DIN

Josef Scherer

Compliance-Managementsystem nach DIN ISO 37301:2021

erfolgreich implementieren, integrieren, auditieren, zertifizieren

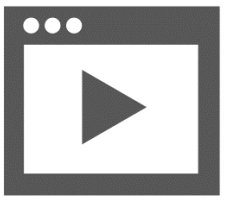
Mit digitalen Arbeitshilfen
erhältlich über die Beuth-Mediathek

Beuth

Compliance-Managementsystem nach DIN ISO 37301:2021

Mehr zu diesem Titel

… finden Sie in der Beuth-Mediathek



Zu vielen neuen Publikationen bietet der Beuth Verlag nützliches Zusatzmaterial im Internet an, das Ihnen kostenlos bereitgestellt wird.
Art und Umfang des Zusatzmaterials – seien es Checklisten, Excel-Hilfen, Audiodateien etc. – sind jeweils abgestimmt auf die individuellen Besonderheiten der Primär-Publikationen.

Für den erstmaligen Zugriff auf die Beuth-Mediathek müssen Sie sich einmalig kostenlos registrieren. Zum Freischalten des Zusatzmaterials für diese Publikation gehen Sie bitte ins Internet unter

www.beuth-mediathek.de

und geben Sie den folgenden Media-Code in das Feld „Media-Code eingeben und registrieren“ ein:

M309077664

Sie erhalten Ihren Nutzernamen und das Passwort per E-Mail und können damit nach dem Log-in über „Meine Inhalte“ auf alle für Sie freigeschalteten Zusatzmaterialien zugreifen.

Der Media-Code muss nur bei der ersten Freischaltung der Publikation eingegeben werden. Jeder weitere Zugriff erfolgt über das Log-In.

Wir freuen uns auf Ihren Besuch in der Beuth-Mediathek.

Ihr Beuth Verlag

Compliance-Managementsystem
nach DIN ISO 37301:2021

(Leerseite)

DIN

Prof. Dr. Josef Scherer

Compliance-Managementsystem nach DIN ISO 37301

erfolgreich implementieren, integrieren, auditieren, zertifizieren

1. Auflage 2022

Herausgeber:

DIN Deutsches Institut für Normung e. V.

Beuth Verlag GmbH · Berlin · Wien · Zürich

Herausgeber: DIN Deutsches Institut für Normung e. V.

Berlin · Wien · Zürich
Am DIN-Platz
Burggrafenstraße 6
10787 Berlin

Telefon: +49 30 2601-0
Telefax: +49 30 2601-1260
Internet: www.beuth.de
E-Mail: kundenservice@beuth.de

Titelbild: © WrightStudio, Nutzung unter Lizenz von adobestock.com
Satz: Beuth Verlag GmbH, Berlin
Druck: L&C, Kraków

Gedruckt auf säurefreiem, alterungsbeständigem Papier nach DIN EN ISO 9706

ISBN 978-3-410-30907-9
ISBN (E-Book) 978-3-410-30908-6

Autorenporträt

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

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

Seit 2001 arbeitet er auch als Insolvenzverwalter in verschiedenen Amtsgerichtsbezirken.

Prof. Dr. Scherer fungiert in diversen Unternehmen/Körperschaften als Compliance-Ombudsperson sowie externer Compliance-Beauftragter/Qualitätsmanagement-Beauftragter und 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 12 Jahren renommierten und akkreditierten berufsbegleitenden Masterstudiengang Risikomanagement und Compliancemanagement 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 Beirates 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 Manager-Enthaftung, Governance-, Risiko- und Compliancemanagement, Nachhaltigkeit (ESG/CSR), Integrierte Human Workflow Managementsysteme und Digitalisierung sowie Vertrags-, Produkthaftungs-, Sanierungs- und Insolvenzrecht, Arbeitsrecht und Personalmanagement.

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

www.scherer-grc.net

(Leerseite)

Vorwort

Dieses Praktiker-Handbuch für die Implementierung, Integration, Auditierung und Zertifizierung eines Compliance-Managementsystems gemäß DIN ISO 37301:2021-11 ist ein Leitfaden / eine „Gebrauchsanweisung“ für alle Führungskräfte in einer Organisation, die in ihrem Arbeitsumfeld Verantwortung für eine rechtssichere (Ablauf-)Organisation haben.

Es zeigt auch, wie sich Compliance-, Qualitäts-, Risiko- und weitere Managementsysteme integrieren lassen.

Das Buch eignet sich für Einsteiger, bietet aber auch für Profis noch viele praxisrelevante Tipps zur Vertiefung und Erhöhung des Reifegrades des eigenen Systems.

Zahlreiche Arbeitshilfen machen die theoretischen Ausführungen eines Standards „griffig“.

Es werden hier nicht nur Vorgaben der DIN-ISO-Norm aufgezeigt, sondern auch von Gesetzen und aus der Rechtsprechung, die u. U. über den Vorgaben der Norm stehen.

Ein weiterer Vorteil, den die Implementierung eines Compliance-Managementsystems mit sich bringt, besteht darin, dass Compliance einen ganz wesentlichen Bestandteil der ökonomischen, sozialen und ökologischen Nachhaltigkeit (ESG/CSR) darstellt.

Deggendorf, April 2022

Prof. Dr. Josef Scherer

Hinweis: Dieses Buch erhebt weder einen Anspruch auf Vollständigkeit noch garantiert es die Wiedergabe sämtlicher rechtlicher Vorgaben zu jeder Zeit. Es ersetzt keine fachmännische (Rechts-)Beratung. Vielmehr spiegelt es die Auffassung des Verfassers zum Zeitpunkt der Veröffentlichung wider.

Im Sinne einer besseren Lesbarkeit des Dokuments wurde die männliche Form von personenbezogenen Bezeichnungen gewählt. Dies impliziert keinesfalls eine Benachteiligung eines anderen Geschlechts. Jegliches Geschlecht möge sich von den Inhalten gleichermaßen angesprochen fühlen.

(Leerseite)

Inhaltsverzeichnis

Gebrauchsanweisung

Diese Gebrauchsanweisung hilft, diesen Leitfaden für das Compliance-Managementsystem individuell passend zu verwenden:

Inhaltsverzeichnis

Das Inhaltsverzeichnis ist angelehnt an die „Harmonized Structure“ der ISO (vgl. dazu Kapitel 1), ebenso an DIN ISO 37301 (Compliance), ISO 9001 (QM), ISO/IEC 27001 (Informationssicherheit), ISO 14001 (Umwelt) etc.

Dadurch wird die Möglichkeit der Integration diverser Managementsysteme erleichtert.

Jedes Kapitel beinhaltet folgende Abschnitte:

I) Summary

Das Summary gibt einem kurzen Überblick über das zu behandelnde Kapitel.

II) Normtext (DIN ISO 37301)

Abdruck des Original-Normtextes.

III) Anhang zum Normtext (DIN ISO 37301)

Abdruck der Original-Anhänge zum Normtext.

IV) Was bedeutet der Normtext?

Hier wird der Text des Standards verständlich interpretiert.

V) Interpretation der Anforderungen im Lichte von Gesetzgebung, Rechtsprechung und Wissenschaft

Dieser Abschnitt vertieft das Wissen für fortgeschrittene Anwender durch Hinweise auf einschlägige Gesetze, Rechtsprechung und Ansichten aus der Wissenschaft.

VI) Kompetenzziele

Dieses Kapitel geht der Frage nach: Was sollten Mitarbeiter bezüglich des Normabschnittes wissen?

VII) Checkfragen

Hier findet sich eine Auswahl von Audit-Checkfragen.

VIII) Anmerkungen eines Lead-Auditors

Hier kommentiert ein erfahrener Lead-Auditor, worauf bei einer Zertifizierung besonders geachtet wird.

