Prof. Dr. jur. Josef Scherer

Rechtsanwalt und Consultant, Professor für Compliance, Risiko- und Krisenmanagement sowie Sanierungs- und Insolvenzrecht und Leiter des Stabsbereichs ESGRC an der Technischen Hochschule Deggendorf; Richter am Landgericht a.D..

Scherer

Das gefährlich alte Neue an der ISO 9001:2026

- **Haftungsbewehrte Pflicht zur angemessenen Integration von Governance-, Risiko-, Compliance- und Prozessmanagement in das Qualitäts-Managementsystem (Teil 1)**

  Deggendorf, 1.1.2026

Dieser Artikel ist der erste einer Serie, die sich mit den (alten und) neuen Anforderungen der revisionierten ISO 9001:2026 (Qualitäts-Managementsystem) aus Governance-, Risk- und Compliance-Perspektive beschäftigt und einen Überblick über die noch zu vertiefenden Themen gibt.

Der derzeitige Plan von ISO und DIN sieht vor, die endgültige Fassung der ISO 9001:2026 voraussichtlich im September 2026 zu veröffentlichen. Anschließend soll eine Übergangsfrist für den Wechsel von der ISO 9001:2015 zur neuen Norm gelten. Bereits zur letzten Revision der ISO 9001 in 2015 zeigten *Scherer und Fruth*[1], dass Governance-, Risiko-, Compliance- (GRC) und *angemessenes* Prozessmanagement im Qualitätsmanagement unverzichtbar sind.

Die GRC- und Prozess-Anforderungen gelten inzwischen *für alle Managementsystem-Standards.*

Dies wurde nach Ansicht des Autors nun 10 Jahre lang von QM- und sonstigen Managementsystem-Beauftragten, in- und externen Auditoren und Zertifizierungsstellen häufig ignoriert, ohne explizit klarzustellen, was im konkreten Anwendungsfall *nicht* betrachtet wurde. Dies erzeugt in der Praxis mehr Schein als Sein und gefährliche Suggestiv-Sicherheit. Damit sollte nun Schluss sein. Mit der neuen DIN ISO 9001 besteht eine Chance, das Qualitäts-Managementsystem aufzuwerten. Umgekehrt würde eine Risiko- und Compliance-freie Interpretation des Standards den Wert eines QM-Systems enorm reduzieren und wäre ohne klarstellenden Hinweis sogar gefährlich.

Die neue DIN ISO 9001 bietet also viele Chancen bei kritischer und korrekter, aber auch erhebliche Risiken bei unreflektierter Anwendung ohne GRC-Kompetenzen. Die aktuelle Transformation in allen Bereichen erfordert auch ein grundlegendes Umdenken im Qualitätsmanagement.

1. Geplante Änderungen und Ausstrahlung auf andere Standards

2026 werden neben der ISO 9001 (Qualitäts-Managementsystem) die ISO 14001 (Umwelt-Managementsystem) und 2027 die ISO 45001 (Arbeitsschutz und betriebliches Gesundheitsmanagement) mit jeweils einer dreijährigen Übergangsphase revisioniert.

Nachfolgende Ausführungen betreffen grundsätzlich sämtliche Managementsystem-Standards.

Der für Herbst 2026 erwartete neue ISO-Standard 9001:2026 (Qualitäts-Managementsystem)[2] weist etliche, für implementierungs- oder zertifizierungswillige Organisationen, Geschäftsführer, Vorstände, QM-Beauftragte, in- und externe Auditoren und Zertifizierungsstellen mehr oder weniger haftungsträchtige Änderungen auf.

Dieser Standard ist Basis für weitere branchenspezifische Standards, so dass die Ausführungen in diesem Artikel auch dafür (und auch bereits jetzt) zu berücksichtigen sind:

Beispiele:

Automotive Industrie: Die IATF 16949, eine internationale Norm für Qualitätsmanagement in der Automobilzulieferindustrie setzt die ISO 9001 vollständig voraus und ergänzt sie um branchenspezifische Anforderungen.

---

[1] Vgl. *Scherer, Fruth*, Danke, ISO! Über die neue ISO 9001:2015 (Qualitätsmanagementsystem) zum integrierten, ganzheitlichen Managementsystem mit Governance, Risk und Compliance (GRC), BCM - Berufsverband der Compliance Manager, Compliance 2015 - Perspektiven einer Entwicklung, Regensburg 2015, S. 83 - 107, zum kostenlosen Download unter: https://www.scherer-grc.net/files/fil/danke-iso.pdf.

[2] Vgl. DIN EN ISO 9001 Qualitätsmanagementsysteme – Anforderungen (ISO / DIS 9001:2025-9).

Automobil-Service & -Aftermarket (VDA 6.1): Die VDA-6.x-Reihe, einschließlich VDA 6.1, bildet einen eigenständigen deutschen QM-Standard für Hersteller und Zulieferer der Automobilindustrie, historisch aus der ISO 9001 entstanden, heute jedoch als unabhängiges Zertifizierungssystem geführt.

Luft- und Raumfahrt: Die EN 9100 / AS 9100 / JISQ 9100 sind QM-Normen für die Aerospace-Industrie in Europa, USA und Japan. Die ISO 9001 stellt den Kern dar, erweitert um strenge Sicherheits- und Dokumentationsanforderungen.

Kliniken: Die EN 15224 ist eine europäische Qualitätsmanagementnorm für das Gesundheitswesen, basiert auf der ISO 9001, erweitert um spezifische Anforderungen zu klinischen Prozessen, patientenbezogenen Risiken, Sicherheit und evidenzbasierter Versorgung.

Medizinprodukte: Die ISO 13485[3] ist ein eigenständiger Qualitätsmanagement-Standard für Medizinprodukte, orientiert sich in Teilen an der ISO 9001, ist aber deutlich stärker regulierungsorientiert und risikobasiert ausgestaltet, mit spezifischen Vorgaben zu Produktsicherheit, Rückverfolgbarkeit und behördlichen Anforderungen.

Telekommunikation / ICT: Die TL 9000, ein QM-Modell für Telekommunikation und IT-Hardware/Software basiert auf ISO 9001, enthält aber noch zusätzliche Mess- und Leistungsmetriken.

Energieversorgung: Die ISO 19443 regelt das Qualitätsmanagement für die nukleare Lieferkette und erweitert die ISO 9001 um Safety- und Risikomanagement.

Bildungsdienstleistungen: Die ISO 21001 (EOMS) stellt ein QM-System speziell für Bildungsorganisationen dar.

Erdöl-, Gas- und Petrochemie (API Q1 / Q2): Die API-Spezifikationen Q1 und Q2 sind eigenständige QM-Standards des American Petroleum Institute für Produktions- und Serviceorganisationen der Öl- und Gasindustrie, basieren auf Qualitätsmanagement-Prinzipien ähnlich ISO 9001 und ergänzen diese um umfangreiche risikobezogene, sicherheitsrelevante und produktionsspezifische Anforderungen.

Eisenbahnindustrie: Die ISO 22163 (IRIS) enthält den QM-Standard für den Bahnsektor, ist strukturell an ISO 9001 angelehnt und enthält zusätzliche Leistungsanforderungen.

Behörden & öffentliche Organisationen: Die ISO 18091 ist der QM-Standard für kommunale Verwaltungen, zugeschnitten auf öffentliche Dienstleistungen und baut auf ISO 9001 auf.

Die geplanten Änderungen der ISO 9001 sind wenig spektakulär, wenngleich zahlreiche Berater, Zertifizierer und sonstige davon Profitierende erheblichen – kostenpflichtigen – Beratungsbedarf entdecken könnten:

„Änderungen[4]

Gegenüber DIN EN ISO 9001:2015-11 und DIN EN ISO 9001/A1:2024-11 wurden folgende Änderungen vorgenommen:

a) aktuelle Vorgaben der in den ISO-Direktiven festgelegten „harmonisierten Struktur für Managementsystemnormen“ eingearbeitet und entsprechende Inhalte sprachlich präzisiert und vereinheitlicht;

[3] Die ISO 13485:2016 wurde im November 2025 von der ISO als bis 2030 unverändert gültig benannt (reconfirmed).
[4] Vgl. DIN EN ISO 9001 Qualitätsmanagementsysteme – Anforderungen (ISO / DIS 9001:2025-9)

b) in diesem Zusammenhang in Abschnitt 3 die Begriffe 3.1 bis 3.20 aus der harmonisierten Struktur für Managementsystemnormen ergänzt (ohne den Bezug zu DIN EN ISO 9000, Qualitätsmanagementsysteme — Grundlagen und Begriffe, zu ändern);

c) die Inhalte von DIN EN ISO 9001/A1:2024-11 mit Ergänzungen zu klimabezogenen Maßnahmen wurden integriert;

d) Anmerkungen zu Anforderungen wurden auf Aktualität und Vollständigkeit geprüft und zum Teil angepasst;

e) zusätzliche Anforderungen und Anmerkungen wurden u. a. in 5.1.1, 8.2, 8.3.1, 8.3.3, 8.5.1, 9.3.2 und 10.2.1 aufgenommen;

f) 5.1.1 wurde um die Anforderung i) „Förderung einer Qualitätskultur und ethischen Verhaltens“ ergänzt;

g) in 5.2.1 zu Qualitätspolitik wurde die Anforderung e) ergänzt, nach der Kontext der Organisation und strategische Ausrichtung beachtet werden muss;

h) 6.1 „Maßnahmen zum Umgang mit Risiken und Chancen“ wurde ergänzt um 6.1.2 „Maßnahmen zum Umgang mit Risiken“ und 6.1.3 „Maßnahmen zum Umgang mit Chancen“;

i) an die Planung von Änderungen werden erweiterte Anforderungen in 6.3 e), f) und g) gestellt;

j) in 7.3 „Bewusstsein“ wurde die Anforderung e) „Qualitätskultur der Organisation und ethisches Verhalten“ ergänzt;

k) zur Unterstützung des Verständnisses der Anforderungen wurde der informative Anhang A „Erläuterung der Struktur, Terminologie und Konzepte“ grundlegend überarbeitet. Änderungen zur Vorgängerversion werden nicht mehr aufgeführt;

l) informativen Anhang B „Andere Internationale Normen des ISO/TC 176 zu Qualitätsmanagement und Qualitätsmanagementsystemen“ ersatzlos gestrichen;

m) die aktuelle deutsche Übersetzung der harmonisierten Struktur wurde verwendet und in dem Zusammenhang wurde z. B. die Verwendung von „lenken/Lenkung“ in Bezug auf dokumentierte Information durch „steuern/Steuerung“ ersetzt sowie zwei neue nationalen Fußnoten N1 und N3 aufgenommen;

n) Dokument redaktionell überarbeitet.“

Der Standard weist nach wie vor Schwächen und Klarstellungsbedürftigkeit auf; einige neue Ansätze sind begrüßenswert.

Die Anforderungen an ein (Qualitäts-) Managementsystem sind (bereits jetzt schon) *aus der Compliance-Perspektive* anspruchsvoller als in der aktuellen und revisionierten Version auf den ersten Blick dargestellt. Hier besteht tatsächlich – bereits jetzt schon - dringender Handlungsbedarf:

2. Klarstellung der Rechtsnatur von Managementsystem-Standards und des Vorrangs rechtlich verpflichtender Anforderungen: Fehlanzeige

Für Managementsysteme finden sich, da keine gesetzlich vorgegebenen Definitionen (Legaldefinitionen) existieren, unterschiedliche Bezeichnungen und Ansichten, wie „Führungssystem“ oder andere Begriffe.[5]

Zunächst der Versuch einer Definition von „Managementsystem“:

„*Ein Managementsystem besteht aus formell vorgegebenen, idealerweise vernetzten und miteinander interagierenden Komponenten, wie Aufbau- und Ablauforganisation, Ressourcen, input und output, mit dem Zweck, eine Organisation bei Zielsetzung, Planung, Steuerung und Überwachung zur Erreichung zwingender und fakultativ gesetzter Ziele zu unterstützen*.“[6]

Jede „lebende“ Organisation hat bereits per se ein Managementsystem. In jeder Organisation bewegt sich etwas, es gibt eine Aufbau- und Ablauforganisation, einen Regelkreislauf, oft chaotisch, oft nicht dokumentiert, oft unbewusst, manchmal schon ganz passabel oder sogar „best practice“.

Die ISO 9001 bestimmt „*Anforderungen*“ an Qualitäts-Managementsysteme.

Beim neuen QM-9001-Standard fehlt, wie bei vielen anderen Standards auch, zunächst die Erklärung der erforderlichen Art des Zustandekommens und Rechtsqualität eines Standards („*antizipiertes Sachverständigengutachten*“) und der Hinweis auf den absoluten Vorrang von rechtlich verbindlichen Anforderungen.[7]

Es wird auch nicht ausgeführt, ob diese Norm den „anerkannten Stand von Wissenschaft und Praxis“ (die „anerkannten Regeln der Technik“) widerspiegelt oder den „Stand der Technik“ oder den „neuesten Stand von Wissenschaft und Technik“.[8]

---

[5] Vgl. *Scherer*, Nachhaltige Führung und Überwachung von Organisationen (Governance) nach DIN ISO 37000, Erfolgreich umsetzen, auditieren und reporten, Herausgeber DIN, DIN Media Verlag, 2025, Kapitel Einleitung.
[6] Vgl. auch DIN EN ISO 9001 Qualitätsmanagementsysteme – Anforderungen (ISO / DIS 9001:2025) und ISO 37301:2021 (Compliance Management Systems); dort wird ein Managementsystem als *Satz miteinander verbundener oder sich wechselseitig beeinflussender Elemente beschrieben, mit deren Hilfe Politik und Ziele festgelegt und diese Ziele erreicht werden sollen.*
[7] Vgl. *Scherer*, Nachhaltige Führung und Überwachung von Organisationen (Governance) nach DIN ISO 37000, Erfolgreich umsetzen, auditieren und reporten, Herausgeber DIN, DIN Media Verlag, 2025, Kapitel 1.
[8] Vgl. *Scherer, Fruth*, Technik-Governance, Sonderdruck BCM-Berufsverband der Compliance Manager, 2016, zum kostenlosen Download unter: https://www.scherer-grc.net/files/fil/bcmtechnikgovernance.pdf und *Scherer*, Nachhaltige Führung und Überwachung von Organisationen (Governance) nach DIN ISO 37000, Erfolgreich umsetzen, auditieren und reporten, Herausgeber DIN, DIN Media Verlag, 2025, Kapitel Einleitung.

