Fragen finden und im internen Audit richtig einsetzen
1. Auflage

TÜV Media

Der Auditfragenkatalog zur ISO 37301

- Leseprobe -

TÜVRheinland
Genau. Richtig.

Autor:

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

- Leseprobe -

Bibliografische Informationen 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.

ISBN 978-3-7406-0769-2 (Print)
ISBN 978-3-7406-0770-8 (E-Book)

© by TÜV Media GmbH, TÜV Rheinland Group, 1. Auflage, Köln 2022
www.tuev-media.de

®TÜV, TUEV und TUV sind eingetragene Marken.
Eine Nutzung und Verwendung bedarf der vorherigen Zustimmung.

Die Inhalte dieses Werks wurden von Verlag und Redaktion nach bestem Wissen und Gewissen erarbeitet und zusammengestellt. Eine rechtliche Gewähr für die Richtigkeit der einzelnen Angaben kann jedoch nicht übernommen werden. Gleiches gilt auch für Websites, auf die über Hyperlinks verwiesen wird. Es wird betont, dass wir keinerlei Einfluss auf die Inhalte und Formulierungen der verlinkten Seiten haben und auch keine Verantwortung für sie übernehmen. Grundsätzlich gelten die Wortlaute der Gesetzestexte und Richtlinien sowie die einschlägige Rechtsprechung.

Zur Nutzung der Broschüre

Zielsetzung der Broschüre

Interne Systemaudits gehören zum Alltag für alle Organisationen, die ein zertifiziertes Managementsystem unterhalten. In dieser Fachbroschüre erhalten Sie einleitende Informationen dazu, auf welchen Grundlagen interne Audits beruhen und welche normativen Regelwerke dabei zu berücksichtigen sind.

Aufbau

Im Kern dieser Broschüre erfahren Sie, wie Sie interne Audits nach dem internationalen Standard ISO 37301 „Compliance-Managementsysteme – Anforderungen mit Leitlinien zur Anwendung " durchführen können. Zur Bildung von Auditfragen stellen wir Ihnen dazu die Textanalyse und die Turtle-Analyse vor, die beiden gebräuchlichen Methoden, mit denen Sie recht einfach passende Auditfragen generieren können.

Außerdem erhalten Sie Hinweise zu korrektem Kommunikationsverhalten in verschiedenen Auditsituationen und zur richtigen Fragetechnik, mit der Sie im Audit die für eine Bewertung notwendigen Auditinformationen erhalten.

Der Fragenkatalog

Zu Ihrer Zeitersparnis finden Sie einen direkt verwendbaren Auditfragenkatalog für das interne Systemaudit, basierend auf den Forderungen der ISO 37301:2021, beigefügt. Den Fragenkatalog können Sie an die Erfordernisse Ihrer Organisation anpassen und um firmenspezifische Belange ergänzen.

Arbeitshilfen zum Download

Die im Text angeführten Klammersymbole verweisen auf Arbeitshilfen, die Sie bei der Generierung von Auditfragen unterstützen und die wir Ihnen zum Download bereitgestellt haben:

Auditfragenkatalog zum internen Systemaudit nach ISO 37301

Fragenkatalog_ 37301.docx

Der Auditfragenkatalog für das interne Systemaudit wurde für Sie auf der Grundlage der Forderungen der ISO 37301:2021 mittels Textanalyse generiert. Den Fragenkatalog können Sie an die Erfordernisse Ihrer Organisation anpassen und um firmenspezifische Belange ergänzen.

Auditfragen generieren mit Turtle-Analyse

Turtle-Analyse_ 37301.docx

Neben der Textanalyse lassen sich auch mit der Methode der Turtle-Analyse aus den Prozessen der Organisation nachvollziehbar und systematisch Auditfragen entwickeln. Über das strukturierte Formular werden alle relevanten Einflussfaktoren erfasst und zudem die Prozesse und ihre möglichen Risiken dargestellt. Sinnvollerweise werden auf diesem Formular auch Infos zu Prozesseigner, die Prozessbezeichnung und die Prozessstützen erfasst. Als Beispiel ist exemplarisch das Muster einer Turtle-Analyse für den Prozess „Interne Audits" beigefügt.

