Compliance-Management und Haftungsfragen

Inhaltsverzeichnis

PETER WINTZER – KIEFERNWEG 5 – 55457 GENSINGEN – TEL. 06727 / 1054 – EMAIL: PWMP-MOB@T-ONLINE.DE

Compliance-Management und Haftungsfragen

PETER WINTZER – KIEFERNWEG 5 – 55457 GENSINGEN – TEL. 06727 / 1054 – EMAIL: PWMP-MOB@T-ONLINE.DE

Compliance-Management und Haftungsfragen

1 Einleitung

Immer häufiger werden Organisationen mit der Forderung nach Implementierung eines **Compliance-Managementsystems** und der Benennung eines **Compliance-Beauftragten** konfrontiert.

Was steckt dahinter?

Das Wort „**Compliance**“ kommt aus dem Englischen und wird ins Deutsche übersetzt mit ***Einhaltung, Übereinstimmung, Regelbefolgung, Folgebereitschaft, Befolgung, Zustimmung, Einwilligung, Erfüllung, Konformität***, um nur die wesentlichsten zu benennen.

Diesen Begriff habe ich am 26.12.2016 in WIKIPEDIA eingegeben, **Bild 1.1** war das Ergebnis.

Compliance

Das Wort **Compliance** ([kəmˈplaɪəns], englisch für *Einhaltung, Befolgung*) bzw. **Komplianz** oder **Regelkonformität** steht für

- Compliance (Medizin), die Einhaltung von Verhaltensmaßregeln, Gesetzen und Richtlinien durch Patienten
- Compliance (Physiologie), als ein Maß für die Dehnbarkeit von Körperstrukturen
- Compliance (BWL), die Einhaltung von Verhaltensmaßregeln, Gesetzen und Richtlinien durch Unternehmen
- Compliance (Film), ein US-amerikanischer Thriller des Regisseurs Craig Zobel aus dem Jahr 2012
- IT-Compliance, die Einhaltung von Verhaltensmaßregeln, Gesetzen und Richtlinien im IT-Bereich
- Tax-Compliance, Steuerehrlichkeit
- Cross Compliance, die Bezeichnung eines Regelwerkes in der Agrarpolitik
- reziproke Steifigkeit in der technischen Mechanik

Bild 1.1

Demnach haben wir es hier mit der „**Einhaltung von Verhaltensmaßregeln, Gesetzen und Richtlinien durch Unternehmen**“ zu tun, einem Sachverhalt, den wir aus allen Managementsystemnormen und –Regelwerken bereits kennen. Insoweit ist es für Managementsystem-Beauftragte kein Neuland und alle Organisationen sollten unbedingt darauf achten, dass hier keine Parallelwelt zu vorhandenen Managementsystemen entsteht, doch dazu später mehr.
Der Ansatz zum Compliance-Management kommt ohne Zweifel aus der betriebswirtschaftlichen Sicht auf eine Organisation. Diese These wird dadurch unterstützt, dass es bis Ende 2016 nur die beiden Regelwerke **IDW PS 980** und **TR CMS 101:2011** gab, die die Beschreibung zu einem Compliance-Managementsystem enthalten.

ISO 19600:2016-12 definiert „***Compliance***“ unter Abschnitt 3.16 wie folgt: *Einhalten aller bindenden Verpflichtungen (3.16) der Organisation.*

PETER WINTZER – KIEFERNWEG 5 – 55457 GENSINGEN – TEL. 06727 / 1054 – EMAIL: PWMP-MOB@T-ONLINE.DE

Compliance-Management und Haftungsfragen

Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW)
Bereits zum 11.02.2010 wurde der Entwurf zu einem Prüfungs-Standard veröffentlicht, der als **IDW PS 980** zum 11.03.2011 verabschiedet wurde und ab 30.09.2011 anzuwenden ist. Dieser Prüfungsstandard ist Grundlage für eine Prüfung durch Wirtschaftsprüfer, dessen Ergebnis in einem Bericht dokumentiert wird.

TÜV Rheinland, Köln
Mit dem Regelwerk **TR CMS 101:2011** wurde 2011 ein weiteres Dokument zu diesem Thema veröffentlicht, dessen Einhaltung durch den TÜV mittels eines Zertifikates bestätigt werden kann.

Wie zu erwarten war, hat sich dann auch ein ISO Komitee mit diesem Thema beschäftigt und Ende 2014 die Systemnorm **ISO 19600:2014-12 Compliance Management Systeme – Leitlinien** verabschiedet. Seit Dezember 2016 liegt jetzt auch die deutsche Fassung als **ISO19600:2016-12** vor und es wurde von mir die Auditkriterienliste erstellt.

Den im Internet abrufbaren Kommentaren zum Vergleich der ISO 19600 mit den anderen beiden Regelwerken kann entnommen werden, dass es keine relevanten Überschneidungen gibt. Die Regelwerke sich also nicht inhaltlich wiedersprechen.

Die folgenden Ausführungen basieren jetzt auf der Analyse der **ISO 19600:2016-12** durch **PWMP**, unter Berücksichtigung auch der beiden anderen Regelwerke. Sie sollen für betroffene Organisationen eine praktische Hilfestellung sein, erheben jedoch keinen Anspruch auf Vollständigkeit und Richtigkeit.

Peter Wintzer
Seit 1981 Managementsystem-Berater

- EOQ Quality Systems Manager
- EOQ Quality Auditor
- Prozessauditor in der Lieferkette gem. VDA 6.3 (TÜV®) First and Second Party Auditor
- IATF 16949 1st/2nd party Auditor (Certificate number: IATF-1802-C-1293)

Gensingen, den 20. Januar 2017
Aktualisiert: 05. März 2019

Compliance-Management und Haftungsfragen

2 Zielstellung eines Compliance-Managementsystems

Auch wenn letztendlich alle drei Regelwerke das gleiche Ziel verfolgen, gibt es unterschiedliche Erläuterungen zur Zielstellung, wie im Folgenden erkennbar.

Die **Zielstellung** der ISO 19600:2016-12 kann dem Abschnitt 0 Abs. 3 entnommen werden:

Ein wirksames, organisationsweites Compliance-Managementsystem erlaubt es einer Organisation, ihre Bekenntnis zur Regelkonformität, also der Einhaltung der geltenden Gesetze, Branchenkodizes und Organisationsstandards, sowie der Berücksichtigung von Grundsätzen der Corporate Governance, von Best Practice, der Ethik und gesellschaftlicher Erwartungen zum Ausdruck zu bringen.

Die **Zielstellung** von **IDW PS 980** kann der Textzeile 14 entnommen werden:

Ziele einer umfassenden CMS-Prüfung (Wirksamkeitsprüfung) ist es, dem Prüfer anhand der von dem Unternehmen zugrunde gelegten CMS-Grundsätzen (vgl. Tz. 8) eine Aussage mit hinreichender Sicherheit darüber zu ermöglichen,

- *ob die in der CMS-Beschreibung enthaltenen Aussagen über die Grundsätze und Maßnahmen des CMS in allen wesentlichen Belangen angemessen dargestellt sind (vgl. Tz. 19),*
- *dass die dargestellten Grundsätze und Maßnahmen in Übereinstimmung mit den angewandten CMS-Grundsätzen geeignet sind, mit hinreichender Sicherheit sowohl Risiken für wesentliche Regelverstöße rechtzeitig zu erkennen als auch solche Regelverstöße zu verhindern (vgl. Tz. 20) und dass die Grundsätze und Maßnahmen zu einem bestimmten Zeitpunkt implementiert waren und*
- *während eine bestimmten Zeitraums wirksam (vgl. Tz. 21) waren.*

Die **Zielstellung** von TR CMS 101:2011 ist im Abschnitt 2 dokumentiert:

Ziel des Compliance Management Systems ist es, systematisch die Voraussetzungen in der Organisation dafür zu schaffen, dass Verstöße gegen Compliance-Anforderungen vermieden bzw. wesentlich erschwert und eingetretene Verstöße erkannt und behandelt werden können.

Aus diesen Zielstellungen ist aber immer noch nicht zu entnehmen, wie sich ein CMS von anderen Managementsystemen unterscheidet, welche Bereiche oder Sachthemen in einer Organisation davon erfasst werden.

