

**Interpretation der Anforderungen**  
**1. Auflage**

Die ISO 37301:2021

-Leseprobe-

Herausgegeben von TÜV Rheinland Cert GmbH, Köln, TÜV Rheinland Group

**Autoren:**

Walter Schlegel  
TÜV Rheinland Cert GmbH  
Dipl.-Ing. Techn. Betriebswirt  
Graduate Engineer, Business Economist,  
Product Manager Compliance  
[walter.schlegel@de.tuv.com](mailto:walter.schlegel@de.tuv.com)

Stefan Pawils  
SAT GmbH & Co KG  
Geschäftsführer/Managing Partner  
Compliance Officer (TÜV Rheinland)  
Auditor für Compliance-Management-Systeme im Auftrag des TÜV Rheinland  
IRCA-ISMS-Auditor nach ISO/IEC 27001  
[s.pawils@sat-team.org](mailto:s.pawils@sat-team.org)

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 978-3-7406-0642-8 (Print)

ISBN 978-3-7406-0643-5 (E-Book)

© by TÜV Media GmbH, TÜV Rheinland Group, 1. Auflage, Köln 2021  
[www.tuev-media.de](http://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. Gleichermaßen 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.

## Über die Broschüre

Diese Broschüre richtet sich an Compliance-Beauftragte/Officer, Compliance-Auditoren, Unternehmen, Organisationen und Berater sowie an alle, die am Aufbau und an der Pflege eines Compliance-Management-Systems (CMS) beteiligt sind.

Sie interpretiert und erläutert die Anforderungen der ISO 37301. Ziel der Broschüre ist es, das Verständnis für die Normenforderungen zu erhöhen und anhand zahlreicher Praxisbeispiele sinnvolle Anregungen für ihre unmittelbare Umsetzung zu geben.

Im Teil A der Broschüre erhält der Leser eine Einführung in Zielsetzung, Struktur und die wichtigsten Merkmale der ISO 37301.

Im Teil B, werden die Anforderungen der Norm in Tabellenform stichwortartig aufgelistet und praxisorientiert interpretiert. Mit Hinweisen zur Umsetzung soll dem Leser veranschaulicht werden, in welcher Form Anforderungen erfüllt werden können. Diese Beispiele sind auch dazu geeignet, den Nachweis der Umsetzung zu dokumentieren.

Die dabei in der letzten Spalte der Tabelle angeführten Kennzahlen spiegeln die Möglichkeiten von Beispielen wider, die zur Messbarkeit und Steuerung von Compliance-Prozessen herangezogen werden können, um die Wirksamkeit des CMS ständig zu verbessern.

Die im Text angeführten Klammersymbole verweisen auf die Arbeitshilfe, die Sie bei der Durchführung einer Audit- und Selbstbewertung unterstützen soll.

Diese ist in der Anlage des E-Books enthalten und steht auch zum Download bereit unter:

[www.tuev-media.de/download/60642.php](http://www.tuev-media.de/download/60642.php)

Passwort: [REDACTED]

## Audithilfe

Das umfangreiche Word-Dokument ermöglicht Ihnen die Prüfung nach der ISO 37301. Es enthält die vollständige Tabelle aus Teil B.

Sie können das Dokument frei bearbeiten und durch Hinzufügen oder Löschen von Spalten und Zeilen an die jeweilige Situation in Ihrer Organisation anpassen. Es sind die Anforderungen der Norm in Tabellenform stichwortartig aufgelistet und praxisorientiert interpretiert. Mit Hinweisen zur Umsetzung soll dem Leser veranschaulicht werden, in welcher Form Anforderungen erfüllt werden können. Diese Beispiele sind auch dazu geeignet, den Nachweis der Umsetzung zu dokumentieren.

Die angegebenen Kennzahlen spiegeln die Möglichkeiten von Beispielen wider, die zur Messbarkeit und Steuerung von Compliance-Prozessen herangezogen werden können, um die Wirksamkeit des CMS ständig zu verbessern. Die Tabelle ist ergänzt um eine Spalte „Auditnotiz“. So können Sie das Dokument auch als Grundlage für eine Audit- und Selbstbewertung nutzen.

Für Sie als ...