IX) Hinweis auf Hilfsmittel

Die Hinweise sind chronologisch angeordnet. Sie können wie eine Art Checkliste für eine „Toolbox“ benutzt werden. Zum Teil werden Ihnen die Hilfsmittel in der Mediathek zur Verfügung gestellt. Diese Hilfsmittel sind entsprechend gekennzeichnet: 

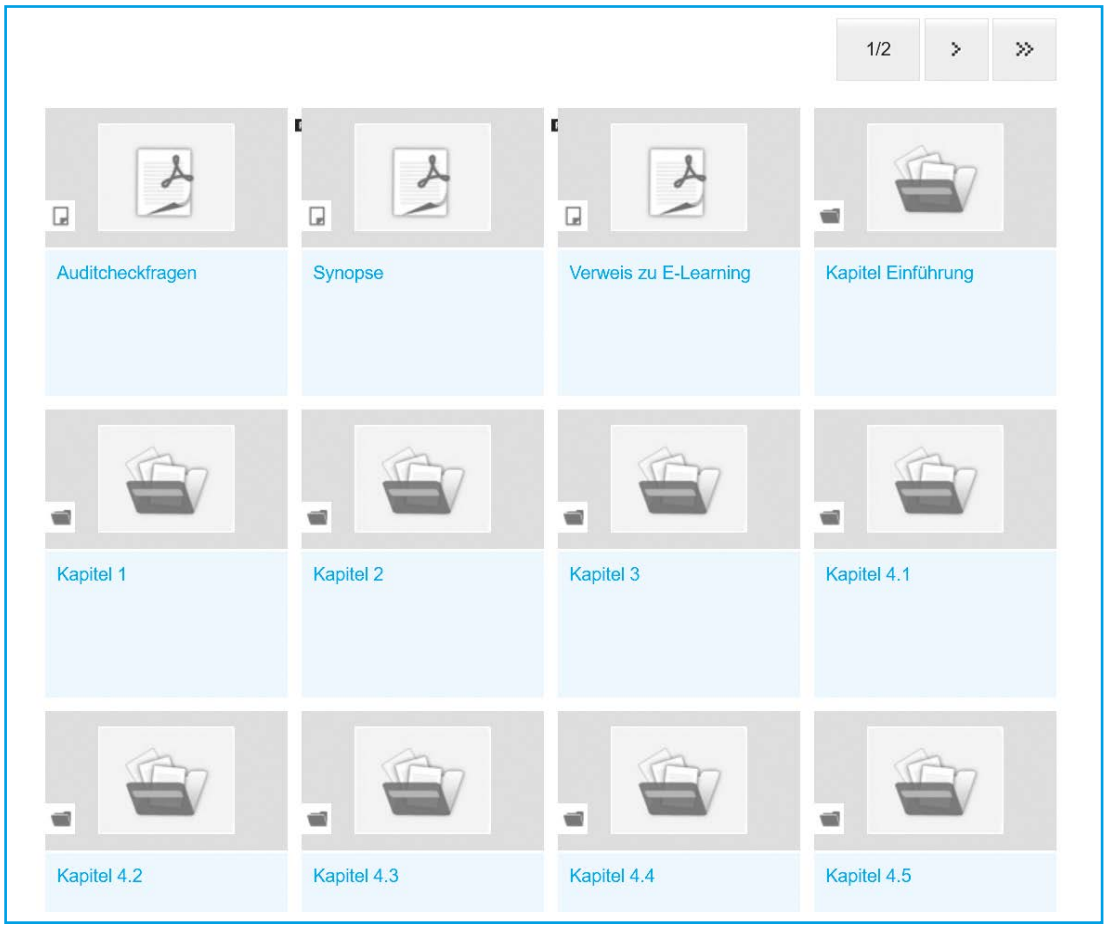


Bild 1: In der Beuth-Mediathek finden Sie hilfreiche Dateien zum Buch

In der Beuth-Mediathek finden sich zum Beispiel:

- **Anlagen**

  Hier sind z. B. wichtige Urteile in Auszügen oder vertiefende Artikel gesammelt.

- **E-Learning**

  Hier finden sich Hinweise (auch auf frei zugängliche) E-Learning Programme.

- **Tools, Prozessabläufe und Synopsen**

  Hier wird eine Auswahl gängiger Werkzeuge und Methoden dargestellt.

  Prozessabläufe helfen, eigene Prozesse zu modellieren und zu digitalisieren. Die vorgestellten Muster können angepasst und für eigene Zwecke verwendet werden. Dies ermöglicht den Aufbau eines Integrierten Managementsystems.

  Die Synopsen zeigen, dass andere Compliance-Standards und auch Standards anderer Managementsystem-Inseln (Qualitäts-, Risiko-, Informationssicherheits-, Umwelt-, Energieeffizienz- und andere -Managementsysteme) oft das Gleiche fordern.

Für die Richtigkeit, Aktualität und Angemessenheit von Mustern, Vorlagen etc. wird keine Gewähr übernommen. Setzen Sie diese bitte nur nach kompetenter Prüfung und eventuell notwendigen Anpassungen ein.

Einleitung

Integriertes Compliance-Managementsystem als wesentliche Komponente von Governance (GRC), Nachhaltigkeit (ESG/CSR) und Digitalisierung

Definitionen, Trends und wesentliche Compliance-Rechtsprechung[1]

Was versteht man unter Governance, Compliance-, Risiko-, Nachhaltigkeitsmanagement und Digitalisierung?[2]

Governance

(Corporate) Governance heißt in etwa „Angemessene Interaktion zwischen den Organen (Gesellschafter, Leitung (Vorstand/Geschäftsführer) und Aufsichtsgremium (Aufsichtsrat/Beirat/Verwaltungsrat sowie ordnungsgemäße Unternehmensführung und -überwachung".

Governance[3] ist mehr als Management. Governance soll auch gesellschaftliche Verantwortung (Corporate Social Responsibility (CSR) mit ökonomischer, sozialer und ökologischer Nachhaltigkeit) sowie Integrität/Ethik umfassen, vgl. hierzu ISO 37000:2021 (Governance of organizations).

Compliance

Compliance bedeutet pflichtgemäßes Verhalten in Hinblick auf allgemein verbindliche Regeln (Gesetze, Rechtsprechung), aber auch in Hinblick auf für verbindlich erklärte (interne) Vorgaben (z. B. Regelungen aus dem „Code of Conduct" (unternehmensspezifische Verhaltensregelungen) oder Anstellungsvertrag).

Risiko-management

Risikomanagement beschäftigt sich mit Unsicherheiten bei Entscheidungen und der Zielerreichung. (Unternehmerische) Tätigkeiten und Ziele sind immer mit Unsicherheiten verbunden. Aufgabe des Risikomanagements ist es, die Chancen und Risiken systematisch zu identifizieren und sie hinsichtlich potenzieller Auswirkungen auf das Unternehmen zu bewerten.

Der Begriff *Risiko* wird als Streuung um einen Erwartungswert definiert. Nach dieser Definition werden sowohl positive Abweichungen (*Chancen*) als auch negative Abweichungen (*Gefahren*) berücksichtigt.[4]

Nachhaltigkeit (ESG/CSR)

Nachhaltigkeit[5] **(ESG**[6]**/CSR**[7]**)** könnte mit *„bei Fortschritt bewahrend ausgerichtetes Entscheiden und Handeln"* oder gemäß der Weltkommission für Umwelt und Entwicklung *als „Entwicklung, die dem gegenwärtigen Bedarf Rechnung trägt, ohne künftigen Generationen die Möglichkeit zur Deckung ihres eigenen Bedarfs zu nehmen"*[8] beschrieben werden.

Oder, einfacher ausgedrückt (nicht nur mit Blick auf die nächsten Generationen): „Niemand sollte auf Kosten anderer leben."

---

1 Die Rechtsprechung bezieht sich hier auf *deutsche* Gerichte.

2 Vgl. *Scherer, Romeike, Grötsch*, Unternehmensführung 4.0: CSR/ESG, GRC & Digitalisierung integrieren, 2021, zum kostenlosen Download auf scherer-grc.net/publikationen.

3 Vgl. *Grötsch,* Erklärung zum Deutschen Corporate Governance Kodex, 2021, aufrufbar unter: www.risknet.de.

4 Zu den Zielen und positiven Effekten eines Risikomanagements vgl. https://www.risknet.de/wissen/risk-management-prozess/.

5 Vgl. *Scherer, Kollmann, Birker*, Integriertes Nachhaltigkeits-Managementsystem, 2019, zum kostenlosen Download auf scherer-grc.net/Publikationen.

