Compliancemanagement richtig implementieren und integrieren
1. Auflage

TÜV Media

Die ISO 37301 im IMS

TÜVRheinland
Genau. Richtig.

Die ISO 37301 im IMS – Compliancemanagement richtig implementieren und integrieren

Autor:

Dr.-Ing. Wolfgang Kallmeyer
Partner der TÜV Rheinland Consulting GmbH

Bibliografische Informationen der Deutschen Nationalibliothek
Die Deutsche Nationalibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie. Detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

ISBN 978-3-7406-0790-6 (Print)
ISBN 978-3-7406-0791-3 (E-Book)

Zur Nutzung der Broschüre

Vorschriften, Vorschriften, Vorschriften

Kein Unternehmen auf dieser Welt kommt ohne Berührung mit dem Thema Compliance aus. Rechtsvorschriften sind allgegenwärtig, sei es im Straßenverkehr, beim Betrieb von Anlagen oder bei der Produktion von Produkten und deren Auswirkungen in der Nutzungsphase. Von der Wiege bis zur Bahre ist der Weg mit Rechtsvorschriften und anderen Regeln gespickt, es beginnt mit der Geburtsurkunde und endet mit dem Totenschein, denn beide sind Rechtsakte, die auf gesetzlicher Grundlage des Staates beruhen.

Zielsetzung der Broschüre

In dieser Broschüre erfahren Sie, was die ISO mit der Managementsystemnorm ISO 37301:2021 „Compliance-Managementsystem" erreichen möchte, welche Ziele sie damit verfolgt und was alles unter Compliance-Verpflichtungen zu verstehen ist. Im Sinne der Norm sind damit nicht nur gesetzliche Vorschriften und Genehmigungen, also bindende Verpflichtungen, gemeint, sondern auch weitere Verpflichtungen externer Art, die von regelsetzenden Stellen erlassen werden. Darunter fallen z. B. Normen, Spezifikationen, technische Regeln, Vorschriften. Als dritte Säule kommen freiwillige Verpflichtungen des Unternehmens hinzu, z. B. Verträge, Patente, Mitgliedschaften in Organisationen oder interne Regeln in Form von Leitlinien, -fäden, Richtlinien, ethischen Grundsätzen, Verhaltenskodizes.

Wir geben einen Überblick über den Aufbau und die Struktur der Rechtsnormen in Deutschland und ihre Wechselwirkung mit dem Europäischen und dem Völkerrecht. Außerdem erläutern wir Ihnen, wie die Unternehmen in Deutschland in diese Rechtsstruktur eingebettet sind und wie man die für die Organisation relevanten Rechtsvorschriften ermittelt, systematisiert und deren Umsetzung organisieren kann. Dabei werden u. a. folgende Fragen beantwortet:

- Welche Bedeutung haben die beiden Teilgebiete „Legal Compliance" und „Corporate Compliance" für die Compliance?
- Welchen Einfluss hat die Compliancekonformität auf den Unternehmenserfolg?
- Was kann die Führung tun, um das Thema Compliance im Unternehmen zu managen, um den Unternehmenserfolg zu steigern?
- Wie trägt das Kano-Modell unter Berücksichtigung der Nachhaltigkeit zur Stakeholderzufriedenheit und zum Unternehmenserfolg bei?

Umsetzung der Forderungen

Im Weiteren erfahren Sie, wie Sie die Forderungen der ISO 37301 implementieren und in ein Integriertes Managementsystem (IMS) integrieren können, dass aus ISO 9001 (Qualität), ISO 14001 (Umweltschutz) und ISO 45001 (Arbeits- und Gesundheitsschutz) besteht. Das heißt, wo Sie mögliche Synergien mit anderen Managementsysteme nutzen können, um beim Aufbau des Compliance-Managementsystems (CMS) überflüssige Mehrarbeit zu vermeiden. Dazu haben wir Abschnitt 6 in Listenform aufgebaut. In der jeweiligen Liste werden zuerst die Forderungen der ISO 37301 genannt und dann werden Wege vorgestellt, wie Sie diese Forderungen in ein bestehendes IMS integrieren. Die dritte Position der Liste enthält praktische To-dos, wie und mit welchen Dokumenten man die Forderungen der ISO 37301 in das IMS integrieren kann. Die vierte Listenposition enthält ggf. spezielle Hinweise zur Umsetzung mit Erläuterungen oder Verweisen auf mitgeltende Anforderungen.

Arbeitshilfen

Wir unterstützen Sie rund um das Thema Compliancemanagement mit Arbeitshilfen und Mustern in Form von Formularen und Tabellen, die Ihnen beim Aufbau und bei der Integration der ISO 37301 in ein IMS hilfreich sein können. An geeigneter Stelle im Text weisen wir mit Klammersymbolen auf die jeweiligen Arbeitshilfen hin:

Verweismatrix der Normen im betrachteten IMS

Verweismatrix_ 9001_14001_45001_ 37301.xlsx

Die Arbeitshilfe „Verweismatrix_9001_14001_45001_37301“ stellt über eine Verweismatrix die Normkapitel der Standards ISO 9001, ISO 14001, ISO 45001 und ISO 37301 in der Kapitelstruktur bis herab auf die dritte Gliederungsebene mit deren Gemeinsamkeiten sowie Unterschieden einander gegenüber.