Zielsetzung

Teil A

Teil B

Kennzahlen

Arbeitshilfe  
zum Download

   
Audithilfe.docx

**Inhalt**

<b>Über die Broschüre .....</b>	3
<b>Teil A ISO 37301:2021 – eine Einführung.....</b>	7
1 Allgemeines.....	7
1.1 Ziel der Norm .....	7
1.2 Grundsätze des Compliance-Managementsystems .....	7
1.3 Struktur der Norm.....	9
1.4 Bedeutung des Standards für Unternehmen und andere Organisationen.....	10
2 Wichtige Aspekte zur wirksamen Umsetzung des CMS.....	11
3 Nachhaltiger Erfolg durch Einbindung bereits vorhandener Managementsysteme.....	12
4 Belastbare Nachweisführung.....	13
<b>Teil B Interpretation der Anforderungen der ISO 37301 .....</b>	15
5 Erläuterungen zu den Tabellen .....	15
5.1 Normanforderungen ISO 37301:2021.....	15
5.2 Interpretation/Aktivitäten .....	15
5.3 Dokumentationsbeispiele/Nachweise .....	15
5.4 Beispiele für messbare Indikatoren (Kennzahlen).....	15
Normkapitel 4: Kontext der Organisation.....	17
Normkapitel 5: Führung .....	20
Normkapitel 6: Planung .....	23
Normkapitel 7: Unterstützung .....	24
Normkapitel 8: Betrieb .....	29
Normkapitel 9: Bewertung der Leistung.....	31
Normkapitel 10: Verbesserung.....	35

## Teil A ISO 37301:2021 – eine Einführung

### 1 Allgemeines

#### 1.1 Ziel der Norm

Die ISO 37301 erläutert die Grundsätze eines Compliance-Managementsystems (CMS) in einem Anforderungskatalog, der sowohl zum Aufbau eines CMS als auch zu dessen Zertifizierung herangezogen werden kann.

Indem die ISO 37301 sagt, dass die Einführung eines CMS eine strategische Entscheidung der Organisation sein sollte, richtet sie sich zuallererst an die Leitung einer Organisation, also in der Regel an die Geschäftsführung. Sie unterstützt die oberste Leitung bei der Führung der Organisation, um die spezifischen Ziele der Organisation zu erreichen.

Sie setzt damit voraus, dass das CMS ein integraler Bestandteil des Führungssystems ist. Mithilfe dieses Führungssystems hat die oberste Leitung eine Möglichkeit, die Compliance-Anforderungen zu steuern und zu erfüllen.

Zertifizierbarer Standard

Unterstützung der Führung

Compliance steuern und erfüllen

Schaffung einer Compliance-Kultur

Prinzipien

Organisationsprozess für gesetzliche und regulatorische Vorgaben

Grundsätze

Compliance-Kultur

Führung

#### 1.2 Grundsätze des Compliance-Managementsystems

Die Kernaufgabe eines CMS ist die Schaffung und Erhaltung einer nachhaltigen Compliance-Kultur. Ferner beweckt ein CMS, hinreichend sicherzustellen, dass Compliance-Risiken für wesentliche Regelverstöße rechtzeitig erkannt und dass diese verhindert werden.

Folgende Prinzipien bilden dabei die Säulen eines CMS:

- Integrität
- gute Führung
- Verhältnismäßigkeit
- Transparenz
- Rechtschaffenheit
- Nachhaltigkeit

Zur Sicherstellung der originären Geschäftsziele müssen alle Organisationen unabhängig von der Branche, der Größe, ob im Inland oder auch im Ausland ansässig, den jeweiligen gesetzlichen und regulatorischen Vorgaben nachkommen. Dies regelt sich nicht von selbst, sondern bedarf gewisser organisatorischer Vorgaben und Maßnahmen, die in den einzelnen Organisationsprozessen umzusetzen sind. Die ISO 37301 beschreibt in ihren einzelnen Kapiteln, welche Vorgaben erforderlich sind, um ein transparentes und effektives CMS zu erfüllen. Dabei soll die Angemessenheit für die jeweilige Organisation berücksichtigt werden.