Hier helfen zunächst die **Begriffserläuterungen** dieser Regelwerke weiter:

ISO 19600 Abschnitt 3.14 Compliance-Anforderungen:
Anforderung (3.13), die eine Organisation (3.1) erfüllen muss

PETER WINTZER – KIEFERNWEG 5 – 55457 GENSINGEN – TEL. 06727 / 1054 – EMAIL: PWMP-MOB@T-ONLINE.DE

Compliance-Management und Haftungsfragen

***IDW PS 980* Textzeile 6**
Unter einem Compliance Management System sind die auf der Grundlage der von den gesetzlichen Vertretern festgelegten Ziele (vgl. Tz. 23) eingeführten Grundsätze und Maßnahmen eines Unternehmens zu verstehen, die auf die Sicherstellung eines regelkonformen Verhaltens der gesetzlichen Vertreter und der Mitarbeiter des Unternehmens sowie ggf. Dritten abzielen, d.h. auf die Einhaltung bestimmter Regeln und damit auf die Verhinderung von wesentlichen Verstößen (Regelverstöße) (vgl. Tz. A5). Ein CMS i.S.d. IDW Prüfungsstandards kann sich insb. auf Geschäftsbereiche, auf Unternehmensprozesse (z.B. Einkauf) oder auf bestimmte Rechtgebiete (z.B. Kartellrecht) beziehen (abgegrenzte Teilbereiche) (vgl. Tz. A3)

***TR CMS 101*:2011 Abschnitt 3:**
Alle Regeln, die von der Organisation und den dort tätigen Personen zu beachten sind, unabhängig davon, ob es sich um gesetzliche oder behördliche Compliance-Anforderungen handelt oder solche, deren verbindliche Anwendbarkeit der Organisation für sich selbst oder eine andere Organisation für seine Mitglieder festgelegt hat.

Zusammenfassung: Übereinstimmend sagen hier alle Regelwerke aus, dass es sich um regelkonformes Verhalten der Beschäftigten einer Organisation handelt bzw. mit Hilfe des CMS Verstöße gegen die Regeln verhindert bzw. reduziert werden sollen.

3 Anwendungsbereich des Compliance Managements

Alle drei Regelwerke haben hier teilweise unterschiedliche Blickwinkel, auch wenn sie letztlich alle das Gleiche meinen.

***ISO 19600 Abschnitt 0 Absatz 3*:**
Ein wirksames, organisationsweites Compliance-Managementsystem erlaubt es einer Organisation, ihre Bekenntnis zur Regelkonformität, also der Einhaltung der geltenden Gesetze, Branchenkodizes und Organisationsstandards, sowie der Berücksichtigung von Grundsätzen der Corporate Governance, von Best Practice, der Ethik und gesellschaftlicher Erwartungen zum Ausdruck zu bringen.

IDW PS 980 unter Textzeile A3
Beispielsweise können einzelne der folgenden abgegrenzten Teilbereiche Gegenstand einer CMS-Prüfung sein (vgl. Tz 1):

Rechtsgebiete:
- *Wettbewerbs- und Kartellrecht*
- *Antikorruptionsrecht (z.B. § 299 StGB oder Foreign Corrupt Practices Akt FCPA)*
- *Börsenrecht (z.B. Vorschriften zum Insiderhandeln oder zu Ad-hoc-Meldepflichten)*
- *Vorschriften zur Unternehmensführung und –überwachung (z.B. nach dem deutschen Corporate Governance Kodex)*
- *Geldwäschegesetz*
- *Umweltrecht*

PETER WINTZER – KIEFERNWEG 5 – 55457 GENSINGEN – TEL. 06727 / 1054 – EMAIL: PWMP-MOB@T-ONLINE.DE

Compliance-Management und Haftungsfragen

- *Außenwirtschaftsrecht und Exportkontrolle*
- *Außensteuerrecht*
- *Datenschutz- und Datensicherheitsvorschriften*
- *Arbeitsrecht und Persönlichkeitsrechte (z.B. Allgemeines Gleichstellungsgesetz)*
- *Arbeitssicherheitsrecht*
- *Zollrecht*
- *Patentrecht*
- *Produkthaftungsrecht*
- *Arbeitssicherheit und technische Sicherheit*

TR CMS 101:2011
Eine vergleichbare Erläuterung ist nicht enthalten, allerdings wird im Abschnitt 4.2.1 Absatz 2) auf nachfolgende „Vorgabedokumente“ hingewiesen:

a) *Rechtsquellen; darunter Gesetze, Verordnungen, Verwaltungsakte, Satzungen, verbindliche Standards oder Kodizes,*

Zusammenfassung: Mit Hilfe eines CMS soll erreicht werden:

- Alle relevanten Rechtsquellen, die für die jeweilige Organisation bzw. den jeweiligen Geltungsbereich zutreffen, sind ermittelt
- Die aus den zutreffenden Rechtsquellen resultierenden Forderungen sind festgestellt und in die Organisation integriert
- Die Strategie und Politik der Organisation berücksichtigt diese Forderungen und setzt sie in eine Organisationskultur um
- Alle an der Organisation interessierten Kreise/Personen (interne wie externe) sind über diese Forderungen informiert und wissen, welche Konsequenzen mit der Nichteinhaltung verbunden sind
- Die mit der Nichteinhaltung der Forderungen verbundenen Risiken sind auf ein Minimum reduziert

4 Abgleich zu anderen Managementsystemen

Grundsätzlich gilt, dass alle Managementsystemnormen die Forderung enthalten, gesetzliche und behördliche Forderungen zu ermitteln und einzuhalten. Dazu im Folgenden einige Beispiele:

4.1 Qualitätsmanagement

Textauszug ISO 9001:2015-11 Abschnitt. 0.1 Absatz 2a
die Fähigkeit, beständig Produkte und Dienstleistungen zu liefern, die die Kundenanforderungen und zutreffende gesetzliche und behördliche Anforderungen erfüllen;

PETER WINTZER – KIEFERNWEG 5 – 55457 GENSINGEN – TEL. 06727 / 1054 – EMAIL: PWMP-MOB@T-ONLINE.DE

Compliance-Management und Haftungsfragen

Textauszug ISO 9001:2015-11 Abschnitt. 1.Absatz 1 b)
danach strebt, die Kundenzufriedenheit durch wirksame Anwendung des Systems zu erhöhen, einschließlich der Prozesse zur fortlaufenden Verbesserung des Systems und der Zusicherung der Einhaltung von Anforderungen der Kunden und von zutreffenden gesetzlichen und behördlichen Anforderungen.

Textauszug ISO 9001:2015-11 Abschnitt. 4 Absatz 1
Aufgrund ihrer Auswirkung bzw. ihrer potentiellen Auswirkung auf die Fähigkeit der Organisation zur beständigen Bereitstellung von Produkten und Dienstleistungen, die die Anforderungen der Kunden und die zutreffenden gesetzlichen und behördlichen Anforderungen erfüllen, muss die Organisation

Textauszug ISO 9001:2015-11 Abschnitt. 8.2.2 Absatz 2 a)
a) die Anforderungen an das Produkt und die Dienstleistung festgelegt sind, einschließlich:
1) jeglicher zutreffender gesetzlicher und behördlicher Anforderungen;

Die IATF 16949:2016-10 bezieht sich, ergänzend zur ISO 9001, in den folgenden Abschnitten ebenfalls auf die Einhaltung gesetzlicher Vorgaben:

- 4.4.1.1 Abs. 1
- 4.4.1.2 Abs. 1 a)
- 7.1.5.2.1 Abs. 1
- 7.2.2 Abs. 1
- 7.5.3.2.1 Abs. 1
- 8.3.3.1 Abs. 1 g)
- 8.4.2.2
- 8.4.3.1 Abs. 1
- 8.6.5

4.2 Arbeits- und Gesundheitsschutzmanagement

Textauszug ISO 45001 Abschnitt 6.1.3 Abs. 1 c)
diesen rechtlichen Verpflichtungen und anderen Anforderungen Rechnung zu tragen, wenn sie ihr SGA-Managementsystem festlegt, verwirklicht, aufrechterhält und fortlaufend verbessert.

4.3 Umweltmanagement

Textauszug ISO 14001:2015-11 Abschnitt. 3.2.9 Absatz 1
rechtliche Verpflichtungen und andere Anforderungen (zulässiger Begriff) rechtliche Verpflichtungen, die eine Organisation (3.1.4) erfüllen muss und andere Anforderungen (3.2.8), die eine Organisation erfüllen muss oder zu deren Erfüllung sich eine Organisation entschließt

Textauszug ISO 14001:2015-11 Abschnitt. 4.2 Absatz 1

PETER WINTZER – KIEFERNWEG 5 – 55457 GENSINGEN – TEL. 06727 / 1054 – EMAIL: PWMP-MOB@T-ONLINE.DE

Compliance-Management und Haftungsfragen

Die Organisation muss: die interessierten Parteien, die für ihr Umweltmanagementsystem relevant sind bestimmen; die relevanten Erfordernisse und Erwartungen (d. h. Anforderungen) dieser interessierten Parteien bestimmen; bestimmen, welche von diesen Erfordernissen und Erwartungen zu bindenden Verpflichtungen werden.