Übersicht der für deutsche Unternehmen relevanten Rechtsgebiete

Rechtsgebiete.xlsx

In der Arbeitshilfe finden Sie eine alphabetische Aufstellung der gängigen Rechtsgebiete, die für Unternehmen in Deutschland im Rahmen ihres CMS von Bedeutung sein könnten.

Muster zur Ermittlung der Unternehmensaktivitäten

Compliance_ Ermittlung.xlsx

Die Arbeitshilfe ist ein Muster zur tabellarischen Erfassung der Rechts- und sonstigen Pflichten ausgehend von den Unternehmensaktivitäten. Sie kann als Vorlage zur eigenen Complianceermittlung genutzt werden. In einem ergänzenden Tabellenblatt finden Sie eine mögliche Zuordnung der unternehmensrelevanten Rechtsgebiete zu den Rechtsfeldern im CMS, die Sie an Ihr Unternehmen anpassen können

Kompatibilität ISO 37301 zu ISO 9001, ISO 14001, ISO 45001

Kompatibilitäts- matrix_IMS.xlsx

Die Arbeitshilfe stellt in einer Matrix die ISO 37301 den Standards ISO 9001, ISO 14001 und ISO 45001 gegenüber und gibt durch farbliche Kennzeichnung Hinweise über die Kompatibilität der grundlegenden Anforderungen im IMS.

Muster für ein Rechtskataster

R-Kataster.xlsx

Das Muster ist ein Beispiel für ein Rechtskataster in Tabellenform.

Muster für ein Genehmigungskataster

G-Kataster.xlsx

Das Muster ist ein Beispiel für ein Genehmigungskataster in Tabellenform.

Muster für ein Pflichtenkataster

P-Kataster.xlsx

Auch das beispielhafte Muster zur Erfassung von Pflichten aus dem Rechts- und Genehmigungskataster ist in Tabellenform ausgearbeitet.

Muster für eine Matrix zur Compliancerelevanzanalyse nach Nohl

RA_Nohl.xlsx

Die Methode nach Nohl nutzt zur Risikobewertung zwei Kriterien, zum einen die Wahrscheinlichkeit, dass sich das Risiko realisiert, und zum anderen den dadurch entstehenden Schaden (Schadenshöhe). Als Muster ist eine Matrix zur Compliancerelevanzanalyse nach Nohl beigefügt.

Muster für eine Matrix zur Compliancerelevanzanalyse gemäß FMEA

RA_FMEA.xlsx

Die Methode nach Nohl nutzt zur Risikobewertung zwei Kriterien, zum einen die Wahrscheinlichkeit, dass sich das Risiko realisiert, und zum anderen den dadurch entstehenden Schaden (Schadenshöhe). Dieses Kriterium berücksichtigt die Wirksamkeit bestehender Kontroll- oder Frühwarnmaßnahmen hinsichtlich Non-Compliance. Als Muster ist eine Matrix zur Compliancerelevanzanalyse gemäß FMEA beigefügt.

Muster für eine CMS-Kennzahlenmatrix

CMS-Kennzahlen- matrix.xlsx

Das Muster für eine CMS-Kennzahlenmatrix enthält einige Beispiele zur CMS-Datensammlung/Kennzahlen und kann hinsichtlich der betrieblichen Bedürfnisse angepasst werden.

Download

Die Arbeitshilfen stehen für Sie zum Download bereit unter:

www.qm-aktuell.de/60790-2/

Passwort: [redacted]

Sie können die Dokumente frei bearbeiten und an Ihre eigenen betrieblichen Anforderungen anpassen.

Inhalt

Zur Nutzung der Broschüre ... 3

1 Compliance im Wandel der Zeit ... 7

2 Ziel und Zweck der ISO 37301:2021 ... 9

3 Die ISO 37301, Harmonized Structure und Integration ... 13

4 Bindende Verpflichtungen einer Organisation ... 17
- 4.1 Was versteht die Norm unter „bindenden Verpflichtungen“ ... 17
  - 4.1.1 Regelsetzende Anforderungen in der ISO 9001:2015 ... 17
  - 4.1.2 Regelsetzende Anforderungen in der ISO 14001:2015 ... 18
  - 4.1.3 Regelsetzende Anforderungen in der ISO 45001:2018 ... 19
- 4.2 Gliederung des Rechts in Rechtsgebiete ... 21
  - 4.2.1 Allgemeines ... 21
  - 4.2.2 Deutsches Recht ... 22
  - 4.2.3 Völkerrecht und Europäisches Recht ... 23
- 4.3 Rechtliche Anforderungen aus Unternehmenssicht ... 24

