BVMed-Akademie

04.11.2026

Struktur und Aufbau einer Compliance-Organisation für MedTech Unternehmen

Referenten:

RAin Christiane Döring, Ahrensburg

RA Prof. Dr. Hendrik Schneider, Wiesbaden

Agenda

A. Compliance-Risikoanalyse
B. Hinweisgebersystem
C. Grundelemente eines Compliance-Management-Systems (CMS)
D. **Compliance-Audit**
   - I. **Einstiegsfall**
   - II. **Sinn & Zweck Compliance-Audits**
   - III. **DIN ISO 367301 vs. IDW PS 980**
   - IV. **Inhalt des Audits**
   - V. **Prüfbericht**

E. Interne Untersuchung
F. Haftungsprävention

1. Einstiegsfall

Einstiegsfall – Umstrukturierung bei der Medcare GmbH

Die MedCare Holding SE ist ein Medizintechnikunternehmen, das auf Prothesen spezialisiert ist. Sie verfügt seit Jahren über ein etabliertes CMS mit regelmäßigen Risikoanalysen, Compliance-Schulungen und internen Audits.

Im letzten Jahr führte die MedCare eine Umstrukturierung durch, bei welcher sie mehrere Tochterunternehmen veräußerte und die OrthoFix GmbH erwarb. Die Mitarbeiteranzahl der MedCare reduzierte sich dadurch um knapp 20%.

Die OrthoFix produziert Sprunggelenks- und Fußlagerungsorthesen, welche sie zum Teil in Krankenhäusern und Arztpraxen in Notfalldepots aufbewahrt.
Zudem produziert sie Hilfsmittel, die nicht für das Notfalldepot bestimmt sind. Ob gleichwohl Depots damit bestückt werden, lässt sich nicht ohne weiteres klären.



Einstiegsfall – Umstrukturierung bei der Medcare GmbH

- Die letzte umfassende CMS-Prüfung liegt 18 Monate zurück und ergab keine wesentlichen Mängel.
- Die Compliance-Risiko-Analyse wurde nach der Umstrukturierung aktualisiert und berücksichtigt auch die Übernahme der OrthoFix. Insgesamt bewertet die Geschäftsführung das Risikoprofil aufgrund des verkleinerten Konzerns als unverändert.
- Die zentrale Compliance-Abteilung wurde entsprechend der verkleinerten Konzernstruktur um 15 % reduziert.
- Die OrthoFix GmbH verfügt über eigene Compliance-Richtlinien und Freigabeprozesse. Ihre vollständige Integration in das konzernweite CMS ist bislang nicht erfolgt.

Die Geschäftsführung hält das bisherige Auditprogramm für ausreichend. Das CMS habe sich über Jahre bewährt; außerdem sei die OrthoFix bereits mit einer eigenen Compliance-Organisation ausgestattet.

Aufsichtsratsmitglied A regt dagegen eine umfassende externe CMS-Prüfung nach IDW PS 980 an.

Sollte dem nachgekommen werden?

2. Sinn & Zweck

Sinn & Zweck

- Überprüfung der Funktionsfähigkeit des CMS untergliedert nach dessen Angemessenheit und Wirksamkeit. Angemessenheit ist ein relationaler Begriff. Er steht im Zusammenhang mit den unternehmensspezifischen Compliance-Risiken und der Größe des Unternehmens
- Regelmäßige Überprüfungen sollen Organisations- und Kontrolldefizite erkennen lassen und zur Verbesserung des CMS beitragen. Die Compliance-Organisation ist eine lernende Organisation und der Ausbau des Compliance-Programms ist ein nicht abgeschlossener Prozess.
- Compliance-Audits sind Bestandteil der Überwachung des CMS wobei zwischen internen und externen Audits zu unterscheiden ist.
- Compliance-Audits werden relevant bei M&A Prozessen. Es wird vielfach eine Integrity Due Diligence durchgeführt, die auf Compliance-Audits aufbauen kann
- Ein aussagekräftiges Audit deckt Schwachstellen auf, minimiert Bußgelder und Haftungsrisiken und ist geeignet, Reputationsschäden frühzeitig abzuwenden.