4.4 Risikomanagement

Textauszug ISO DIN 31000:2018-10 Abschnitt. 5.4.1 Abs. 2
Die Untersuchung des externen Kontextes einer Organisation kann unter anderem Folgendes enthalten: soziale, kulturelle, politische, rechtliche, behördliche, finanzielle, technologische, wirtschaftliche und umweltbezogene Faktoren seien sie internationaler, nationaler, regionaler oder lokaler Art;

4.5 Informationssicherheits-Managementsysteme

Textauszug DIN ISO/IEC 27001 :2015-03. Abschnitt A.5.1 Abs. 1
Ziel: *Vorgaben und Unterstützung für die Informationssicherheit sind seitens der Leitung in Übereinstimmung mit geschäftlichen Anforderungen und den relevanten Gesetzen und Vorschriften bereitgestellt.*

4.6 Energiemanagementsysteme

Textauszug DIN EN ISO 50001 :2018-12. Abschnitt 5.2 Abs. 1d)
eine Verpflichtung zur Erfüllung geltender rechtlicher Anforderungen und anderer Anforderungen (siehe 4.2) im Zusammenhang mit Energieeffizienz, Energieeinsatz und Energieverbrauch enthält;

4.7 Fazit

Es spielt also keine Rolle, von welcher Managementsystemnorm geredet wird. Immer geht es neben den fachlichen Themen der jeweiligen Norm darum, dass auch die zutreffenden gesetzlichen und behördlichen Vorschriften ermittelt, geprüft, auf die Organisation übertragen und eingehalten werden.

Hieraus kann man zunächst den Schluss ziehen, dass ein CMS nicht zusätzlich benötigt wird. Das ist allerdings nur ein Teil der Wahrheit, denn keine der zuvor genannten Systemnormen beschäftigen sich ausschließlich mit der Fragestellung, wie bewusstes oder unbewusstes menschliches Fehlverhalten vorhergesagt, erkannt, verhindert oder die Wahrscheinlichkeit des Eintretens minimiert werden kann.

Doch es gibt eine wesentliche Ausnahme, die Norm ISO 31000:2018-10:

PETER WINTZER – KIEFERNWEG 5 – 55457 GENSINGEN – TEL. 06727 / 1054 – EMAIL: PWMP-MOB@T-ONLINE.DE

Compliance-Management und Haftungsfragen

In der deutschsprachigen Ausgabe lautet der **Einleitungstext** wie folgt:

Organisationen jeglicher Art und Größe unterliegen externen und internen Faktoren und Einflüssen, die das Erreichen ihrer Ziele unsicher machen können.
Das Umgehen mit Risiken basiert auf den Grundsätzen dem Rahmenwerk und dem Prozess, wie sie in diesem Dokument beschrieben und in Bild 1 dargestellt sind. Diese Komponenten bestehen möglicherweise bereits vollständig oder teilweise in der Organisation, müssten aber möglicherweise angepasst oder verbessert werden, damit das Umgehen mit Risiken effizient, wirksam und konsistent erfolgt.

Hier ist klar erkennbar, dass grundsätzlich auch das bewusste oder unbewusste Fehlverhalten von Menschen als Risiko anzusehen ist und somit über diesen Weg vorhergesagt, erkannt, verhindert oder die Wahrscheinlichkeit des Eintretens minimiert werden kann.

Es handelt es sich deshalb nach meiner Meinung bei dieser Norm nicht um eine **Systemnorm**, sondern um die Beschreibung einer **Methode** zur Risikofeststellung und –behandlung. Die Integration dieser Methode in die Systemnormen bleibt davon unberührt.

5 Struktur eines Compliance-Managementsystems

Alle drei in dieser Abhandlung zitierten Regelwerke zum CSM haben hier einen deutlich unterschiedlichen Ansatz, der sicherlich auf die unterschiedliche berufliche Herkunft bzw. Aufgabenstellung zurückzuführen ist.

5.1 ISO 19600:2016

Diese Norm orientiert sich vollständig an der „**High-Level-Structur**“ aller Systemnormen. Es gibt aber einen wesentlichen Unterschied zu den Systemnormen wie. z.B. ISO 9001 oder ISO 14001.

Die ISO 19600 ist eine reine **Empfehlungsnorm**, sie enthält im Gegensatz zu anderen Systemnormen keine **„muss-„ oder „kann-Bedingungen“** sondern verwendet ausschließlich die Formulierung „sollte“. Damit zählt sie nicht zu den klassischen „Zertifizierungsnormen“, was aber nicht bedeutet, dass man sich nicht nach dieser Norm zertifizieren lassen kann.

Stellt man im Internet eine Abfrage nach „ISO 19600“ und „Zertifizierung“ findet man entsprechende Angebote von Zertifizierungsgesellschaften.

5.2 Institut der Wirtschaftsprüfer und IDW PS 980

PETER WINTZER – KIEFERNWEG 5 – 55457 GENSINGEN – TEL. 06727 / 1054 – EMAIL: PWMP-MOB@T-ONLINE.DE

Compliance-Management und Haftungsfragen

IDW PS 980 beschreibt von Textzeile A14 bis A20 die Grundelemente eines CMS, das heißt von **insgesamt 49 Seiten** des Regelwerkes sind lediglich **4 Seiten** der Systembeschreibung vorbehalten, die restlichen Seiten sind Erläuterungen bzw. Vorgaben für die Prüfungsdurchführung.

Es gibt auch keine Strukturvorgabe, sondern lediglich Aussagen, welche Themen in der CMS-Beschreibung mindestens zu behandeln sind bzw. zu denen Vorgaben in der Systembeschreibung vorhanden sein müssen. Es handelt sich hier um die Themenblöcke

- A14 Compliance-Kultur
- A15 Compliance-Ziele
- A16 Compliance-Risiken
- A17 Compliance-Programm
- A18 Compliance-Organisation
- A19 Compliance-Kommunikation
- A20 Compliance-Überwachung und Verbesserung

Zu den einzelnen Themenblöcken ist beschrieben, was inhaltlich erwartet wird und teilweise auch in welcher Form die Beschreibung vorliegen kann.

5.3 TÜV und TR CMS 101:2011

Bei diesem Regelwerk handelt es sich um ausschließlich um Vorgaben zum Inhalt und zur Struktur eines CMS. Es orientiert sich weitgehend an der Struktur anderer Managementsystemvorgaben, hier ganz besonders an der ISO 9001:2008 und enthält keinerlei Erläuterungen bzw. Vorgaben für die Prüfungsdurchführung.

Aus den Hauptüberschriften können Rückschlüsse auf die Themenblöcke gezogen werden, auch die Verbindungen zur ISO 9001:2008 sind darin erkennbar:

- 0 = Einleitung
- 1 = Anwendungsbereich
- 2 = Ziele des CMS
- 3 = Begriffe
- 4 = Compliance Managementsystem
- 5 = Verantwortung der Leitung
- 6 = Management von Ressourcen
- 7 = Compliance-Prozesse und Umsetzung
- 8 = Systemüberwachung, -analyse und -verbesserung

5.4 Fazit

PETER WINTZER – KIEFERNWEG 5 – 55457 GENSINGEN – TEL. 06727 / 1054 – EMAIL: PWMP-MOB@T-ONLINE.DE

Compliance-Management und Haftungsfragen

Wenn auch diese Regelwerke sehr unterschiedliche Inhalte und Strukturen haben, verfolgen sie doch das gleiche Ziel. Die IDW PS 980 lässt dabei vollkommen offen, auf welchen Wegen eine Organisation dieses Ziel verfolgt, während die TR CMS 101 und die ISO 19600 Vorschläge zur Struktur und zu Inhalten enthalten.

In allen Fällen muss eine Organisation jedoch genau darauf achten, dass mit der Implementierung eines CMS nicht ein Parallelsystem entsteht, welches immer Doppelbeschreibungen nach sich zieht. Die Vermeidung einer derartigen Doppelbeschreibung ist am Ersten bei der ISO 19600 gegeben, da sie der Struktur aller anderen Systemnormen folgt und somit leichter in bestehende Systeme bzw. Geschäftsprozesse integrierbar ist.

PETER WINTZER – KIEFERNWEG 5 – 55457 GENSINGEN – TEL. 06727 / 1054 – EMAIL: PWMP-MOB@T-ONLINE.DE

Compliance-Management und Haftungsfragen

6 Integrierte Managementsysteme und CMS

Auch wenn ich persönlich noch keine Organisation bei der Implementierung eines CMS beratend unterstützt habe, ergibt sich aber aus den Forderungen der zuvor genannten Regelwerke eine Vorgehensweise, die sich in keiner Weise von der Integration anderer Managementsysteme in eine vorhandene Systembeschreibung zu Geschäftsprozessen unterscheidet. Dazu im Folgenden eine Vorgehensweise, die darauf ausgerichtet ist, die Grundsatzforderungen beider Regelwerke in das vorhandene Managementsystem bzw. die vorhandenen Prozessbeschreibungen zu integrieren.