5 Bedeutung der Rechtskonformität für eine Organisation ... 29
- 5.1 Compliance und Führung ... 29
- 5.2 Compliance und Unternehmenserfolg ... 30
  - 5.2.1 Thema: Nachhaltigkeit ... 33
  - 5.2.2 Thema: Klimaschutz ... 34

6 Integration der Forderungen des CMS in ein IMS ... 35
- 6.1 Einführung ... 35
- 6.2 Kontext der Organisation ... 37
  - 6.2.1 Verstehen der Organisation und ihres Kontextes ... 37
  - 6.2.2 Erfordernisse und Erwartungen interessierter Parteien ... 37
  - 6.2.3 Verstehen des Anwendungsbereichs des CMS ... 37
  - 6.2.4 Compliance-Managementsystem ... 38
  - 6.2.5 Compliance-Verpflichtung ... 38
  - 6.2.6 Compliance-Risikobeurteilung ... 39
- 6.3 Führung ... 41
  - 6.3.1 Führung und Verpflichtung Kompatibilität ... 41
  - 6.3.2 Compliance-Politik ... 44
  - 6.3.3 Rollen, Verantwortlichkeiten und Befugnisse ... 45
- 6.4 Planung ... 47
  - 6.4.1 Umgang mit Risiken und Möglichkeiten/Chancen ... 47
  - 6.4.2 Complianceziele und Planung zur Erreichung ... 48
  - 6.4.3 Planung von Änderungen ... 48
- 6.5 Unterstützung ... 49
  - 6.5.1 Ressourcen ... 49
  - 6.5.2 Kompetenz ... 49
  - 6.5.3 Bewusstsein ... 51
  - 6.5.4 Kommunikation ... 51
  - 6.5.5 Dokumentierte Information ... 52
- 6.6 Betrieb ... 54
  - 6.6.1 Betriebliche Planung und Steuerung ... 54
  - 6.6.2 Festlegung der Steuerung und Verfahren ... 55
  - 6.6.3 Äußern von Bedenken ... 56
  - 6.6.4 Untersuchungsprozesse ... 59

6.7 Bewertung der Leistung 60
6.7.1 Überwachung, Messung, Analyse und Bewertung 60
6.7.2 Internes Audit Kompatibilität 64
6.7.3 Managementbewertung Kompatibilität 65
6.8 Verbesserung 67
6.8.1 Fortlaufende Verbesserung 67
6.8.2 Nichtkonformität und Korrekturmaßnahmen 68

7 Quellen 69

Compliance im Wandel der Zeit

1 Compliance im Wandel der Zeit

Rechtsvorschriften sind fast so alt wie die Menschheit. Ohne für alle verbindliche Rechtsnormen würde das Zusammenleben der Menschen wohl nicht funktionieren. Unsere Zivilisation, auf die wir so stolz sind, wäre ohne allgemeingültige Regeln in Form eines kodifizierten Rechtsverständnisses so nicht möglich. Das wusste schon der sumerische König Hammurapi I., Herrscher über das Großreich von Babylon, um 1792 vor Christus. Seine steinernen Gesetzesstelen und Tontafeln enthalten in Keilschrift mit dem Codex Hammurapi die erste überlieferte Gesetzessammlung der Menschheit, und was darin steht, kommt uns allen sehr vertraut vor, z. B.:

Früher

„Baut ein Baumeister ein Haus und macht es zu schwach, sodass es einstürzt und den Bauherrn tötet: Dieser Baumeister ist des Todes. Kommt ein Sohn des Bauherrn dabei um, so soll ein Sohn des Baumeisters getötet werden. Kommt ein Sklave dabei um, so gebe der Baumeister einen Sklaven von gleichem Wert. Wird bei dem Einsturz Eigentum zerstört, so ersetze der Baumeister den Wert und baue das Haus wieder auf."

Heute

Die moderne Version des Codex Hammurapi steht im § 823 Absatz 1 des Bürgerlichen Gesetzbuchs (BGB): *„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."*

Motive

Im rechtlichen Kontext fällt obiges Beispiel in den Bereich „Produkthaftung". Kein Unternehmen, das Produkte, seien sie materiell oder immateriell, herstellt, ist davon ausgenommen. Das Strafmaß war damals noch ursprünglicher am Ausmaß der Tat orientiert, aber auch die heutigen Strafen können ein Unternehmen und/oder seine Führungskräfte hart treffen. Auch die Zehn Gebote Moses' sind eine Sammlung von Regeln, um das Zusammenleben der Menschen zu erleichtern. Das zehnte Gebot lautet: *„Du sollst nicht begehren deines nächsten Haus, Hof, Vieh und alles, was sein ist."* Doch die Nachrichten dieser Welt sind täglich voll von Raub, Bestechung, Unterschlagung, Betrug und Korruption. Das zentrale Motiv dabei ist Habgier, etwas zu besitzen, das mir nicht gehört. Meist sind es monetäre Aspekte, die zu diesen Rechtsbrüchen verleiten. Es können aber auch Machtambitionen und Geltungssucht dabei eine Rolle spielen. Im Geschäftsleben spielt Habgier eine nicht zu vernachlässigende Rolle und ist häufig die Triebfeder für Rechtsbrüche bis in höchsten Unternehmensspitzen. Bespiele dafür sind Dieselgate 2015 oder faule Bankgeschäfte, die Auslöser für die Weltfinanzkriese 2008 waren.