Die Arbeitshilfen stehen für Sie zum Download bereit unter:

www.qm-aktuell.de/60769-2/

Passwort: [redacted]

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

Leseprobe

Inhalt

Zur Nutzung der Broschüre ... 3

1 Auditprozess und seine Grundlagen ... 7

2 Leiten und Lenken von internen Audits ... 9

3 Struktur der ISO 37301 ... 11

4 Auditierung des CMS in Verbindung mit anderen Managementsystemen ... 13

5 Methoden zur Generierung von Auditfragen ... 17

5.1 Allgemeines ... 17

5.2 Textanalyse der Norm ... 18

5.3 Frageliste zur ISO 37301 ... 19

5.4 Turtle-Methode ... 20

6 Kommunikationsverhalten ... 25

7 Auditfragen und Auditinterview ... 27

7.1 Fragetechniken ... 27

7.2 Auditinterview ... 29

8 Quellen ... 30

Anhang 1: Auditfragen zur ISO 37301 ... 31

- Leseprobe -

1 Auditprozess und seine Grundlagen

Definition Audit

Nach der ISO 9000 [1] (Normkapitel 3.13.1) ist ein Audit ein „systematischer, unabhängiger und dokumentierter Prozess zur Erlangung von Auditnachweisen und zu deren objektiver Auswertung, um zu ermitteln, inwieweit Auditkriterien erfüllt sind".

ISO 19011

Zur Vorbereitung und Durchführung von internen Audits und Lieferantenaudits wurde die ISO 19011 [2] entwickelt. Das Management von Zertifizierungsaudits wird in der ISO/IEC 17021-1 [3] geregelt, die ISO 19011 kann dabei als Hilfestellung herangezogen werden.

Tabelle 1 gibt einen zusammenhängenden Überblick über die Auditarten, ihre Bezeichnungen und ihre normative Zuordnung.

Tabelle 1: Auditarten, Bezeichnungen und Anwendungsbereiche von ISO 19011 und ISO/IEC 17021

Auditarten	Internes Audit	Externes Audit	
		Lieferantenaudit (ggf. Kundenaudit)	Zertifizierungsaudit
Alternative Bezeichnungen	First-Party-Audit	Second-Party-Audit	Third-Party-Audit
Anwendungsbereich der Normen	ISO 19011	ISO/IEC 17021	

Bewertung und Verbesserung

Das Ziel eines internen Systemaudits (First-Party-Audit) besteht darin, das gesamte installierte Compliance-Managementsystem (CMS) eines Unternehmens nach ISO 37301 [4] systematisch zu bewerten und zu verbessern. Die Durchführung obliegt dabei meist geschulten Mitarbeitern des Unternehmens. Bei einem Systemaudit wird die gesamte Aufbau- und Ablauforganisation eines Unternehmens daraufhin überprüft, ob die Normenforderungen der ISO 37301 erfüllt sind und die eigenen Complianceziele erreicht werden konnten.

Die Anforderungen an Interne Audits der ISO 37301 unterscheiden sich im Grundsatz nicht von den Anforderungen anderer Systemnormen wie der ISO 9001, 14001 oder 45001. Methodisch ist ein vergleichbares Vorgehen und eine integrierte Auditdurchführung jederzeit möglich.

Rechtssicherheit steigern

Wird das gesamte CMS eines Unternehmens durch regelmäßige Audits überprüft, können Abweichungen von der Rechtskonformität im Hinblick auf Gesetze, Verordnungen, Genehmigungen usw. früh erkannt und rechtzeitig korrigiert werden. Dies senkt das Risiko von Non-Compliance-Vorfällen und der damit verbundenen materiellen und immateriellen Schäden. Da Compliance-Audits immer auch darauf abzielen, Verbesserungsmöglichkeiten zu finden, selbst wenn der Ablauf in Bezug auf die Einhaltung rechtlicher Vorgaben und Regeln relativ reibungslos funktioniert (z. B. Verhindern von Straftaten und Ordnungswidrigkeiten), können diese regelmäßigen Überprüfungen auch dazu genutzt werden, das Niveau des Compliance-Managementsystems in seiner Wirksamkeit kontinuierlich zu steigern. Der Schwerpunkt eines internen Audits liegt dabei neben der Absicherung der Compliancekonformität auf der Suche nach Verbesserungspotenzial zur Weiterentwicklung des Managementsystems und der Unternehmensprozesse. Die Erfüllung der Normenforderung spielt, im Gegensatz zu einem Zertifizierungsaudit, nur eine nachrangige Rolle.