Ausgangsbasis hierfür ist die Struktur der ISO 19600:2016-12.

6.1 Kontext der Organisation

Themen aus Abschnitt 4:
Dieses umfasst zunächst die Ermittlung der Grundlagen für die inhaltliche Gestaltung des CMS.

1. Feststellung der interessierten Parteien und deren Anforderungen
2. Festlegung des Anwendungsbereiches
3. Feststellen der bindenden Verpflichtungen
4. Ermitteln der Compliance-Risiken (Abschnitt 4) und Maßnahmen (Abschnitt 6.1)

Die Punkte 1. bis 3. sind bereits Forderungen, die in allen anderen Systemnormen enthalten sind. Somit ist eine Vorgehensweise vorhanden und muss ggf. um Compliance-Forderungen ergänzt werden.
Auch für Pkt. 4 gibt es vielfach schon praktizierte Methoden, da Risikobetrachtungen ebenfalls durch alle Systemnormen gefordert werden, allerdings immer eingeschränkt auf die jeweiligen Sachthemen. Sie umfassen häufig nicht die in Pkt, 3 dieser Abhandlung genannten Rechtsgebiete. Insofern ist eine Ausweitung auf diese Rechtgebiete erforderlich, was die Einbindung von internen Funktionseinheiten (wie z.B. Rechnungswesen) erforderlich macht, die bisher nicht oder nur am Rande betroffen waren.

6.2 Führung

Themen aus Abschnitt 5:
Hier werden im Wesentlichen die folgenden Themen behandelt:

1. Politik
2. Verantwortungen und Befugnisse

PETER WINTZER – KIEFERNWEG 5 – 55457 GENSINGEN – TEL. 06727 / 1054 – EMAIL: PWMP-MOB@T-ONLINE.DE

Compliance-Management und Haftungsfragen

6.2.1 Politik

ISO 19600:2016-12 Abschnitt 5.2.1 Abs. 1:
Das oberste Organ und die oberste Leitung sollten, vorzugsweise in Absprache mit den Beschäftigten, eine Compliance-Politik festlegen, die…. (es folgt eine Aufzählung von Detailinhalten)

IDW PS 980 spricht unter Textzeile A14 von **Compliance-Kultur**, ebenso wie TR CMS 101unter Abschnitt 5.1 b).

Damit ist die Grundsatzhaltung der obersten Leitung zum Compliance-Thema gemeint und wie sie diese Haltung den Beschäftigten der Organisation vermittelt.

Andere Managementsystembeschreibungen stellen Forderungen zur Festlegung und Vermittlung einer Politik (z.B.: Qualität, Umwelt, Arbeits- und Gesundheitsschutz, Risiko, IT). Diese werden in der Regel als Strategie, Politik und/oder Leitsätze der Organisation verfasst und vermittelt.

Somit können die Grundsätze zur **Compliance-Politik** in die vorhandenen Aussagen zur Politik der Organisation integriert und den Beschäftigten vermittelt werden. Sicherlich ist gerade bei diesem Punkt die besondere Verpflichtung der obersten Leitung zu sehen, da Verstöße gegen die Compliance-Politik auch disziplinarische Konsequenzen haben müssen, da sonst die Wirkung verpuffen wird.

Fazit: Ergänzung vorhandener Beschreibungen, ggf. zusätzliche Erstschulungsmaßnahmen, die dann in die Wiederholungsschulungen integriert werden können.

6.2.2 Verantwortungen und Befugnisse

ISO 19600:2016-12 Abschnitt 5.3.1 Abs. 1:
Die oberste Leitung sollte sicherstellen, dass die Verantwortlichkeiten und Befugnisse für relevante Rollen zugewiesen und innerhalb der Organisation bekannt gemacht werden.

IDW PS 980 spricht unter Textzeile A18 von **Compliance-Organisation**, während die TR CMS 101 unter Abschnitt 4 vom **Compliance Management System**, unter 5.2.1 von **Verantwortung und Befugnis** und unter 5.2.2 vom **Compliance-Beauftragten** spricht. Inhaltlich sind keine relevanten Unterschiede feststellbar.

Zu diesem Bereich finden sich in der TR CMS 101 deutlich mehr Detailforderungen, deren Inhalte aber weitgehend mit den Forderungen aus allen anderen Managementsystemen identisch sind. Insoweit kann man hier von „nichts Neues“ sprechen.

Fazit: Alle genannten Forderungen sollten bereits jetzt Bestandteile bestehender Beschreibungen zu Geschäftsprozessen sein, selbstverständlich muss die Vollständigkeit geprüft werden, aber wenn überhaupt, kann es sich nur um geringfügige Ergänzungen handeln. Die Forderung nach einem „**Compliance-Beauftragten**“ ist eine solche Ergänzung.

PETER WINTZER – KIEFERNWEG 5 – 55457 GENSINGEN – TEL. 06727 / 1054 – EMAIL: PWMP-MOB@T-ONLINE.DE

Compliance-Management und Haftungsfragen

ISO 19600:2016-12 Abschnitt 5.3.2 Abs. 3:
*In vielen Organisationen gibt es eine **beauftragte Person** (z. B. einen Compliance-Officer), die für das Compliance-Management im Tagesgeschäft verantwortlich ist; in einigen Organisationen gibt es ein funktionsübergreifendes Compliance-Komitee, das Compliance innerhalb der gesamten Organisation koordiniert.*

Compliance-Beauftragter:
IDW PS 980 fordert unter Textzeile A18 lediglich die „Bestimmung" eines Compliance-Beauftragten oder eines Compliance-Gremiums. Hier geht TR CMS 101 unter Abschnitt 5.2.2 deutlich weiter, indem konkretere Details zu Kompetenzen und Aufgaben benannt sind.

Wie alle anderen Beauftragten auch, hat der **Compliance-Beauftragte** eine Stabsfunktion, der bestimmte Aufgaben zugewiesen sind. Lt. TR CMS 101 z. B. die Folgenden:

- CMS-Prozesse einführen, verwirklichen und aufrechterhalten
- Berichtspflicht an die oberste Leitung
- Bewusstseinsförderung und Sicherstellung der Kommunikation
- Eigeninitiativ CSM-relevante Vorgänge aufgreifen und darüber berichten

Ähnliche Formulierungen stehen auch in den anderen Managementsystemnormen.

Hieraus ist nicht abzuleiten, dass der Compliance-Beauftragte eine Sonderstellung mit Weisungsbefugnissen gegenüber anderen Beschäftigten der Organisation hat.

Dieses wäre nur dann gegeben, wenn in der Stellen- oder Aufgabenbeschreibung dieses Beauftragten entsprechende **konkrete Befugnisse** festgelegt, vom Beauftragten ausdrücklich akzeptiert wurden und diese auch in der Organisation bekannt gemacht sind.

Zusatzanmerkung: Gerade hier sind haftungsrechtliche Aspekte zu beachten. Um welche es sich dabei handeln kann, kann dem Absatz 7 entnommen werden.

Auch diese Forderungen sind Bestandteil aller anderen Systemnormen. Damit können vorhandene Systembeschreibungen um die entsprechenden CSM-Kriterien ergänzt werden. Zu beachten ist hier die **besondere Betonung** auf die Pflichten der obersten Leitung.

6.3 Compliance-Ziele

ISO 19600:2016-12 Abschnitt 6.2 Abs. 1:
Die Organisation sollte Compliance-Managementsystem-Ziele auf relevanten Funktionen und Ebenen festlegen.

IDW PS 980 spricht unter Textzeile A15 von **Compliance-Zielen**, ebenso wie TR CMS 101unter Abschnitt 5.1 c). Die Anmerkung 3 zum Abschnitt 3.9 der ISO 19600 lautet wie folgt: *Ein Ziel kann auf andere Weise ausge-*

PETER WINTZER – KIEFERNWEG 5 – 55457 GENSINGEN – TEL. 06727 / 1054 – EMAIL: PWMP-MOB@T-ONLINE.DE

Compliance-Management und Haftungsfragen

drückt werden, z. B. als beabsichtigtes Ergebnis, als Zweck, als betriebliches Kriterium, als Compliance-Ziel oder durch andere Wörter mit ähnlicher Bedeutung (en: aim, goal, target). Im Abschnitt 9.16 listet die ISO 19600 auch einige Beispiele für Compliance-Ziele auf.

Auch alle anderen Managementsystembeschreibungen fordern die Festlegung von Zielen. Somit sollten die entsprechenden Strukturen zur Festlegung, Erfassung und Bewertung von Zielen vorhanden sein und müssten lediglich um Compliance-Ziele ergänzt werden. Um welche Ziele kann es sich hier handeln? Dazu in **Bild 6.2.1** ein Auszug aus Wikipedia vom 08.06.2016.