Regelungsflut

Die Rechtsregeln des Hammurapi waren für seine Zeit schon sehr anspruchsvoll und vielfältig. Es bedurfte vieler Tontafeln, um sie zu dokumentieren. Die Zehn Gebote waren da schon fast spartanisch übersichtlich. Heutige Rechtsvorschriften und Regeln füllen weltweit Bibliotheken und/oder lasten ganze Rechenzentren aus. Darüber den Überblick zu behalten ist für einen einzelnen Menschen unmöglich. Auch große Organisationen benötigen dafür ganze Abteilungen mit rechtskundigen Spezialisten. Aber absolute Sicherheit gegen das Auftreten von Non-Compliance bietet das alles nicht, wie uns die Erfahrung lehrt.

Lösungsansatz Managementsystem!

Was in der Praxis häufig fehlt, ist der systematische Ansatz, mit diesem Thema proaktiv umzugehen. Das Thema muss gemanagt werden, und es muss im Fokus der obersten Leitung stehen. Was könnte dafür besser geeignet sein als ein Managementsystem. Bei diesen Worten höre ich schon das Aufstöhnen in den Chefetagen: Noch ein Managementsystem! Haben wir denn davon nicht schon genug? Doch dann sollte man sich die Frage stellen, ob gegen Unternehmen verhängte Milliardenstrafen und angeklagte, verurteilte und inhaftierte höchste Führungskräfte zukünftig zur Imagepflege und Kundengewinnung von Unternehmen dienen sollen. Oder ist es nicht

so, dass Rechtskonformität eine Basisanforderung der Kunden an ein Unternehmen ist. Kein Kunde schreibt in seine Bestellung Rechtskonformität als besondere Anforderung, er setzt sie voraus.

Im Kern geht es doch darum, weshalb es so viele Gesetze und Vorschriften gibt. Es sind seit Hammurapis Zeiten ja nicht weniger geworden. Die Frage lässt sich aus Sicht von Juristen einfach beantworten, weil in unserer kleinteiligen, sehr dynamischen und vernetzten Welt ohne diese vielen Rechtsvorschriften das Zusammenleben der verschiedenen Gesellschaften und Nationen nicht funktionieren würde. Ob man in dem einen oder anderen Fall wirklich eine Rechtsvorschrift zu einem Thema braucht, darüber mag man trefflich streiten. Im Kontext macht der Wegfall einiger weniger Vorschriften die Aufgabe der Leitung, Rechtskonformität in einem Unternehmen sicherzustellen, aber auch nicht wirklich leichter.

Werkzeug zum Managen von Compliance

Weil das Thema Compliance so wichtig für das Ansehen und den Erfolg einer Organisation ist, hat die International Standard Organization (ISO) auf Wunsch der nationalen Normenorganisationen, auch der deutschen DIN, es als notwendig erachtet, den Organisationen und Unternehmen ein Werkzeug zum Managen von Compliance an die Hand zu geben, die ISO 37301:2021. Diese steht im Kontext mit anderen Managementsystemen, gleichberechtigt mit der ISO 9001 „Qualitätsmanagement", der ISO 14001 „Umweltmanagement" und/oder der ISO 45001 „Sicherheit und Gesundheit bei der Arbeit", um nur die drei bekanntesten und am häufigsten weltweit genutzten Managementsysteme zu nennen.

Managementsystem integrieren

Der ISO 9001 fällt in der Praxis im IMS häufig die Rolle des Leitsystems zu. Das Qualitätsmanagementsystem war das erste zertifizierfähige ISO-Managementsystem. Es ist seit 1987 aktiv und wurde bereits dreimal überarbeitet. Die letzte Revision stammt aus dem Jahr 2015. Wegen der wachsenden Bedeutung des Umweltschutzes wurde im Jahre 1996 mit der ISO 14001 das zweite Managementsystem auf den Markt gebracht. Sicherheit und Gesundheit bei der Arbeit bekamen erst 1999 durch die OHSAS 18001 eine Zertifizierungsgrundlage, die 2018 durch die ISO 45001 ersetzt wurde. Häufig findet man diese drei Systeme verbunden zu einem Integrierten Managementsystem (IMS) in den Unternehmen im Einsatz. Die Bedeutung dieser drei Managementsysteme für Unternehmen lässt sich auch an der Zahl der weltweiten Zertifizierungen erkennen. Sie machen in Summe mehr als 90 % aller Zertifizierungen aus.