6 ESG ist ein Akronym und steht für *„Environmental, Social, Governance"* (zu Deutsch: Umwelt, Soziales und Unternehmensführung).

7 CSR ist ein Akronym und steht für *„Corporate Social Responsibility"*, d. h. eine unternehmerische Gesellschaftsverantwortung bzw. unternehmerische Sozialverantwortung.

8 *World Commission on Environment and Development*; Our Common Future; Oxford University Press, Oxford 1987, S. 43.

Governance, Risk, Compliance: GRC

Governance, Risk, Compliance und Nachhaltigkeit „zusammen“, also **„GRC“** bzw. **ESG/CSR** ist unter Umständen etwas anderes als die Summe der vier Komponenten. Eine Legal-Definition gibt es hier nicht. GRC bzw. ESG/CSR könnte mit *„Integre, nachhaltige, complianceorientierte und risikobasierte Unternehmensführung und -überwachung“* übersetzt werden.

Nachhaltigkeits-Berichterstattung

Nachhaltigkeits-Berichterstattung[9]**:** Nachdem die „großen“ Unternehmen nachhaltigkeitsberichtspflichtig wurden und der Bericht auch verpflichtet, die Business Partner (insbesondere Lieferanten/Supplier) auf Nachhaltigkeit zu überprüfen, setzt sich auch im Mittelstand der kombinierte Nachhaltigkeits- und Geschäftsbericht durch. Außerdem **soll die CSR-Berichtspflicht künftig ab 01.01.2024 für das Geschäftsjahr 2023 auch gesetzlich auf den Mittelstand ab 250 Mitarbeitern ausgeweitet**[10] werden.

Digitalisierung

Digitalisierung heißt, zunächst zu prüfen, ob das bisherige Geschäftsmodell ganz oder teilweise durch ein digitales Modell (z. B. Plattformlösung) ersetzt oder ergänzt wird.

Sofern die bisherigen Prozesse bestehen bleiben, ergibt sich eine verstärkt „geistige Leistung“ (intellectual property / digital assets), die aus Wissen und Informationen in Form von Prozessen mit zugehörigen Komponenten (Rollen, Ziele, Ressourcen), IT-Systemen und IT-Tools, Algorithmen, Robotern und an vielen verbleibenden Stellen *Menschen* mit angemessenen Kompetenzen und Einstellungen besteht.

Diese unterschiedlichen Komponenten eines Unternehmens werden, sofern sinnvoll, auf die digitale Transformation ausgerichtet.

Die meisten unternehmerischen Aktivitäten sind als Prozesse so zu modellieren, dass sie die diversen Anforderungen aus Compliance, Technik, Betriebswirtschaft, Risikomanagement, Nachhaltigkeit etc. erfüllen und dafür sorgen, die gesetzten Ziele zu erreichen.

Zugleich ist zu analysieren, welche Aktivitäten künftig noch von Menschen oder (teil-)automatisiert durch Anwendungen, IT-Systeme, Roboter, Algorithmen oder sonstigen Tools aus den Bereichen Digitalisierung und Artificial Intelligence (AI) ersetzt bzw. unterstützt werden.

Digitalisiertes Integriertes GRC-/ESG-(CSR-) Managementsystem

Ein **Digitalisiertes Integriertes GRC-/ESG-(CSR-)Managementsystem** ist ein Managementsystem[11], das mehrere Unternehmensfunktionen bzw. Prozesse (z. B. **Compliance-**, Nachhaltigkeits-, Risiko-, Qualitäts-, Umwelt-, Arbeitssicherheits- und Personalmanagement) digitalisiert und zu einem „Unternehmensführungs-System“ integriert.

Vernünftiges Verhalten

Idealerweise deckt sich pflichtgemäßes und nachhaltiges Verhalten mit „vernünftigem Verhalten“,[12]

- so, wie ein Bauarbeiter heutzutage beispielsweise von selbst und freiwillig Schutzkleidung (Helm, Sicherheitsschuhe etc.) trägt und auf Alkohol auf der Baustelle verzichtet,
- ein Autofahrer sich angurtet oder
- vor der Vergabe von Aufträgen die Vertragspartner (Lieferanten) „gecheckt“ werden in Hinblick auf Compliance, Qualität, Risiko, Nachhaltigkeit etc. …

9 Eine verpflichtende Nachhaltigkeits-Berichterstattung – die sogenannte CSR-Berichtspflicht, basierend auf der EU-Richtlinie 2014/95/EU, wurde in Deutschland 2017 für kapitalmarktorientierte Unternehmen mit mehr als 500 Arbeitnehmern, 40 Mio. EUR Umsatz und/oder einer Bilanzsumme von 20 Mio. EUR eingeführt (§ 289b HGB). Diese nicht-finanzielle Unternehmensberichterstattung beruht auf den Leitlinien der *Global Reporting Initiative (GRI)* und muss in den Lagebericht eingebunden werden, vgl. www.globalreporting.org/standards.

10 Vgl. dazu nachfolgend in diesem Kapitel und *PwC*, CSR-Richtlinie: Heute beginnt eine neue Ära in der Nachhaltigkeitsberichterstattung, 2021, zuletzt aufgerufen am 28.09.2021 und *Grötsch, Andreas*, Corporate Social Responsibility-Berichtspflicht und die Folgen von Rechtsverstößen, KOR (Zeitschrift für internationale und kapitalmarktorientierte Rechnungslegung), 2021.

11 Aufbau- und Ablauforganisation, bestehend aus Komponenten (z. B. Rollen, Prozessabläufe, Delegationen und Interaktionen etc.), mit dem Zweck, eine Organisation bei Entscheidungen, Zielsetzung und Planung, Umsetzung sowie Steuerung und Überwachung zur Erreichung zwingender und fakultativ gesetzter Ziele zu unterstützen.

12 Vgl. *Scherer/Fruth* (Hrsg.), Integriertes Compliance-Managementsystem mit GRC, 2018.

Auch Nachhaltigkeitsmanagement sollte vernunft- und faktenbasiert sein, was leider noch längst nicht immer der Fall sein dürfte.[13] Das war – zum Teil – früher anders. In den letzten Jahren hat sich hier jedoch vieles verändert. Fallen Ihnen dazu weitere (insbesondere positive) Beispiele ein?

Das „Neue" an Governance, Risiko- und Compliancemanagement (GRC) ist, dass nicht – wie früher üblich – nur gelöscht wird, wenn es brennt, und dann (reaktiv!) gewartet wird, bis es erneut brennt. GRC kümmert sich stattdessen proaktiv um den Brandschutz, bevor es überhaupt zu brennen beginnt. Und: Ein funktionierendes „Brandschutzsystem" (der Nachweis, dass gesetzliche, behördliche und Anforderungen der „interested parties" (z. B. Kunden, Aufsichtsfunktionen etc.) erfüllt werden) ist schließlich Voraussetzung für die Erlaubnis, das Unternehmen überhaupt zu betreiben!

ESG/CSR und GRC als Klammer um die „Managementsystem-Inseln"

Nachhaltigkeitsmanagement (ESG/CSR) und Governance, Risk- und Compliancemanagement (GRC) als „Klammer" um die zahlreichen „Managementsystem-Inseln" und Unternehmensfunktionen:

Da die Einhaltung der Grundsätze ordnungsgemäßer Unternehmensführung (GoU) und -überwachung (GoÜ) – *Governance* – die Aufgaben der Geschäftsleitung umfassend beinhaltet, kann Governance, angereichert mit den modernen Methoden von Risiko- und Compliancemanagement, als „GRC-Funktion" eine effektive und effiziente Klammerwirkung um sämtliche Unternehmensfunktionen erzielen.

Egal, ob privatwirtschaftliche Unternehmen oder die öffentliche Hand (Regierungen, Kommunen, kommunale Unternehmen, Parteien etc.), profitorientierte oder nicht-profitorientierte Organisationen, alle setzen sich derzeit mit den Themen „Neue Arbeitswelten, Nachhaltigkeit, Regulierung und Compliance, Risikomanagement, Digitalisierung sowie Informationssicherheit" auseinander.