3. Angemessener Hinweis auf Compliance und Haftungsverantwortung der Organe und QM-Beauftragten: Fehlanzeige

3.1 Zwingende Anforderungen nach Legalitätsprinzip

Zunächst müssen (Management-) Systeme, Produkte, Dienst-, Werk- oder sonstige Leistungen[9], Prozesse etc. zwingenden Verpflichtungen (Gesetzen / Rechtsprechung / Anerkannten Regeln oder Stand der Technik[10] etc.) entsprechen (Compliance-basierter Ansatz und allgemeine Legalitätspflicht).[11]

3.2 Verweise und Muss-Anforderungen auf Compliance in der (neuen) ISO 9001

Der Entwurf der revidierten ISO 9001 enthält *an vielen verschiedenen Stellen* die *Anforderung, rechtliche Vorgaben für Produkte und Dienstleistungen zu identifizieren, zu bewerten und einzuhalten*, was einem Compliance-Management in Bezug auf die Leistungserstellung einer Organisation entspricht.

Ein paar Beispiele von vielen (Zitate aus dem Text des Entwurfs der DIN ISO 9001 neu):

„Einleitung

(…) Die in diesem Dokument festgelegten Anforderungen an ein Qualitätsmanagementsystem ergänzen die Anforderungen an Produkte und Dienstleistungen. (…)

In diesem Dokument werden die folgenden Verbformen verwendet: ***„muss" gibt eine Anforderung an****; „sollte" gibt eine Empfehlung an; „darf" gibt eine Zulässigkeit an; „kann" gibt eine Möglichkeit oder ein Vermögen an. (…)"*[12]

Hinweis des Verfassers: Aus der Formulierung „*Die in diesem Dokument festgelegten Anforderungen an ein Qualitätsmanagementsystem ergänzen die Anforderungen an Produkte und Dienstleistungen"* darf nicht geschlossen werden, dass die DIN ISO 9001, Qualitätsmanagement-Beauftragte, Auditierer und Zertifizierungsstellen rechtliche Anforderungen an Produkte und Leistungen außer Betracht lassen würden / dürften, weil dies ja anderweitig geregelt sei.

Dies stünde in Widerspruch zu den im Normtext sich ständig wiederholenden Anforderungen, rechtliche Anforderungen erfüllen zu müssen und würde die DIN ISO 9001 nicht nur zu einer unbrauchbaren, sondern sogar gefährlichen, weil Sicherheit suggerierenden, Norm machen. Sofern diese

[9] Entgegen ihrem irreführenden Wortlaut behandelt die ISO 9001 nicht nur Produkte und „Dienstleistungen", sondern auch Werkleistungen, Handel, Engineering, u.v.m., also *jede* Art von Leistungserstellung.
[10] Vgl. *Scherer*, Nachhaltige Führung und Überwachung von Organisationen (Governance) nach DIN ISO 37000, Erfolgreich umsetzen, auditieren und reporten, Herausgeber DIN, DIN Media Verlag, 2025, Kapitel 1.
[11] Vgl. *Scherer,* Compliance-Managementsystem nach DIN ISO 37301:2021 erfolgreich implementieren, integrieren, auditieren, zertifizieren, 1. Aufl., Herausgeber DIN, DIN Media-Verlag, 2022, Kapitel Einleitung.
[12] Aus DIN EN ISO 9001, Qualitätsmanagementsysteme – Anforderungen (ISO/DIS 9001:2025), Abschnitt Einleitung.

weder grammatikalisch oder teleologisch gedeckte Text-Interpretation von den Verantwortlichen (QMBs, Auditierer, Zertstellen, etc.) vertreten werden sollte, müsste dies gegenüber Stakeholdern klargestellt werden.[13]

Wenn im Übrigen ein „*muss"* im Text des Standards eine „*Anforderung*" impliziert, muss eine Zertifizierungsstelle bei Erteilung des Zertifikats auch dafür einstehen, dass diese Anforderung erfüllt ist.

„1 Anwendungsbereich

Dieses Dokument legt Anforderungen an ein Qualitätsmanagementsystem fest, wenn eine Organisation a) ihre Fähigkeit darlegen muss, beständig Produkte und Dienstleistungen bereitstellen zu können, ***die*** *die Anforderungen der Kunden und* ***die zutreffenden gesetzlichen und behördlichen Anforderungen erfüllen****, und*

b) danach strebt, die Kundenzufriedenheit durch wirksame Anwendung des Systems zu erhöhen, einschließlich der Prozesse zur Verbesserung des Systems und ***der Zusicherung[14]*** **der Einhaltung** *von Anforderungen der Kunden und* ***von zutreffenden gesetzlichen und behördlichen Anforderungen****. (…).*

ANMERKUNG 2 ***Gesetzliche und behördliche Anforderungen können auch als rechtliche Anforderungen bezeichnet werden****. (…)".*

Hinweis des Verfassers: Die Formulierungen in Bezug auf „*gesetzliche und behördliche Anforderungen*" sind irreführend und weisen auf ein grundsätzlich fehlendes Compliance-Verständnis der Normersteller hin. Eine Organisation muss – unabhängig von irgendwelchen Standards – bereits aufgrund der Legalitätspflicht „rechtliche" oder auch „verpflichtende" Anforderungen einhalten: Diese *rechtlichen Anforderungen* sind vielfältiger als nur gesetzliche oder behördliche Anforderungen:

Dazu gehören u.a. – keinesfalls abschließend – auch noch Anforderungen aus (EU-) Verordnungen, der Rechtsprechung, technischer Entwicklungsstände (z.B. Anerkannte Regeln oder Stand der Technik), sowie intern verbindlichen Regelungen (z.B. aus Richtlinien / Policies, Betriebsvereinbarungen, Verträgen, etc.).[15]

„3. Definitionen (…)

3.14 Anforderung

[13] Vgl. unten 6.
[14] Der Begriff „Zusicherung" ist im deutschen vertraglichen Leistungsstörungsrecht ein sog. „unbestimmter Rechtsbegriff" mit weitreichenden (oft negativen) Folgen für den Zusichernden, wie eine u.U. verschuldensunabhängige, der Höhe nach nicht beschränkten Schadensersatzhaftung bei Fehlen der zugesicherten Eigenschaft. Ohne Kenntnis der Bedeutung und Reichweite einer – von einer Versicherung nicht per se gedeckten Risikoerhöhung – sollte eine Zusicherung nicht abgegeben werden.
[15] Vgl. *Scherer,* Compliance-Managementsystem nach DIN ISO 37301:2021 erfolgreich implementieren, integrieren, auditieren, zertifizieren, 1. Aufl., Herausgeber DIN, DIN Media-Verlag, 2022, Kapitel 4.5.

Erfordernis *oder Erwartung,* das *oder die festgelegt, üblicherweise vorausgesetzt* oder verpflichtend ist *(…) Anmerkung 4 zum Begriff: Anforderungen können von verschiedenen interessierten Parteien oder durch die Organisation selbst aufgestellt werden.*

3.15 Konformität

Erfüllung einer Anforderung (3.14) Anmerkung 1 zum Begriff: Die Benennung „conformance" stellt im Englischen ein abzulehnendes Synonym dar. Die Benennung „compliance" stellt im Französischen ein abzulehnendes Synonym dar. (…)"

Hinweis des Verfassers: Durch die Formulierung in Anmerkung 4 („*Anforderungen können von verschiedenen interessierten Parteien oder durch die Organisation selbst aufgestellt werden.")* und durch die Interpretationshilfe in Anhang A („*Anhang A (informativ) (…) A.3 Anwendbarkeit (…) Die zutreffenden gesetzlichen und behördlichen Anforderungen, die in Abschnitt 1a) erwähnt werden, werden von der Organisation bestimmt, wobei diejenigen Anforderungen zu berücksichtigen sind, die sich auf die Fähigkeit der Organisation beziehen, durch die wirksame Anwendung des Qualitätsmanagementsystems beständig konforme Produkte und Dienstleistungen bereitzustellen* (…)."**)** entsteht bei Zertifizierungsstellen, QMBs, Dozenten und Auditoren bisweilen die völlig abstruse Ansicht, dass von der Organisation selbst beliebig die dann zu auditierenden Anforderungen aufgestellt werden können und die rechtlich verbindlichen Anforderungen keine Rolle mehr spielten.[16] Zu den Interessierten Parteien gehört immerhin auch der Staat mit Legislative, Exekutive und Judikative, die u.a. über die Einhaltung des Legalitätsprinzips wachen. Zudem ist das „oder" in Anmerkung 4 nicht alternativ, sondern kumulativ zu sehen.

Genau umgekehrt ist also zu auditieren:

Werden die rechtlich verpflichtenden Anforderungen eruiert, bewertet und sind Aktivitäten zur Erfüllung dieser Anforderungen in Prozessen und Köpfen der Organisation? Und dann: Welche sonstigen Anforderungen, die den obigen Anforderungen nicht widersprechen, gab sich die Organisation?

Dass im übrigen „Konformität" in den englischen und französischen Texten als Synonym zu compliance oder conformance abgelehnt werden soll, dürfte dem fehlenden Compliance-Verständnis der Normersteller entspringen. Eine Begründung für diese unverständliche Ansicht ist nicht zu finden.

Hinweis des Verfassers: Auch im Abschnitt 5 des Entwurfs finden sich deutliche Muss-Anforderungen, adressiert an die Organe („Oberste Leitung: Z.B. Vorstand / Geschäftsführer), bzgl. Compliance-Anforderungen:

[16] Etwas überzeichnet könnte die Organisation nach dieser – falschen - Ansicht die Anforderung aufstellen, das Produkt müsse auf einem selbstgewählten Sicherheits- und Compliance-Stand sein, der nicht den tatsächlich verbindlichen Vorgaben entspricht. Der Auditor würde dann bei Feststellung eines entsprechenden Prozesses mit diesem negativen Output bestätigen: „Anforderung erfüllt" und die Zertifizierungsstelle würde ein Zertifikat erteilen …

„5.1.2 Kundenorientierung[17]

Die oberste Leitung muss Führung und Verpflichtung im Hinblick auf die Kundenorientierung dadurch nachweisen, dass:

a) Kundenanforderungen sowie ***anwendbare gesetzliche und regulatorische Anforderungen bestimmt, verstanden und konsequent erfüllt werden***,

b) die Risiken *und Chancen, welche die* ***Konformität von Produkten und Dienstleistungen*** *sowie die Fähigkeit zur Steigerung der Kundenzufriedenheit beeinflussen können,* ***bestimmt und behandelt werden***, *(…)."*

Hinweis des Verfassers: Im Abschnitt 8 finden sich weitere Muss-Anforderungen, die den Anforderungen aus der DIN ISO 37301, Abschnitt 4.5 Compliance-Verpflichtungen, entsprechen:

„8.2.2 Bestimmen von Anforderungen für Produkte und Dienstleistungen

Bei der Bestimmung von Anforderungen an die Produkte und Dienstleistungen, die Kunden angeboten werden sollen, ***muss die Organisation sicherstellen, dass****:*

a) ***die Anforderungen an das Produkt und die Dienstleistung festgelegt sind, einschließlich: 1) jeglicher zutreffender gesetzlicher und behördlicher Anforderungen****; (…)*

8.2.3.1 Die Organisation muss sicherstellen, dass sie die Fähigkeit besitzt, die Anforderungen an die Produkte und Dienstleistungen, die Kunden angeboten werden, zu erfüllen.

Die Organisation muss*, bevor sie eine Verpflichtung eingeht, ein Produkt an einen Kunden zu liefern oder eine Dienstleistung für einen Kunden zu erbringen,* ***eine Überprüfung durchführen, die Folgendes einschließt:***

a) die vom Kunden festgelegten Anforderungen, (…)

b) ***die vom Kunden nicht angegebenen Anforderungen, die jedoch für den festgelegten oder den beabsichtigten Gebrauch, soweit bekannt, notwendig sind****;*

c) von der Organisation festgelegte Anforderungen;

d) ***gesetzliche und behördliche Anforderungen, die für die Produkte und Dienstleistungen zutreffen****;*

e) Anforderungen im Vertrag oder Auftrag, die sich von den zuvor angegebenen Anforderungen unterscheiden.

8.2.3.2 Sofern zutreffend, ***muss dokumentierte Information als Nachweis verfügbar sein für****:*

a) die Ergebnisse der Überprüfung;

*b****) jegliche neuen oder geänderten Anforderungen an die Produkte und Dienstleistungen****.(…)"*

Hinweis des Verfassers: Gerade derzeit gibt es in der europäischen und deutschen Regulierung mit Bezug zu (IT- und KI-) (Product-) Compliance sehr viele und komplexe Neuerungen:

[17] Aus DIN EN ISO 9001, Qualitätsmanagementsysteme – Anforderungen (ISO/DIS 9001:2025), Abschnitt 5.1.2 „Kundenorientierung", S. 20.

Es bleibt hier „kein Stein auf dem anderen“, etwa durch den AI Act, insbesondere die Regulierung hochriskanter KI, durch Änderungen des Produkthaftungsrechts (KI oder Produkte mit KI-Komponenten gehören zu den Produkten i.S. des ProdHG und werden auch unter den Produktbegriff der ISO 9001 fallen), für die bereits ein Entwurf vorliegt, durch das Produktsicherheitsgesetz und die EU-Produktsicherheitsverordnung, durch ein verschärftes Kreislaufwirtschafts- und Umweltstrafrecht, die Entwaldungs-VO, die Green-Claims-Directive, den Cyber Resilience Act und vieles mehr.