Abgrenzung

Kriterium	Compliance-Risikoanalyse	Compliance-Audit	Interne Untersuchung
Anlass	Aufbau und Weiterentwicklung des CMS: Änderung der Risikolage	Regelmäßige oder Anlassbezogene Überprüfung des CMS	Konkrete Verdachtsmomente: Hinweise oder Auffälligkeiten
Ziel	Identifizierung und Bewertung möglicher Compliance-Risiken	Überprüfung der Angemessenheit und Wirksamkeit eines CMS	Aufklärung eines konkreten Verdachts auf einen Regelverstoß
Ausrichtung	Präventiv und zukunftsorientiert	Überwachend, kontrollierend und verbesserungsorientiert	Reaktiv und sachverhaltsbezogen
Ergebnis	Risikoinventar, Risikobewertung und Maßnahmenkatalog	Auditbericht mit Feststellungen und erforderlichen Verbesserungsmaßnahmen	Untersuchungsbericht mit Sachverhaltsdarstellung und rechtlicher Bewertung

3. DIN ISO 37301 vs. IDW PS 980

DIN ISO 37301 vs. IDW PS 980

- ISO 37301 und IDW PS 980 sind keine Alternativen.
- Während die ISO 37301 das CMS gestaltet, regelt der IDW PS 980 die Beurteilung des CMS.
- Die ISO 37301 ist im Private Sector verbreitet, IDW PS 980 im Public Sector, obwohl es zunehmend auch im Private Sector Anwendung findet

DIN ISO 37301

- CMS aufbauen, betreiben und überwachen

Internes Audit nach DIN ISO 37301

- Regelmäßige Prüfung durch eigene oder beauftragte Auditoren

Externe CMS-Prüfung nach IDW PS 980

- Unabhängige Überprüfung durch mit förmlichem Prüfungsurteil

Exkurs: Diversifizierung der Compliance-Aufgaben

- Zunehmend erkennbar: Diversifizierung des CMS
- Unterscheidung zwischen einzelnen Risikobereichen, die unterschiedlichen Funktionen im Unternehmen zugeordnet werden und unter dem Dacht von Compliance organisiert werden.
- Beispiel nicht nur Datenschutz, KI-Compliance und ESG-Compliance, sondern auch Tax-Compliance. Hierzu gibt es einen

Emerging Field

IDW Praxishinweis 1/2016:
Ausgestaltung und Prüfung eines
Tax Compliance Management Systems
gemäß IDW PS 980
(IDW Praxishinweis 1/2016)

DIN ISO 37301 vs. IDW PS 980

	DIN ISO 37301:2021	IDW PS 980
Anwendungsbereich	**Managementsystemstandard**	**Prüfungsstandard**
Zweck	Anforderungen an Aufbau, Betrieb und Verbesserung eines CMS	Unabhängige Prüfung eines CMS
Schwerpunkt	Compliance-Organisation und laufende Überwachung	Angemessenheit, Implementierung und Wirksamkeit
Auditpflicht	Interne Audits in geplanten Abständen	Keine allgemeine Pflicht zu externer Prüfung
Prüfer	Unabhängige interne oder beauftragte externe Auditoren	Unabhängiger Wirtschaftsprüfer
Prüfungsumfang	Risikoorientierte Prüfung einzelner Prozesse oder Systembereiche	Abgegrenztes CMS unter Einbeziehung aller CMS-Elemente
Ergebnis	Auditfeststellungen und Verbesserungsmaßnahmen	Förmlicher Prüfungsbericht mit Prüfungsurteil

Interne- und externe Prüfung

Prüfungsform	Wer prüft?	Zweck
Internes Audit nach ISO 37301	Unternehmensinterne, objektive und unparteiische Auditoren	Regelmäßige Überwachung und Verbesserung des CMS
Extern beauftragtes internes Audit nach ISO 37301	Externer Auditor im Auftrag des Unternehmens	Erfüllung der internen Auditfunktion mit externer Unterstützung
Externe CMS-Prüfung nach IDW PS 980	Unabhängiger Wirtschaftsprüfer	Förmliche Beurteilung des CMS mit hinreichender Prüfungssicherheit
ISO-37301-Zertifizierungsaudit	Zertifizierungsstelle	Feststellung der Konformität mit der ISO 37301 zu Zertifizierungszwecken

4. Inhalt des Audits

Allgemeine Regeln eines Auditprogramms

Geplante und strukturierte Durchführung

Häufigkeit, Methoden, Verantwortlichkeiten, Planung und Berichterstattung berücksichtigen

Auswahl der Prüfungsgegenstände unter Berücksichtigung vorheriger Audits.