2 Ziel und Zweck der ISO 37301:2021

„Wir sind nicht nur verantwortlich für das, was wir tun, sondern auch für das, was wir nicht tun." – Molière

Im Compliancemanagement bewegen wir uns zu einem nicht unerheblichen Teil im Bereich des Rechts. Gegen Rechtsnormen zu verstoßen wird mit Sanktionen seitens des Staates geahndet. Aber auch Nichthandeln, wenn die Pflicht zum Handeln besteht, erfüllt einen juristischen Tatbestand, den des Unterlassens; auch dies wird strafrechtlich sanktioniert. Und auch wenn wir gegen andere, nichtrechtliche Regeln verstoßen, zum Beispiel gegen Verträge oder Patente, kommen wir schnell wieder auf rechtliches Terrain. Das Zivilrecht mit den Vorschriften des BGB und des HGB sorgt in Deutschland dafür, dass wir für den Schaden des Geschädigten aufkommen müssen. Daneben gibt es aber bei Complianceverstößen noch weitere Schäden, deren finanzielles Ausmaß größer sein kann als das der rechtlichen, z. B. Imageschäden in der Öffentlichkeit, die ggf. auch die Existenz des Unternehmens gefährden können.

Wie kann ich es managen?

Sich mit dem Thema Compliancekonformität und der Frage *„Wie kann ich es managen?"* intensiv auseinanderzusetzen, sollte daher auf den Führungsetagen eine Selbstverständlichkeit sein. Um etwas zu managen, was nicht zum Kerngeschäft einer Organisation gehört, gibt es seit Ende der Achtzigerjahre von der ISO Unterstützung durch Managementsysteme. Seit 2021 gibt es die ISO 37301 „Compliance-Managementsystem" [1].

Was die Zielrichtung der ISO 37301 im Grundsatz ist, wurde in der Einleitung schon umrissen: die Rechtskonformität einer Organisation oder eines Unternehmens in Prozessen methodisch nachvollziehbar zu institutionalisieren. Doch die ISO 37301 macht nur Vorgaben, was in einem Compliance-Managementsystem zu regeln ist. Die Form der Umsetzung müssen die Unternehmen selbst bestimmen. Das methodische Vorgehen beim Aufbau von Managementsystemen sollte bei den meisten Unternehmen seit der Einführung anderer ISO-Managementsysteme wie der ISO 9001:2015 [2], der ISO 14001:2015 [3] oder der ISO 45001:2018 [4] bekannt sein.

Voraussetzung Compliancekultur

Für ein lebendiges CMS ist zuerst eine von der gesamten Belegschaft getragene Compliancekultur notwendig. Diese in der Organisation aufzubauen bedeutet viel Kommunikation in Form von Information, Schulung und Vorbildgeben. Complianceanforderungen beschränken sich nicht nur auf Teile einer Organisation, sondern betreffen in ihrer Querschnittsfunktion das gesamte Unternehmen. Das heißt, jeder Mitarbeiter ist davon betroffen. Unterschiedlich ist nur der Grad der Betroffenheit. Ein Staplerfahrer im Lager ist von Compliancevorschriften weniger betroffen als der Betriebsleiter oder der Geschäftsführer. Dass ein Mitarbeiter in einem Unternehmen keine Compliancevorschriften zu beachten hat, gibt es nicht. Dazu ist das Netz von rechtlichen Regelungen im Arbeits- und Umweltschutz in Deutschland zu dicht gesponnen.

Ein wirksames CMS versetzt die Organisation in die Lage, die Einhaltung einschlägiger Gesetze, regulatorischer Anforderungen (z. B. Genehmigungen oder Vertragsverpflichtungen), Industrie- oder anderweitiger Normen sowie freiwilliger Verpflichtungen (z. B. aus der Mitgliedschaft im Global-Compact-Netzwerk der UN) zu gewährleisten. Die Forderungen der ISO 37301 und die im Normanhang A dokumentierten Erläuterungen zur Verwendung der Norm geben den Unternehmen dafür eine große Hilfestellung. Zentrale Bausteine des betrieblichen CMS sind jedoch die Führung und die Mitarbeiter des Unternehmens, die das CMS täglich wirksam leben müssen.

Besondere Verantwortung der Leitung

Der Leitung kommt dabei eine besondere Verantwortung zu, da ihr Umgang mit den zentralen Werten der gesellschaftlichen Ethik und den allgemein anerkannten Normen der Good Governance (verantwortliche Unterneh-

mensführung) als Vorbild für regelkonformes Verhalten für alle dient. So kann die Umsetzung von Maßnahmen zur Förderung von regelkonformem Verhalten bei den Mitarbeitern gelingen. Compliance trägt darüber hinaus zu einer Verbesserung des sozialverantwortlichen Verhaltens im Unternehmen bei. Gelingt dies der Leitung nicht, ist das Auftreten von Non-Compliance in der Organisation ein Stück wahrscheinlicher geworden. Abbildung 1 stellt in grafischer Form die Zusammenhänge eines CMS dar.