Nach der KI-Verordnung darf „verbotene KI“ seit 2025 - bußgeldsanktioniert - nicht mehr eingesetzt werden und wohl[18] ab August 2026 ist Hochrisiko-KI mit dem Schutzziel „Menschenrechte“ reguliert.

Hinweis: Auch einfache KI – egal, ob als Software pur oder in anderen Produkten implementiert -, die nach KI-VO als nicht riskant eingestuft wird, kann unter Produkthaftungsaspekten „hochriskant“ wegen Gefahr für Leib und Leben sein.

3.3 Haftungsverantwortung bei Qualitäts-Managementsystem ohne angemessene Compliance-Elemente

Zertifizierungsgesellschaften, Qualitätsmanagement-Beauftragte und interne Auditoren ebenso, wie der Geschäftsführer bestätigen, dass die Anforderungen an das Qualitäts-Managementsystem wirksam erfüllt werden:

Wenn die regulatorischen Vorgaben für Produkte oder Leistungen nicht erfüllt werden und es zu Personen- oder Sachschäden kommt, steht die Haftung der Organe (Vorstand, Geschäftsführer, Aufsichtsrat[19]), Führungskräfte und der Qualitätsmanagement-Beauftragten im Raum; insbesondere, wenn sich dann herausstellt, dass die zuvor genannten Verantwortlichen sich um diese Anforderungen nur oberflächlich oder gar nicht gekümmert haben.

Beispiel: Im Fall „*Müller Brot*" wurden im Münchner Raum laut Medien *strafrechtlich Ermittlungen auch gegen die Leiter Qualitätsmanagement* und Produktion geführt:[20]

---

[18] Sicher ist die Rechtslage aufgrund eines „Digital-Omnibus“, der die KI-VO und die DSGVO ändern soll, nicht: Vgl. *Tagesspiegel Background*, „Digitalisierung & KI, Der Digitale Omnibus – Versuch einer Einordnung“, abrufbar unter: https://background.tagesspiegel.de/digitalisierung-und-ki/briefing/der-digitale-omnibus-versuch-einer-einordnung

[19] Zur Verantwortung eines Aufsichtsratsmitglieds vgl. jüngst BGH, Urteil vom 14.10.2025 – II ZR 78/24, erklärt in Beck aktuell vom 27.11.25, Zitat: *„(…) Das Gericht machte deutlich, dass die Überwachung nicht erst mit erkennbaren Risiken beginne. (…) Nach § 90 Abs. 1 S. 1 Nr. 3, Abs. 2 Nr. 3 AktG muss der Vorstand den Aufsichtsrat „regelmäßig, mindestens vierteljährlich" über den Gang der Geschäfte und die Lage der Gesellschaft informieren. (…) Bei ausbleibenden Berichten dürfe der Aufsichtsrat sich nicht passiv verhalten. Er müsse diese aktiv einfordern und auf eine strukturierte Informationslage dringen. (…) Fehlen formelle Berichte wie hier, habe der Aufsichtsrat nachzuhaken und notfalls Druck auszuüben. Diese Pflicht treffe jedes einzelne Mitglied. (…) Anders als die Vorinstanzen hielt das Gericht die Kausalität auch nicht für ausgeschlossen. (…) Die Darlegungs- und Beweislast für fehlendes Verschulden liegt gemäß §§ 116, 93 AktG beim Aufsichtsrat (…).“*

[20] Vgl. *Ehrenstein*, Wenn „Gier und Preisdruck" über die Hygiene siegen, Welt, 12.02.2012, abrufbar unter https://www.welt.de/dieweltbewegen/article13864527/Wenn-Gier-und-Preisdruck-ueber-die-Hygiene-siegen.html.

„(…) erhebt die Staatsanwaltschaft Landshut Anklage gegen drei frühere Geschäftsführer (…). Außerdem im Focus: der ehemalige Betriebsleiter, ***der Produktionsleiter und die Leiterin des Qualitätsmanagements.*** *(…)*“[21].

Beispiel: Der „Transrapid“-Fall[22] zeigte, dass bei fehlenden oder nicht korrekten Prozessbeschreibungen nicht nur einzelne direkte Verursacher, sondern gleich mehrere Verantwortliche, insbesondere auch einfache Vorgesetzte, im Fokus von Ermittlungen, Anklagen und Verurteilungen stehen.

Die Haftung von Organen und Führungskräften kann persönlich zivil-, straf- und bußgeldrechtlich relevant werden. Die Zahl der Verurteilungen von Managern steigt stetig und die neueste Rechtsprechung regelt, ob und wann bei wissentlichen Pflichtverletzungen, insbesondere Kardinalpflichtverletzungen die D&0-Versicherung Deckungsschutz versagen kann.[23]

3.4 Enthaftende Wirkung eines Compliance-Mangementsystems

Enthaftend wirkt in diesen Fällen nach höchstrichterlicher Rechtsprechung nicht ein Qualitäts-, sondern ein Compliance-Managementsystem (CMS):[24]

Seit 2017 entschieden diverse Senate des BGH, der EuGH, aber inzwischen auch Instanzgerichte, dass ein Compliance-Managementsystem bei Pflichtverstößen unterhalb der Leitungsebene für die Organe und Führungskräfte enthaftend wirken kann.

3.5 Rechtssicheres Qualitäts-Managementsystem

Ein Blick in die Abschnitte 4.5 und 4.6 der ISO 37301[25] (CMS) ist für die Rechtssicherheit des Qualitäts-Managementsystems sehr empfehlenswert:

Die DIN ISO 37301:2021(CMS) verlangt im Abschnitt 4.5 zu Recht eine *systematische* Vorgehensweise, um relevante, zwingende *Compliance-Verpflichtungen* (aktuelle und auch neue oder geänderte Anforderungen) zu identifizieren, zu bewerten und für deren (nachweisliche) Einhaltung zu

---

[21] Zitat nach *Schweikl*, Müller-Brot-Skandal, BR vom 28.9.2026.
[22] Vgl. *Werner*, Transrapid-Unfall 2006: Bewährungsstrafen für zwei Fahrdienstleiter, Mitteldeutsche Zeitung, 03.03.2011, abrufbar unter https://www.mz.de/panorama/transrapid-unfall-2006-bewahrungsstrafen-fur-zwei-fahrdienstleiter-2268246.
[23] Vgl. hierzu *Scherer, Seehaus*, Pflicht zu Governance mit Risikofrüherkennung, Resilienz und Transformation als Kardinalpflicht von Organen und Führungskräften, ZInsO 31/2025, S. 1515-1538, 31.07.2025, in Deutsch, zum kostenlosen Download unter: https://www.risknet.de/elibrary/paper/pflicht-zu-governance-mit-risikofrueherkennung-resilienz-und-transformation-als-kardinalpflicht-von-organen-und-fuehrungskraeften/ und
Scherer, Seehaus, Managerhaftung, D&O-Versicherung und Risikofrüherkennung im Lichte aktueller Rechtsprechung, 2026, zum kostenlosen Download auf Risknet.de.
[24] Vgl. hierzu *Scherer, Seehaus*, Pflicht zu Governance mit Risikofrüherkennung, Resilienz und Transformation als Kardinalpflicht von Organen und Führungskräften, ZInsO 31/2025, S. 1515-1538, 31.07.2025, in Deutsch, zum kostenlosen Download unter: https://www.risknet.de/elibrary/paper/pflicht-zu-governance-mit-risikofrueherkennung-resilienz-und-transformation-als-kardinalpflicht-von-organen-und-fuehrungskraeften/ *Scherer, Seehaus*, Managerhaftung, D&O-Versicherung und Risikofrüherkennung im Lichte aktueller Rechtsprechung, 2026, zum kostenlosen Download auf Risknet.de.
[25] Vgl. *Scherer,* Compliance-Managementsystem nach DIN ISO 37301:2021 erfolgreich implementieren, integrieren, auditieren, zertifizieren, 1. Aufl., Herausgeber DIN, DIN Media-Verlag, 2022, Kapitel 4.6 und 4.7.

sorgen.

Dazu definiert die DIN ISO 37301:2021 im Abschnitt 3.25 – *Compliance-Verpflichtungen*:

„Anforderungen, die eine Organisation zwingend erfüllen muss sowie die Anforderungen, der sie sich freiwillig unterwirft."

und regelt in Abschnitt 4.5 Anforderungen bzgl. *Compliance-Verpflichtungen*:

„Die Organisation muss systematisch ihre aus ihren Aktivitäten, Produkten und Dienstleistungen resultierenden Compliance-Verpflichtungen identifizieren und deren Auswirkung auf ihren Betrieb beurteilen."

Dies erinnert aus gutem Grund an einen *Risikomanagement-Prozess:* Jeder Verstoß bzw. jede Nicht-Beachtung von Compliance-Verpflichtungen stellt ja zugleich ein Compliance-Risiko dar, vgl. dazu ISO 37301 Normabschnitt 4.6.

3.6 Identifikation der Compliance-Verpflichtungen und deren Risiken

Identifikation verpflichtender Anforderungen

Die Identifikation muss sicherstellen, dass sämtliche einzuhaltende Anforderungen, auch internationale, soweit relevant[26], bekannt sind.

Diese Vorgaben lassen sich in einem agilen und sich ständig weiterentwickelnden prozessbezogenen *Rechtskataster* abbilden.[27]

Dabei ist sicherzustellen, dass auch alle zukünftigen (neue und sich ändernde) Anforderungen erkannt und nachweisbar eingehalten werden, wenngleich dies eine komplexe Aufgabe darstellt:[28]

Beispielsweise entschied der *BGH,* dass ein Händler bei Werbung mit einem Foto eines *Ferrari* die CO2-Emissionen gemäß PKW-EnVKV angeben muss, selbst wenn dieser gar keine Ferraris verkauft.[29]

Und auch hier gilt: *Nichtwissen schützt vor Strafe nicht*, vgl. das Buchhändler-Urteil.[30]

Grundlegende Methodik zur Identifikation verpflichtender Anforderungen[31]

Zunächst müssen wohl viele der bereits identifizierten und ebenso auf Basis eines entsprechenden Prozesses fortlaufend neu identifizierten Anforderungen aus unterschiedlichsten fachlichen und

---

[26] Vgl. *Scherer, Butt, Reimertshofer*, Risiken der internationalen Produkthaftung aus der Sicht eines Unternehmers in: Der Betrieb, Heft 9 vom 5.3.1998, S. 469 – 474.
[27] Vgl. *Scherer,* Compliance-Managementsystem nach DIN ISO 37301:2021 erfolgreich implementieren, integrieren, auditieren, zertifizieren, 1. Aufl., Herausgeber DIN, DIN Media-Verlag, 2022, Kapitel 4.6 und 4.7.
[28] Vgl. *Raum*, Artikel „Compliance im Zusammenhang straf- und bußgeldrechtlicher Pflichten", in: *Hastenrath* (Hrsg.), Compliance-Kommunikation, 2017, S. 33.
[29] Vgl. *BGH*, Urteil vom 30.04.2020 – I ZR 115/16.
[30] Vgl. *BGH*, Urteil vom 18.10.2020 – 2 StR 246/20
[31] Vgl. *Scherer*, *Ketelsen*, Technical Product Compliance, Bavarian Journal of Applied Sciences, 2022.

wissenschaftlichen Disziplinen (Recht, Technik, Ökologie etc.) in eine (nicht nur für die Juristen und Techniker) verständliche Sprache „übersetzt“ werden.

Dabei kommt es, nicht nur bei der Technical Product Compliance, sondern auch im Gesundheitswesen, in der Immobilien- und Energiewirtschaft etc. zu einer allgemeinen auftretenden Schwierigkeit, den sog. *„Unbestimmten Rechtsbegriffen“*[32]*.*

Bei freiwillig zu erfüllenden Anforderungen („soll“) in Bezug auf Produkte und Leistungen ist bei relevanten Entscheidungen die *Business Judgment Rule* (§ 93 Abs. 1 S. 2 AktG) anzuwenden. Entscheidungen sollten typischerweise auf Analyse und Auswertung von Daten und Informationen beruhen, die Begründung von Entscheidungen sollte auf einer nachvollziehbaren, logischen Argumentation und auf verlässlichen Datenquellen aufbauen.[33]

Als effektive und effiziente Vorgehensweise bewährt sich, zunächst funktional / aufbauorganisationsbezogen die Unternehmensbereiche oder (moderner) ablauforganisationsbezogen die Prozesse des Unternehmens zu definieren.

Sodann sind diesen Bereichen bzw. Prozessen die dort relevanten Anforderungen aus Rechtsgebieten und aber auch sonstigen verpflichtenden Anforderungen (aus anderen Quellen) zuzuordnen.[34]

Hierzu steht im Anhang zu DIN ISO 37301:2021 (CMS) im Abschnitt A.4.5 – *Compliance-Verpflichtungen:*

„Die Organisation sollte die Compliance-Verpflichtungen nach Abteilungen, Funktionen und verschiedenen Arten von Aktivitäten der Organisation identifizieren, um zu bestimmen, wer von diesen Compliance-Verpflichtungen betroffen ist.“

Hinweis: Verpflichtende Anforderungen ergeben sich aus vielfältigen (!) externen (z. B. Gesetze, Rechtsprechung, behördliche Auflagen etc.) und internen (z. B. aus Richtlinien (Policies), Verträgen, Anweisungen) Quellen.

Risikobasierter Ansatz:

Da es sehr schwierig ist, stets sämtliche Compliance-Verpflichtungen zu identifizieren und zu erfüllen, sollte auf Basis einer Compliance-Risiko-Analyse mit den risikobehaftetsten Verpflichtungen

---

[32] Vgl. *BVerfG*, Beschluss vom 08.08.1978 – 2 BvL 8/77 und *Detterbeck*, Allgemeines Verwaltungsrecht mit Verwaltungsprozessrecht, 18. Auflage, 2020, S. 105 f. sowie *Scherer*, *Ketelsen*, Technical Product Compliance, Bavarian Journal of Applied Sciences, 2022.