Im Rahmen der Durchführung eines internen Audits sollen Informationen durch geeignete Stichprobenverfahren in Bezug auf die Auditziele und die Auditkriterien gesammelt werden. Darin enthalten sind auch Informationen, die sich auf Schnittstellen zwischen Funktionsbereichen, Tätigkeiten und Prozessen beziehen. Um an die notwendigen Auditinformationen zu kommen, müssen verschiedene Methoden der Informationsbeschaffung genutzt werden.

- Leseprobe -

Methoden der Informations-beschaffung

Gängige Methoden der Informationsbeschaffung in einem Audit sind:

- Führen von Interviews mit Mitarbeitern,
- Beobachten von Tätigkeiten und Prozessabläufen,
- Prüfen dokumentierter Information (Dokumente, Nachweise),
- Begehung des Standorts und Begutachtung von Standards zur Compliance-absicherung

Das Interview und die Befragung von Mitarbeitern und Führungskräften der auditierten Organisation sind die wichtigsten Instrumente zur Generierung von Auditfeststellungen für den Auditor. Dazu sind die richtigen Fragen zur richtigen Zeit am richtigen Ort zu stellen.

- Leseprobe -

2 Leiten und Lenken von internen Audits

Leitfaden

Die Anforderungen an interne Audits sind im Normkapitel 9.2 der ISO 37301 festgelegt. Die Beschreibung, was im Unternehmen genau zu tun ist, um die Normenforderung zu erfüllen, ist aber nicht im Detail ausgeführt. Daher hat die International Standard Organization (ISO) den „Leitfaden zur Auditierung von Managementsystemen" (ISO 19011) herausgebracht. Die ISO 37301 verweist explizit im Kapitel A.9.2 auf die Mitgeltung dieses Regelwerks. Der Leitfaden leistet den Unternehmen Hilfestellung bei der Planung und Durchführung von internen Audits. Die Ausführungen in diesem Leitfaden sind kein Muss, aber ein *Sollte* oder *Könnte,* um die Anforderungen an interne Audits zielgerichtet für das Unternehmen festzulegen und umzusetzen.

Die Gliederung der ISO 19011 zeigt die Abbildung 1.