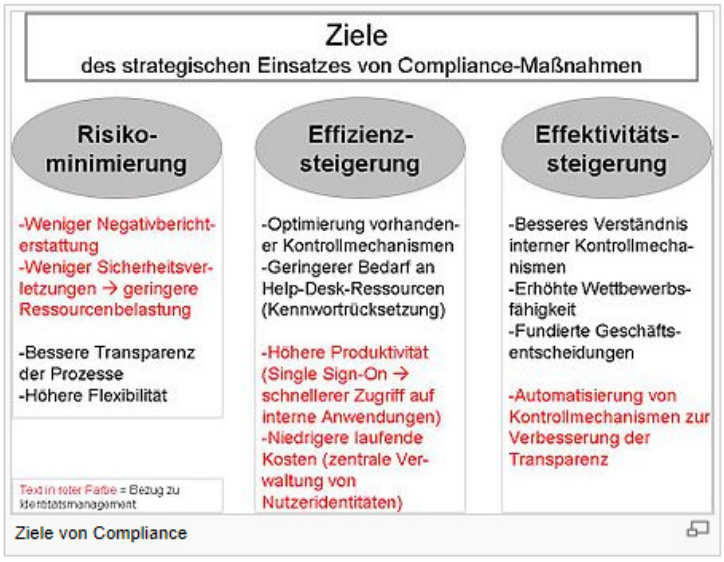

Bild 6.2.1

Fazit: Ergänzung der vorhandenen Beschreibungen (z.B.: Zielvereinbarungen, Zielebaum, Balance-Score-Card) zu Unternehmenszielen und Aufnahme in die Bewertungsroutinen.

6.4 Ressourcen

Zu den Ressourcen zählen in allen Systemnormen gleichermaßen

- Wissensbedarf
- Kompetenzen und Schulungsbedarf
- Bewusstsein
- Kommunikation
- Dokumentation
- Technische Einrichtungen und Umfeld

Lediglich zum **Verhaltenskodex** gibt es in der ISO 19600:2016-12 spezifische Zusatzanforderungen

PETER WINTZER – KIEFERNWEG 5 – 55457 GENSINGEN – TEL. 06727 / 1054 – EMAIL: PWMP-MOB@T-ONLINE.DE

Compliance-Management und Haftungsfragen

- *Unter Abschnitt 7.3.1.c): Personen, die unter Aufsicht der Organisation Tätigkeiten verrichten, sollten sich:.. der Folgen einer Nichterfüllung der Anforderungen des Compliance-Managementsystems bewusst sein.*
- *unter Abschnitt 7.3.2.1: Verhalten, das Compliance schafft und unterstützt, sollte gefördert werden; Verhalten, das Compliance beeinträchtigt, sollte nicht geduldet werden.*
- unter Abschnitt 7.3.2 eine große Anzahl von Verhaltensspielregeln, die bei der Implementierung des CMS zu berücksichtigen sind.

Allerdings enthalten bestehende Systemnormen auch Formulierungen, die einem ähnlichen Zweck dienen, wie z.B. ISO 9001:2015-11 unter Abschnitt 7.3
Die Organisation muss sicherstellen, dass die Personen, die unter Aufsicht der Organisation Tätigkeiten verrichten, sich Folgendem bewusst sind: .. der Folgen einer Nichterfüllung der Anforderungen des Qualitätsmanagementsystems

Im Folgenden generelle Aussagen der CMS-Normen und Regelwerke zum Thema „Ressourcen“:

ISO 19600:2016-12 Abschnitt 7.1 Abs. 1:
Die Organisation sollte die erforderlichen Ressourcen für den Aufbau, die Entwicklung, die Verwirklichung, die Bewertung, die Aufrechterhaltung und die fortlaufende Verbesserung des Compliance-Managementsystems bestimmen, entsprechend ihrer Größe, Komplexität, Struktur und operativen Tätigkeiten.

ISO 19600:2016-12 Abschnitt 7.1 Abs. 3:
Zu den Ressourcen zählen finanzielle und personelle Ressourcen sowie der Zugang zu externem Rat und Fachkenntnissen, betriebliche Infrastruktur, zeitgemäßes Referenzmaterial zu Compliance-Management und gesetzlichen Verpflichtungen, fachliche Fortbildung und Technologie.

IDW PS 980 Textzeile A15
Abstimmung mit den verfügbaren Ressourcen.

TR CMS 101 Abschnitt 6.1
Die Organisation muss die erforderlichen Ressourcen ermitteln und bereitstellen, um das Compliance Management System zu verwirklichen, aufrechtzuerhalten und seine Wirksamkeit ständig zu verbessern.

Auch hier ist festzuhalten, dass es sich um Forderungen handelt, die bereits in allen anderen Systemnormen enthalten sind. Bei den bestehenden Verfahren zur Ressourcenermittlung muss also lediglich eine Ergänzung um den Ressourcenbedarf für das CMS vorgenommen werden.

6.5 Planung und Steuerung

Hierbei geht es um die Prozessbeschreibung, die mit der Risikofeststellung beginnt, die Konsequenzen aus den Bewertungsergebnissen umfasst, Reaktionen im Abweichungsfall berücksichtigt, sowie erforderliche Korrektur-/Vorbeugungsmaßnahmen beschreibt.

ISO 19600:2016-12 Abschnitt 8.1 Abs. 1:

PETER WINTZER – KIEFERNWEG 5 – 55457 GENSINGEN – TEL. 06727 / 1054 – EMAIL: PWMP-MOB@T-ONLINE.DE

Compliance-Management und Haftungsfragen

Die Organisation sollte die Prozesse zur Erfüllung der bindenden Verpflichtungen und zur Durchführung der unter 6.1 bestimmten Maßnahmen planen, verwirklichen und steuern, indem sie:

IDW PS 980 Textzeile A17 Compliance-Programm:
Ein Compliance-Programm setzt sich aus den Grundsätzen und Maßnahmen zusammen, die auf die Begrenzung der Compliance-Risiken und damit auf ein regelkonformes Verhalten abzielen.

TR CMS 101 Abschnitt 7 der TR CMS 101:
Die Organisation muss über Abläufe verfügen, mit denen sichergestellt werden kann, dass die zur Erfüllung der Compliance-Anforderungen angemessenen Maßnahmen getroffen und die der Größe und Struktur der Organisation, der Art ihrer Tätigkeit sowie den Regionen, in denen sie tätig ist, angemessenen Prozesse eingeführt werden.

Diese Prozessbeschreibung muss auch den Sachverhalt der „**ausgegliederten Prozesse**“ enthalten (siehe Abschnitt 8.3 der ISO 19600), was aber für alle anderen Systemnormen auch zutrifft.

Fazit: In vielen Organisationen sind Prozessbeschreibungen zur Risikobetrachtung vorhanden. In diesen Fällen muss geprüft werden, ob diese Beschreibungen alle Anforderungen erfüllen, ggf. müssen Ergänzungen vorgenommen werden. Ansonsten ist der Prozess neu zu beschreiben.

6.6 Compliance-Überwachung

Der Abschnitt 9 der ISO 19600 umfasst die Themen

- Überwachung der CMS-Prozesse
- Audit
- Managementbewertung

ISO 19600:2016-12 Abschnitt 9.1.1 Abs. 1:
Die Organisation sollte bestimmen:

a) was überwacht und gemessen werden muss und warum;
b) die Methoden zur Überwachung, Messung, Analyse und Bewertung, sofern zutreffend, um gültige Ergebnisse sicherzustellen;
c) wann die Überwachung und Messung durchgeführt werden sollte;
d) wann die Ergebnisse der Überwachung und Messung analysiert, bewertet und berichtet werden sollten.

IDW PS 980 spricht unter Textzeile A20 von **Compliance-Überwachung und Verbesserung**, während in der TR CMS 101 unter Abschnitt 8 die Überschrift „**Systemüberwachung, -analyse und -verbesserung**“ verwendet wird. In allen Fällen geht es gleichermaßen um oben genannten Maßnahmen, die die Wirksamkeit des CMS sichern sollen.

PETER WINTZER – KIEFERNWEG 5 – 55457 GENSINGEN – TEL. 06727 / 1054 – EMAIL: PWMP-MOB@T-ONLINE.DE

Compliance-Management und Haftungsfragen

Fazit: Alle diese Forderungen sind uneingeschränkt Bestandteile bestehender Beschreibungen zu Geschäftsprozessen und müssen deshalb nur um die zusätzlichen Aspekte, die aus Compliance-Blickwinkel erforderlich sind, ergänzt werden. Um welche zusätzlichen Aspekte es sich handeln könnte, kann den Beispielsammlungen unter dem Hauptabschnitt 9 der ISO 19600 entnommen werden.