Zusammenhänge im CMS

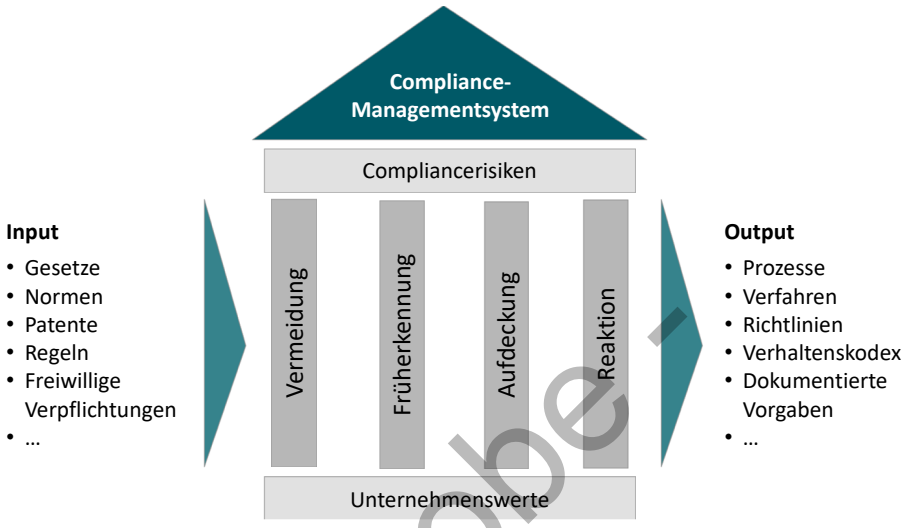

Abb. 1: Struktur eines Compliance-Managementsystems

Tragendes Gerüst aus vier Säulen

Das Compliance-Managementsystem eines Unternehmens gleicht einem Gebäude auf vier Säulen. In das Gebäude hinein kommen die Complianceforderungen aus den unterschiedlichsten Quellen, die dem Kontext der Organisation zuzurechnen sind. Das Fundament des Gebäudes sind die Werte und die Kultur des Unternehmens. Je fester dieses Fundament auf gesellschaftlich akzeptierten ethischen Grundsätzen beruht, desto geringer ist die Anfälligkeit der Organisation für Non-Compliance. Das tragende Gerüst des Gebäudes besteht aus den vier Säulen:

- Vermeidung von Non-Compliance durch Maßnahmen der Prävention
- Rechtzeitiges Erkennen von Non-Compliance durch Frühwarnmaßnahmen
- Aufdeckung von Non-Compliance durch regelmäßige Controllingaktivitäten
- Zielorientierte Reaktionen zur schnellen Beseitigung von Non-Compliance

Dachkonstruktion

Diese vier Säulen tragen dafür Sorge, dass die Statik der Dachkonstruktion die Compliancerisiken der Organisation sicher trägt. Damit dieses Gebäude seine Sicherheitsfunktionen erfüllt, generiert das Managementsystem die dazu notwendigen Vorgaben in Form von dokumentierten Prozessen, Verfahren, Richtlinien und anderen notwendigen Dokumenten zur Umsetzung, Überwachung und Weiterentwicklung des CMS.

Ergebnisse

Die Norm soll aktiv dazu beitragen, das Unternehmen und seine Leitung bei der Entwicklung, Implementierung und Weiterentwicklung einer funktionsfähigen Compliancekultur zu unterstützen. Dies umfasst das wirksame Management von Compliancerisiken, das in der Lage ist, folgende Ergebnisse zu erzeugen:

- Förderung von Businesserfolgen
- Stärkung des Ansehens und der Glaubwürdigkeit des Unternehmens
- Erfüllen der Erwartungen interessierter Parteien (wo immer möglich)

- Verpflichtung der Organisation, ihre Compliancerisiken wirksam zu managen
- Stärkung des Vertrauens externer Parteien in den nachhaltigen Erfolg der Organisation
- Minimieren des Risikos eines Complianceverstoßes
- Vermeiden von hohen Kapital- und Imageschäden durch Non-Compliance

Das Ergebnis der Bemühungen ist das Vermitteln von Integrität mit ethischen Grundsätzen und gesellschaftlichen Normen nach innen wie nach außen, um das gegenseitige Vertrauen zu stärken, sodass ein solides Managen von Compliancerisiken auch als Chance für das Unternehmen und seine Führung begriffen werden kann.

Grundelemente

Die Grundstruktur eines CMS nach ISO 37301 folgt den bekannten Vorgaben anderer ISO-Managementsysteme. Zu den Grundelementen gehören:

- Compliancekultur
- Compliancezíele
- Compliancerisiken
- Complianceprogramm
- Complianceorganisation
- Compliancekommunikation
- Complianceüberwachung

Mittels definierter verbindlicher Regelungen zu den in der Aufzählung genannten Themen können der Aufbau, die Umsetzung, die Aufrechterhaltung und die Verbesserung eines wirksamen CMS gelingen. Um das Rad dabei nicht mehrfach neu zu erfinden, können Elemente und Strukturen bereits implementierter Managementsysteme des IMS für das CMS partiell genutzt werden.