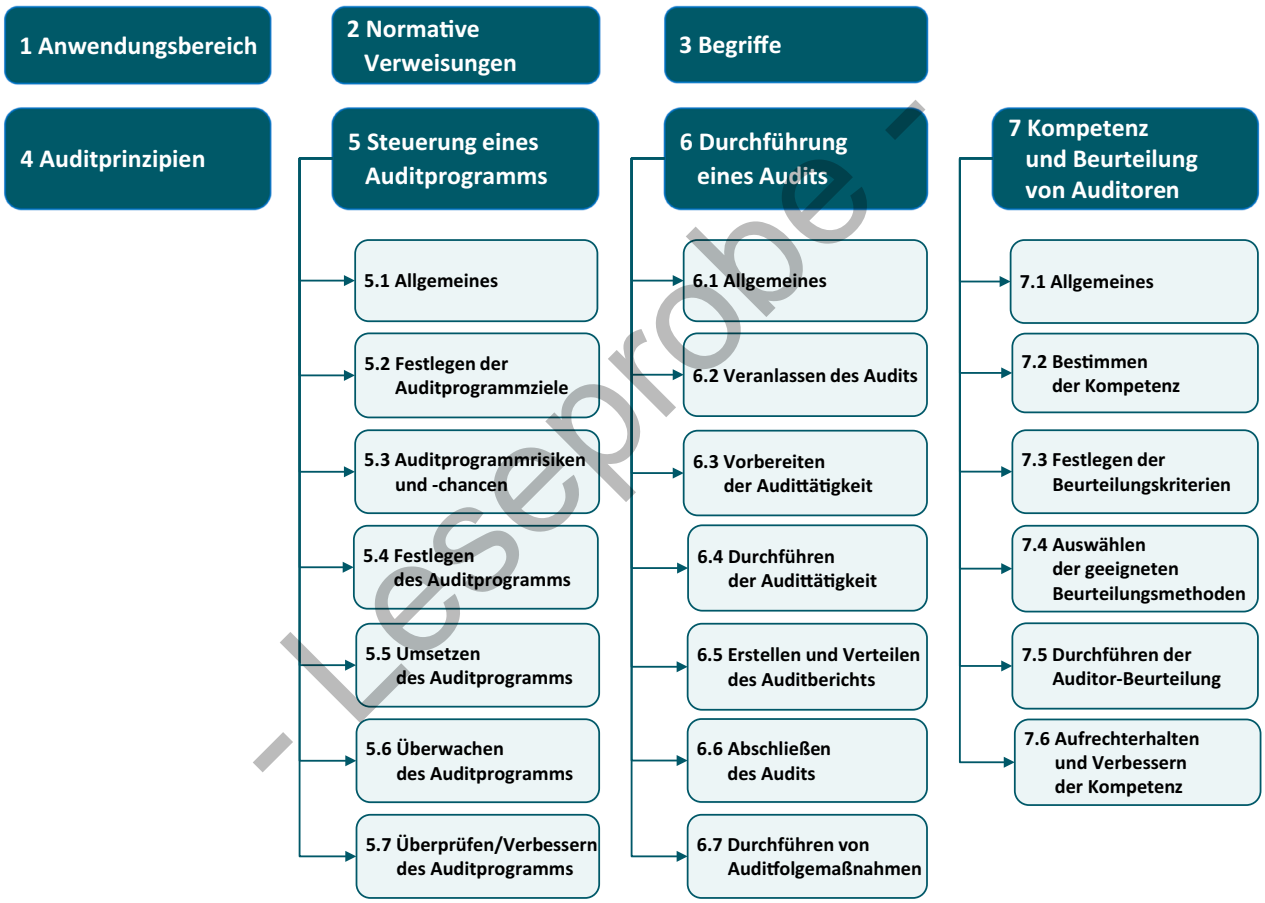


Abb. 1: Gliederung der ISO19011

Der Auditor

Das Normkapitel 4 „Auditprinzipien" beschreibt zum einen den Verhaltenskodex für den Auditor hinsichtlich der Qualität seiner Arbeit sowie die ethischen Anforderungen an seine Person und zum anderen die Grundlagen einer unabhängigen, dem Auditerfolg geschuldeten Auditdurchführung.

Auditplanung

Jede Tätigkeit, die von Erfolg gekrönt sein soll, setzt an ihren Anfang die Planung, als geistige Vorwegnahme zukünftigen Handelns, um Fehler zu vermeiden. Diesem Grundsatz folgt auch das Normkapitel 5 „Steuerung eines Auditprogramms". Zentrales Werkzeug der Planung eines Audits ist das Auditprogramm, das die Auditaktivitäten eines geplanten Zeitraums (z. B. ein Jahr) übersichtlich darstellt. Der zweite wesentliche Punkt im Normkapitel 5 ist die Analyse des Auditprozesses und des Auditprogramms mittels einer Chancen- und Risikobetrachtung, um deren Wirksamkeit abzusichern.

- Leseprobe -

Auditdurchführung

Für die direkte Auditdurchführung enthält das Normkapitel 6 „Durchführung eines Audits“ die Hilfestellung für den Auditor und Auditteamleiter, die diese benötigen, um ein einzelnes Audit vor Ort wirksam zu planen und durchzuführen. In den Geltungsbereich dieses Normkapitels fällt auch die Vorbereitung auf ein Audit mit der Erstellung der Auditfrageliste und deren Anwendung in der Auditkommunikation.