Vergleicht man nun die – wenig bekannten – konkreten und vor allem messbaren (!) Anforderungen aus gesetzlichen Regelungen und Standards, so zeigen sich auffällig viele Redundanzen von Governance bzw. GRC und Nachhaltigkeit (ESG/CSR) sowie Compliance. Dies erleichtert und reduziert vor allem den Aufwand bei der Einführung und der operativen Umsetzung eines Compliance- bzw. GRC- oder Nachhaltigkeits- und Risiko-Managementsystems enorm.

Jede Komponente aus Governance bzw. GRC (z. B. Compliance-, Qualitäts-, Risiko- oder Personalmanagement) stellt bereits zugleich eine wesentliche Komponente von Nachhaltigkeit dar.

Und „größere" Kunden verlangen in diesem Trend[14] von ihren Lieferanten/Suppliern verstärkt und ernsthaft Nachweise über wirksame Compliance-, Nachhaltigkeits-(CSR-/ESG-) und GRC-Systeme.

Nachhaltigkeits-Komponenten

Nachhaltigkeits-Komponenten: *„Das saubere Dutzend"*[15]:

Ein Nachhaltigkeits-Managementsystem bzw. die CSR-Berichterstattung beschäftigt sich nach herrschender Meinung in Literatur und Nachhaltigkeits-Standards (GRI, Global Compact etc.)

13 Vgl. *Rosling*, Factfulness, 2019 und *Kahneman/Sunstein*, Noise, 2021.

14 Vgl. hierzu das Lieferkettengesetz (das „Lieferkettensorgfaltspflichtengesetz (LkSG)" wurde am 11. Juni 2021 im Bundestag verabschiedet) sowie die Berichtspflichten bzgl. Nachhaltigkeit in der Supply Chain.

15 Vgl. *Scherer*, Nachhaltigkeits-(ESG-/CSR-)Compliance- und -Risikomanagement – die wesentlichen Pfeiler, auch für Resilienz, 2021, zum kostenlosen Download unter scherer-grc.net/publikationen.

in der Regel primär mit den folgenden 12 Themen bzw. aktuellen themenspezifischen *Spezial*-Standards[16])[17]:

1) **Governance (Ordnungsgemäße, ethische Unternehmensführung) (ISO 37000:2021 *Governance of organizations*)**[18]
2) **Compliance (ISO 37301:2021**[18] **/ IDW PS 980)**
3) **Anti-Korruption (ISO 37001:2016**[18]**)**
4) **Risikomanagement (ISO 31000:2018 / ÖNORM D 4900 ff.:2021**[18] **/ IDW PS 981)**
5) Umweltmanagement (ISO 14001:2015)
6) Klimaschutz und Treibhausgas-Neutralität (ISO 14064-1:2019)
7) Energieeffizienz/Ressourcenmanagement (ISO 50001:2018)
8) **Arbeitssicherheit** und Betriebliches Gesundheitsmanagement **(ISO 45001:2018)**
9) **Arbeitsrecht, Arbeitsstrafrecht** und faire Arbeitsbedingungen (Diversity, Gleichbehandlung der Geschlechter, keine Zwangs- und Kinderarbeit)
10) Verantwortungsvoller Umgang mit Informationen (Digitalisierung, **IT-Compliance, Informationssicherheit** (ISO/IEC 27000 ff., Datenschutz))
11) Sicherstellung von Nachhaltigkeit in Lieferketten und bei Geschäftspartnern
12) **Anonymitätsbewahrendes Hinweisgebersystem** für Nachhaltigkeits-Risiken und Compliance-Verstöße (ISO 37002:2021)[18]

Viele dieser Komponenten sind zugleich Bestandteil eines Compliance-Managementsystems!

ISO 37000:2021 Guidance for the Governance of Organizations

Governance und GRC:

Der DIN-Normungsausschuss 175-00-01 AA[19] erarbeitete die **ISO 37000:2021 *Guidance for the Governance of Organizations*** mit folgenden Punkten als **Kernbereich:**

1) Mission, Werte, Kultur
2) Nachhaltige Wertschöpfung
3) Strategie
4) **Rechtlicher Rahmen / Compliance: Gesetze, Normen, Regeln, Richtlinien**
5) Verantwortungsbewusstsein[20]
6) Stakeholder-Relationship
7) **Führung und Werte**[21]
8) **Daten und Entscheidungen**[22]
9) **Risikobasierte Unternehmensführung**[23]

16 Standards sind in der Regel keine verpflichtenden Vorgaben, sondern spiegeln unter Umständen (!) den „Anerkannten Stand von Wissenschaft und Praxis“ zum Zeitpunkt des Erlasses wider. Sie geben Hilfestellung bei der Frage, wie der betreffende Bereich konzeptioniert und umgesetzt werden soll.

17 Klarstellender Hinweis: Um ein angemessenes Nachhaltigkeits-Managementsystem zu implementieren, ist es nicht erforderlich, sämtliche aufgeführten Standards in „Insel-Managementsystemen“ umzusetzen oder zu zertifizieren.

18 Der Autor ist Mitglied der einschlägigen Arbeitsgruppe zur Erarbeitung des ISO-Dokuments.

19 Der Autor ist Mitglied der Arbeitsgruppe.

20 „Fit & proper“-Kompetenzen, Transparenz und Vertrauen.

21 Werte definieren und die Organisation nachhaltig, ethisch und effektiv führen.

22 Daten als wertvolle Ressource für Entscheidungsvorbereitung und -fällung.

23 Steuerung der Unsicherheiten bzgl. strategischer Ziele.

10) Soziale Verantwortung[24]

11) Nachhaltigkeit[25]

Auch hier stehen wieder etliche Komponenten in direkten Bezug zu einem **Compliance**-Managementsystem.

Nachhaltigkeit (ESG/CSR) = GRC![26]:

Nachhaltigkeit (ESG/CSR) = GRC!

Vergleicht man nun die oben dargestellten, konkreten und messbaren (!) Anforderungen aus gesetzlichen Regelungen und Standards, so zeigen sich auffällig die enormen Redundanzen zwischen Governance bzw. GRC, Compliance und Nachhaltigkeit (ESG/CSR). GRC und Nachhaltigkeit (ESG/CSR) sind weitestgehend identisch.

Jede Komponente aus Governance bzw. GRC (z. B. Compliance-, Qualitäts-, Risiko- oder Personalmanagement) stellt bereits zugleich eine wesentliche Komponente von Nachhaltigkeitsmanagement dar.

Hinweis: Auch die ISO wird sich künftig mit Nachhaltigkeit/ESG beschäftigen: Im Oktober 2021 fand das erste Treffen der vom ISO Technical Management Board (ISO/TMB) gegründeten *ISO Strategic Advisory Group on Environmental, Social, Governance (ESG) Ecosystem* statt.

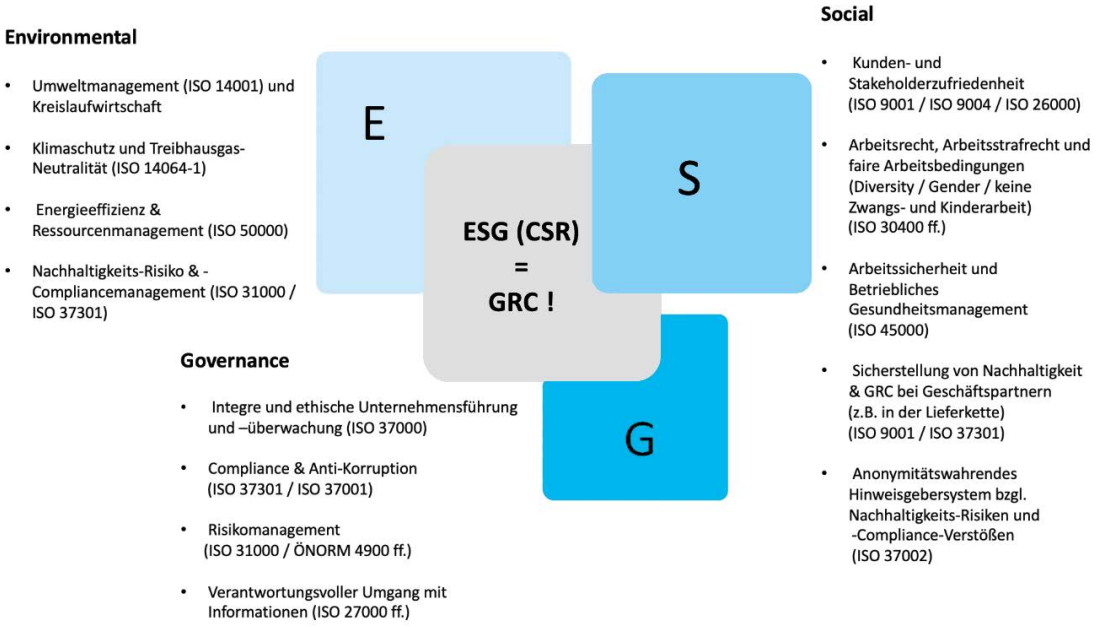


Bild 2: Environmental, Social, Governance = GRC

Das **Compliance**-Managementsystem kann – ebenso wie ein Umwelt-, Arbeitssicherheits-, Risiko-, Qualitäts-, bzw. ein anderes -Managementsystem – grundsätzlich aufgrund der entsprechenden Erwähnung in Standards als **isoliertes Inselsystem** implementiert werden.