[33] In „0.2 Grundsätze des Qualitätsmanagements“ wird „faktengestützte Entscheidungsfindung;“ als einer von sieben Grundsätzen genannt, vgl. DIN EN ISO 9001:2025-09, 0.2 QMP 6 „Faktengestütze Entscheidungsfindung“, aber auch A.6.2 „Qualitätsziele und Planung zu deren Erreichung“.

[34] Vgl. *Scherer,* Compliance-Managementsystem nach DIN ISO 37301:2021 erfolgreich implementieren, integrieren, auditieren, zertifizieren, 1. Aufl., Herausgeber DIN, DIN Media-Verlag, 2022, Kapitel Einleitung – *„Das Richtige richtig tun“* und Kapitel 8.1 – *Digitalisierung und Anreicherung der diversen Führungs-, Kern- und Unterstützungsprozesse*.

begonnen werden.

„Risikobasiert“ heißt in diesem Kontext aber nicht, dass weniger wichtige Verpflichtungen dauerhaft unbeachtet bleiben dürfen.

Dazu heißt es in der DIN ISO 37301:2021 im Kapitel A.4.5 – *Compliance-Verpflichtungen*:

*„Ein **risikobasierter Ansatz** sollte gewählt werden, d. h. Organisationen sollten mit der Identifizierung der wichtigsten Compliance-Verpflichtung, die für das Geschäft relevant ist, beginnen und sich anschließend auf alle anderen Compliance-Verpflichtungen konzentrieren (Pareto-Prinzip).“*

Hinweis: Der Ausdruck Pareto-Prinzip, also die „80 / 20-Regel“, ist – obwohl dies so im Standard steht – falsch. Bei Compliance dürfen auch weniger wichtige Themen nicht ausgespart werden.

3.7 Rechtskataster

Für das Thema *Compliance in Bezug auf die Leistung (Produkte, Dienstleistungen etc.)* sollte eine Art (prozess-) themenbezogenes (Einkauf, Vertrieb etc.) „Rechtskataster“ angelegt und gepflegt werden. Dieses stellt den für diesen Bereich maßgeblichen rechtlichen Rahmen dar.

Dazu heißt es in der DIN ISO 37301:2021 im Abschnitt A.4.5 – *Compliance-Verpflichtungen*:

„Wo zweckmäßig, sollte die Organisation ein einzelnes Dokument (wie etwa ein Register oder Protokoll) erstellen und aufrechterhalten, das alle Compliance-Verpflichtungen der Organisation aufführt und über einen Prozess zur regelmäßigen Aktualisierung des Dokuments verfügen.“

Schon bei der Zuordnung von Rechtsgebieten zu den Bereichen / Prozessen zeigt sich, dass manche Rechtsgebiete / Anforderungen (z. B. IT-Sicherheits-Anforderungen) in nahezu jedem Bereich / Prozess vorkommen, andere Anforderungen/Rechtsthemen schwerpunktmäßig jedoch in nur einzelnen Bereichen / Prozessen (z. B. Antikorruption häufig in Einkauf und Vertrieb).

Ein Dokument, eine Excel etc. mit unzähligen rechtlichen Anforderungen genügt aber nicht, um die Erfüllung der rechtlichen Anforderungen sicherzustellen:

Diese Regelungen müssen noch in eine verständliche Sprache und Prozessschritte zur Erfüllung der Anforderungen übersetzt und in Aufbau- und Ablauforganisation und die Köpfe der jeweiligen (Compliance-) Risk-Owner implementiert werden:

Implementierung von Aktivitäten zur Erfüllung der Anforderungen in die Prozesse

Wenn nun feststeht oder entschieden wurde, welche *konkrete* Anforderung (priorisiert) zu erfüllen ist, müssen noch Prozessschritte, Aktivitäts- und Kompetenzvermittlungs-Maßnahmen abgeleitet, in die Prozesse implementiert und zur Wirksamkeit gebracht werden, um sicherzustellen, dass die Anforderung messbar, revisionssicher und dokumentiert erfüllt wird / wurde.

Dies gelingt mit führenden Workflows, Automation, digitalen Prozess-Zwillingen[35] und Unternehmenskultur, Awareness, Kompetenz (Wissen, Verstehen, Können und Wollen) sowie einem wirksamen „Lines of defense"-Steuerungs- und Überwachungssystem.

Bei der Zuordnung von verpflichtenden Anforderungen zu Prozessen sollte wieder an die sogenannte *RACI-Methode* gedacht werden: Die jeweiligen Prozessanwender, die „Responsibles" (R) sollten die Anforderungen in ihrem Prozess kennen und beachten. Die „Prozesseigner", also die für Aktualität, Konformität etc. Verantwortlichen („Accountables" (A), z. B. Leitung Vertrieb für die Vertriebsprozesse) sollten mit Unterstützung durch die Fachspezialisten („Consulted" (C)) dafür sorgen, dass der jeweilige Prozess stets allen relevanten Anforderungen entspricht. Die relevanten Stakeholder („Informed") sollten stets über Prozess-Änderungen informiert werden.

3.8 Risiko-Bewertung bzgl. verpflichtender Anforderungen

Eine Nichteinhaltung der verpflichtenden Anforderungen kann je nach Ausmaß – z. B. bei Gefahr für Leib und Leben Dritter oder Umweltgefährdung – für die Organisation und die verantwortlichen Organe und / oder Mitarbeiter zu existenzvernichtender Wirkung, Freiheitsstrafen, Geldstrafen und Schadensersatzforderungen einschließlich Reputationsverlust führen.[36]

Die Risiko-Bewertung hat auch für Compliance-Risiken (!) *angemessen*, also nach anerkanntem Stand von Wissenschaft und Praxis, zu erfolgen: Quantifizierung, Aggregation und die Betrachtung der Risikotragfähigkeit ist inzwischen Gesetz, Stand der Technik und wird in vielen Standards gefordert.[37]

3.9 Risiko-Steuerung bzgl. verpflichtender Anforderungen

Zur Risiko-Steuerung ist es notwendig, die Ausrichtung und Compliance-Kultur des Unternehmens über regelmäßige Schulungen und den „Tone-from-the-Top" den Mitarbeitern kontinuierlich ins Bewusstsein zu rücken, damit diese stets im Sinne des CMS handeln.[38]

Die Implementierung und Wirksamkeit von Aktivitäten zur Sicherstellung der Verpflichtungen in die

---

[35] Vgl. *Rieger, Scherer*, Der Digitale Prozess-Zwilling im Gesundheitswesen – auch als Beitrag zu Nachhaltigkeit (ESG, CSR), systemische Existenzsicherung (Resilienz) und Governance in: Journal für Medizin- und Gesundheitsrecht, Ausgabe 2-2021 (zum kostenlosen Download auf scherer-grc.net/publikationen).

[36] Vgl. *BAG*, Urteil vom 29.04.2021, Az.: 8 AZR 246/20 und United States District Court for the District of Columbia, Consent Decree Civil Action Nos. 1:20-cv-2564, 1:20-cv-2565, 14. September 2020, S. 41 f., online verfügbar unter: https://www.epa.gov/enforcement/daimler-ag-and-mercedes-benz-usa-llc-clean-air-act-civil-settlement-consent-decree (zuletzt geprüft: 25.09.2021).

[37] Vgl. hierzu *Scherer, Seehaus*, Pflicht zu Governance mit Risikofrüherkennung, Resilienz und Transformation als Kardinalpflicht von Organen und Führungskräften, ZInsO 31/2025, S. 1515-1538, 31.07.2025, in Deutsch, zum kostenlosen Download unter: https://www.risknet.de/elibrary/paper/pflicht-zu-governance-mit-risikofrueherkennung-resilienz-und-transformation-als-kardinalpflicht-von-organen-und-fuehrungskraeften/ *Scherer, Seehaus*, Managerhaftung, D&O-Versicherung und Risikofrüherkennung im Lichte aktueller Rechtsprechung, 2026, zum kostenlosen Download auf Risknet.de und *Scherer*, *Romeike*, *Gursky*, Mehr Risikokompetenz für eine Neue Welt in: *Journal für Medizin- und Gesundheitsrecht*, Ausgabe, 3-2021, S. 159 – 165.

[38] Vgl. *Scherer*, *Fruth* (Hrsg.), Governance-Management Band II (Standard & Audit), 1. Auflage, 2015, S. 130.

Prozesse ist wesentlich effektiver als lediglich Richtlinien und dergleichen zu erlassen.

Durch das „Lines-of-Defense"-Modell mit Compliance, Risikomanagement, IKS und Revision[39], die Einrichtung von (KI-gestützten) Monitoring-Prozessen[40], neutralen Ombudspersonen[41] sollte die Überwachung und Reifegradbewertung gewährleistet werden. Dadurch werden auch Risiken der Abweichungen von Vorgaben identifiziert und Aktivitäten zu Verbesserungen des Prozesses und der Komponenten abgeleitet.

4. „Risiko- und chancenbasiertes Denken": Angemessene Darstellung der zwingenden Anforderungen an das Risikomanagement beim Qualitätsmanagement: Fehlanzeige

Im Entwurf der neuen DIN ISO 9001 ist in der Einleitung, an diversen weiteren Stellen im Standard und im informativen Anhang A von *„risikobasiertem Denken"* die Rede:

„Einleitung
0.4 Zusammenhang mit anderen Managementsystemnormen
In diesem Dokument kommt die harmonisierte Struktur zur Anwendung, um eine Angleichung der ISO-Managementsystemnormen zu erreichen. Dieses Dokument ermöglicht einer Organisation die Anwendung des prozessorientierten Ansatzes in Verbindung mit dem PDCA-Zyklus, ***dem risikobasierten Denken und dem chancenbasierten Denken****, um ihr Qualitätsmanagementsystem an die Anforderungen anderer Managementsystemnormen anzugleichen oder es zu integrieren. (…)."*[42]

„Anhang A (informativ) (…)
A.6.1.2 ***Risikobasiertes Denken***
(…) Dieses Dokument legt Anforderungen an die Organisation dafür fest, dass sie ihren Kontext versteht (siehe 4.1) und die Risiken als Grundlage zur Planung (siehe 6.1) bestimmt. Dies verkörpert die Anwendung von risikobasiertem Denken bei der Planung und Umsetzung von Prozessen des Qualitätsmanagementsystems (siehe 4.4) (…).
Obwohl in 6.1 festgelegt ist, dass die Organisation Maßnahmen zum Umgang mit Risiken planen muss, ***sind keine formellen Methoden für das Risikomanagement oder ein dokumentierter Risikomanagementprozess erforderlich. Organisationen können entscheiden, ob sie eine ausgedehntere Vorgehensweise für das Risikomanagement, als von diesem Dokument gefordert wird, entwickeln möchten,*** *z.B. durch die Anwendung anderer Leitlinien oder Normen.*
ANMERKUNG 1 Siehe ISO 31000 [9] für Leitlinien zum Risikomanagement.
ANMERKUNG 2 Siehe ISO 31073 [10] für Begriffe im Risikomanagement. (…)"[43]

---

[39] Vgl. ebenda, S. 188 f.
[40] Vgl. *Noack*, Künstliche Intelligenz und die Unternehmensleitung in: Festschrift für Christine Windbichler zum 70. Geburtstag am 8. Dezember 2020, S. 956.
[41] Vgl. *Scherer*, *Fruth* (Hrsg.), Governance-Management, Band I, 2015, S. 186.
[42] Vgl. DIN EN ISO 9001 Qualitätsmanagementsysteme – Anforderungen (ISO / DIS 9001:2025-9), Abschnitt Einleitung.
[43] Vgl. DIN EN ISO 9001 Qualitätsmanagementsysteme – Anforderungen (ISO / DIS 9001:2025-9), Anhang.

Das „*risikobasierte Denken*“ bleibt auch in der neuen Fassung der DIN ISO 9001 unverständlich, rechtlich bedenklich und praxisfern.

Der allgemein – auch von Rechtsprechung und Wirtschaftsprüfern anerkannte – „*risikobasierte Ansatz“* bedeutet, dass auf Basis einer angemessenen Risikoanalyse die wichtigen Dinge zuerst / priorisiert zu erledigen sind.

Dabei sind die Steuerung von Risiken für Leib und Leben, persönliche Sanktionen Beschäftigter und finanzielle Einbußen, die die Risikotragfähigkeit der Organisation beeinträchtigen würden, an erster Stelle. Die bloße Forderung nach „*risikobasiertem Denken“ ohne auch risikobasiertes Entscheiden und entsprechendes Handeln* mit zu inkludieren, ist den Anerkannten Regeln der Technik beim Management von Risiken fremd.

Wenn „*Maßnahmen zum Umgang mit Risiken und Chancen*“ gefordert werden, muss dies auch Compliance-Risiken umfassen.

Es gibt keinen sachlichen Grund, ein so großes Feld mit potenziell existenzbedrohenden Risiken auszuklammern. Dies wäre zudem pflichtwidrig im Sinne der §§ 43 GmbHG, 93, 116 AktG, vgl. LG München („Neubürger-Urteil“).

Geradezu paradox und juristisch irreführend ist die Forderung nach risikobasiertem Denken und der Planung von Maßnahmen zum Umgang mit Risiken einerseits und andererseits die unzutreffende und „gefährliche“ Aussage:

„*Obwohl in 6.1 festgelegt ist, dass die Organisation Maßnahmen zum Umgang mit Risiken planen muss,* ***sind keine formellen Methoden für das Risikomanagement oder ein dokumentierter Risikomanagementprozess erforderlich. Organisationen können entscheiden, ob sie eine ausgedehntere Vorgehensweise für das Risikomanagement, als von diesem Dokument gefordert wird, entwickeln möchten,*** (…)“.