Im Folgenden sind die Grundsätze zusammengefasst, die sich aus den Vorgaben der ISO 37301 ergeben:

1. Die Compliance-Kultur stellt die wesentliche Grundlage für jede Organisation dar. Dies bedeutet, dass die Führung, durch aktives Vorleben erst die Voraussetzungen für das Annehmen, die Beachtung und das Umsetzen der Compliance-Vorgaben durch die Mitarbeiter oder sonstigen Organisationsangehörigen schafft.
2. Die Führungskräfte haben eine Vorbildfunktion und müssen sich zur Einhaltung gesetzlicher, regulatorischer und ggf. auch eigener ethischer Vorgaben verpflichten und dies durch entsprechendes Verhalten vorleben. Genauso strikt müssen sie dies auch von ihren Mitarbeitern oder sonstigen Organisationsangehörigen einfordern.

<b>Einbeziehung der Mitarbeiter</b>	3. Auf allen Ebenen werden Mitarbeiter im täglichen Arbeitsleben mit gesetzlichen Anforderungen direkt oder indirekt konfrontiert. Oftmals ist es dem Einzelnen nicht immer bewusst, dass seine Tätigkeit gesetzlichen Vorgaben genügen muss. Diesbezüglich ist eine Sensibilisierung der Mitarbeiter erforderlich. Sie sind es, die zum überwiegenden Teil die gesetzlichen Vorgaben im Unternehmen oder in Organisationen berücksichtigen und umsetzen bzw. einhalten müssen.
<b>Administration durch den Compliance-Beauftragten</b>	4. Jedes funktionierende Compliance-System bedarf eines gewissen administrativen Aufwands, damit wesentliche überwachende Aufgaben, steuernde Aktivitäten sowie Auswertungs- und Berichterstattungstätigkeiten vollzogen werden. Dies geschieht nicht von selbst; daher ist eine Stelle erforderlich, die diese Funktionen und Aufgaben wahrnimmt, der Compliance-Beauftragte.
<b>Compliance-Risikoanalyse</b>	5. Ohne eine Standortbestimmung durch eine Risikoanalyse wird es jeder Organisation schwerfallen, die richtigen Entscheidungen zu treffen. Dies gilt umso mehr, wenn es um Gesetzeskonformität geht. Die Organisation muss sich einen Überblick über ihr organisatorisches Umfeld (Rechtsform der Gesellschaft bzw. Organisation, Produkte, Dienstleistungserbringung bzw. sonstige Aufgabenerfüllung, nationales oder internationales Agieren etc.) verschaffen, um die sich daraus ergebenden Compliance-Risiken richtig zu bewerten. Nur wenn man sich dieser Risiken bewusst ist, kann man ihnen entsprechende Vorkehrungen zu ihrer Vermeidung bzw. Minderung treffen. Diese Vorkehrungen müssen dann in die entsprechenden Prozesse und Arbeitsabläufe integriert werden.
<b>Systemorientierter Managementansatz</b>	6. Ermitteln, Verstehen, Leiten und Lenken von miteinander in Wechselbeziehung stehenden Prozessen als Systemansatz tragen zur Wirksamkeit und Effizienz ihrer Compliance-Ziele bei. Compliance sollte kein Zufallsprodukt, sondern das Ergebnis von klaren Vorgaben und deren Umsetzung sein. Nur ein systematischer Ansatz, z. B. dem Deming-Kreis folgend, der Transparenz der Vorgaben und der Nachweise garantiert, ist belastbar und kann zur Entlastung der Organisation und der Führung herangezogen werden.
<b>Überwachung, Analyse und Verbesserung</b>	7. Systemüberwachung, -analyse und -verbesserung mit folgenden Elementen: <ul style="list-style-type: none"> <li>– Die ständige Verbesserung der Gesamtleistung der Organisation ist ein permanentes Ziel der Organisation. Dazu wird das Compliance-Managementsystem durch verschiedenste Maßnahmen, z. B. durch</li> <li>– interne Compliance-Audits,</li> <li>– Tests der internen Kontrollen (gesetzte Maßnahmen oder Einrichtung zur Erkennung von Compliance-Verstößen) oder</li> <li>– Überwachung durch externe Prüfer/Prüfstellen,</li> <li>– analysiert.</li> <li>– Diese Analyse aller verwertbaren Informationen sollte dann zur Verbesserung des Compliance-Managementsystems genutzt werden. Letztlich sollte jede Organisation das Ziel anstreben, Compliance-Verstöße zu verhindern und durch entsprechende Maßnahmen einen Schaden für die Organisation oder die Gesellschaft so gering wie möglich zu halten.</li> </ul>
<b>Langfristiger Erfolg</b>	Organisationen, die langfristig erfolgreich sein möchten, müssen eine Kultur der Integrität und Compliance in Anbetracht der Bedürfnisse und Erwartungen interessierter Parteien einführen und aufrechterhalten. Integrität und Compliance sind daher nicht nur die Grundlage, sondern auch eine Möglichkeit für eine erfolgreiche und nachhaltige Organisation.