Auditorkompetenz

Das letzte Normkapitel der ISO 19011 beschäftigt sich mit der Kompetenz von Auditoren und wie man diese erreichen und erhalten kann. Denn das Vertrauen in den Auditprozess und die Güte der Auditergebnisse hängt in wesentlichem Maße von der Kompetenz und der Eignung der eingesetzten Auditoren ab.

Neben den Ausführungen in den Normkapiteln 4 bis 7 bietet die ISO 19011 im Anhang A noch weitere nützliche Informationen vertiefend zum Normkapitel 6 „Durchführung eines Audits“ an. Gerade für Auditoren, die am Anfang ihrer Tätigkeit stehen, sind die Ausführungen in den Unterkapiteln des Anhangs A sehr hilfreich.

Weitere Informationen

Umfassende Informationen zur Vertiefung des Themas interne Audits finden Sie in der Fachbroschüre „Audits erfolgreich vorbereiten und durchführen mit ISO 19011“ [5].

- Leseprobe -

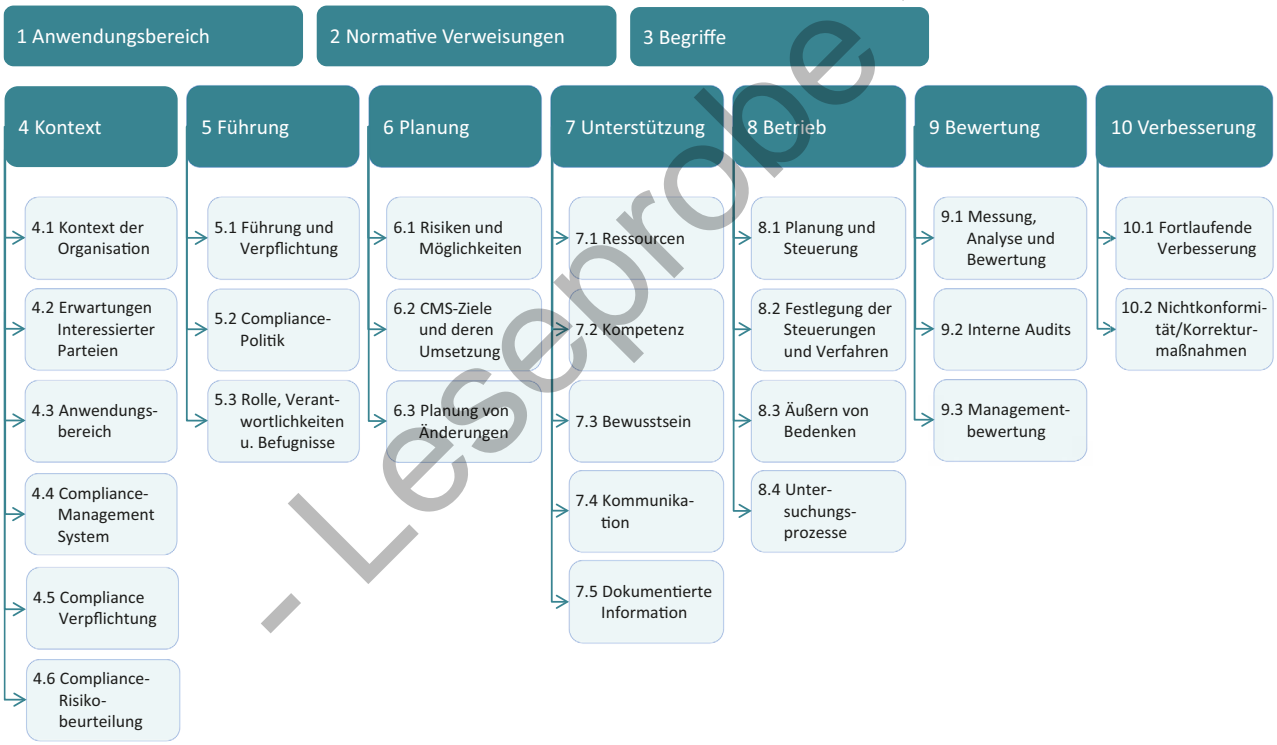
3 Struktur der ISO 37301

High Level Structure (HLS)

Die High Level Structure (HLS) wurde 2013 durch die ISO eingeführt, damit die Struktur von ISO-Managementsystemnormen, die Zertifizierungsgrundlage sind, einen einheitlichen Aufbau aufweist. Mit der Revision der ISO 9001 im Jahr 2015 wurde die HLS auch für diese weltweit am häufigsten als Zertifizierungsgrundlage dienende Norm eingeführt. Weitere ISO-Normen, die als Zertifizierungsgrundlage dienen, folgten heute dieser Struktur, so auch die ISO 37301.