Es kann aber auch ein führendes **Integriertes Managementsystem (IMS)** verschiedene Bereiche wie **Compliancemanagement**, Personalmanagement, Qualitätsmanagement, Risikomanagement etc. verbinden.

24 Gesellschaftliche Verantwortung (CSR/ESG).

25 Ökonomische, soziale und ökologische Wertschöpfung.

26 Vgl. *Scherer*, Nachhaltigkeits-(ESG-/CSR-)Compliance- und -Risikomanagement – die wesentlichen Pfeiler, auch für Resilienz, 2021, zum kostenlosen Download unter scherer-grc.net/publikationen.

Hierzu ein Zitat aus der Einleitung zur DIN ISO 37301:2021:

> „Dieses Dokument ist geeignet, um Compliance-bezogene Anforderungen in anderen Managementsystemen zu verstärken […]

Compliancemanagement als wesentlicher Baustein von Nachhaltigkeits-Berichterstattung:

Diverse Standards für Nachhaltigkeits-Berichterstattung (z. B. *Global Reporting Initiative (GRI), Global Compact,* der aktuelle Entwurf der *EFRAG* etc.) sehen vor, dass sich die berichtenden Organisationen umfassend zum Thema Compliance äußern.

Anforderungen an Nachhaltigkeits-Berichterstattung nach Standard „Global Reporting Initiative" (GRI) mit Bezug auf Compliance:

Ziel (abgeleitet aus einer „Wesentlichkeitsanalyse"): Rechtssicherheit (Business Compliance) / „Manager- und Mitarbeitersicherheit" / Rechtssichere Organisation

Nachhaltigkeits-Berichterstattung: „Business Compliance"

Verantwortung für dieses Thema: Compliance-Officer / Leitung Recht / Vertretung: N. N.

Nachhaltigkeitsberichterstattung nach Standard „*Global Reporting Initiative*" (GRI):

- GRI 103: Managementansatz für ein Compliance-Managementsystem
- GRI 205 Korruptionsbekämpfung
- GRI 205-1 Betriebsstätten, die auf Korruptionsrisiken geprüft wurden
- GRI 205-2 Kommunikation und Schulungen zu Richtlinien und Verfahren zur Korruptionsbekämpfung
- GRI 205-3 Bestätigte Korruptionsvorfalle und ergriffene Maßnahmen
- GRI 206 Wettbewerbswidriges Verhalten (Anti-competitive Behaviour)
- GRI 307 Umwelt-Compliance
- GRI 403: Arbeitssicherheit und Gesundheitsschutz
- GRI 406-1 Diskriminierung
- GRI 419 Sozioökonomische Compliance
- GRI 419-1: Nichteinhaltung von Gesetzen und Vorschriften im sozialen und wirtschaftlichen Bereich

EU-weite Regulierung im Bereich Nachhaltigkeit (ESG)

EU-weite Regulierung im Bereich Nachhaltigkeit (ESG):

Gemäß des Entwurfes der *Corporate Sustainbility Reporting Directive (CSRD)*, die endgültig wohl bis spätestens Juni 2022 als EU-Richtlinie verabschiedet werden wird, müssen ab 01.01.2024 große Kapitalgesellschaften und haftungsbeschränkte Personengesellschaften mit mehr als 250 Mitarbeitern, 20 Mio. Euro Bilanzsumme oder 40 Mio. Euro Umsatz (zwei dieser drei Voraussetzungen reichen) für das Geschäftsjahr 2023 über ökonomische, soziale und ökologische Nachhaltigkeit berichten.[27]

27 Vgl. *Richter, Meyer*, Nachhaltigkeitsreporting: Warum die neue EU-Richtlinie wegweisend ist, 03.11.2021, zum Download im Internet.

European Financial Reporting Advisory Group (EFRAG)

Die ***European Financial Reporting Advisory Group (EFRAG)*** will im Juni 2022 Standards für diese Berichterstattung vorschlagen und den ersten Satz der Standards im Oktober 2022 und den zweiten Satz im Oktober 2023 verbindlich setzen.

Diese Standards werden in 9 Cluster aufgeteilt[28]:

- **Cluster 1** enthält konzeptionelle Leitfäden zur ***„doppelten Wesentlichkeit“*** (Welche Nachhaltigkeits-Risiken wirken einerseits auf die Organisation / das Unternehmen? Aber auch andererseits: Welche Nachhaltigkeitsrisiken entstehen durch das Unternehmen / die Organisation für die Gesellschaft und die Umwelt?) und zu den **Anforderungen an Art und Qualität der einzelnen Informationen** (z. B. über bestimmte Kennzahlen zu bestimmten Themen in digitalem, auswertbarem Format[29]).

  Darüber hinaus enthält Cluster 1 sogenannte „Querschnittsnormen“ zu ***Themen der Resilienz***, wie

  1) Geschäftsmodell und Strategie
  2) Wesentliche Nachhaltigkeits-Risiken, -Chancen und -Auswirkungen
  3) Nachhaltige Unternehmensführung (Governance) und Organisation/Prozesse
  4) Grundsätze, Richtlinien und Ziele in Bezug auf Nachhaltigkeit
  5) Abgeleitete Planung von Projekten/Maßnahmen und dafür erforderliche Ressourcen

  Dies entspricht in etwa den bereits über die Standards *„Global Compact“* oder *„Global Reporting Initiative“* bekannten Analysen wesentlicher Nachhaltigkeitsthemen und strategischer Ziele („*Wesentlichkeits-Analyse*“) mit zugehörigem „*Managementansatz*“.[30]

Die weiteren Cluster umfassen:

- **Cluster 2:** Umwelt: Klimawandel und Anpassung
- **Cluster 3:** Umwelt: Wasser- und Meeres-Ressourcen, Umweltverschmutzung, Kreislaufwirtschaft, Biodiversität und Ökosysteme
- **Cluster 4:** Soziales: Eigenes Personal / Human Resources
- **Cluster 5:** Soziales: Personal in der Wertschöpfungskette, betroffene Gemeinschaften, Verbraucher
- **Cluster 6:** Governance: Unternehmensführung und Überwachung, mit

  a) Governance, Risk und Compliance, interne Steuerung und Überwachung
  b) verantwortungsvolle Geschäftspraktiken
  c) Produkte und Leistungen, Innovation, Management und Qualität der Beziehungen zu Geschäftspartnern
- **Cluster 7:** Branchenspezifische Besonderheiten
- **Cluster 8:** Leitfäden für kleine und mittlere Unternehmen (KMU)
- **Cluster 9:** Regelt die Digitalisierung der Berichterstattung

28 *EFRAG*, Project Task Force on European Sustainability Report Standards (PTF-ESRS), Endorsement Status Report, 25.3.2022, zum Download im Internet.

29 XHTML/ESEF-Datenformat, vgl. *Richter/Meyer*, Sind Unternehmen für die künftigen Anforderungen der Nachhaltigkeitsberichterstattung gewappnet? 02.06.2021, zum Download im Internet.