Alle in der ISO 37301 festgelegten Anforderungen sind allgemeiner Natur (generisch) und auf alle Organisationen einschließlich öffentlicher Einrichtungen anwendbar, unabhängig von ihrer Art und Größe, der regionalen Ansässigkeit und der Art der bereitgestellten Produkte oder Dienstleistungen.

Die Abbildung 1 veranschaulicht zudem die Ziele, die Prinzipien, den PDCA-Zyklus und das Organisationsumfeld der Norm im Überblick.

**Generischer Ansatz**

**Ziele, Prinzipien, PDCA und Umfeld**

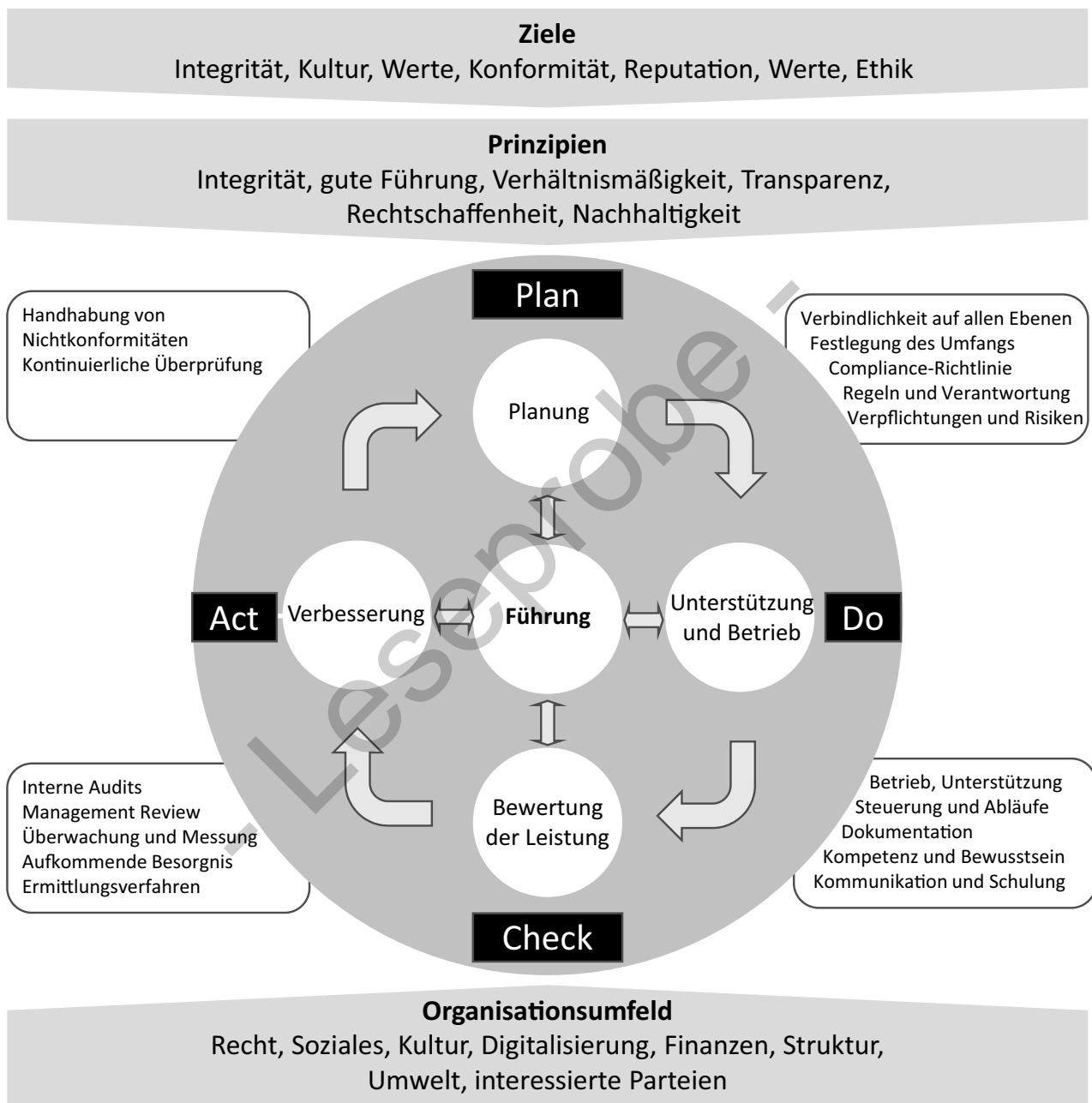


Abb. 1: Ziele, Prinzipien, PDCA-Zyklus und Organisationsumfeld

### 1.3 Struktur der Norm

Die Norm gliedert sich in zehn Kapitel (s. Abbildung 2), von denen die ersten drei – wie in ISO-Normen üblich – die Kapitel zum Anwendungsbereich, zu normativen Verweisen und zu Begriffen sind. Die darauffolgenden Normkapitel 4 bis 10 sind nach dem Plan-Do-Check-Act(PDCA)-Zyklus strukturiert. Damit folgt die Norm dem Muster der von der ISO festgelegten High Level

**10 Kapitel nach High Level Structure**

Structure (HLS), der standardisierten Grundstruktur für Managementsystem-normen.

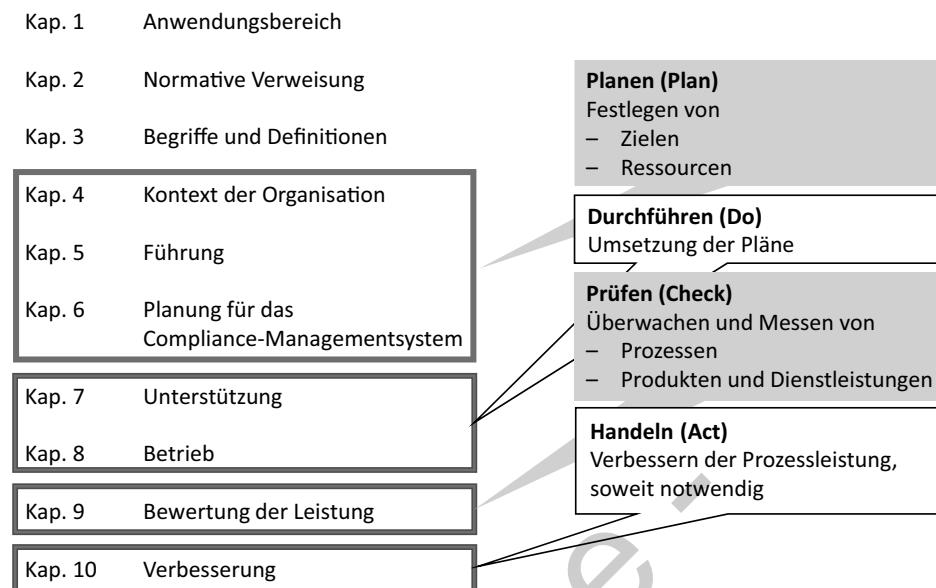


Abb. 2: Gliederung und Gliederungsstruktur der ISO 37301

#### 1.4 Bedeutung des Standards für Unternehmen und andere Organisationen

**Systematischer Nachweis mitunter überlebenswichtig**

Erstellung, Einführung und Umsetzung eines Compliance-Managementsystems werden als eine präventive strategische Entscheidung einer Organisation verstanden. Dazu ist es wichtig, einen systematischen Nachweis eines gelebten Managementsystems, das zur Rechtskonformität der Organisation, seiner Aufsichtsorgane und Mitarbeiter beiträgt, führen zu können. Es ist sicherzustellen, dass bei einem Regelverstoß kein organisatorisches bzw. Managementverschulden vorliegt. Mithilfe der ISO 37301 wird daher das unternehmerische Risiko verringert. Da sich die regulatorischen Anforderungen auch in Anbetracht einer stetig fortschreitenden Globalisierung ändern und oftmals nicht nur nationale Gesetze greifen, ist es für Organisationen überlebenswichtig, mithilfe eines CMS den Anforderungen gerecht zu werden. Bei einigen Regelverstößen können die daraus folgenden Sanktionen unter Umständen die Existenz bzw. den Fortbestand der Organisation gefährden.