6.7 Compliance-Verbesserung

ISO 19600:2016-12 Abschnitt 10.1: Nichtkonformität, Non-Compliance und Korrekturmaßnahmen

IDW PS 980 spricht unter Textzeile A20 von **Compliance-Überwachung und Verbesserung**, während in der TR CMS 101 unter Abschnitt 8 die Überschrift „**Systemüberwachung, -analyse und -verbesserung**“ verwendet wird. In allen Fällen geht es gleichermaßen um Maßnahmen, die der Verbesserung des CMS dienen sollen.

Der Abschnitt 10.1.2 der ISO 19600 enthält noch eine Besonderheit, die als **Eskalation** betitelt wurde. Während andere Systemnormen diesen Begriff nicht oder nur im Zusammenhang mit Produkten/Projekten verwenden, betrifft hier die Eskalation alle Geschäftsprozesse. Daraus ist die Notwendigkeit abzuleiten, die Eskalationsverfahren auch auf alle Prozesse auszudehnen bzw. entsprechende Prozessbeschreibungen bzw. Verfahrensanweisungen zu dokumentieren.

Fazit: Die Forderungen gemäß Abschnitt 10.1.1 sind Bestandteile bestehender Beschreibungen zu Geschäftsprozessen und müssen deshalb nur um die zusätzlichen Aspekte, die aus Compliance-Blickwinkel erforderlich sind, ergänzt werden. Hierzu liefert die ISO 19600 im genannten Abschnitt diverse Beispiele. Zur „Eskalation“ sind ggf. neue Beschreibungen erforderlich.

ISO 19600:2016-12 Abschnitt 10.2: Fortlaufende Verbesserung

Keine Neuigkeit, da dieser Aspekt in allen anderen Systemnormen ebenfalls behandelt wird.

7 Zusammenfassung

7.1 Einleitung

Prüfungen zur Einhaltung von Gesetzen, Verordnungen, Richtlinien und sonstiger behördlicher Vorschriften aber auch interner Regeln erfolgen bereits heute im **Rahmen von Zertifizierungsverfahren und bei Betriebsprüfungen.** Sie ersetzen allerdings jetzt und in absehbarer Zukunft nicht die Arbeit der vom Gesetzgeber beauftragten Aufsichtsbehörden/Kontrollgremien. Das vordergründige Interesse der Zertifizierer von spezifischen Managementsystemen ist auch weiterhin auf die Gewährleistung der Lieferfähigkeit / Lieferzuverlässigkeit ausgerichtet, die ein wesentlicher Schwerpunkt der Kundenzufriedenheit ist.

PETER WINTZER – KIEFERNWEG 5 – 55457 GENSINGEN – TEL. 06727 / 1054 – EMAIL: PWMP-MOB@T-ONLINE.DE

Compliance-Management und Haftungsfragen

Deshalb ist auch vorhersehbar, dass zur Prüfung der Einhaltung von Compliance-Regeln eigene Prüfungs- und/oder Zertifizierungsverfahren geben wird. Als Organisation sollten Sie in jedem Fall den mit der Einrichtung bzw. der Pflege von Geschäftsprozessen verbundene Aufwand nutzen, um zu einer „**rechtssicheren**“ Dokumentation zu kommen, die im Streitfall von den Beteiligten dazu verwendet werden kann, zu belegen, dass alles zumutbare getan wurde, um das Auftreten des Schadens zu verhindern.

7.2 Interne Audits und Auditkriterienlisten

Forderungen an die Organisation, die aus Normen, Regelwerken, Gesetzen oder Vorschriften resultieren, sind für jede Konformitätsprüfung relevant. Deshalb ist es auch logisch, die Überprüfung der Einhaltung aller Forderungen in das System der internen Audits mit einzubinden. Voraussetzung ist, dass der jeweilige **„Beauftragte“** auch eine Analyse dieser Gesetze oder Vorschriften vorgenommen und daraus prüfbare Auditkriterien abgeleitet hat.

Für die Integration des Compliance-Managements in eine bestehende Struktur bedeutet das, dass neben den zu prüfenden Kriterien aus Normen und Regelwerken auch die Gesetze, Verordnungen und Vorschriften zu ermitteln sind, aus denen spezifische Compliance-Anforderungen an die Organisation abzuleiten sind. Diese sind in das bestehende Auditmanagement zu integrieren. Im Bedarfsfall kann hier **PWMP** Unterstützung leisten.

Nachfolgend ein Auszug aus der Auflistung der im Industriemodell von PWMP verwalteten aktuellen Auditkriterienlisten.

Pos.	Norm/Regelwerk	Titel/Erläuterung	Anmerkungen
1.1	9001:2015-11 DIN EN ISO	Qualitätsmanagementsysteme - Anforderungen	(*)
1.2	13485:2016-08 DIN EN ISO	Medizinprodukte Qualitätsmanagementsysteme Anforderungen für regulatorische Zwecke	(*)
1.3	14001:2015-11 DIN EN ISO	Umweltmanagementsysteme - Anforderungen mit Anleitung zur Anwendung	(*)
1.4	16949:2016-10 IATF	Qualitätsmanagement-System-Standard der Automobilindustrie	(*)
1.5	45001:2018-06 DIN ISO	Managementsysteme für Sicherheit und Gesundheit bei der Arbeit Anforderungen mit Anleitung zur Anwendung	(*)
1.6	27001:2015-03 ISO/IEC	Informationstechnik IT-Sicherheitsverfahren Informationssicherheits-Managementsysteme Anforderungen	(*)
1.7	50001:2018-12 DIN EN ISO	Energiemanagementsysteme - Anforderungen mit Anleitung zur Anwendung	(*)
1.8	Gefährdungsbeurteilung	Kriterien zur Durchführung einer Gefährdungsbeurteilung nach § 5 des Arbeitsschutzgesetzes	(*)

PETER WINTZER – KIEFERNWEG 5 – 55457 GENSINGEN – TEL. 06727 / 1054 – EMAIL: PWMP-MOB@T-ONLINE.DE

Compliance-Management und Haftungsfragen

1.9	Produktaudit	Kriterien zur Durchführung von Produktaudits über alle Geschäftsprozesse	(*)

Die vollständige Auflistung kann auf der Webseite von PWMP abgerufen oder bei k+k information services GmbH angefordert werden.

7.3 Abschlussbewertung

Mit der **ISO 19600:2016-12** liegt ein Regelwerk vor, dass jederzeit als Grundlage für den Aufbau eines Compliance-Managementsystems verwendet werden kann, unabhängig davon, ob es zu einer eigenständigen Zertifizierung kommt oder nicht. Organisationen, die ein Compliance-Managementsystem einrichten wollen, sollten unbedingt darauf achten, dass dieses in die bestehenden Beschreibungen zu Geschäftsprozessen integriert wird und keinesfalls zu einem Eigenleben führen darf.

Für den Erfolg eines Compliance-Managementsystems ist es aber auch besonders wichtig, dass die oberste Leitung der Organisation in vollem Umfang und mit persönlichem Einsatz die Implementierung unterstützt und über die konsequente Wahrnehmung einer regelmäßigen Überwachung, z.B. im Rahmen von Bewertungsverfahren, die nachhaltige Funktionsfähigkeit gewährleistet.

PETER WINTZER – KIEFERNWEG 5 – 55457 GENSINGEN – TEL. 06727 / 1054 – EMAIL: PWMP-MOB@T-ONLINE.DE

Compliance-Management und Haftungsfragen

8 Haftungskriterien

8.1 Einleitung

Eines vorweg: Dieses ist keine juristische Abhandlung, da ich kein Jurist bin. Mit meinen Worten schildere ich, was auf die Mitglieder einer Organisation aus Haftungssicht zukommen könnte. Deshalb kann niemand aus der Anwendung dieser Abhandlung Haftungsansprüche ableiten.

Bisher ist mir persönlich kein Fall bekannt, dass es aus einem Zertifizierungsverfahren heraus zu haftungsrechtlichen Konsequenzen gekommen wäre. Diese Konsequenzen sind allerdings immer dann zu erwarten, wenn es als Folge der Nichteinhaltung von gesetzlichen Bestimmungen zu einem unerwünschten Ereignis kam. Zu unerwünschten Ereignissen zählen u.a.:

- Ein Arbeitsunfall
- Im Rahmen einer behördlichen Überprüfung wurde ein Verstoß festgestellt
- Ein Kunde reklamiert eine Vertragsverletzung
- Ein Produktanwender erlitt einen Personen- oder Sachschaden
- Ein Lieferant liefert nicht vertragsgerecht
- Ein Fremdfertiger verursacht einen Personen- oder Sachschaden
- Es wurde ein Umweltschaden verursacht

8.2 Haftungsgrundsätze

Grundsätzlich ist ein Haftungsanspruch immer aus dem Bürgerlichen Gesetzbuch § 823 abzuleiten.

