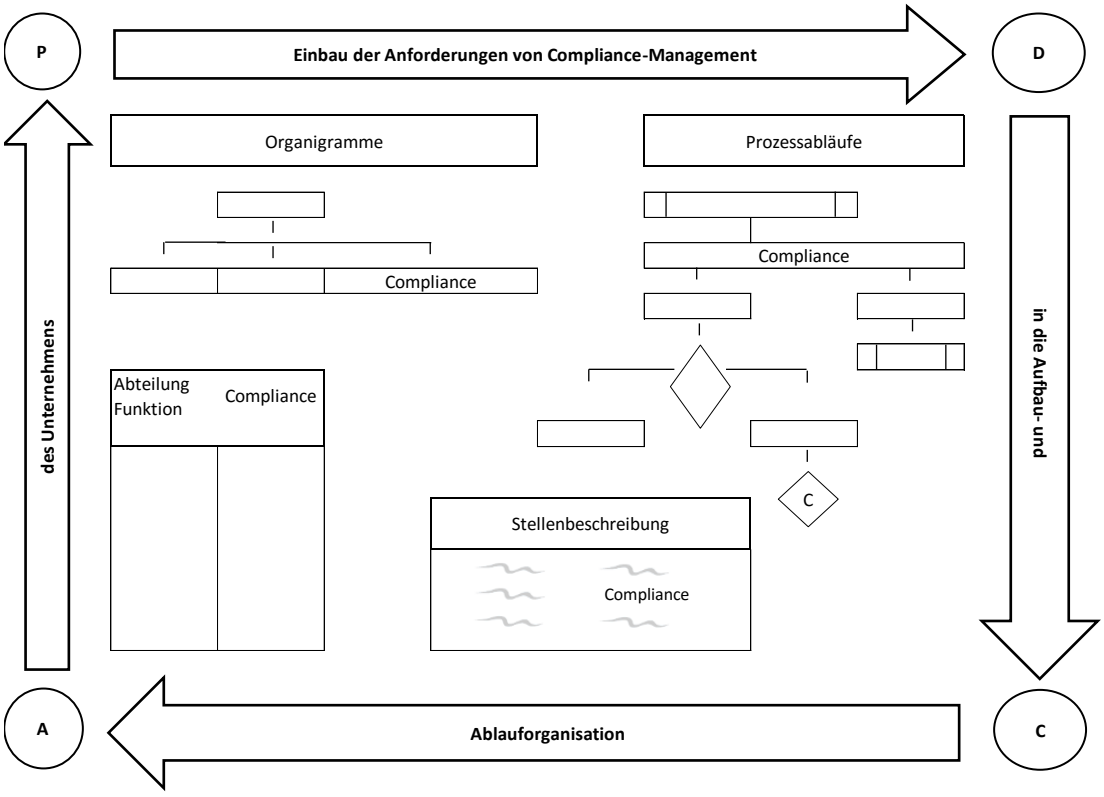

Abbildung 18: First Line: Anreicherung der Aufbau- und Ablauforganisation mit Compliance-Prophylaxe-Maßnahmen.

CRP 3.1.2 Second Line: Internes Compliance-Steuerungs- und Überwachungs-System: (Audits / Controlling / Risikomanagement / etc.)

Die Interne Unternehmensüberwachung gehört zu den Aufgaben der „gewissenhaften" Geschäftsleitung, ist damit zugleich Bestandteil einer ordnungsgemäßen Unternehmensführung und **muss** daher angemessen ausgeführt werden.

Zur Gesamtheit der internen Steuerungs-, Überwachungs- und Kontrollmechanismen zählen z.B.: Internes (rechnungslegungsbezogenes) Kontrollsystem (IKS), Teile aus dem Controlling und (externen) Rechnungswesen, Teile aus Risikomanagement, Teile aus dem Compliancemanagement, Kontrollpunkte in Prozessabläufen, Interne Audits, etc.

Diese überwachen und bewerten u.a. auch die Erfüllung von Compliance-Anforderungen.

CRP 3.1.3 Third Line: Assurance / Revision / Investigation / etc.

Im Rahmen der Third Line **muss** sichergestellt sein, dass anlassbezogen oder periodisch einzelne Themen / Vorfälle investigativ angemessen untersucht werden können. Dies ist ein sehr sensibler Bereich, da hier u.a. auch gegebenenfalls in Zusammenarbeit mit Aufsichts- oder Ermittlungsbehörden (z.B. Staatsanwaltschaft) Maßnahmen durchzuführen sind, bei denen Rechte Betroffener (Datenschutz, Persönlichkeits- und Grundrechte) zu beachten sind.

Eine gute Vernetzung zu den diversen Behörden und Abstimmungen in Bezug auf die Frage der *Angemessenheit* von Prophylaxemaßnahmen wirken hier sehr förderlich.

CRP 3.1.4 "Fourth Line": Steuerung / Überwachung durch "interested parties" (Business Partner / Betriebsrat / externe Aufsichtsorgane / Medien / etc.)