30 Vgl. *Scherer/Fruth/Grötsch* (Hrsg.), Digitalisierung, Nachhaltigkeit und „Unternehmensführung 4.0“ (GRC), 2021, Leseprobe unter scherer-grc.net/publikationen.

Taxonomie-Verordnung der EU

Taxonomie-Verordnung der EU:

Darüber hinaus führt bereits jetzt die sogenannte *Taxonomie-Verordnung* zu erheblichen Auswirkungen auf Unternehmen/Organisationen.[31]

Finanz-, Versicherungs-, aber auch bestimmte Nicht-Finanz-Unternehmen müssen bereits ab dem Jahr 2022 (!) aufgrund des *Delegierten Rechtsaktes zu Art. 8 der EU-Taxonomie-Verordnung* zu (derzeit noch primär ökologischer) Nachhaltigkeit berichten.

Bezüglich der (ökologisch) nachhaltigkeitswirksamen Aktivitäten müssen beispielsweise auch Nicht-Finanzunternehmen berichten, welchen Anteil diese an Betriebs- („OpEx") und Kapitalausgaben („CopEx"), aber auch am Umsatz haben.

Am 20.12.2021 veröffentlichte die Europäische Kommission lesens- und beachtenswerte *„Frequently Asked Questions (FAQ)"* zu diesen Berichtspflichten.[32]

Compliance- und Risikomanagement – die wesentlichen Pfeiler

Compliance- und Risikomanagement – die wesentlichen Pfeiler für Governance (Unternehmensführung) und Nachhaltigkeit[33]:

Wie funktioniert Compliance, Unternehmensführung und Nachhaltigkeit? In der Einleitung zu DIN ISO 37301 heißt es:

> […] Compliance ist daher nicht nur Grundlage, sondern auch Gelegenheit für eine nachhaltig erfolgreiche Organisation. […]

Es zeigt sich, dass bei Unternehmensführung und Nachhaltigkeit (CSR/ESG) insbesondere Compliance- und Risikomanagement die Grundvoraussetzungen sind, um die vielen Anforderungen zu identifizieren und zu erfüllen.

Das „Was und Wie" ist rechtlich vorgegeben

Das „Was und Wie" des Nachhaltigkeits- und Governancemanagements ist nicht eine von der betriebswirtschaftlichen Lehre, der Politik-, Sozial- oder Umweltwissenschaft beurteilte Ermessenssache, sondern in erster Linie rechtlich vorgegeben:

Erfüllung der Pflichten ohne jeglichen Spielraum (Compliance)

Zu den Anforderungen und Zielen des Governance- und Nachhaltigkeitsmanagements gehören **primär die Erfüllung der Pflichten ohne jeglichen Spielraum (Compliance)** und das Agieren im vorgegebenen, zwingenden Rahmen (z. B. im Rahmen gesetzlicher oder sonstiger verpflichtender Vorgaben) und erst anschließend Ziele, deren Erreichung nicht zwingend vorgegeben, aber von entscheidungsbefugten Interessensgruppen gewünscht ist.[34]

„Legalitäts-Pflicht-Urteil" des BGH

„Legalitäts-Pflicht-Urteil" des *BGH* zur allgemeinen Pflicht aller Rechtssubjekte (Personen und Unternehmen), sich an Gesetze zu halten:

→ 2_Kapitel Einleitung → Anlagen zu Einleitung.pdf, Anlage 1

31 Vgl. den Entwurf der EU-Kommission vom 31.12.2021 und *Rat für nachhaltige Entwicklung*, EU-Taxonomie: So steht es auf dem Weg zur nachhaltigen Wirtschaft, 22.10.2021, zum kostenlosen Download im Internet.

32 Vgl. *Flick*, Art. 8 Taxonomie-Verordnung: FAQ und weiteres Informationsmaterial zu den neuen Berichtspflichten veröffentlicht, Artikel vom 22.12.2021, zum Download im Internet.

33 Vgl. *Scherer*, Nachhaltigkeits-(ESG-/CSR-), Compliance- und Risikomanagement – die wesentlichen Pfeiler, auch für Resilienz, 2021, zum kostenlosen Download unter scherer-grc.net/publikationen.

34 Vgl. *Scherer*, Good Governance und ganzheitliches, strategisches und operatives Management: Die Anreicherung des „unternehmerischen Bauchgefühls" mit Risiko-, Chancen- und Compliance-Management, in: Corporate Compliance Zeitschrift (CCZ), 6/2012, S. 202 ff. mit Ausführungen zum „Risks of Changes-Management", zum kostenlosen Download auf scherer-grc.net/publikationen.

Aus dem „Legalitäts-Pflicht-Urteil“ des *BGH* ergibt sich für alle Rechtssubjekte (Personen und Unternehmen) die Pflicht, sich an Gesetze zu halten. Es ist als erstes zu fragen, was Geschäftsleitung/Entscheider tun *müssen*, ohne Alternativen bzgl. des „Ob“ und des „Wie“, was also *verpflichtend*, bzw. *Compliance-Anforderung* ist:

Beispielsweise gehört die Erstellung des Jahresabschlusses unter Umständen mit Nachhaltigkeitsberichterstattung (§ 289 ff. HGB) oder das Abführen von Sozialversicherungsbeiträgen (vgl. § 266a StGB) zur (ökonomischen und sozialen) Nachhaltigkeit. Hier sind sowohl zeitliche als auch inhaltliche Anforderungen gesetzlich vorgeschrieben.

Hinsichtlich der rechtlich zwingenden Anforderungen bezüglich Governance- und Nachhaltigkeitsmanagement gibt es eine Vielzahl von *zu priorisierenden Quellen*.

Aufgabe des Compliancemanagements ist es u. a., für eine entsprechende Organisation im Zusammenwirken mit anderen (Fach-)Abteilungen zu sorgen, die es ermöglicht, einen Überblick über die aktuelle Rechtslage und rechtliche Änderungen zu behalten. Die verpflichtenden Anforderungen müssen identifiziert, bewertet und in eine verständliche Sprache übersetzt werden. Sodann müssen Aktivitäten, die die Erfüllung der Anforderungen sicherstellen und kontrollieren, in die Prozessabläufe implementiert werden.

Prioritätskaskade für Governance- und Nachhaltigkeitsmanagement-Anforderungen

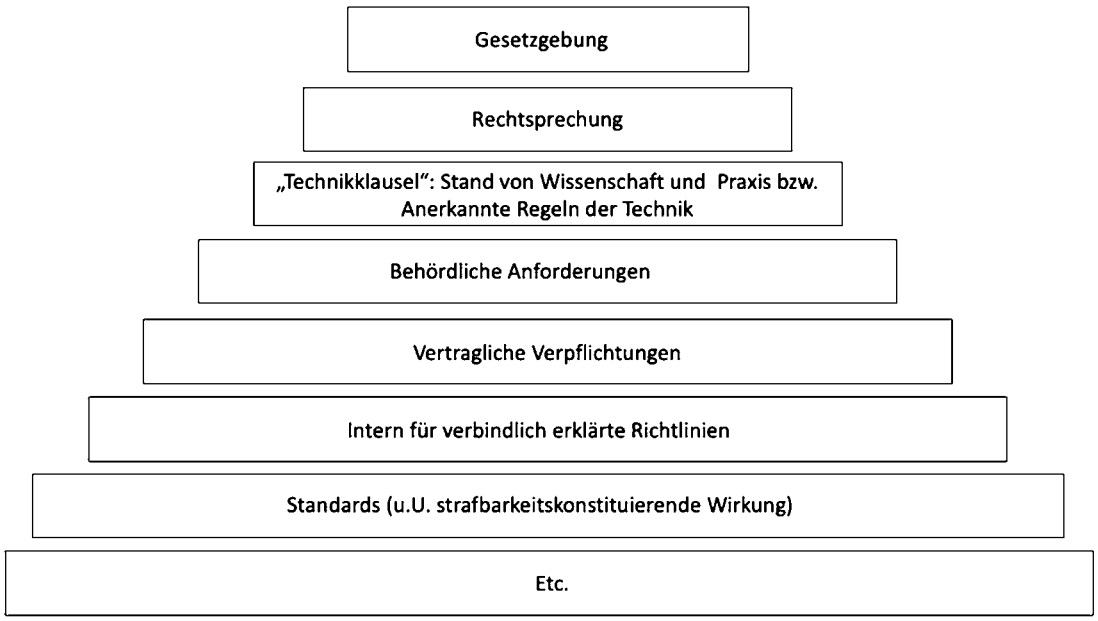


Bild 3: Prioritätskaskade für Governance- und Nachhaltigkeitsmanagement-Anforderungen[35]

Vgl. hierzu auch Kapitel 4.5.