Diese Aussage ist wohl der Angst vor der Konkurrenz der Risikomanagement-Standards oder vor der für das Qualitätsmanagement völlig neuen Materie, insbesondere wenn man Compliance-Risiken mit einbezieht, geschuldet.[44]

Wenn aber Kundenzufriedenheit das Ziel der ISO 9001 ist, dann sollte der Geschäftspartner des Kunden sehr wohl ein angemessenes Risiko- (und Business Continuity-) Managementsystem haben, um sicherzustellen, dass er nicht in eine Betriebsablaufunterbrechung oder Krise gerät, die die Erfüllung der vertraglichen Pflichten gefährden würde: Versorgungssicherheit zu gewährleisten ist

[44] Vgl. DIN EN ISO 9001, Qualitätsmanagementsysteme – Anforderungen (ISO/DIS 9001:2025), Abschnitt 6.1 „Maßnahmen zum Umgang mit Risiken und Chancen“, S. 21.

eines der Hauptziele eines modernen Supplier Screening und unverzichtbare Voraussetzung für Kundenzufriedenheit.

Maßnahmen zum Umgang mit Risiken sind – entgegen dem Wortlaut der neuen Norm - stets angemessen und gemäß rechtlicher Anforderungen zu planen. Hier hätte ein klarstellender Hinweis erfolgen müssen, dass es zahlreiche zwingende Anforderungen an Risikofrüherkennung und -management aus Gesetzen[45], Rechtsprechung, Anerkannten Regeln der Technik etc. gibt, die verpflichtend sind.

Beispiel für eine aus dem Qualitätsmanagement entlehnte und an die alte Version der FMEA[46] angelehnte, in einem Standardwerk[47] für Qualitätsmanagement vorgeschlagene – unzutreffende - Methode der Risikobewertung:

Sinngemäß wird folgender Sachverhalt angenommen:

Das Risiko eines möglichen Produktfehlers, der sich wohl nur jährlich (Rubrik Exposition (E) selten: (E) Wert 1 (von 0,5 bis 10)) mit einer geringen Wahrscheinlichkeit (W) („wenig geläufig“: (W) Wert 3) mit der zweithöchsten Schwere (S): „äußerst ernsthaft“ „z.B. ein Toter“ (S) Wert 15 (von 1 – 40) auswirkt, wurde identifiziert und bewertet. Nach der (falschen) Bewertung, dass ein Toter nicht gleich zur höchsten Schadensausmaßbewertung führen soll und als mathematisches Produkt mit 3 Faktoren ergäbe sich im Beispiel die (falsch) bewertete Risiko-Prioritätszahl (RPZ) mit einem Wert 45 (1 x 3 x 15) mit der Handlungsempfehlung von lediglich: „*Vorsicht geboten*“, nicht jedoch die nächsten Stufen: „*Maßnahmen erforderlich*“ (70 bis 200) oder gar: „*sofortige Verbesserung unerlässlich*“ (200 bis 400) oder höchste Stufe (ab 400): Sofort handeln!“

– Sollte sich das so dokumentierte Risiko realisieren, würden Staatsanwaltschaft und Gericht nicht von fahrlässiger, sondern von vorsätzlicher Tötung ausgehen: Es wurde ja ein Todesfall für möglich gehalten und es wurde sich – aufgrund falscher Bewertung – sich damit abgefunden: Das ist Eventualvorsatz: Dolus Eventualis.

5. „Prozessorientierter Ansatz“: Angemessene Darstellung der Anforderungen an Prozessmanagement im Qualitätsmanagement: Fehlanzeige

Im Entwurf der neuen DIN ISO 9001 nimmt im Text des Standards der „prozessorientierte Ansatz“ besonderen Raum ein:

„Einleitung

[45] Vgl. § 1 StaRUG.
[46] Fehler-Möglichkeits- und Einfluss-Analyse.
[47] Vgl. die 3. Auflage eines von DIN im Beuth-Verlag herausgegebenes im Übrigen sehr gutes Werk zu: Erfolgreiches Qualitätsmanagement nach DIN EN ISO 9001:2015, in dem eine der FMEA entlehnte Methode aus dem QM für Risikobewertung herangezogen wurde. In den neueren Auflagen findet sich dieses Beispiel so nicht mehr. Auch der VDMA hat inzwischen seine FMEA-Methode korrigiert.

0.3 Prozessorientierter Ansatz

0.3.1 Allgemeines

Dieses Dokument fördert die Umsetzung eines prozessorientierten Ansatzes bei der Einrichtung, Verwirklichung und Verbesserung der Wirksamkeit eines Qualitätsmanagementsystems, um die Kundenzufriedenheit durch Erfüllen der Kundenanforderungen zu erhöhen. Spezifische Anforderungen, die für die Umsetzung eines prozessorientierten Ansatzes von wesentlicher Bedeutung sind, sind in 4.4 enthalten. (…)

Der prozessorientierte Ansatz umfasst die systematische Bestimmung und Steuerung von Prozessen und deren Wechselwirkungen, so dass die beabsichtigten Ergebnisse mit der Qualitätspolitik und der strategischen Ausrichtung der Organisation übereinstimmen. ***Die Steuerung der Prozesse*** *und des Systems als Ganzes* ***kann durch den PDCA-Zyklus (siehe 0.3.2) erreicht werden, dessen Hauptaugenmerk auf risikobasiertem Denken (siehe A.6.1.2) und chancenbasiertem Denken (siehe A.6.1.3) liegt, um Chancen zu nutzen und unerwünschte Ergebnisse zu verhindern.*** *(…).“*[48]

„5 Führung

5.1 Führung und Verpflichtung 5.1.1 Allgemeines

Die oberste Leitung muss in Bezug auf das Qualitätsmanagementsystem Führung und Verpflichtung zeigen, indem sie:

a) sicherstellt, dass die Qualitätspolitik und die Qualitätsziele festgelegt und mit der strategischen Ausrichtung der Organisation vereinbar sind;

b) **sicherstellt, dass die Anforderungen des Qualitätsmanagementsystems in die Geschäftsprozesse der Organisation integriert werden***; (…).*[49]

Obwohl Prozessmanagement in der Praxis tatsächlich noch häufig lediglich als Annex zum Qualitätsmanagement von Qualitätsmanagement-Beauftragten betreut wird, ist die Wichtigkeit aufgrund Digitalisierung und KI-Unterstützung erheblich gestiegen und wäre es wert, seitens der Leitung mit höherer Bedeutung ausgestattet zu werden.

Dabei sind die Anforderungen an Prozesse und Prozessmanagement in erster Linie juristisch festgelegt.[50] Lediglich mit „riskobasiertem Denken“ ohne Rechtsicherheit gewährleistendes Prozess-Compliancemanagement sind „unerwünschte Ergebnisse“ i.S.v. Compliance-Verstößen nicht „zu verhindern“.

Der bereits oben erwähnte Transrapid-Fall[51] zeigte, dass bei entsprechenden Versäumnissen im Prozessmanagement nicht nur einzelne direkte Verursacher, sondern gleich mehrere Verantwortliche, insbesondere auch einfache Vorgesetzte, im Fokus von Ermittlungen, Anklagen und Verurteilungen stehen.

---

[48] Vgl. DIN EN ISO 9001, Qualitätsmanagementsysteme – Anforderungen (ISO/DIS 9001:2025), Abschnitt Einleitung.
[49] Vgl. DIN EN ISO 9001, Qualitätsmanagementsysteme – Anforderungen (ISO/DIS 9001:2025), Abschnitt 5.1.1.
[50] Vgl. z.B. die „Transrapid-Entscheidung“ und Anforderungen an eine rechtssichere Organisation in *Scherer*, Nachhaltige Führung und Überwachung von Organisationen (Governance) nach DIN ISO 37000, Erfolgreich umsetzen, auditieren und reporten, Herausgeber DIN, DIN Media Verlag, 2025, Kapitel 4.2, S. 74.
[51] Vgl. *Werner*, Transrapid-Unfall 2006: Bewährungsstrafen für zwei Fahrdienstleiter, Mitteldeutsche Zeitung, 03.03.2011, abrufbar unter https://www.mz.de/panorama/transrapid-unfall-2006-bewahrungsstrafen-fur-zwei-fahrdienstleiter-2268246.

Jedes der ca. 20 (Prozess-)Themenfelder einer Organisation stellt ein Hauptprozessfeld als Bestandteil der unternehmensweiten Prozesslandschaft dar (z. B. der Vertriebsprozess, der mit den übrigen Prozessfeldern vernetzt sein sollte). [52]

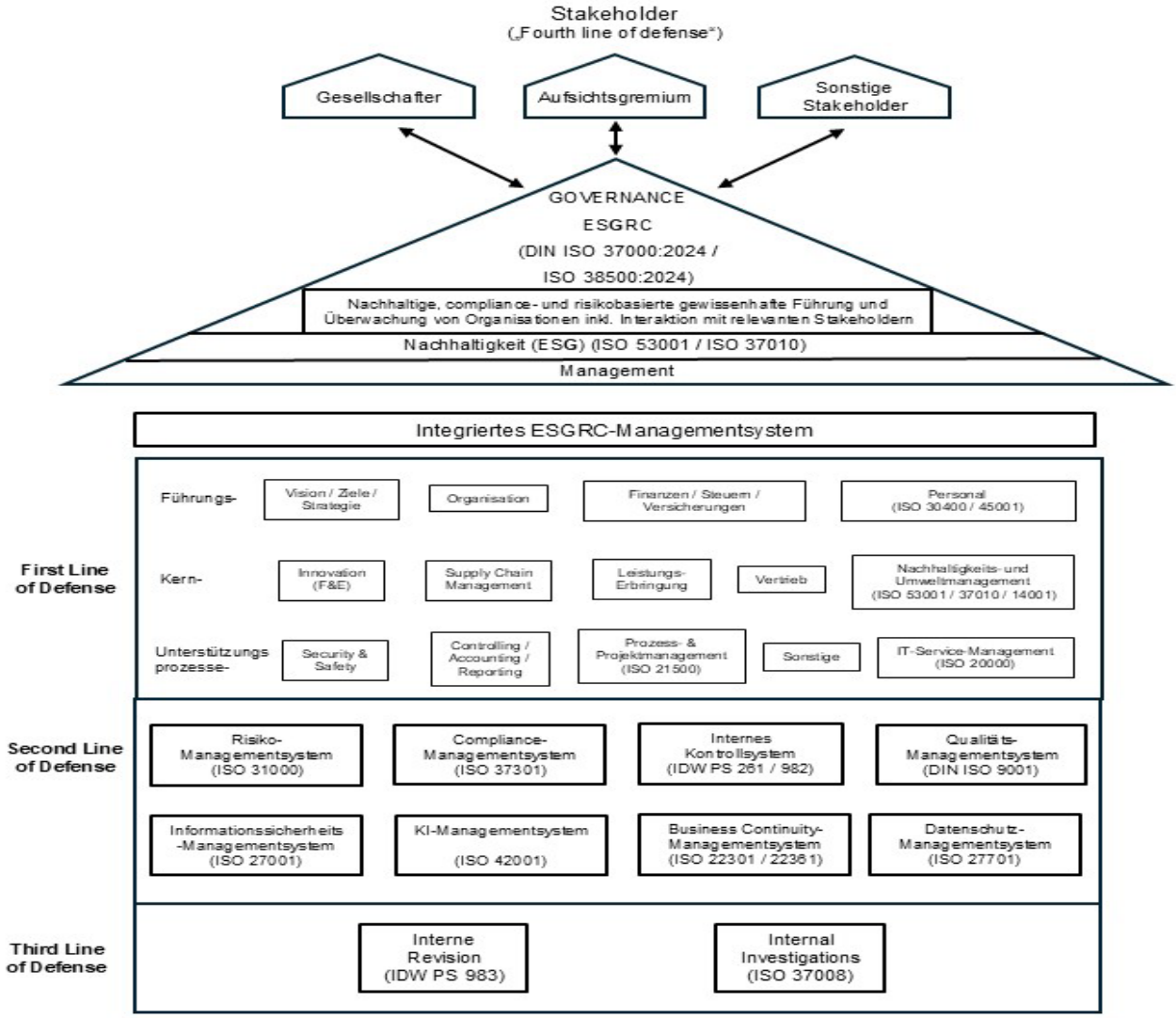

Abbildung 1: Das „ESGRC-Haus"[53]

Jedes Hauptprozessfeld kann als Flussdiagramm (in veralteter Form sogar noch in Excel, word oder Powerpoint anzutreffen, nach Stand der Technik modelliert in BPMN 2.0) mit zugehöriger Beschreibung von input und output, Prozessschritten, Prozess- Ausführungsverantwortlichen, -Eignern bzw. -Verantwortlichen (vgl. RACI), mitgeltenden Dokumenten, Compliance-Anforderungen und Risiken, Kontrollpunkten etc. dargestellt werden und besteht aus weiteren Unter- / Teil-Prozessfeldern (z. B.

[52] Vgl. *Scherer*, Nachhaltige Führung und Überwachung von Organisationen (Governance) nach DIN ISO 37000, Erfolgreich umsetzen, auditieren und reporten, Herausgeber DIN, DIN Media Verlag, 2025, Kapitel 8.1.
[53] Vgl. *Scherer*, Nachhaltige Führung und Überwachung von Organisationen (Governance) nach DIN ISO 37000, Erfolgreich umsetzen, auditieren und reporten, Herausgeber DIN, DIN Media Verlag, 2025, S. 19.

beim Hauptprozess „Vertrieb“: Marketing / Akquise, Anfragemanagement, Kundenanlage etc. bis hin zu After Sales, Produktbeobachtung und Reklamationsmanagement).