6 Integration der Forderungen des CMS in ein IMS

6.1 Einführung

Integrierte Managementsysteme sind in Unternehmen heute eher die Regel als die Ausnahme. Dank der Harmonized Structure (HS), deren gemeinsamer Struktur und der Harmonisierung der bestehenden Managementsysteme gibt es in den Normen viele Kapitel mit vergleichbaren Forderungen. Dies gilt insbesondere für die systemrelevanten Kapitel, die allgemeingültige Anforderungen bezüglich Aufbau, Kontrolle und Überwachung der Systeme formulieren. In diesen Fällen kann und sollte auch die Erfüllung dieser Forderung integriert erfolgen, z. B. nur eine Regelung für interne Audits oder dokumentierte Information. In anderen Fällen reicht eine normenspezifische Ergänzung (z. B. zur ISO 37301) zu einer bestehenden Regelung (Prozess/Verfahren) im IMS aus, um die Lücke zu schließen. Einen möglichen Weg zur Integration der ISO 37301 in ein IMS bestehend aus der ISO 9001, ISO 14001 und ISO 45001 beschreiben die folgenden Abschnitte: Kontext der Organisation (Abschnitt 6.2), Führung (Abschnitt 6.3), Planung (Abschnitt 6.4), Unterstützung (Abschnitt 6.5), Betrieb (Abschnitt 6.6), Bewertung der Leistung (Abschnitt 6.7) und Verbesserung (Abschnitt 6.8).

Übereinstimmungen und Unterschiede

Die Kompatibilitätsmatrix stellt die ISO 37301 den Standards ISO 9001, ISO 14001 und ISO 45001 in einer Übersicht gegenüber und gibt durch farbliche Kennzeichnung Hinweise über die Kompatibilität der grundlegenden Anforderungen im IMS.

Kompatibilitätsmatrix_IMS.xlsx

Ein direkter Vergleich der Forderungen der ISO 37301:2021 mit dem, was die anderen Normen des IMS (ISO 9001, 14001, 45001) bereits an Regelungen mitbringen, zeigt, dass in den meisten Fällen schon die Erfüllung der Forderungen dieser Normen ausreicht, um auch den Anforderungen der ISO 37301 zu genügen (s. Kompatibilitätsmatrix, grüne Felder). Ein kleinerer Teil erfüllt die Forderungen nur zum Teil, d. h., die bestehenden Regelungen im IMS müssen hinsichtlich der ISO 37301 ergänzt werden (s. Kompatibilitätsmatrix, gelbe Felder). Es gibt aber auch einen restlichen Teil an Forderungen in der ISO 37301, die keinen oder nur mangelhaften Bezug zu Regelungen in den anderen Normen im IMS haben. Diese Kapitel müssen mit systemspezifischen Regelungen zum CMS neu erstellt werden (s. Kompatibilitätsmatrix, rote Felder).

Direkter Vergleich

Für eine Organisation, die ein Compliance-Managementsystem nach ISO 37301 erstmals einführen möchte, stellen sich zwei Aufgaben gleichzeitig: der Aufbau des Managementsystems und die Integration der Anforderungen in das bestehende normative Gerüst des IMS. Das große Ziel sollte dabei am Ende sein: erstens die Implementierung eines zertifizierfähigen CMS gemäß den Anforderungen der ISO 37301 und zweitens die Nutzung von bestehenden Regelungen des IMS für vergleichbare Forderungen der ISO 37301, um Redundanzen im Gesamtsystem zu vermeiden.

Um ein zertifizierbares CMS zu implementieren, sollte man die Erfordernisse und Erwartungen der interessierten Parteien im Vorfeld kennen, die diese später zertifizieren sollen. Die Sichtweise eines Zertifizierungsauditors zu kennen und beim Aufbau des eigenen CMS zu berücksichtigen erleichtert die Aufgabe ungemein. In welcher Art CMS-Auditoren auf die ISO 37301:2021 blicken, lässt sich in deren Interpretation der Anforderungen nachvollziehen [8]. In einer chronologischen Rheihenfolge sind die Normenanforderungen der ISO 37301, die daraus abzuleitenden Aktivitäten (inkl. Erläuterungen) und die Art der benötigten (dokumentierten) Nachweise und Indikatoren (Kennzahlen) dargelegt. Die Ausführungen wurden bei den nachfolgenden Kapiteln zum Aufbau und zur Integration des CMS berücksichtigt.