Bspw. Zusammenarbeit mit Ärzten, Sponsoring, Provisionssysteme, neue Regulatorik

Festlegen:	Bedeutung	Beispiel
Auditziel*	Was soll das Audit feststellen?	Funktioniert der Genehmigungsprozess bei HCP-Verträgen
Auditkriterien*	An welchen Anforderungen wird geprüft?	Richtlinien, Freigabeprozess, relevante G esetze
Auditumfang*	Welche Vorgänge werden untersucht?	Verträge aus 2025/2026 eines be-stimmten Vertriebsbereichs

* DIN ISO 27301:2021 9.2.2. a)

Regeln eines Compliance-Audits

Die zentralen Anforderungen eines Compliance-Audits nach DIN ISO 37310:2021

- Systematische und nachvollziehbare Vorgehensweise.
- Objektivität und Unparteilichkeit der Auditoren.
- Vorherige Festlegung von Auditzielen, Kriterien und Umfang.
- Risikoorientierte Auswahl von Prüfungsgegenständen und Methoden.
- Gewinnung und Auswertung geeigneter Auditnachweise.
- Dokumentation und Berichterstattung an die zuständigen Leitungsebenen.

Geeignete Nachweismethoden



Interviews

Befragung von Geschäftsführung, Compliance-Verantwortlichen, Fachbereichsleitern und Mitarbeitern



Dokumentenprüfung

Einsicht in Verträge, Richtlinien, Genehmigungen, Rechnungen, Protokolle und Leistungsnachweise



Stichprobenprüfung

Auswahl einzelner Vorgänge aus einer definierten Grundgesamtheit, beispielsweise HCP-Verträge oder Sponsoringzahlungen.



System- und Datenprüfung

Auswertung (elektronischer) Freigabeprotokolle, Zugriffsrechte, Ausnahme-regelungen und Transaktionen

Beispiel Interviews

Im externen Audit kann sich der Prüfer anhand öffentlich zugänglicher Quellen über das Unternehmen vorinformieren (Unternehmenskennzahlen, gesellschaftsrechtliche Grundlagen, Wechsel der Geschäftsführung/Gesellschafter, Produkte usw.). Mit dem Audit steigt er ein, um eine konkrete Compliance-Risiko-Analyse vorzubereiten:

- Wo ist das Unternehmen aktiv: Export- und Embargo-Compliance, landesspezifische Risiken- und Compliance-Regelungen; z.B. FCPA und UK Bribery Act
- Was sind die Kunden des Unternehmens: Verkauf nur an Großhandel (B2B) oder Verkauf an Abnehmer wie HCI (B2C): Bestimmung der hieraus abzuleitenden Compliance-Risiken.
- Größe der Compliance-Organisation und personelle Kontinuität: Anzahl der mit Compliance befassten Mitarbeiter, weitere Aufgabenfelder neben Compliance (z.B. Rechtsabteilung), seit wann implementiert.
- Gab es in der Vergangenheit Ermittlungsverfahren wegen Betriebs- oder Unternehmenskriminalität: Ergänzung der Compliance-Risiko-Analyse; Anknüpfungspunkt für weitere Fragen.

Beispiel Dokumentenprüfung

Ausgangssituation:

Ein Medizinproduktehersteller unterhält vertragliche Beziehungen zu HCP und HCI. Eine interne Richtlinie regelt die Voraussetzungen der Vertragsbeziehungen.