Der prozessorientierte Ansatz wird von aktuellen Standards, nicht nur der neuen ISO 9001, sondern z.B. auch von der DIN ISO 37000 (Governance) gefordert.[54]

Prozesse sind Ablaufbeschreibungen. Die angemessene Detailtiefe einer Prozessbeschreibung hängt beispielsweise davon ab, wie oft ein Prozess ausgeführt wird und wer bzw. wie viele Personen daran beteiligt sind. Dabei können vier Prozessebenen unterschieden werden:[55]

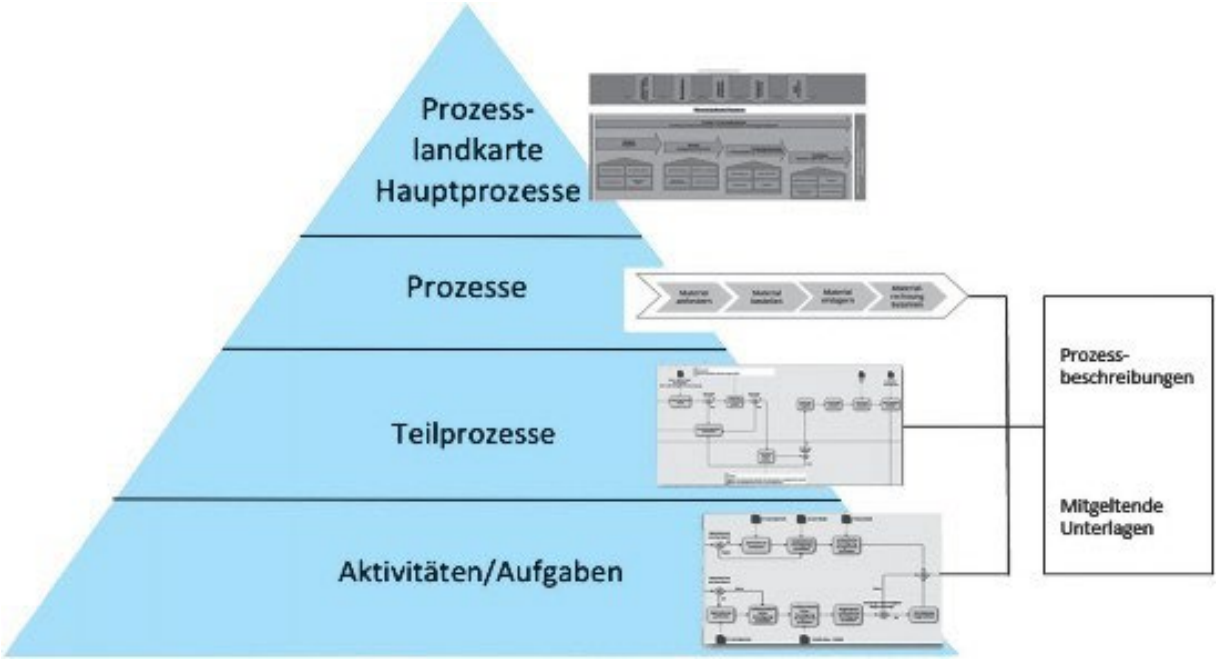

Abbildung 2: Prozessmodell mit vier Ebenen[56]

Eine wesentliche Voraussetzung, um das Digitalisierungspotenzial von Abläufen zu erkennen, ist zunächst die Betrachtung des derzeitigen Ist-Zustandes. Da Prozesse häufig nicht oder nicht aktuell dokumentiert sind, sind diese zunächst zu modellieren.

[54] Vgl. *Scherer*, Nachhaltige Führung und Überwachung von Organisationen (Governance) nach DIN ISO 37000, Erfolgreich umsetzen, auditieren und reporten, Herausgeber DIN, DIN Media Verlag, 2025 Kapitel „Einleitung“ und Kapitel 8.1 „Exkurs: Umsetzung von Governance-Maßnahmen und Projekten und mit Governance-Komponenten angereicherte, gelebte Prozesse“.
[55] Vgl. *Feddern*, Digitale Transformation prozessorientiert umsetzen, 2019, S. 24.
[56] Quelle: Eigene Darstellung in Anlehnung an *Feddern*, Digitale Transformation prozessorientiert umsetzen, 2019, S. 24.

Für eine „echte digitale Transformation“ sind Integrierte Human-Workflow-Managementsysteme notwendig[57].

Die nachfolgende Abbildung zeigt sinnbildlich, wie ein standardisierter Kernprozess (nach ISO 9001:2015) in Anlehnung an BPMN 2.0 modelliert werden könnte. Der Abschnitt ganz unten, die Swimlane „IT-Systeme“, soll zeigen, dass bei Durchführung der einzelnen Prozessschritte diverse IT-Systeme zum Einsatz kommen. Die Abbildung zeigt auch, dass neben vielfältigen, speziellen IT-Systemen (SAP/Office/Dokumentationssystem/CRM etc.) unterschiedlichste Komponenten der Digitalisierung bzw. der KI sowie der Mensch an unterschiedlichen Stellen in der Prozesslandschaft zum Einsatz kommen können.

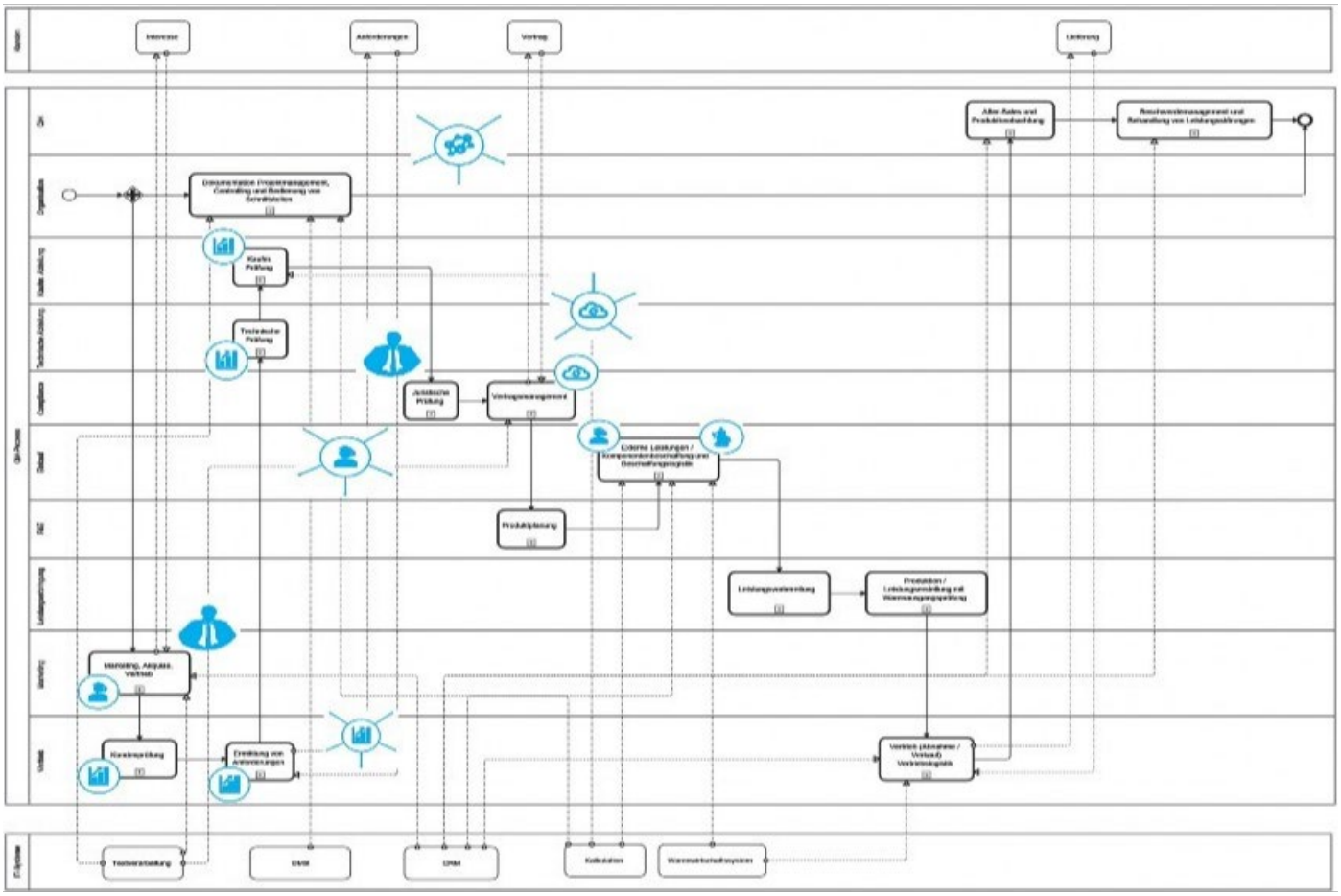

Abbildung 3: Mensch und Komponenten der Digitalisierung in der Prozesslandschaft[58]

[57] Vgl. *Scherer*, Compliance-Managementsystem nach DIN ISO 37301:2021 – erfolgreich implementieren, integrieren, auditieren, zertifizieren, DIN Media, 2022, Kapitel 8.1: Exkurs: Umsetzung von Governance-Maßnahmen und Projekten und mit Governance-Komponenten angereicherte, gelebte Prozesse.
[58] Eigene Darstellung aus *Scherer*, Compliance-Managementsystem nach DIN ISO 37301:2021 – erfolgreich implementieren, integrieren, auditieren, zertifizieren, DIN Media, 2022, Kapitel Einleitung.

Künstliche Intelligenz wird wohl auch das Business Process Modelling (BPM) grundlegend verändern. Dies wird auch eine Anpassung des BPM-Modeller-Tool-Marktes zur Folge haben. Diese Entwicklungen sind kontinuierlich im Auge zu behalten.

Die meisten unternehmerischen Aktivitäten laufen als Prozesse ab. Auch künftig werden diese zum Teil noch von Menschen ausgeführt. Auch, um auf der Prozessebene das Richtige richtig zu tun, ist für das Management und die Mitarbeiter die angemessene Einstellung auf der kognitiven und emotionalen Ebene enorm wichtig: *Tone from the top*, Kultur, Awareness, Kompetenzen, Motivation u. v. m.. Erst dann kann eine Ablauforganisation „wirksam“ („gelebt“) werden.

Die DIN ISO 9001 betont, dass ein QM-System aus miteinander in Wechselwirkung stehenden Prozessen besteht, die zusammen ein Prozesssystem bilden. Diese Norm fördert ausdrücklich die Anwendung eines prozessorientierten Ansatzes, einschließlich Entwicklung, Verwirklichung und Verbesserung der Wirksamkeit eines Qualitätsmanagementsystems, um die Kundenzufriedenheit durch Erfüllung der Anforderungen zu erhöhen.[59] Der neue Standard verlangt ausdrücklich die Berücksichtigung von (Compliance-) Risiken und Chancen in Bezug auf Prozesse und Ergebnisse. Maßnahmen zum Umgang mit Risiken und Chancen sind in die Prozesse des Qualitätsmanagementsystems zu integrieren und dort wirksam umzusetzen.

[59] Sinngemäß aus DIN EN ISO 9001 (aktuelle Fassung), Vorwort und Abschnitt 0.1/0.2 zum prozessorientierten Qualitätsmanagementsystem.

Check: Der Reifegrad des Prozessmanagements: Wo steckt Ihre Organisation gerade und wo sollte sie (zeitnah) hin?

Evolutionsstufe 1: Der Prozess existiert noch nicht bzw. nur im Kopf

Eventuell existieren „gute Prozessabläufe“ in den Köpfen von „alten Hasen“, sind jedoch nicht dokumentiert. Gefahr: Was passiert, wenn diese Beschäftigten weg (krank oder in Rente) sind?

Evolutionsstufe 2: Aus dem Kopf ins Dokument (analog oder digital)

Wenn Wissen und Know-how (aktuell) dokumentiert sind, könnte es im Idealfall auch von anderen (Kollegen / Nachfolgern / Anzulernende) verwendet werden. In der Praxis finden sich hier Versionen in Papier und analogen Aktenordnern oder aber auch PDF-Dokumente, Excel-Dateien und vieles andere mehr…

Evolutionsstufe 3: Prozessschritte visualisieren und alle relevanten Informationen den einzelnen Prozessschritten zuordnen

Visualisierte Prozessschritte mit verfügbaren relevanten Informationen „vor Ort“ helfen, zu „wissen“ und zu „verstehen“. Sehr häufig fehlen in der Praxis an den jeweiligen Prozess-Schritten noch Komponenten, die die Erfüllung der Anforderungen aus QM, Risk, Compliance, IKS oder Revision sicherstellen.

Evolutionsstufe 4: Anreicherung der Prozesse mit Risk-, IKS- oder Compliance-Elementen.

Die Prozesse sind mit den Aktivitäten zur Erfüllung der Anforderungen aus QM, Risk, Compliance, IKS oder Revision anzureichern. Die Erfahrung zeigt, dass Prozesse, die von den betroffenen Prozess-Schritt-Eignern (R und A) modelliert wurden, eher akzeptiert und gelebt werden. Digitale Prozesshandbücher in Excel, Word und sonstige „tote“ Dokumente sind jedoch nicht mehr „Stand der Technik“. „Stand der Technik“ im Prozessmanagement und z. B. auch im IT-Sicherheitsgesetz, im Datenschutz oder im Arbeitsschutz sind stattdessen (teil-) automatisierte, führende Prozesse:

Evolutionsstufe 5: Modellierung von Prozessen mit Business Process Management (BPM 2.0) und Verknüpfung mit „Repository“ (Datenraum)

Die Modellierung von Prozessen in BPMN 2.0 ist Stand der Technik. Die vielen auf dem Markt konkurrierenden Modeller-Tools[60] ermöglichen, dass die Accountables ganz ohne teure IT-Spezialisten ihre Prozesse jederzeit selbst aktualisieren können.

Nun müssten auch noch bei jedem Prozessschritt die richtigen mitgeltenden Dokumente (Musterformulare, Checklisten etc.) zur Verfügung stehen. Dafür sorgt nun eine digitale Vernetzung aller Aktivitäten zur Erfüllung der in den Elementen von Gesetzen, Normen, Standards, Richtlinien enthaltenen Anforderungen mit einem sogenannten „Repository".