Neben einer einheitlichen Kapitelstruktur gibt die ISO mit identischen Textbausteinen, gemeinsamen Begriffen und Definitionen auch eine Harmonisierung der Sprache vor, die – wo immer möglich – den Kern von neuen und überarbeiteten Managementsystemnormen bilden soll und somit die Klarheit in der Aussage der Forderungen verbessert. Die einheitliche Kapitelstruktur ist von großem Vorteil bei der Zusammenführung von mehreren Managementsystemen zu einem integrierten System (vgl. [6]).

Die Kapitelstruktur der ISO 37301 gibt Abbildung 2 wieder.



- Leseprobe -

Abb. 2: HLS-Struktur der ISO 37301

Risiken-Möglichkeiten-Bewertung

Das Normkapitel 4 und seine Unterkapitel bilden den Rahmen für das Compliance-Managementsystem (CMS). Im Normkapitel 5 sind die Aufgaben und die Verantwortung der Leitung für die Organisation und die Aufrechterhaltung sowie Wirksamkeit des CMS niedergelegt. Das Normkapitel 6 enthält den planerischen Ansatz des Managementsystems. Die Bewertung von Risiken und Möglichkeiten soll es ermöglichen, Vorbeugemaßnahmen gezielt zu ergreifen, um negative Auswirkungen auf die Organisation zu verhindern und positive Auswirkungen zur Verbesserung zu nutzen. Ebenso dient die verbindliche Festlegung von Zielen und ihrer Umsetzung der Verbesserung des CMS und seiner Prozesse. Das Normkapitel 7 enthält Regelungen zur Bereitstellung der notwendigen Ressourcen, Personen und Mittel, die in einem CMS als Erfolgsfaktor unabdingbar sind.

Umgang mit Fehlern

Das für das operative Geschäft einer Organisation wichtigste ist das Normkapitel 8. In ihm werden die Anforderungen an den Betrieb einer Organisation bezüglich der Planung und Steuerung der CMS-Prozesse und der dazu notwendigen Verfahren, bis zum Umgang mit geäußerten Bedenken und den dazu notwendigen Untersuchungsprozessen, vorgestellt. Zur Überwachung und Steuerung benötigen ein Managementsystem und seine Prozesse bestimmte Instrumente. Das Normkapitel 9 stellt diese Instrumente zur Verfügung. Da Fehler (inkl. Non-Compliance) und deren Folgen nie ganz auszuschließen sind, werden in Normkapitel 10 Forderungen zu Korrekturmaßnahmen von Fehlern aufgestellt. Neben Anleitungen zur Beseitigung von Fehlern enthält dieses Kapitel aber auch die Forderung nach Instrumenten zur fortlaufenden Verbesserung.

- Leseprobe -

Besonderheiten und Verbindungen

4 Auditierung des CMS in Verbindung mit anderen Managementsystemen

Vielfältige juristische Verantwortlichkeiten

In der heutigen globalisierten Welt sind viele Unternehmen in weltweite Handels- und Lieferketten eingebunden. Dabei ist nicht zu übersehen, dass solche Wirtschaftsaktivitäten auch vielfältige juristische Verantwortlichkeiten mit sich bringen. Unternehmen, egal ob sie Produkte oder Dienstleistungen anbieten, unterliegen einer Vielzahl von Rechtsanforderungen. Diese betreffen die Organisation (Organisationshaftung) als solche, die Prozesse der Produktion/ Dienstleistungserbringung (Produzentenhaftung) sowie die Produkte/Dienstleistungen in der Nutzung selbst (Produkthaftung).