Das Audit untersucht:

- Die Angemessenheit und Aktualität sowie Vollständigkeit der internen Richtlinie
- Die Einhaltung der Vorgaben der internen Richtlinie anhand der abgelegten Verträge
- Den gesamten Purchase to Pay Prozess: Vertragsanbahnung, Vertragsschluss, DHG, Bankverbindung, Zahlung. Einhaltung interner Freigabeprozesse
- Je nach Volumen und Untersuchungszeitraum: Stichprobenziehung (Orientierung an der deskriptiven Statistik hinsichtlich Größe und Schichtung) oder Vollerhebung
- Prüfung der Ablagesystematik und des Dokumentenmanagements (Revisionssicherheit, Erkennbarkeit der Risikoeigner etc.)

Compliance Elemente nach IDW PS 980

1. Compliance-Kultur
2. Compliance-Ziele
3. Compliance-Risiken
4. Compliance-Programm
5. Compliance-Organisation
6. Compliance-Kommunikation
7. Compliance-Überwachung und Verbesserung

- Ein umfassendes CMS Audit nach dem IDW PS 980 untersucht das Zusammenwirken der verschiedenen Elemente. Es werden sämtliche Elemente innerhalb des ausgewählten Prüfungsbereichs berücksichtigt.

- Ein einzelnes internes Audit nach DIN ISO 37301:2021 darf dagegen einen engeren Prüfungsgegenstand haben.

Compliance Elemente nach IDW PS 980

Elemente IDW PS 980	Beschreibung
Compliance-Kultur	„Tone from the Top“ – Geschäftsleitung und Führungskräfte leben Compliance sichtbar vor.
Compliance-Ziele	Konkrete, messbar und aus der Risikoanalyse abgeleitete Ziele.
Compliance-Risiken	Risikoorientierte Steuerung des Unternehmens durch systematische Analyse und Identifikation der wesentlichen Risikobereiche. (Branche, Geschäftsmodell, Länderbezug, Geschäftspartner und Prozesse betrachten).
Compliance-Programm	Implementierung konkreter Maßnahmen zur Risikobegrenzung wie Richtlinien, Prozesse, Genehmigungsverfahren, Kontrollen, Schulungen.

Compliance Elemente nach IDW PS 980

Elemente IDW PS 980	Beschreibung
Compliance-Organisation	Festlegung von Zuständigkeiten und Verantwortlichkeiten durch Compliance-Beauftragte, Berichtslinien, Eskalationsmechanismen und die Einbindung von Geschäftsleitung sowie Aufsichtsorganen.
Compliance-Kommunikation	Nach Innen: Regelmäßige Information und Schulung von Mitarbeitern und relevanten Dritten. Nach außen: Hinweisgeber-System (verpflichtend ab 50 MA, § 12 Abs. 2 HinSchG), Berichterstattung.
Compliance-Überwachung & Verbesserung	Laufende Überwachung und Überprüfung & Weiterentwicklung des CMS durch Kontrollen, Audits, interne Untersuchungen sowie Maßnahmen zur kontinuierlichen Verbesserung.

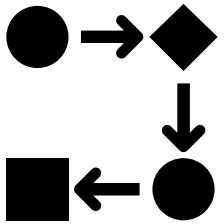
Grundproblem der Grundelemente

- Die Merkmale sind äußerst abstrakt und kaum greifbar.
- Compliance-Kultur ist bspw. allenfalls indirekt messbar: Es ist möglich, Rückschlüsse auf die Compliance-Kultur aus den Gesamtanstrengungen abzuleiten, die ein Unternehmen in Compliance investiert, z.B. Durchführung interner und externer Audits, zur Verfügungstellung personeller und sachlicher Ressourcen für Compliance. Reaktion auf festgestellte Compliance-Verstöße.
- Ein Compliance-Programm muss sich niederschlagen in: Jährlichen Besprechungen zu den Compliance-Zielen, Einhaltung von in Compliance-Richtlinien festgelegten Prozessen, wie bspw. das Compliance-Reporting

 Es ist Aufgabe der Geschäftsführung gemeinsam mit der Leitung Compliance die abstrakten Grundelemente mit Leben zu füllen.

Prüfungsmaßstab System-Audit IDW PS 980

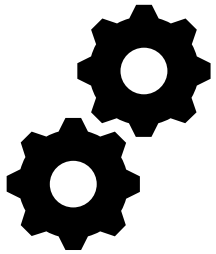
Entwicklung



Auf Basis eine Compliance-Risiko-Analyse wird ein CMS entwickelt.