„(Technische) Entwicklungsstände“

Dabei sind „(technische) Entwicklungsstände“ nicht nur in den Naturwissenschaften, sondern auch bei Nachhaltigkeit, Governance, Risiko- und Compliancemanagement etc. ebenfalls Messlatte für Gerichte, die entscheiden, ob Pflichtverletzungen seitens der Organisation oder deren Organe vorliegen.

35 Vgl. die Rechtsprechung des *BGH* vom 27.08.2010 zur Legalitätspflicht im Fall „RWE-Tochter.“ *BGH* 2 StR 1 11/09 Urteil vom 27.08.2010 („Müllentsorgung und Schwarze Kassen im Ausland“) abgedruckt und kommentiert bei *Scherer*, „Das interessiert Kapitalgeber“ – Antifragilität und der „Achilleskörper“ des Ordentlichen Kaufmanns, 2019, S. 13, zum kostenlosen Download auf scherer-grc.net.

Was ist der „Stand der Technik“?

Der Frage: *Was ist der „Stand der Technik“?* geht unter anderem die sog. *Kalkar*-Entscheidung des *BVerfG* nach:

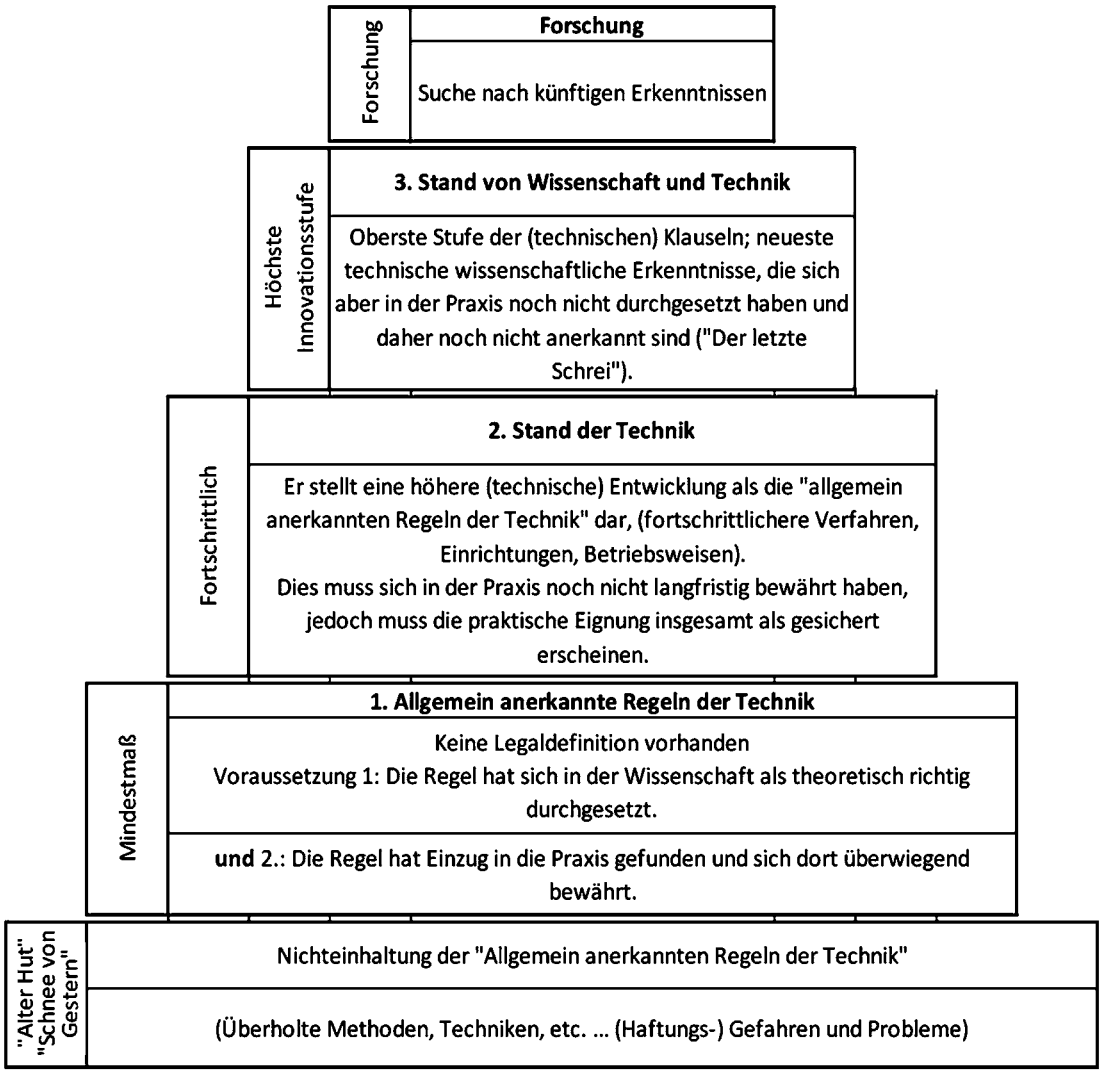


Bild 4: „Technikklauseln“ nach BVerfG („Kalkar-Entscheidung“ 1978)[36]

„Die 3-Stufen-Theorie“ des Bundesverfassungsgerichtes

Die sogenannte „3-Stufen-Theorie“ des *Bundesverfassungsgerichts* („Kalkar-Entscheidung“, 1978) zu sogenannten Technikklauseln beantwortet die Frage: Was sind z. B. „Anerkannte Regeln der Technik“ oder was versteht man unter dem „Stand der Technik“ und welche rechtliche Bedeutung haben diese für Compliance?

→ 2_Kapitel Einleitung → Anlagen zu Einleitung.pdf, Anlage 2

Geschäftsleitung und sonstige Verantwortliche *müssen* die jeweiligen von ihnen betreuten (Prozess-)Themenfelder/Bereiche und auch die Komponenten von Nachhaltigkeit (CSR/ESG) und GRC *an aktuellen Anforderungen aus Gesetzgebung und Rechtsprechung* sowie dem *„Anerkannten Stand von Wissenschaft und Praxis“* („hard law“) ausrichten.

36 *Scherer, Fruth* (Hrsg.), Governance-Management Band 1, 2015, S. 63 ff.

In der Einleitung zur DIN ISO 37301:2021 heißt es hierzu:

> Dieses Dokument ist geeignet, um Compliance-bezogene Anforderungen in anderen Managementsystemen zu verstärken und Organisationen bei der Verbesserung des übergreifenden Managements all ihrer Compliance-Verpflichtungen zu unterstützen.

Zahlreiche (internationale) Einzelgesetze und die Rechtsprechung beschäftigen sich mit zwingend zu beachtenden Teilgebieten von GRC und Nachhaltigkeit (ESG/CSR), wie zum Beispiel das gesamte öffentlich- und privatrechtliche (Umwelt-)Recht, Arbeitsrecht, Arbeitssicherheits- und Gesundheitsschutzrecht, Straf- und Ordnungswidrigkeitenrecht u.v.m.