Compliance gehört in den seltensten Fällen zu den Kernkompetenzen eines Unternehmens, mit denen es Geld verdienen will (eine Ausnahme bilden Rechtsanwaltskanzleien). Auf der anderen Seite erwarten interessierte Parteien, dass die Unternehmen rechtskonform arbeiten. Das ist eine Basisanforderung, die erfüllt sein muss. Wer möchte schon gerne Geschäfte mit der Mafia machen. Außerdem kann Non-Compliance auch ganz schön ins Geld gehen. Diese Erfahrung haben einige deutsche Automobilhersteller in den USA jüngst gemacht (Stichwort Dieselgate).

Managementsysteme und Rechtsgebiete

Die bisherigen ISO-Normen haben das Thema Compliance nur punktuell im Hinblick auf ihre spezifischen Bedürfnisse aufgegriffen. Tabelle 2 gibt für eine Auswahl wesentlicher ISO-Normen eine Übersicht über die damit verbundenen Rechtsgebiete.

Tabelle 2: Zuordnung von Managementsystemen zu Rechtsgebieten

Managementsystem	Rechtsgebiete
Qualitätsmanagement (ISO 9001)	Produkt- und Produzentenrecht
Umweltmanagement (ISO 14001)	Umwelt- und Gefahrenabwehrrecht
Management für Sicherheit und Gesundheit bei der Arbeit (ISO 45001)	Arbeits- und Sozialrecht, Gefahrstoff- und Gefahrgutrecht
Energiemanagement (ISO 50001)	Energieerzeugungs-, -verteilungs- und -nutzungsrecht

Leseprobe

Die aufgeführten Rechtsgebiete decken aber nur einen kleinen Bereich der Rechtsvorschriften ab, die ein Unternehmen bei seinem Handeln berücksichtigen muss, häufig neben deutschen auch Rechtsvorschriften von Ländern, in denen das Unternehmen geschäftlich tätig wird. Die Rechtsordnungen anderer Länder weichen häufig vom deutschen Recht ab (z. B. angelsächsisches Recht), was die Einhaltung solcher Rechtsvorschriften nicht vereinfacht.

Alle Unternehmensbereiche betroffen

Compliancefragen betreffen nicht nur einige, sondern fast alle Bereiche eines Unternehmens, es gibt da kaum Ausnahmen. Die Fertigung unterliegt u. a. dem Umwelt-, Sicherheits- und Energierecht, das Personalwesen dem Arbeits- und Sozialrecht, die Buchhaltung dem Steuer- und Gesellschaftsrecht, der Vertrieb dem Wirtschafts- und Korruptionsrecht und einigem mehr. Compliance-Management erfüllt normativ gesehen eine Querschnittsfunktion für das gesamte Unternehmen. Das ist vergleichbar mit anderen Forderungen wie Lenkung dokumentierter Information, internen Audits oder Ressourcenmanagement.

Für das Audit bedeutet dies, dass für die Umsetzung der Complianceanforderungen im gesamten Unternehmen alle Abteilungen zu auditieren sind. Der Umfang, in dem Compliancekonformität geprüft werden muss, richtet sich nach der Relevanz von Rechtsvorschriften für den Betriebsbereich. In der Praxis sind häufig die Kernprozesse am stärksten von rechtlichen Anforderungen betroffen, wenn man berücksichtigt, dass nationale und internationale Normen unter die Complianceregeln fallen (z. B. Ausführungsnormen nach DIN hinsichtlich technischer Ausführungen oder harmonisierte Normen der EU).

Integriertes Managementsystem

Ein Compliance-Managementsystem nach ISO 37301 ist in der Regel gemeinsam mit anderen Managementsystemen eingebunden in ein integriertes Managementsystem. Häufig finden sich in dieser Kombination ISO 9001 (Qualität), ISO 14001 (Umwelt) und/oder ISO 45001 (Arbeits- und Gesundheitsschutz). Dank der High Level Structure der ISO ist die Kapitelstruktur der ISO-Normen vergleichbar aufgebaut, sodass sich vergleichbare Anforderungsinhalte schnell identifizieren lassen. Im Sinne einer integrierten Auditierung ist es wichtig, die Inhalte zu identifizieren, die sich wegen ähnlicher Anforderungen gemeinsam auditieren lassen, und die Inhalte, die nur für das einzelne Managementsystem, hier ISO 37301, von Relevanz sind. In Bild 3 sind die Normenkapitel der ISO 37301 wiedergegeben, die keine inhaltliche Entsprechung in den anderen Normen des oben genannten IMS haben.