Evolutionsstufe 6: Den modellierten Prozess durch Teil-Automatisierung und Anreicherung mit *Künstlicher Intelligenz* „zum Leben erwecken"[61]

Aber: Der lediglich modellierte / gezeichnete Prozess lebt noch nicht: In der nächsten Stufe werden Abläufe voll oder zum Teil automatisiert oder die Workflows führen die Beschäftigten durch ihre Aufgaben. KI-Agenten unterstützen und führen Routinen eigenständig aus.

Evolutionsstufe 7: „Integriertes Kombi-Managementsystem on demand" mit Compliance, QM, Risk, IKS, Informationssicherheits-Managementsystem etc.:

Für die Geschäftsleitung und Beschäftigte bedeuten viele parallele „Insel-Welten" eine nicht lebbare (wirksame) und teure Bürokratie

Die Umrüstung eines vorhandenen Managementsystems auf ein interdisziplinäres, Integriertes GRC-Managementsystem ist einfach und erzielt hohe Wertbeiträge.

Nicht nur einzelne Prozesse oder Teile von Insel-Managementsystemen, sondern das komplette Integrierte GRC-Managementsystem läuft automatisiert bzw. über Human Workflows geführt.

Der „dogmatische Ansatz" zur Ermöglichung eines digitalisierten Integrierten Managementsystems besteht in der Konzentration auf den *End-to-end-Prozess*: In die diversen Teilprozesse werden Aktivitäten zur Erfüllung der relevanten Anforderungen diverser Gesetze, Standards etc. aus diversen Querschnittsthemen wie z. B. Compliance, Qualitätsmanagement, Risk, Nachhaltigkeit etc. integriert, vgl. hierzu sogleich Punkt 6.

[60] ADONIS, iGrafx, Intellior, ARIS, Signavio, Visio, GBTEC, Camunda, Bizagi, Confluence, ProcessMaker, Omni-Tracker etc..
[61] Vgl. *Rieger, Scherer,* Der Digitale Prozess-Zwilling im Gesundheitswesen, JMG 2/2021, S. 83– 91, zum kostenlosen Download auf Scherer-grc.net/Publikationen

6. Darstellung der Anforderungen an ein Integriertes ESGRC-Managementsystem: Fehlanzeige

Die neue Version der DIN ISO 9001 lehnt sich stärker an die Harmonized Structure an, um die Integration von „Managementsysteminseln“ zu ermöglichen, erklärt aber nicht, wie dies konkret auszugestalten ist.

Dies ermöglicht es einigen Beratern, Auditoren, Zertifizierern etc. nach wie vor, ihre aufwändigen und nicht steuerbaren zahlreichen Insel-Managementsysteme zu „verkaufen“.

„Einleitung (…)

0.4 Zusammenhang mit anderen Managementsystemnormen

***In diesem Dokument kommt die harmonisierte Struktur zur Anwendung**, um eine Angleichung der ISO-Managementsystemnormen zu erreichen. **Dieses Dokument ermöglicht einer Organisation** die Anwendung des prozessorientierten Ansatzes in Verbindung mit dem PDCA-Zyklus, dem risikobasierten Denken und dem chancenbasierten Denken, um **ihr Qualitätsmanagementsystem an die Anforderungen anderer Managementsystemnormen anzugleichen oder es zu integrieren**. (…) Dieses Dokument enthält keine spezifischen Anforderungen für andere Managementsysteme, z.B. zum Umweltmanagement, Arbeitsschutzmanagement oder Finanzmanagement. (…)“*

Eine Organisation, die nach und nach das eine oder andere „Managementsystem“ einführt, produziert damit fast zwangsläufig Insellösungen, die nicht gelebt werden. Die Daten dieser Systeme (sofern sie überhaupt eingepflegt werden) stehen aufgrund fehlender Homogenität unter anderem den Möglichkeiten moderner, digitaler Datenanalyse nicht angemessen zur Verfügung.

Aktuelle Umfeldentwicklungen und zwingende rechtliche Anforderungen verlangen einen integrierten Ansatz, der die Komplexität und die Kostenbelastung für Organisationen auflöst.

Die Umrüstung eines Qualitäts-Managementsystems auf ein integriertes ESGRC-Managementsystem ist einfach und erzielt hohe Wertbeiträge.

Dabei wird man erkennen, dass die vielen diversen Standards für Managementsysteme jeweils in redundante oder analoge Elemente aufgegliedert werden können.

Geschätzt kommt es hierbei zu rund 70% Überschneidungen: So wird beispielsweise die Interested parties-Analyse nur ein einziges Mal ausgeführt. Aufgrund der Redundanzen in anderen Standards ist sie sowohl verwendbar für Qualitäts-Management, Risiko-Management, Compliance-Management, Business Continuity-Management etc..

Da nahezu alle Standards (ISO, COSO, IDW, DIIR usw.) für Managementsysteme auf einen einheitlichen, zum großen Teil redundanten Aufbau und Inhalt komprimiert werden können, sollte die Praxis die Gelegenheit nutzen, das vorhandene (Qualitäts-) Managementsystem auf ein

integriertes, ganzheitliches Führungssystem umzurüsten, das nicht nur einzelne Themenfelder, sondern die Anforderungen der Grundsätze ordnungsgemäßer Organisationsführung und -überwachung, also der Governance, insgesamt einzuhalten ermöglicht. Der Aufwand ist überschaubar:

Beispiel: **Die Anreicherung eines Prozessablaufs, mit Aktivitäten zur Erfüllung von Anforderungen diverser Regulierung und Standards als Beispiel für „Integriertes Managementsystem“**: **Beispielhaft** wird hier der *Angebotsmanagement-Prozess* als Teil des Vertriebsprozesses untersucht. Der Einbau von Risiko- oder Compliance-Komponenten in vorhandene Prozessabläufe lässt sich sehr schön am Beispiel der Kundenprüfung (KYC: Know Your Customer) darstellen, nämlich Identitäts-, Bonitäts- und Legalitätsprüfung (zum Beispiel Außenwirtschaftskontrolle und Geldwäsche beim Kunden) als einer der ersten Prozessschritte im Angebotsprozess. Dieser Schritt reduziert nicht nur Gefahren und vermeidet persönliche Haftung, sondern zeigt auch, dass Governance mit Risiko- und Compliance-Management hilft, viel Geld zu sparen.

Die Identitätsprüfung klärt die Frage, wer tatsächlich Vertragspartner ist (Hans Maier (Schreibweise mit ai, ei, ay, ey …?) oder Hans Maier Bau-GmbH oder Hans Maier Holding GmbH & Co. KG oder Hans Maier Bauleistungen AG). Häufig wird nur mit „Fa. Maier“ oder gar mittels unterschiedlicher Briefbögen kommuniziert. Ansprüche gegen den Vertragspartner wären wegen der ungeklärten Frage, wer tatsächlich Partner ist, kaum durchsetzbar.

Auch der „wirtschaftlich Berechtigte“ muss in den aktuellen Zeiten mit Embargi etc. geprüft werden.

Die Vertretungsmacht der für den Vertragspartner handelnden Person kann an dieser Stelle gleichermaßen geklärt werden. Es ist zu prüfen, ob die für den Vertragspartner handelnde Person überhaupt ausreichend legitimiert ist, etwa durch Prokura, Handlungs- oder Einzelvollmacht.

Die Bonitätsprüfung zeigt, ob die Wahrscheinlichkeit, auch an das Entgelt zu kommen, hoch genug ist, um überhaupt ein Angebot stellen zu wollen; zum Beispiel, wenn zwar die Zahlen der anfragenden GmbH gut sind, diese GmbH aber Teil eines kriselnden Konzerns ist (Infektionsgefahr).

Die Legalitätsprüfung (Außenwirtschaftsrecht, Exportkontrolle, Geldwäschegesetz etc.) gibt Auskunft, ob ein Angebot überhaupt abgegeben werden darf.

Auch Nachhaltigkeitseigenschaften und Beachtung von Menschenrechten spielen bei Vertragspartnerprüfungen häufig eine Rolle.

Ebenso z.B. bei IT-Governance-Themen die Frage, wo unsere Daten landen und ob IT-Services einfach abschaltbar sind (Digitale Souveränität).

In der Praxis fehlen entsprechende Prüfschritte häufig völlig, werden oft nur bei Neukunden durchgeführt oder befinden sich im Prozessablauf an ungünstiger Stelle, zum Beispiel erst nach Durchführung von technischer und kaufmännischer Prüfung und den Vertragsverhandlungen, wodurch viel Zeit und Geld verschwendet wird.

Bezüglich einer Bonitäts-, Identitäts- und Legalitätsprüfung des Kunden hat also der erstmalige Einbau oder die Versetzung des Prozessschrittes an die erste Stelle im Angebotsprozess finanzrisiko- und haftungsreduzierende Wirkung.

Es ist beispielsweise zu verhindern, dass durch einen wesentlichen Forderungsausfall eines Kunden mit schlechter Bonität die Organisation im Bestand gefährdet wird. Außerdem würde bei einem wesentlichen finanziellen Verlust wegen fehlender Bonitätsprüfung der Geschäftsführer der Gesellschaft wegen Organisationspflichtverletzung persönlich haften: Das Unterlassen einer Bonitätsprüfung wurde bereits in der Rechtsprechung als Pflichtverstoß der Geschäftsführung angesehen, und demzufolge wurde ein Schadensersatzanspruch aus § 43 Abs. 2 GmbHG gegen den Geschäftsführer konstruiert.[62]

Durch die Ergänzung des Prozesses um den Schritt „Kundenprüfung“ (Identitäts-, Bonitäts- und Legalitätsprüfung, etwa Außenwirtschaftsrecht und Geldwäschegesetz) an der optimalen Stelle, nämlich gleich nachdem dem Kunden, der ein Angebot nachgefragt hat, der Eingang seines Schreibens bestätigt wurde, ergeben sich positive Auswirkungen.

Bei negativer Auskunft wird eine zeit- und geldaufwändige technische und kaufmännische Prüfung nebst Vertragsvorbereitung nicht durchgeführt, es werden also mehrere tausend Euro eingespart. Stattdessen wird aufgrund der freien Kapazität das Angebot für einen „positiven“ Kunden, der möglicherweise aufgrund der im früheren Normalfall langsamen Bearbeitung zum Wettbewerber abgewandert wäre, zeitnah bearbeitet und erfolgreich umgesetzt.

Hinweis: Der KYC-Teilprozess erfüllt zugleich Anforderungen aus dem Qualitäts-, Risiko-, Compliance-, Nachhaltigkeits-Management, aus dem Internen Kontrollsystem uvm. Ebenso aus den einschlägigen Regulierungsanforderungen, den Anerkannten Regeln der Technik und Standards.

Das sind viele Fliegen, die mit einer Klappe geschlagen werden; das ist ein gelebtes Integriertes Managementsystem.

[62] Vgl. zur persönlichen Haftung des Geschäftsführers wegen Unterlassens einer Bonitätsprüfung etwa die Rechtsprechung zu § 43 Abs. 2 GmbHG (Neubürger-Entscheidung des LG München, weitere Nachweise im Literaturverzeichnis).

Und entsprechend geht es weiter, nämlich Analyse und Optimierung aller wichtigen weiteren Prozesse durch Anreicherung mit Schritten zur Erfüllung der Anforderungen aus Risiko- und Compliance-Management etc..

7. Hinweis auf potenzielle Haftungs-Risikoerhöhung durch Führung von Qualitäts-Managementsystem-Zertifikaten[63]: Fehlanzeige

Der Trend zu Zertifizierungen ist ungebrochen und soll die Nachweisführung der Einhaltung von Standards ermöglichen, sowie zu Wettbewerbsvorteilen gegenüber nicht zertifizierten Organisationen führen.

Zahlen der ISO 9001-Zertifikate in Deutschland und weltweit gemäß ISO-Survey 9 / 2025:

Zitat: „(…) *Ende 2024 gab es weltweit 1.474.118 Zertifikate nach ISO 9001 an 2.321.640 Standorten. Im letzten Jahr wurden 837.052 Zertifikate gemeldet, daher scheint sich die Qualität der Daten deutlich verbessert zu haben.*

Deutschland ist laut dieser Auswertung von 41.760 auf 45.983 Zertifikate an 104.193 Standorten gestiegen, was eine Steigerung von 10 % bzw. sogar 64% bedeutet. Wie oben angesprochen ist diese Zahl jedoch nicht verifizierbar bzw. repräsentativ.

Ranking ISO 9001 weltweit

China liegt mit 651.851 Zertifikaten, wie auch in den letzten Jahren, auf Platz 1. Diese Daten werden als zuverlässig gewertet, da sie in diesem Jahr von der offiziellen Regierungsbehörde stammen. Danach liegt Italien mit 101.426 Zertifikaten auf dem 2. Platz. Auf Platz 3 liegt Indien mit 95.007 Zertifikaten, gefolgt von Korea mit 51.647 Zertifikaten. Deutschland kommt auf Platz 5. Dahinter Spanien, Japan, Großbritannien inkl. Nordirland und Amerika auf Platz 9 vor Brasilien.“[64]

Ein funktionierendes QM-System kann auch zur Verteidigung in Vertragsstreitigkeiten oder behördlichen oder gerichtlichen Verfahren von erheblicher Bedeutung sein.

---

[63] Vgl. *Scherer, Friedrich*, „Risikoerhöhung durch Zertifizierung von Qualitäts und Riskmanagementsystemen“, in: ZfAW 10. Jahrgang (2007), S. 15 – 19, zum kostenlosen Download unter: https://www.schererrecht.de/images/Veroeffentlichungen/Risikoerhoehung_durch_Zertifizierung/Beitrag_ZfAW.pdf.