Durch Business Partner und sonstige „interested parties" (z.B. Lieferanten / Kunden / Betriebsrat / Mitglieder der externen Überwachung (Aufsichtsrat / Behörden (Zoll / Staatsanwaltschaft / Gewerbeaufsichtsamt, etc.) / externe Auditoren / etc.) / Öffentlichkeit / Medien / etc.) kann Motivation / Druck in Richtung Compliance-konformes Verhalten bei Unternehmen und Mitarbeiter entstehen.

CRP 3.2 Installation eines Reaktionssystems auf erkannte Compliance-*Risiken* (Gefahren und Chancen)

Sofern relevante Compliance-Risiken identifiziert und bewertet wurden, **müssen** angemessene Steuerungsmaßnahmen (z.B. daraus abgeleitete To Do´s oder Projekte) konsequent und in angemessener Zeit abgearbeitet werden.

4.2.3 Installation eines Compliancemanagement-Zielabweichungs-*(Verstoß)*-Erkennungs-und Reaktions-Prozesses

Synopse[60]

Unter dem Begriff *„nonconformity and corrective action"* **muss** ein Prozess installiert und mit Leben gefüllt werden, der nicht drohende, sondern *eingetretene* Verstöße gegen Compliancemanagement-Grundsätze frühzeitig aufdeckt, bewertet und angemessene Reaktionsmaßnahmen einleitet.

[60] Synopse:
ISO 19600:2014: 6.1 Actions to address compliance risks / 8 Operation / 10.1 Nonconformity, noncompliance and corrective action
IDW PS 980:2011: 3. Rn. 20: …"bereits eingetretene Regelverstöße" …; A 11: "Compliance-Überwachung und Verbesserung"; A 20: Compliance-Überwachung und Verbesserung"
COSO I:2013: Komponente (1): Kontrollumfeld (Control Environment) / Prinzip 5 / Fokuspunkte 16-20
ISO 9001:2015: 10. Verbesserung

Auch hier helfen die diversen *„lines of defense"*, aber auch Hinweisgebersysteme, Verstöße (frühzeitig) zu erkennen. Nach Sachverhaltsermittlung und -bewertung **müssen** ggf. ad-hoc-Maßnahmen eingeleitet und relevante Stellen informiert werden.

Bei Bestätigung eines Verstoßes **muss** über Sanktion entschieden werden und sonstige Maßnahmen (Ursachenanalyse, -beseitigung, Verbesserungsmaßnahmen) sind durchzuführen.

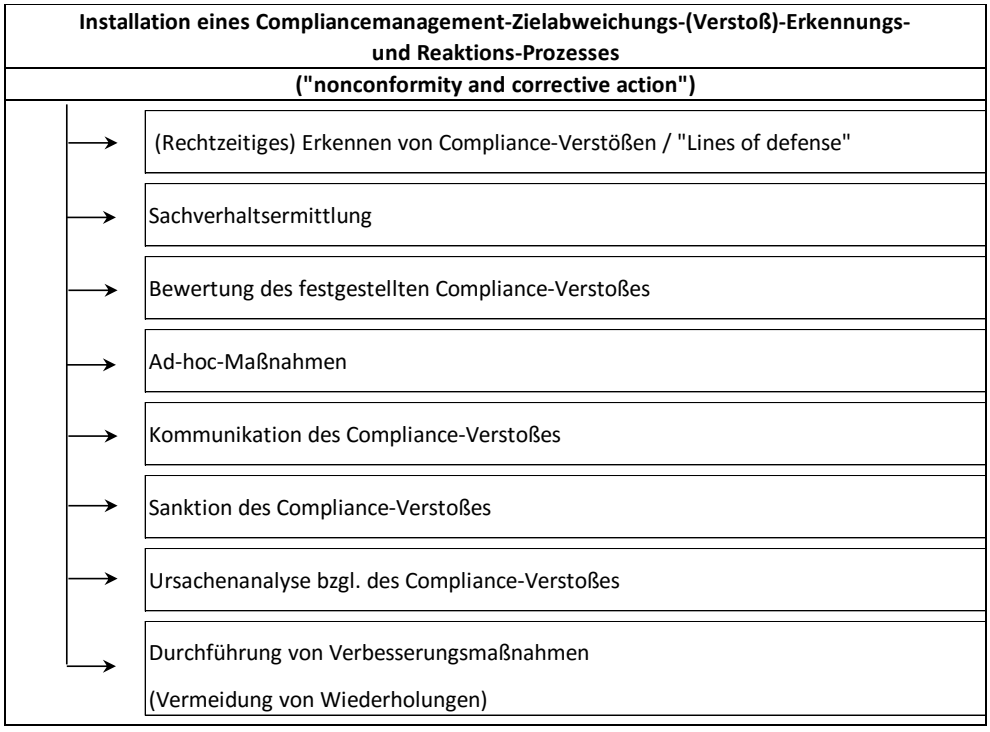

Abbildung 19: Compliancemanagement-Zielabweichungs-(Verstoß)-Erkennungs-und Reaktions-Prozess.

Zahl und Ausmaß sowie der Eintritt von Wiederholungen ähnlicher Verstöße kann ein signifikanter Hinweis sein, dass das Compliance-Managementsystem nicht effektiv ist! In diesem Fall **müssen** unverzüglich angemessene Steuerungsmaßnahmen eingeleitet werden.

- Ende -