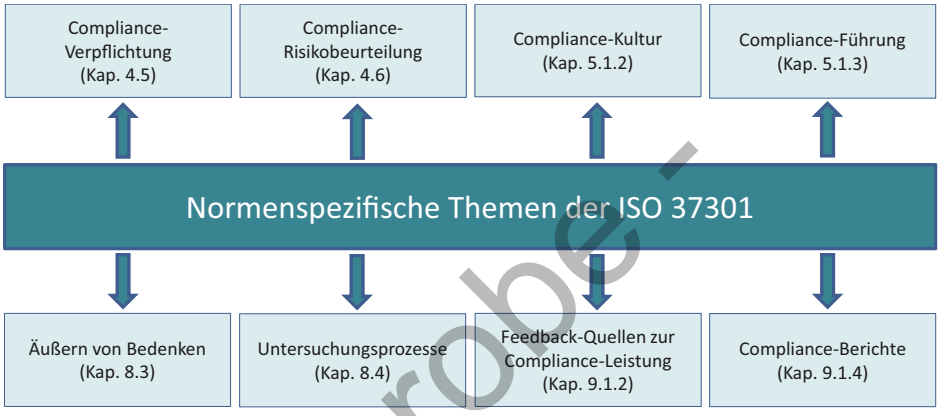


Abb. 3: Spezifische Themen für ein Compliance-Managementsystem

Spezifische Compliancethemen

Im Gegensatz zur ISO 9001 und anderen gängigen ISO-Normen hat das CMS zwei zusätzliche, sehr wichtige Unterkapitel des Normkapitels 4 „Kontext der Organisation". Im Normkapitel 4.5 wird die Forderung nach der Analyse aller Complianceverpflichtungen der Organisation gestellt. Hinsichtlich spezifischer Rechtsgebiete wird eine vergleichbare Forderung in der ISO 14001 und 45001 im Normkapitel 6.1.3 „Bindende Verpflichtung" (ISO 14001) und „Bestimmung rechtlicher Verpflichtung und anderer Anforderungen" (ISO 45001) gestellt. In beiden Fällen geht es aber nur um eine Teilmenge an Rechtsgebieten, denen ein Unternehmen unterliegt (Umweltschutz- sowie Arbeitsschutzrecht). Im Normkapitel 4.6 ist die Bewertung der Compliancerisiken hinsichtlich ihrer Bedeutung für die Organisation gefordert. Diese Forderung umfasst die Einstufung der Gesetze gemäß ihrer Relevanz für das Unternehmen und gilt in der Form nur für die ISO 37301.

Führung

Im Normkapitel 5 „Führung" wird im Unterkapitel 5.1.2 eine Compliancekultur gefordert, die auf allen Ebenen der Organisation wirksam ist. Verantwortlich dafür sind das oberste Organ und die oberste Leitung. Diese Unterscheidung in eine zweistufige Führungshierarchie wird in anderen ISO-Normen nicht gemacht. Im Hinblick auf die Konzernstruktur vieler Unternehmen sind Auswirkungen von größeren Non-Compliance-Vorfällen der Tochtergesellschaft auf den Konzern nicht auszuschließen. Das Compliance-Managementsystem muss also die gesamte Organisation umfassen. Daneben müssen oberstes Organ und oberste Leitung im Speziellen die Compliancefführung (Normkapitel 5.1.3) für das CMS übernehmen, indem sie eine wirksame unabhängige Complianceorganisation für das Gesamtunternehmen implementieren (z. B. Ernennung eines Complianceofficers und anderer Compliancefunktionen).

Whistleblower

Von besonderer Bedeutung für das CMS ist auch das Unterkapitel 8.3 „Äußern von Bedenken" in Normkapitel 8 „Betrieb". Darin geht es um den Umgang mit internen wie externen Informationen, die auf potenzielle Compliancever-

- Leseprobe -