BGB § 823 Schadensersatzpflicht
(1) Wer vorsätzlich oder fahrlässig das Leben, den Körper, die Gesundheit, die Freiheit, das Eigentum oder ein sonstiges Recht eines anderen widerrechtlich verletzt, ist dem anderen zum Ersatz des daraus entstehenden Schadens verpflichtet.
(2) Die gleiche Verpflichtung trifft denjenigen, welcher gegen ein den Schutz eines anderen bezweckendes Gesetz verstößt. Ist nach dem Inhalt des Gesetzes ein Verstoß gegen dieses auch ohne Verschulden möglich, so tritt die Ersatzpflicht nur im Falle des Verschuldens ein.

PETER WINTZER – KIEFERNWEG 5 – 55457 GENSINGEN – TEL. 06727 / 1054 – EMAIL: PWMP-MOB@T-ONLINE.DE

Compliance-Management und Haftungsfragen

Auch das Produkthaftungsgesetz (ProdHaftG) schließt sich in § 1 „Haftung“ diesem Grundsatz an.

Gesetz über die Haftung für fehlerhafte Produkte. Produkthaftungsgesetz (ProdHaftG)
§ 1 Haftung
(1) Wird durch den Fehler eines Produkts jemand getötet, sein Körper oder seine Gesundheit verletzt oder eine Sache beschädigt, so ist der Hersteller des Produkts verpflichtet, dem Geschädigten den daraus entstehenden Schaden zu ersetzen. Im Falle der Sachbeschädigung gilt dies nur, wenn eine andere Sache als das fehlerhafte Produktbeschädigt wird und diese andere Sache ihrer Art nach gewöhnlich für den privaten Ge- oder Verbrauch bestimmt und hierzu von dem Geschädigten hauptsächlich verwendet worden ist.

8.3 Haftungsumfang

Viele Gesetze oder Verordnungen präzisieren die Schadensersatzpflicht, indem sie auf konkrete Strafen hinweisen. Dazu im Nachfolgenden einige Beispiele.

Produkthaftungsgesetzes (ProdHaftG)
Arbeitsschutzgesetz (ArbSchG)
Bundes-Immissionsschutzgesetz (BImSchG)
Kreislaufwirtschafts- und Abfallgesetz (KrW-/AbfG)
Wasserhaushaltsgesetz (WHG)
Chemikaliengesetz (ChemG)

Je nach Gesetz kann es sich hier um Bußgelder, Geldstrafen oder Ordnungswidrigkeiten zwischen 5.000 € und 200.000 € oder Freiheitsstrafen zwischen 1 – 5 Jahren handeln.

8.4 Haftende Personen

Bei Organisationen ab mittlerer Größe finden wir in der Regel folgende Führungsstruktur vor, in Kleinbetrieben spielt sich dieses oft in Personalunion ab:

- Oberste Leitung (z.B.: Geschäftsführung, Vorstand)
- Zweite Führungsebene (z. B.: Abteilungsleiter, Direktoren)
- Untere Führungsebene(n) (z.B.: Meister, Vorarbeiter, Gruppenleiter)
- Personen mit Entscheidungskompetenzen (z.B.: Einzelpersonen aus den Bereichen Einkauf, Verkauf, Personalwesen, Rechnungswesen und auch die sogenannten „Beauftragten“)
- Personen ohne Entscheidungskompetenzen (z. B.: alle Personen, die ihre Tätigkeit auf der Grundlage von Einzelarbeitsaufträgen wie Arbeitspläne, Instandhaltungsaufträge, Fahraufträge verrichten)

Dieser Sachverhalt ist mit unterschiedlichen Haftungsfolgen verbunden, deshalb nachfolgend eine entsprechende Untergliederung.

PETER WINTZER – KIEFERNWEG 5 – 55457 GENSINGEN – TEL. 06727 / 1054 – EMAIL: PWMP-MOB@T-ONLINE.DE

Compliance-Management und Haftungsfragen

8.4.1 Oberste Leitung

Zu den Aufgaben und Verpflichtungen der obersten Leitung einer Organisation gehört, dass der Arbeitsablauf so zu organisieren ist, dass die Arbeiten sicher durchgeführt werden können und schließt die Überwachung der Einhaltung dieser Arbeitsabläufe ein.

Konkret bedeutet das, dass die oberste Leitung im Vorfeld der Tätigkeiten u.a. dafür zu sorgen hat,

- dass Arbeitsabläufe unter Berücksichtigung der zutreffenden Gesetze und Vorschriften geplant werden,
- dass ausreichend/angemessen qualifiziertes Personal (hier ganz besonders Führungskräfte) zum Einsatz kommt,
- dass fähige und sichere technische Einrichtungen (Anlagen, Werkzeuge, Schutzeinrichtungen, Vorrichtungen, Hilfsmittel) vorhanden sind und
- dass dem Personal auch die erforderliche persönliche Schutzausrüstung (z. B. Gehörschutz, Kopfschutz, Sicherheitsschuhe u. ä.) zur Verfügung gestellt wird.

Im nächsten Schritt muss sich die oberste Leitung in unregelmäßigen und angemessenen Zeitabständen auch davon überzeugen, ob bei der oder zur **Ausführung der Tätigkeiten**

- die festgelegten Arbeitsabläufe eingehalten werden,
- die Qualifikation des Personals weiterhin ausreichend/angemessen ist und ganz besonders die Führungskräfte ihre besonderen Aufgaben wahrnehmen,
- die technischen Einrichtungen weiterhin fähig und sicher sind und
- die erforderlichen persönlichen Schutzausrüstungen auch benutzt werden.

Dieses muss nicht durch eine **persönlich ausgeführte Kontrollfunktion** erfolgen, hier kann auch auf andere Führungskräfte sowie das System der internen Audits und der Bewertung der Auditergebnisse zugegriffen werden, wenn die Auditkriterien die durch Gesetze oder Verordnungen geregelten Sachverhalte mit berücksichtigen.

Ein Versäumen vorstehender Pflichten **kann** für die oberste Leitung zu nachfolgenden Konsequenzen führen:

1. Bußgeldbescheide oder Freiheitsstrafen bei Verstößen gegen Gesetze, Vorschriften oder Unfallverhütungsvorschriften (dabei muss noch nicht einmal ein tatsächlicher Schaden eingetreten sein)
2. Zivilrechtliche Haftung bei Sachschäden
3. Zivilrechtliche Haftung bei Personenschäden
4. Strafrechtliche Haftung bei bloßer Gefährdung
5. Strafrechtliche Haftung bei Schädigung eines Menschen

PETER WINTZER – KIEFERNWEG 5 – 55457 GENSINGEN – TEL. 06727 / 1054 – EMAIL: PWMP-MOB@T-ONLINE.DE

Compliance-Management und Haftungsfragen

BGB § 618 Pflicht zu Schutzmaßnahmen
(1) Der Dienstberechtigte hat Räume, Vorrichtungen oder Gerätschaften, die er zur Verrichtung der Dienste zu beschaffen hat, so einzurichten und zu unterhalten und Dienstleistungen, die unter seiner Anordnung oder seiner Leitung vorzunehmen sind, so zu regeln, dass der Verpflichtete gegen Gefahr für Leben und Gesundheit soweit geschützt ist, als die Natur der Dienstleistung es gestattet.

BGB § 619 Unabdingbarkeit der Fürsorgepflichten
Die dem Dienstberechtigten nach den §§ 617, 618 obliegenden Verpflichtungen können nicht im Voraus durch Vertrag aufgehoben oder beschränkt werden.

Aus den beiden vorstehenden §§ des BGB ist die besondere Situation der obersten Leitung abzuleiten, dass sie nicht per Vertrag bestimmte Verantwortungen „nach unten“ delegieren kann. Umso wichtiger ist, dass die oberste Leitung klare **Organisationsstrukturen (Verantwortungen) und klare Prozessabläufe (Prozessbeschreibungen)** nachweist, durch die sie sich im Haftungsfall entlasten kann.

8.4.2 Führungsebenen

Die betrieblichen Führungskräfte wie z. B. Abteilungsleiter, Beauftragte, Meister, Gruppenleiter, Vorarbeiter, aber auch Sachbearbeiter mit Entscheidungskompetenzen müssen, da sie als Linien- aber auch Stabsverantwortliche, im Auftrag der obersten Leitung handeln, ebenfalls dafür sorgen, dass die **Tätigkeiten vor Ort** unter Berücksichtigung der zutreffenden Gesetze und Vorschriften **geplant und ausgeführt werden**.