Zertifizierbares CMS

Kategorien der Kompatibilität

In den nachfolgenden Kapiteln wird der Schwerpunkt der Ausführungen daher auf die Integration, d. h. die Kompatibilität der Forderungen der ISO 37301 mit denen der ISO 9001, ISO 14001 und ISO 45001 gelegt. Die Kompatibilität lässt sich zur Vereinfachung in drei Kategorien unterteilen:

- Anforderungen sind unmittelbar (direkt) vergleichbar (z. B. 4.2 „Verstehen der Erfordernisse und Erwartungen interessierter Parteien", kommt in allen drei IMS-Normen vor);
- Anforderungen sind mittelbar (indirekt) vergleichbar (z. B. 4.5 „Compliance-Verpflichtungen", kommt in der ISO 14001/45001 in 6.1.3 „Bindende Verpflichtungen" vor);
- Anforderungen sind nicht vergleichbar (z. B. 8.3 „Äußern von Bedenken", kommt nur in der ISO 37301 vor).

Um die Kompatibilität bzw. den Kompatibilitätsgrad der Forderungen der ISO 37301 mit denen der Managementsystemen des IMS übersichtlich anzuzeigen, sind die Felder der Forderungen des CMS in den folgenden Abschnitten 6.2 bis 6.8 durch Buchstaben bzw. farblich markiert.

A – Kompatibilität hoch	**B** – Kompatibilität mittel	**C** – Kompatibilität gering

Der Übersichtlichkeit halber sind die Ergebnisse bezüglich Integration in Listenform dargestellt. Zunächst werden die Forderungen der ISO 37301 genannt. Es folgt die Erläuterung der Kompatibilität der Forderungen und der Form der Integration der Anforderung des CMS ins IMS. Dann werden die dazu notwendigen Aktivitäten (To-dos) genannt. Es folgen weitere Hinweise zur Erläuterung der Umsetzung oder Integration. Ggf. sind weitere nützliche Informationen zu den Kapiteln vor- oder nachgestellt.

Normkapitel 4

6.2 Kontext der Organisation

Normkapitel 4.1

6.2.1 Verstehen der Organisation und ihres Kontextes

Kompatibilität

B – Kompatibilität mittel

Forderung des CMS

Relevante interne und externe Themen bestimmen, die sich auf das CMS und seine beabsichtigten Ergebnisse auswirken können (Klartextanalyse).

Integration ins IMS

Anforderungen sind im Prinzip über die bestehenden Managementsysteme des IMS abgedeckt. Eine integrierte Kontextbeschreibung ist für das IMS möglich.

To-dos

Vergleichen, ob alle genannten Kontextthemenbeispiele im IMS erfasst sind. Bezüglich des CMS kommen die Kontextthemen religiös/ethisches Verhalten, Rechtssysteme, Justiz, ggf. auch für unterschiedliche Länder hinzu. Weitere Themen können sich ggf. aus der Aufzählung in Normkapitel 4.1 ergeben, z. B. Rechtssystem, Rechtsprechung, Korruption, politische Einflüsse auf den Rechtsstaat oder politische Stabilität sowie aus dem Schaubild 1 „Elemente des CMS".

Hinweise

Die zukünftig absehbare Entwicklung des Kontexts sollte (Empfehlung aus Anhang A.4.1, keine Forderung) bei der Kontextanalyse mitberücksichtigt werden. Ggf. kann dies auch auf die andere Managementsysteme des IMS ausgeweitet werden.

Normkapitel 4.2

6.2.2 Erfordernisse und Erwartungen interessierter Parteien

Kompatibilität

A – Kompatibilität hoch

Forderung des CMS

Relevante interne und externe interessierte Kreise sowie deren Anforderungen und Erwartungen bezüglich Compliance bestimmen (Stakeholderanalyse). Festlegen des Umgangs der Organisation mit den Stakeholdern und ihren Bedürfnissen.

Integration ins IMS

Anforderungen im Prinzip über die bestehenden Managementsysteme des IMS abgedeckt. Integrierte Beschreibung des Stakeholdermanagements für das IMS möglich.

To-dos

Vergleichen, ob alle Stakeholder im IMS auch für das CMS erfasst sind.

Die ISO 37301 führt in A.4.2 ergänzend Beispiele für mögliche interne/externe Stakeholder an. Bezüglich des CMS könnten als Stakeholder z. B. Richter, Staatsanwälte, Fachanwälte, Justitiare, Wirtschaftsprüfer, Steuerberater, Compliance Officer usw. hinzukommen. Diese sind in die bestehende Stakeholderanalyse des IMS zu integrieren.

Hinweise

Keine

Normkapitel 4.3

6.2.3 Verstehen des Anwendungsbereichs des CMS

Kompatibilität

A – Kompatibilität hoch

Forderung des CMS

Bestimmen der organisatorischen und geografischen Grenzen und des Anwendungsbereichs des CMS. Dabei sind zu berücksichtigen der Kontext (4.1) und die interessierten Parteien (4.2) der Organisation sowie für das CMS die Compliance-Verpflichtung (4.5) und Compliancerisikobeurteilung (6.6). Der Anwendungsbereich muss dokumentiert sein.

Integration ins IMS

Der Geltungsbereich des CMS sollte im Regelfall durch das IMS weitgehend abgedeckt sein. Bei Konzernstrukturen könnte die Konzernzentrale, Stichwort