„Legalitätspflicht" der Geschäftsleitung

Aufgrund der *„Legalitätspflicht"* der Geschäftsleitung und der Anforderungen an einen „gewissenhaften" Geschäftsführer, Vorstand, Aufsichtsrat, Kaufmann (§§ 43 GmbHG, 91, 93, 116 AktG, 347 HGB etc.) sowie der Pflicht, nach §§ 130, 30 OWiG Vorsorge gegen Pflichtverstöße im Unternehmen zu treffen, muss eine entsprechende, angemessene Organisation, die rechtssichere, nachhaltige Unternehmensführung und -überwachung, inklusive der gesamten relevanten (*Nachhaltigkeits-)Compliance*, ermöglicht, vorgehalten werden.[37]

Diesbezüglich kann es nützlich sein, sich an gängigen aktuellen Standards („soft law") zu orientieren, um den Versuch der Einhaltung des „Anerkannten Standes von Wissenschaft und Praxis" zu dokumentieren; auch, um auf Audits, die Abschlussprüfung oder die Zertifizierung gut vorbereitet zu sein. Standards können laut dem Vorsitzenden Richter des 1. Strafsenats des *BGH „strafbarkeitskonstituierend"* sein.[38]

Würde zwingend vorgegebenes Verhalten in Bezug auf Governance und Nachhaltigkeit (ESG/CSR) unterlassen oder nicht in der richtigen Frist und Form erfolgen, stellte dies eine – evtl. auch strafrechtlich – haftungsbewehrte Pflichtverletzung *(Compliancеverstoß)* dar.[39]

Darüber hinaus gibt es *nicht dispositive Pflichtaufgaben* bzgl. des „Ob", jedoch mit Spielraum bzgl. der inhaltlichen Ausgestaltung, des „Wie":

Dazu gehört beispielsweise die Einführung eines Risiko-Managementsystems, die gesetzlich explizit vorgeschrieben ist: Für AGs und große GmbHs nach § 91 Abs. 2 und (neu) 3 AktG (analog)[40] sowie gemäß § 1 StaRUG[41], sowie über die Pflicht, sich wie ein gewissenhafter Geschäftsführer, Vorstand, Aufsichtsrat, Kaufmann etc. zu verhalten (§§ 93, 116 AktG, 43 GmbHG, 347 HGB). Es ist mittlerweile *„Anerkannter Stand von Wissenschaft und Praxis"*, Risikomanagement zu betreiben.

---

37 *Scherer, Romeike, Grötsch*, Unternehmensführung 4.0: CSR/ESG, GRC & Digitalisierung integrieren, 2021, zum kostenlosen Download unter risknet.de/elibrary.

38 Vgl. *Raum*, in: *Hastenrath* (Hrsg.), Compliance-Kommunikation, 2017.

39 Sogenannte „Legalitätspflicht" der Geschäftsleitung, die sowohl im Öffentlichen Recht als auch im Zivilrecht (str.) gilt, vgl. *Zöllner/Noack* in: *Baumbach/Hueck*, GmbHG-Kommentar, 19. Auflage 2010, § 43 GmbHG, Rn. 17, 22, 22 b und 23. Vgl. auch *BGH* 2 StR 1 11/09 Urteil vom 27.08.2010 („Müllentsorgung und Schwarze Kassen im Ausland") abgedruckt und kommentiert bei *Scherer*, „Das interessiert Kapitalgeber" – Antifragilität und der „Achilleskörper" des Ordentlichen Kaufmanns, 2019, S. 13, zum kostenlosen Download auf scherer-grc.net.

40 § 91 Abs. 3 AktG: *„(3) Der Vorstand einer börsennotierten Gesellschaft hat darüber hinaus ein im Hinblick auf den Umfang der Geschäftstätigkeit und die Risikolage des Unternehmens angemessenes und wirksames internes Kontrollsystem und Risiko-Managementsystem einzurichten." – § 1 StaRUG: „Die Mitglieder des zur Geschäftsführung berufenen Organs einer juristischen Person (Geschäftsleiter) wachen fortlaufend über Entwicklungen, welche den Fortbestand der juristischen Person gefährden können. Erkennen sie solche Entwicklungen, ergreifen sie geeignete Gegenmaßnahmen und erstatten den zur Überwachung der Geschäftsleitung berufenen Organen (Überwachungsorganen) unverzüglich Bericht. Berühren die zu ergreifenden Maßnahmen die Zuständigkeiten anderer Organe, wirken die Geschäftsleiter unverzüglich auf deren Befassung hin."*

41 Vgl. *Scherer* in *Scherer/Fruth* (Hrsg.): Geschäftsführer-Compliance, 2009, 4.1.9 „Haftung des GmbH-Geschäftsführers wegen unterlassener Einrichtung eines Risiko-Management-Systems".

Compliance-Urteil des LG München „Neubürger“

Das gilt ebenso hinsichtlich eines Compliance-Managementsystems: Hier existiert mittlerweile eine – bestätigende – Rechtsprechung (vgl. das Compliance-Urteil des LG München *„Neubürger“),* dass ein angemessenes und wirksames Compliance-Managementsystem vorzuhalten ist:

→ 2_Kapitel Einleitung → Anlagen zu Einleitung.pdf, Anlage 3

Bezüglich der inhaltlichen Ausgestaltung (des „Wie?“) wird jedoch *Angemessenheit,* also Geeignetheit zur Zielerreichung, und *„Wirksamkeit“* („gelebt werden“/Effektivität) gefordert.

Dieser „unbestimmte Rechtsbegriff“ der „Angemessenheit“ gibt der Geschäftsleitung jedoch nicht freies Ermessen, sondern wird zum Schluss unter Umständen von Gerichten beurteilt. Dies ist für die Praxis ein erhebliches Problem.

Dazu heißt es in der Einleitung zur DIN ISO 37301:2021:

> […] die Umsetzung kann je nach Größe und Reifegrad des Compliance-Managementsystems einer Organisation und des Kontexts, der Natur und der Komplexität ihrer Aktivitäten und Ziele variieren.

Die Lösung lautet: Die Orientierung am Stand von Wissenschaft und Praxis und an aktuellen und anerkannten Standards!

Hinweis: Mehr zum Problem der „unbestimmten Rechtsbegriffe“ und dessen Lösung finden Sie unter Punkt 5 im Kapitel 4.5.

Aufgaben mit Ermessensspielraum

Aufgaben des Governance- und Nachhaltigkeits-(ESG-/CSR-)Managements *mit Ermessensspielraum*:

Sofern noch nicht verpflichtend geregelt (vgl. oben), können Organisationen sich freiwillig selbst weitere Ziele setzen, z. B.:

- die Erreichung eines bestimmten Reifegrads beim Compliance-, Governance- oder Nachhaltigkeits-Managementsystem
- die Erlangung von Zertifikaten, Siegeln etc.

Wenn die autorisierte Stelle in der Organisation (z. B. Vorstand, Geschäftsleitung etc.) jedoch diese Ziele als *verbindlich* beschließt oder eine entsprechende Richtlinie (policy) als *verbindlich* verabschiedet, werden diese Anforderungen zu „zwingenden Zielen“.

Business Judgment Rule

Bei den Governance-/Nachhaltigkeits-Aufgaben der Geschäftsleitung *mit* Ermessensspielraum ist stets an die sogenannte **Business Judgment Rule**[42] zu denken:

Der Manager muss sich die nötigen Informationen besorgen und das erforderliche Know-how besitzen, um die Informationen mit angemessenen Risiko-Bewertungsmethoden bewerten zu können[43] und dann im Rahmen eines pflichtgemäßen Ermessens entscheiden, *ob* und gegebenenfalls *wie* er die Aufgabe ausführt.

---

42 Vgl. *Scherer*, „Das interessiert Kapitalgeber“ – Antifragilität und der „Achilleskörper“ des Ordentlichen Kaufmanns, 2019, zum kostenlosen Download auf scherer-grc.net und *Sieg/Zeidler*, Business Judgment Rule, in: Hauschka, Corporate Compliance, 2. Auflage 2010, S. 52 ff.

43 Der Beurteilungsspielraum ist durch *objektive Nachvollziehbarkeit* begrenzt, vgl. *Zöllner/Noack* in: *Baumbach/Hueck*, GmbHG-Kommentar, 19. Auflage 2010, § 43 GmbHG, Rn. 22, d. h., der Geschäftsführer muss auch hinsichtlich seiner Informationen vernünftigerweise annehmen dürfen, dass seine darauf beruhende Entscheidung dem Wohl der Gesellschaft dient. Dies ist nur bei entsprechendem Know-how gewährleistet. Vgl. vertiefend *Scherer*, Good Governance und ganzheitliches, strategisches und operatives Management: Die Anreicherung des „unternehmerischen Bauchgefühls“ mit Risiko-, Chancen- und Compliance-Management, in: Corporate Compli-