Sie müssen dafür sorgen

- dass das Personal mit **der vorgesehenen Qualifikation** zum Einsatz kommt,
- dass die **geplanten fähigen und sicheren technischen Einrichtungen** (Anlagen, Werkzeuge, Schutzeinrichtungen, Vorrichtungen, Hilfsmittel) verwendet werden,
- dass das Personal auch die erforderliche **persönliche Schutzausrüstung** (z. B. Gehörschutz, Kopfschutz, Sicherheitsschuhe u. ä.) **benutzt**
- und dass im Abweichungsfall auch die **erforderlichen Korrekturmaßnahmen** veranlasst werden.

Auch dieser Personenkreis muss sich in angemessenen Zeitabständen davon überzeugen, ob die Tätigkeiten richtig und sicher durchgeführt werden. Zumindest die Gruppenleiter oder Vorarbeiter müssen dieser Aufgabe, **durch im Regelfall ständige Präsenz**, nachkommen. So kann z. B. die Fachkraft für Arbeitssicherheit (Beauftragter) die regelmäßigen Betriebsbegehungen in Kombination mit den Sitzungen des Arbeitssicherheitsausschusses und deren Ergebnisdokumentation für diesen Zweck nutzen. Analog gilt dieses auch für den Umweltschutz-Beauftragten. Ein Versäumen dieser Pflichten kann durchaus zu den gleichen Konsequenzen führen, wie bei der obersten Leitung benannt. Hier kommen allerdings die Begriffe

- **fahrlässig, grob fahrlässig und vorsätzlich**

ins Spiel.

PETER WINTZER – KIEFERNWEG 5 – 55457 GENSINGEN – TEL. 06727 / 1054 – EMAIL: PWMP-MOB@T-ONLINE.DE

Compliance-Management und Haftungsfragen

Nach den Grundsätzen der Arbeitnehmerhaftung, haften diese, wenn sie den Schaden im Rahmen einer dem Unternehmen dienenden Tätigkeit verursacht haben, bei **leicht fahrlässiger Schadensverursachung letztlich nicht**. An ihrer Stelle muss die oberste Leitung bzw. die Organisation Ersatz leisten.

Unter **bestimmten Voraussetzungen**, auf die hier nicht eingegangen wird, kann bei grob fahrlässigem oder vorsätzlichem Verschulden eine **direkte Haftung** gegenüber dem Geschädigten oder eine **indirekte Haftung** in Form von Regressansprüchen dritter Stellen (z.B.: Berufsgenossenschaft) eintreten.

Auch hier ist es also wichtig, dass die Führungskraft durch klare Prozessbeschreibungen, Handlungsanleitungen und Aufzeichnungen von Arbeitsergebnissen nachweisen kann, dass die Tätigkeiten wie geplant verrichtet wurden, um hierdurch im Haftungsfall entlasten zu sein.

8.4.3 Personen mit Entscheidungskompetenzen

Es handelt sich hier um den Personenkreis, der in Verbindung mit seiner Arbeitsaufgabe Entscheidungskompetenzen besitzt, aus denen Haftungsansprüche abgeleitet werden könnten. Dazu zählen z. B. Sachbearbeiter, die Lieferanten auswählen oder Verträge mit Kunden abschließen können. In beiden Fällen werden für die Organisation Rechtsgeschäfte abgeschlossen, aus denen im Negativfall auch Haftungsansprüche abgeleitet werden können. Es gelten hier die gleichen Regeln, die auch für Führungskräfte zutreffen.

8.4.4 Personen ohne Entscheidungskompetenzen

Auch eine Person, die in der Organisation nur auf ausdrückliche Weisung tätig ist (hierbei handelt es sich um Tätigkeiten, deren Anfang und Ende immer durch einen neuen Arbeitsauftrag bestimmt ist, wie z. B. ein Produktionsauftrag, ein Instandhaltungsauftrag, ein Fahrauftrag), kann in eine Haftungssituation gelangen.

Allerdings müssen hier „**Vorsatz**“ oder „**Fahrlässigkeit**“ vorliegen.

- **Vorsatz:** Zielgerichtetes, absichtliches Handeln oder die Rechtsgutsverletzung war erkennbar und die Person hat sich damit abgefunden
- **Fahrlässigkeit:** Die erforderliche Sorgfalt wurde außer Acht gelassen (das Ergebnis der Unterlassung war vorhersehbar und vermeidbar)

BGB § 276 Verantwortlichkeit des Schuldners
(1) Der Schuldner hat Vorsatz und Fahrlässigkeit zu vertreten, wenn eine strengere oder mildere Haftung weder bestimmt noch aus dem sonstigen Inhalt des Schuldverhältnisses, insbesondere aus der Übernahme einer Garantie oder eines Beschaffungsrisikos zu entnehmen ist. Die Vorschriften der §§ 827 und 828 finden entsprechende Anwendung.
(2) Fahrlässig handelt, wer die im Verkehr erforderliche Sorgfalt außer Acht lässt.
(3) Die Haftung wegen Vorsatzes kann dem Schuldner nicht im Voraus erlassen werden.

PETER WINTZER – KIEFERNWEG 5 – 55457 GENSINGEN – TEL. 06727 / 1054 – EMAIL: PWMP-MOB@T-ONLINE.DE

Compliance-Management und Haftungsfragen

8.5 Zusammenfassung

Da Haftungsfragen häufig erst dann diskutiert werden, wenn auch ein Haftungsfall eingetreten ist, muss die Führung einer Organisation hier einen Wandel im Denken herbeiführen. In diesem Zusammenhang ist interessant, dass es zu diesem Thema in spezifischen Normen auch indirekte Forderungen gibt.

ISO 19600:2016-12 Abschnitt 7.3.2.1:
Verhalten, das Compliance schafft und unterstützt, sollte gefördert werden; Verhalten, das Compliance beeinträchtigt, sollte nicht geduldet werden.

ISO 19600:2016-12 Abschnitt 7.3.1:
Personen, die unter Aufsicht der Organisation Tätigkeiten verrichten, sollten sich:

a) der Compliance-Politik;

b) ihrer Rolle und ihres Beitrags zur Wirksamkeit des Compliance-Managementsystems, einschließlich der Vorteile einer verbesserten Leistung des Compliance-Managementsystems;

c) der Folgen einer Nichterfüllung der Anforderungen des Compliance-Managementsystems

bewusst sein.

ISO 9001:2015-11 Abschnitt 7.3 Absatz 1
Die Organisation muss sicherstellen, dass die Personen, die unter Aufsicht der Organisation Tätigkeiten verrichten, sich Folgendem bewusst sind:

a) der Qualitätspolitik;
b) der relevanten Qualitätsziele;
c) ihres Beitrags zur Wirksamkeit des Qualitätsmanagementsystems, einschließlich der Vorteile einer verbesserten Leistung;
d) der Folgen einer Nichterfüllung der Anforderungen des Qualitätsmanagementsystems.

ISO 14001:2015-11 Abschnitt 7.3 Absatz 1
Die Organisation muss sicherstellen, dass Personen, die unter Aufsicht der Organisation Tätigkeiten verrichten, sich:

a) der Umweltpolitik;
b) der bedeutenden Umweltaspekte und der damit verbundenen tatsächlichen oder potenziellen Umweltauswirkungen im Zusammenhang mit ihrer Arbeit;
c) ihres Beitrags zur Wirksamkeit des Umweltmanagementsystems, einschließlich der Vorteile einer verbesserten Umweltleistung;
d) der Folgen einer Nichterfüllung der Anforderungen des Umweltmanagementsystems, einschließlich der Nichterfüllung der bindenden Verpflichtungen der Organisation, bewusst sind.

Wie Zertifizierungsauditoren dieses bewerten, wird sich in den nächsten Monaten zeigen, grundsätzlich dürfte es aber in folgende Richtungen gehen:

- Wissen um die Folgen der möglichen Fehler in Richtung Kunden/Anwender
- Wissen um Haftungsaspekte
- Wissen um persönliche Konsequenzen (Haftung, disziplinarische Folgen)

PETER WINTZER – KIEFERNWEG 5 – 55457 GENSINGEN – TEL. 06727 / 1054 – EMAIL: PWMP-MOB@T-ONLINE.DE

Compliance-Management und Haftungsfragen

So sollte man bei den betroffenen Personen in regelmäßigen Abständen das Wissen um Haftungsfragen auffrischen, vor allem auch vor dem Hintergrund das sich die externen Vorgaben immer wieder ändern. Als angemessen kann hier ein Wiederholungszeitraum von 1 -2 Jahren angesehen werden.

Branchenverbände und Versicherungen geben hier sehr häufig (auch unentgeltlich) entsprechende Hilfestellung, die Organisation muss lediglich der Personen und die Zeit zur Verfügung stellen.

PETER WINTZER – KIEFERNWEG 5 – 55457 GENSINGEN – TEL. 06727 / 1054 – EMAIL: PWMP-MOB@T-ONLINE.DE