2026

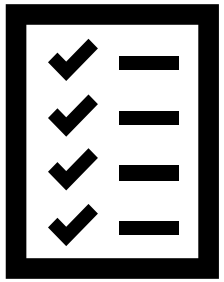
Implementierung



Das Compliance-Programm wird in den Geschäftsprozessen verankert (z.B. Einholung DHG bei HCP)

2027

Angemessenheit



Jetzt kann geprüft werden, ob die Compliance-Organisation und das Compliance-Programm vollständig ist und die wesentlichen Compliance-Risiken abgedeckt werden.

2027

Wirksamkeit



Wurden die Regelungen im Prüfungszeitraum wie vorgesehen angewendet?

2029

IDW PS 980 3.4.2

5. Prüfbericht

Struktur eines internen Compliance-Auditberichts

Berichtsteil	Inhalt
1. Auftrag	Anlass, Ziel und Prüfungsgegenstand
2. Prüfungsmaßstäbe	Gesetze, interne Regeln und gegebenenfalls Normanforderungen
3. Durchführung	Zeitraum, Methoden und untersuchte Stichproben
4. Feststellungen	Nachweisbare Tatsachen und Abweichungen
5. Bewertung	Wesentlichkeit, Risiken und mögliche Ursachen
6. Maßnahmen	Empfehlungen, Verantwortliche und Fristen
7. Follow-up	Vorgesehene Kontrolle der Umsetzung und Wirksamkeit

* Dies dient als Muster; keine unveränderbare ISO-Berichtsgliederung.

Struktur des System-Audits Prüfbericht nach IDW PS 980

A. Prüfungsauftrag
B. Gegenstand, Art und Umfang der Prüfung
C. Feststellungen zum Compliance-Management-System
    I. Konzeption des CMS für ... [Beschreibung des oder der zu prüfenden abgegrenzten Teilbereiche(s) des CMS]
    II. Feststellungen und Empfehlungen
D. Zusammenfassendes Prüfungsurteil

Prüfbericht und Haftungsfragen

- Der Auditbericht kann die Wahrnehmung organisatorischer Überwachung dokumentieren.
- Er macht erkannte Defizite und die Verantwortlichkeit für ihre Beseitigung nachvollziehbar.
- Wesentliche Feststellungen müssen an zuständige Leitungsebenen gelangen.
- Unterlassene Reaktionen auf erkannte erhebliche Defizite können haftungsrechtlich bedeutsam sein.
- Eine ISO-Zertifizierung oder erfolgreiche IDW-Prüfung bewirkt keine automatische Haftungsfreistellung.
- Der BGH erkennt die Bedeutung eines wirksamen CMS und seiner Verbesserung bei der Bemessung einer Unternehmensgeldbuße an (BGH, Urteil vom 9. Mai 2017 – 1 StR 265/16).
    - Der Fall betraf Kick-backs bei Panzerhaubitzen
    - Mehr dazu gleich bei der Haftungsprävention

… Kaffee



… bevor es mit dem Rollenspiel zur Internen Untersuchung weitergeht

Haftungsausschluss und Copyright:

Alle Informationen, die in dieser Präsentation enthalten sind, erheben keinen Anspruch auf Vollständigkeit.

Es wird keine ausdrückliche oder stillschweigende Zusicherung oder Gewährleistung für die Richtigkeit oder Vollständigkeit der in dieser Präsentation enthaltenen Informationen gegeben.

Alle Inhalte dieser Präsentation sind urheberrechtlich geschützt.

© RAin Christiane Döring, © RA Prof. Dr. Hendrik Schneider

Kontakt





Rechtsanwältin Christiane Döring

Hagener Allee 50
22926 Ahrensburg
Tel.: +49 173 2010175
c.doering@doering-rechtsanwalt.de

Prof. Dr. jur. Hendrik Schneider

Taunusstraße 5a
65183 Wiesbaden
Tel + 49 (0) 611 950 08110
schneider@hendrikschneider.eu
www.hendrikschneider.eu

KONTAKT SPEICHERN