**Frei in der Ausgestaltung**

Organisationen können sich nach ihren organisatorischen Belangen und ihrem Umfeld ausrichten und sind frei in der Gestaltung ihres CMS. Die ISO 37301 gibt keine Vereinheitlichung von organisatorischen Strukturen, Prozessen oder Dokumentationen in den Organisationen vor. Sie leistet Hilfestellung und gibt Orientierung für den systematischen Umgang mit einem CMS.

## Teil B Interpretation der Anforderungen der ISO 37301

### 5 Erläuterungen zu den Tabellen

Um den Anwender des Standards bei der Umsetzung der Anforderungen in der Praxis und bei der Vorbereitung und Durchführung interner Audits zu unterstützen, werden in der folgenden Tabelle die einzelnen Normenforderungen interpretiert und durch nützliche Informationen ergänzt. Dabei wird ein durchgängiges Spaltenschema angewendet:

Normenforderungen ISO 37301:2021	Interpretation/Aktivitäten	Dokumentationsbeispiele/Nachweise	Beispiele für Indikatoren (Kennzahlen)
----------------------------------	----------------------------	-----------------------------------	--

#### 5.1 Normenforderungen ISO 37301:2021

Die Anforderungen werden stichwortartig und nicht im Wortlaut aufgeführt. Das erleichtert die Arbeit in der Praxis, ersetzt allerdings nicht die Kenntnis des Originaltextes der Norm.

#### 5.2 Interpretation/Aktivitäten

In dieser Spalte wird erläutert, was unter der Anforderung zu verstehen ist bzw. welche Aktivitäten beispielsweise zur Umsetzung der Anforderung in der Praxis zu ergreifen sind.

#### 5.3 Dokumentationsbeispiele/Nachweise

Diese Spalte enthält Beispiele für Nachweisdokumente, die die Erfüllung der Normenforderungen nachvollziehbar dokumentieren.

#### 5.4 Beispiele für messbare Indikatoren (Kennzahlen)

In dieser Spalte sind praxisnahe Beispiele für messbare Indikatoren aufgelistet. Diese Beispiele sind Orientierungshilfen, die keinen Anspruch auf Vollständigkeit erheben.

#### Arbeitshilfe

Die vollständige Tabelle ist auch als Word-Dokument beigefügt. Die Word-Tabelle ist dabei ergänzt um eine Spalte „Auditnotiz“. So können Sie das Dokument auch als Grundlage für eine Audit- und Selbstbewertung nutzen.

Die Arbeitshilfe ist in der Anlage des E-Books enthalten und steht auch zum Download bereit unter:

[www.tuev-media.de/download/60642.php](http://www.tuev-media.de/download/60642.php)

Passwort: [REDACTED]