[64] Vgl. *Gertz*, ISO Survey 2024 – DakkS verweigert Datentransfer, Qualitätsmanager aktuell vom 21.11.2025, zum kostenlosen Download unter: https://www.qm-aktuell.com/zeitschriften/iso-survey-2024-dakks-verweigert-datentransfer/ Zitat: *„Ende September ist der ISO Survey erschienen, der die ISO-Zertifikatszahlen sowie die Anzahl der Standorte mit Zertifikat bis 31.12.2024 zusammenfasst. (…) Die unter der deutschen Akkreditierungsstelle (DAkkS) akkreditierten Zertifizierungsstellen konnten bzw. wollten ihre Daten für die ISO-Umfrage dem IAF CertSearch nicht zur Verfügung stellen. Auch wenn einige andere deutsche Zertifizierungsstellen ihre Daten direkt an CertSearch übermittelt haben, spiegeln die Ergebnisse daher nicht den vollständigen deutschen Markt wider.“*

Beispiel (Landgericht Verden):

Eine Mandantin des Verfassers wurde wegen eines angeblichen Produktionsfehlers verklagt. Nach der Rechtsprechung des BGH ist ein Nachweis eines sogenannten „Ausreißers“ nötig, um sich zu entlasten, da keine Haftung für zufällige Produktionsfehler besteht. Durch die dokumentierten und zertifizierten Prüfmaßnahmen als Bestandteil des wirksamen Qualitäts-Managementsystems konnte das Unternehmen belegen, dass mit hoher Qualität produziert wurde und keine Auffälligkeiten in der Serie bestanden. Der mögliche Mangel war somit ein unschädlicher Ausreißer. Ergebnis: Abweisung der Klage – wirtschaftlicher Vorteil in sechsstelliger Höhe.

Gleichzeitig entsteht ein neues Risiko:

Oftmals werden Erst-, Überwachungs- oder Rezertifizierungs-Audits nicht risikobasiert, also auf Basis einer angemessenen Analyse, wo die echten Probleme liegen, durchgeführt. Viele Organisationen bringen sich nur kurzfristig in einen „zertifizierungsfähigen Zustand“ und lassen nach Erhalt des Zertifikats die notwendige Pflege des QM-Systems schleifen.

Hinzu kommt: Mit dem Führen eines Zertifikats können sich rechtlich höhere Anforderungen ergeben. Werden diese unterschritten, drohen erhebliche Folgen für Unternehmen und ggf. die Unternehmensleitung.

Ein Zertifikat bestätigt lediglich die Einführung eines Systems nach einem Standard – keine Garantie für „100 % Qualität“ oder „Null Risiko“.

Solange die Zertifizierung rein intern bleibt, erhöht sie die Haftung nicht automatisch.

Problematisch wird es jedoch, wenn Unternehmen mit dem Zertifikat werben (Website, Verpackung, Briefkopf etc.) oder das Vorhalten eines zertifizierten Managementsystems Vertragsbestandteil wird.

Nach § 276 Abs. 1 BGB steigt der Sorgfaltsmaßstab bei werblich herausgestellter Zertifizierung. Ein Unternehmen, das öffentlich mit seinem Zertifikat wirbt, muss höhere Sorgfalt nachweisen als ein nicht zertifiziertes.

Wird öffentlich mit Zertifikaten geworben, müssen die entsprechenden Prozesse tatsächlich durchgeführt werden sein, da andernfalls die Haftung im Rahmen der Sachmängelhaftung (§ 434 ff. BGB) droht.

Dies kann sogar der Fall sein, ohne dass konkrete Qualitätsmängel nachweisbar sind, wenn die Nichtanwendung des beworbenen QM-Systems bereits einen Sachmangel darstellt.

Öffentliche Aussagen, die den Eindruck einer zugesicherten Eigenschaft erzeugen, können als Garantie ausgelegt werden – mit erheblichen Folgen der verschuldensunabhängigen Haftung und Beweislastumkehr zugunsten des Garantie-Begünstigten.

Daher sollten Formulierungen wie: „*Unser zertifiziertes QM-System sorgt für die Fehlerfreiheit unserer Produkte*“ oder Ähnliches vermieden werden.

Wenn in Qualitätssicherungs-Vereinbarungen oder sonstigen Verträgen die Anwendung eines zertifizierten QM-Systems vereinbart wurde, droht bei entstandenen Schäden und Schwachstellen im System u.U. Schadensersatz wegen Pflichtverletzung (§§ 280, 281 BGB), ein außerordentliches Kündigungsrecht (§ 314 BGB), mögliche Vertragsstrafen und pauschalierte Schadenszahlungen.[65]

Ein Managementsystem, das nicht gelebt wird, kann zu erheblichen Sanktionen bis zur persönlichen Haftung der Geschäftsführung und weiterer verantwortlicher Führungskräfte reichen.

8. Darstellung der neuen Anforderungen an Managementsysteme, Manager, Beschäftigte, Auditoren, Managementsystem- und Personenzertifizierungen: Fehlanzeige

Ein Mittel, um die angemessene fachliche Kompetenz für QM-Beauftragte und QM-Auditoren nachzuweisen, sind entsprechende Personenzertifizierungen.

Personenzertifizierungen für QM-Auditoren dienen dem formalen Nachweis, dass eine Person über die erforderliche fachliche, methodische und persönliche Kompetenz verfügt, um Qualitätsmanagementsysteme wie DIN EN ISO 9001 professionell zu auditieren.

Grundlage für die inhaltliche Ausrichtung solcher Zertifizierungen ist vor allem die ***ISO 19011***[66], die Auditprinzipien, den Ablauf von Audits sowie ***in Abschnitt 7 Empfehlungen zu den Kompetenzanforderungen an Auditoren*** *enthält, darunter Kenntnisse der ISO 9001, Branchenwissen, sichere Beherrschung von Auditmethoden sowie persönliche Eigenschaften wie Integrität und Kommunikationsfähigkeit.*

Die *ISO 19011 wird derzeit grundlegend überarbeitet*:

„(…) Zu erwartende Änderungen der neuen ISO 19011:

Remote-Audits und digitale Technologien, Erweiterung durch das Hinzufügen von Remote-Audit-Methoden in Bezug auf ISO/EC TS 17012:2024 (Leitfaden für Remote-Audits), Anleitungen zur Planung und Durchführung von Remote-Audits und Hinweise zu Technologien, Anleitung für virtuelle Standorte, Harmonisierung mit anderen ISO-Normen, Vereinheitlichung von Begriffen und Definitionen, ***Orientierung an der Harmonized Structure (HS)*** *der ISO-Managementsysteme,* ***Stärkung des risikobasierten Ansatzes, Gezielte Priorisierung von***

[65] Vgl. *Scherer, Friedrich*, Risikoerhöhung durch Zertifizierung von Qualitäts- und Riskmanagementsystemen“, ZfAW 10. Jahrgang (2007), S. 15 – 19, zum kostenlosen Download unter: https://www.schererrecht.de/images/Veroeffentlichungen/Risikoerhoehung_durch_Zertifizierung/Beitrag_ZfAW.pdf.

[66] Vgl. DIN EN ISO 19011 Leitfaden zur Auditierung von Managementsystemen (ISO 19011:2018), Abschnitt 7 „Kompetenz und Bewertung von Auditoren“.

***Hochrisikobereichen bei der Auditplanung und -durchführung**, Stärkere Beachtung von Themen wie Klimarisiko und Digitale Systeme, Redaktionelle Überarbeitung der Norm*

Wie geht es weiter mit der Revision?

Aktuell wird unter internationalen Experten ein Entwurf des Leitfadens ISO DIS 19011:2025:3 diskutiert. Der deutsche Text dieses Entwurfs liegt ebenfalls als DIN EN ISO 19011:2025-04 aus dem April 2025 vor. ***Mit der finalen Version des Leitfadens kann voraussichtlich Anfang 2026 gerechnet werden****. (…)"* [67]

Die ***ISO / IEC 17024 beschreibt die Anforderungen an Zertifizierungsstellen, die Personen zertifizieren**,* sie regelt die Entwicklung von Zertifizierungsschemata, Prüfverfahren, Unabhängigkeit, Validität der Bewertung sowie die regelmäßige Rezertifizierung und dient damit als normative Grundlage für externe Auditorenzertifikate.[68]

Für Auditoren, die im Auftrag akkreditierter Zertifizierungsstellen (DakkS) Managementsysteme auditieren, gelten ergänzend die Anforderungen der ISO / IEC 17021-Serie, insbesondere ISO/IEC 17021-1 zur Struktur und Unparteilichkeit von Zertifizierungsstellen und **ISO / IEC 17021-3 zu den spezifischen Kompetenzanforderungen an Auditoren von Qualitäts-Managementsystemen**, die festlegen, wie Qualifikation, Erfahrung und Auditpraxis systematisch bewertet und überwacht werden müssen.[69] Während ISO 19011 selbst kein formales Zertifizierungs- oder Akkreditierungssystem vorgibt, entsteht durch die Kombination dieser Normen ein konsistenter Rahmen, der sicherstellt, dass QM-Auditoren ihre Aufgaben fachlich fundiert, unabhängig und nachvollziehbar erfüllen, wobei formale Personenzertifizierungen insbesondere im externen Auditkontext eine wichtige Rolle spielen. Diese für QM-Beauftragte und QM-Auditoren vorgesehenen Prüfungen und Zertifizierungen sollten nun im Lichte der kommenden ISO 9001:2026 vor allem auch die oben angesprochenen Themen ***Prozess-, Governance- Risiko- und Compliance-Management-Kompetenzen*** umfassen, um angemessen und risikobasiert zu sein.

9. Fazit

Die neue DIN ISO 9001 bietet viele Chancen bei kritischer und korrekter, aber auch erhebliche Risiken bei unreflektierter Anwendung ohne GRC-Kompetenzen.

Die aktuelle Transformation in allen Bereichen erfordert auch ein grundlegendes Umdenken im Qualitätsmanagement.

---

[67] Vgl. *Gut Cert*, Revision des Auditleitfadens ISO 19011, 24.9.2025 zum Download im Internet.
[68] Vgl. DIN EN ISO/IEC 17024 Konformitätsbewertung – Allgemeine Anforderungen an Stellen, die Personen zertifizieren (ISO/IEC 17024:2012).
[69] Vgl. DIN EN ISO/IEC 17021-3 Konformitätsbewertung – Anforderungen für die Auditierung und Zertifizierung von Qualitätsmanagementsystemen (ISO/IEC 17021-3:2017).

Prof. Dr. jur. Josef Scherer

Prof. Dr. jur. Josef Scherer ist Rechtsanwalt und Consulter, Gründer (2012) und Leiter des Internationalen Instituts für Governance, Management, Risk- und Compliance-Management und Leiter der Stabsstelle ESGRC der Technischen Hochschule Deggendorf (THD). Seit 1996 ist er Professor für Unternehmensrecht (Compliance), Risiko- und Krisenmanagement, Sanierungs- und Insolvenzrecht an der THD. Zuvor arbeitete er als Staatsanwalt an diversen Landgerichten und als Richter am Landgericht in einer Zivilkammer.

Neben seiner Tätigkeit als Seniorpartner der auf Wirtschaftsrecht und Governance, Risiko- und Compliance-Management (GRC) spezialisierten Kanzlei Prof. Dr. Scherer & Partner mbB erstellt er wissenschaftliche Rechtsgutachten und agiert als Richter in Schiedsgerichtsverfahren.

Von 2001 bis 2024 arbeitete er auch als Insolvenzverwalter in verschiedenen Amtsgerichtsbezirken.

Prof. Dr. Scherer ist in diversen Unternehmen und Körperschaften als Compliance-Ombudsperson oder externer Compliance-Beauftragter tätig. Er ist gesuchter Referent bei Managementschulungen in namhaften Unternehmen sowie im Weiterbildungsprogramm des Senders BR-alpha und der Virtuellen Hochschule Bayern (VHB).

In Kooperation mit dem TÜV konzipierte er als Studiengangsleiter den seit über 15 Jahren renommierten und akkreditierten berufsbegleitenden Masterstudiengang Risikomanagement und Compliance-Management an der THD und leitet den Zertifikatskurs „Nachhaltigkeit und GRC“ sowie den berufsbegleitenden Bachelor „Nachhaltigkeit, Governance und Digitalisierung“.

Seit 2015 ist Prof. Dr. Scherer Mitglied des Beirats des Instituts für Risikomanagement und Regulierung (FIRM), Frankfurt (www.firm.fm).

Seit 2016 ist er Mitglied des DIN-Normenausschusses Dienstleistungen (Arbeitsausschuss Personalmanagement NA 159-01-19 AA) zur Erarbeitung von ISO/DIN-Standards im Personalmanagement und seit 2017 Mitglied der Delegation ISO TC 309 Governance of Organizations (Arbeitsausschuss Governance und Compliance NA 175-00-01-AA) zur Erarbeitung von ISO/DIN-Standards im Bereich Unternehmensführung und -überwachung (Corporate Governance), Compliance und Whistleblowing.

Seit 2016 ist Prof. Dr. Scherer Fachlicher Leiter der „User Group Nachhaltige Unternehmensführung (ESG/CSR/GRC) und Compliance“ der Energieforen Leipzig, seit 2018 Mitglied der Arbeitsgruppe 252.07 von Austrian Standards International zur Erarbeitung einer ÖNORM D 4900 ff. (Risiko-Managementsystem-Standards) und seit 2021 Mitglied im DICO (Deutsches Institut für Compliance e. V.).

Seine Forschungs- und Tätigkeitsschwerpunkte liegen auf den Gebieten Nachhaltigkeit (ESG), Integrierte ESGRC-Managementsysteme, Managerenthaftung, Governance-, Risiko- und Compliance-Management, Integrierte Human Workflow Managementsysteme und Digitalisierung sowie Vertrags-, Produkthaftungs-, Sanierungs- und Insolvenzrecht, Arbeitsrecht und Personalmanagement.

Prof. Dr. Scherer ist auf dem Gebiet angewandte Forschung und Lösungen / Tools im Bereich ESG/GRC, Digitalisierung und integrierte Workflow-Managementsysteme Gesellschafter-Geschäftsführer der Governance-Solutions GmbH und Aufsichtsrat in diversen Unternehmen und Stiftungen.

www.scherer-grc.net

Linkedin: Prof. Dr. Josef Scherer
Der Verfasser publiziert über LinkedIn regelmäßig aktuelle Urteile, Gesetze, Artikel etc. zu ESGRC-Themen.