Hilfe zur Vorbereitung und Durchführung interner Audits

#### Spaltenschema

##### 1. Spalte

##### 2. Spalte

##### 3. Spalte

##### 4. Spalte

Office  
Audithilfe.docx

#### Download

## Normkapitel 4: Kontext der Organisation

Normanforderung ISO 37301:2021	Interpretation/ Aktivitäten	Dokumentationsbeispiele/ Nachweise	Beispiele für Indikatoren
<b>4.1 Verständnis der Organisation und ihres Kontexts</b>			
<ul style="list-style-type: none"> <li>Unternehmens-Compliance-Umfeldanalyse</li> <li>Strategische Ausrichtung</li> </ul>	<ul style="list-style-type: none"> <li>Identifikation der relevanten Compliance-Themenbereiche</li> <li>Analyse der identifizierten Compliance-Themenbereiche</li> </ul>	<ul style="list-style-type: none"> <li>Rechtskataster</li> <li>Genehmigungskataster für genehmigungspflichtige Anlagen</li> <li>Liste der identifizierten internen und externen Compliance-Themenbereiche</li> <li>Übersicht zum Beauftragtenwesen</li> <li>Bericht zur Compliance-Analyse/Bewertung</li> </ul>	
<b>4.2 Verständnis der Erfordernisse und Erwartungen interessierter Parteien</b>			
<ul style="list-style-type: none"> <li>Identifizierung der relevanten interessierten Parteien</li> <li>Anforderungen der interessierten Parteien an das CMS</li> </ul>	<ul style="list-style-type: none"> <li>Identifikation der relevanten Compliance-Themenbereiche und interessierter Parteien</li> <li>Analyse der identifizierten Compliance-Themenbereiche und interessierter Parteien</li> </ul>	<ul style="list-style-type: none"> <li>Rechtskataster</li> <li>Genehmigungskataster für genehmigungspflichtige Anlagen</li> <li>Übersicht zum Beauftragtenwesen</li> <li>Liste der identifizierten Compliance-Themenbereiche und interessierten Parteien (Kunden, Shareholder, Öffentlichkeit, Verbände, Mitarbeiter, Behörden etc.)</li> <li>Bericht zur Compliance-Analyse/Bewertung</li> </ul>	
<b>4.3 Festlegung des Anwendungsbereichs des Compliance-Managementsystems</b>			
<ul style="list-style-type: none"> <li>Festlegung des CMS-Anwendungsbereichs</li> </ul>	<p>Zu berücksichtigen sind:</p> <ul style="list-style-type: none"> <li>Größe und Struktur der Organisation, Art ihrer Tätigkeit</li> <li>Regionen, in denen die Organisation tätig ist,</li> <li>bereitgestellte Produkte, angewendete Prozesse,</li> <li>Umfeld, sich verändernde Erfordernisse,</li> <li>spezifische Risiken der Organisation und</li> <li>besondere Ziele der Organisation.</li> <li>Identifikation der relevanten Compliance-Themenbereiche</li> <li>Analyse der identifizierten Compliance-Themenbereiche</li> <li>Bewertung der identifizierten Compliance-Themen</li> </ul>	<ul style="list-style-type: none"> <li>CMS-Handbuch</li> <li>Compliance-Richtlinie oder sonstige Vorgabedokumente, die das CMS und den Anwendungsbereich beschreiben</li> </ul>	

Normanforderung ISO 37301:2021	Interpretation/ Aktivitäten	Dokumentationsbeispiele/ Nachweise	Beispiele für Indikatoren
<b>4.4 Compliance-Managementsystem</b>			
<ul style="list-style-type: none"> <li>• Prozessidentifikation</li> <li>• Prozessabfolge und Wechselwirkungen</li> <li>• Prozesslenkung</li> <li>• Prozessressourcen</li> <li>• Prozessüberwachung</li> <li>• Prozessakzeptanz</li> <li>• Prozessverbesserung</li> </ul>	<p>Aufbau, Verwirklichung, Aufrechterhaltung und Verbesserung einer regelkonform orientierten Organisation durch</p> <ul style="list-style-type: none"> <li>• direkten Zugang der Compliance-Funktion zu den Führungsgremien (Vorstand, Geschäftsführung, Aufsichtsrat etc.)</li> <li>• Unabhängigkeit der Compliance-Funktion (Stabsstelle, keine Linienfunktion)</li> <li>• angemessene Ausstattung der Compliance-Funktion mit Kompetenzen und Ressourcen</li> <li>• Definition, Festlegung und Darstellung von angemessenen und verständlichen Prozessen, ihrer Abfolge und Wechselwirkung</li> <li>• Festlegung von Wirksamkeitskriterien</li> <li>• Einbeziehung von Art, Umfang und Lenkung ausgelieterter Prozesse</li> </ul> <p>mit dem Ziel der Verbesserung des Compliance-Managementsystems</p>	<ul style="list-style-type: none"> <li>• CMS-Handbuch/CMS-Leitlinie/Compliance-Richtlinien</li> <li>• Corporate Governance</li> <li>• Stellen- und Funktionsbeschreibungen</li> <li>• Rechtskataster</li> <li>• Genehmigungskataster</li> <li>• Prozesse/Verfahrensanweisungen und andere mitgetragende Dokumente</li> <li>• Prozessablaufpläne</li> <li>• Managementreview</li> <li>• Maßnahmenpläne</li> <li>• Organigramme</li> <li>• Selbstbewertungen</li> <li>• Analysepläne</li> <li>• Prüfpläne/Prüfberichte</li> <li>• Schulungsunterlagen und Nachweise</li> </ul>	<ul style="list-style-type: none"> <li>• Überarbeitungsfrequenz der CMS-Dokumentation</li> </ul>
<b>4.5 Compliance-Verpflichtungen</b>			
<ul style="list-style-type: none"> <li>• Gesetze/behördliche Anforderungen und Verpflichtungen identifizieren</li> <li>• Compliance-Anforderungen analysieren und identifizieren</li> <li>• Auswirkungen der Compliance-Anforderungen auf die eigene Organisation feststellen</li> <li>• Bereitstellung und Kommunikation der aktuellen und gültigen Compliance-Anforderungen</li> </ul>	<ul style="list-style-type: none"> <li>• Kenntnis aller relevanten Compliance- Anforderungen und Verpflichtungen <ul style="list-style-type: none"> <li>– Gesetze und Verordnungen</li> <li>– Regeln oder Leitlinien von Regulierungsbehörden</li> <li>– Urteile von Gerichten oder Verwaltungsgerichten</li> <li>– Abkommen mit Kommunen</li> <li>– Verträge mit Behörden und Kunden</li> <li>– Organisationsanforderungen wie Richtlinien und Verfahren</li> <li>– Freiwillige Grundsätze oder Verhaltenskodizes, Umweltverpflichtungen</li> <li>– Industriestandards</li> </ul> </li> <li>• Verbreitung der Compliance- Anforderungen bei den betroffenen Stellen und Mitarbeitern</li> <li>• Erstellung einer Übersichtsliste der relevanten Compliance- Anforderungen</li> <li>• Compliance- Anforderungen liegen als gelenkte Dokumente vor</li> </ul>	<ul style="list-style-type: none"> <li>• Prozess-/Verfahrensbeschreibung</li> <li>• Rechtskataster</li> <li>• Genehmigungskataster</li> <li>• Liste der gesetzlich vorgeschriebenen Beauftragten</li> <li>• Liste der Adressaten für Compliance-Anforderungen</li> <li>• Compliance-Liste/Bericht zu den Auswirkungen für die Organisation</li> <li>• Aktualisierungsprotokolle</li> </ul>	<ul style="list-style-type: none"> <li>• Zahl der regulativen Änderungen</li> <li>• Zahl der dadurch bedingten Maßnahmen</li> <li>• Ressourcenaufwand</li> </ul>

Normanforderung ISO 37301:2021	Interpretation/ Aktivitäten	Dokumentationsbeispiele/ Nachweise	Beispiele für Indikatoren
<b>4.6 Compliance-Risikobewertung</b>			
<ul style="list-style-type: none"> <li>• Compliance-Umfeld-analyse aufgrund neuer oder geänderter Unternehmensaktivitäten</li> <li>• Identifizierung und Bewertung der Compliance-Risiken</li> </ul>	<ul style="list-style-type: none"> <li>• Identifikation, Analyse und Bewertung der relevanten Compliance-Themengebiete (aufgrund regulatorischer Anforderungen und Änderungen)</li> <li>• Erkenntnisse aus Compliance-Verstößen</li> <li>• Einleitung angemessener Vorbeugungsmaßnahmen</li> <li>• Regelmäßige Berichterstattung neuer/geänderter Compliance-Risiken an die Führung (Vorstand, GF etc.)</li> </ul>	<ul style="list-style-type: none"> <li>• Rechtskataster</li> <li>• Genehmigungskataster</li> <li>• Liste der gesetzlich vorgeschriebenen Beauftragten</li> <li>• Liste der identifizierten Compliance-Themengebiete</li> <li>• Bericht zur Compliance-Analyse/Bewertung</li> <li>• Maßnahmenkatalog</li> <li>• Compliance-Risikobericht</li> </ul>	<ul style="list-style-type: none"> <li>• Sanktionskosten Bußgelder, Strafgelder, Auflagen etc.</li> <li>• Anzahl der Anzeigen/ Beschwerden</li> <li>• Anzahl der Verstöße/versuchten Verstöße</li> <li>• Anzahl der regulativen Änderungen</li> </ul>

- Leseprobe -