Prof. Dr. Josef Scherer

Rechtsanwalt, Vorstand des Internationalen Instituts für Governance, Management, Risk- und Compliancemanagement der Technischen Hochschule Deggendorf. Mitglied diverser ISO/ DIN-Normenausschüsse (Governance, Compliance, Personalmanagement) und von Austrian Standards International (Risiko-Managementsystem).

Dipl.-Kfm. Prof. Dr. Andreas Grötsch

Rechtsanwalt, Steuerberater, Fachanwalt für Steuerrecht Professor für Corporate Social Responsibility und Tax Compliance an der THD Deggendorf.

Neu! ÖNORM 4900 ff.: 2021 (Risk), ISO 37 301: 2021 (Compliance) und ISO / IEC Directives, Part 1: 2021 (Harmonized Structure: HS)

(Kombi-) Zertifizierung von Compliance-Risiko-Managementsystemen und Komponenten von Nachhaltigkeits- (ESG-) Berichten

im Lichte von Unternehmenssanktionsrecht[1], Lieferkettengesetz, Informationssicherheits-, Pandemie- und Nachhaltigkeits-Risiken

1. Einleitung

Neue Standards

Ganz aktuell stehen neue Standards für die Zertifizierung von Risiko- und Compliance-Managementsystemen zur Verfügung:

Gender-Hinweis: In diesem Artikel wird aus Gründen der besseren Lesbarkeit das generische Maskulinum verwendet. Weibliche und anderweitige Geschlechteridentitäten werden dabei ausdrücklich mitgemeint **Hinweis** zu Links: Der Artikel enthält Links zu externen Websites Dritter, auf deren Inhalte wir keinen Einfluss haben. Deshalb können wir für diese fremden Inhalte auch keine Gewähr übernehmen. Für die Inhalte der verlinkten Seiten ist stets der jeweilige Anbieter oder Betreiber der Seiten verantwortlich. Die verlinkten Seiten wurden zum Zeitpunkt der Verlinkung auf mögliche Rechtsverstöße überprüft. Rechtswidrige Inhalte waren zum Zeitpunkt der Verlinkung nicht erkennbar.

[1] Vgl. *Scherer/Grötsch* Unternehmenssanktionsrecht, interne Untersuchungen und Whistleblowing als ESG-Elemente im Koalitionsvertrag, 08.12.2021, auf Scherer-GRC.net/Publikationen zum kostenlosen Download verfügbar

ÖNORM 4900 ff: 2021 [in Anlehnung an ISO 31000: 2018 (Risikomanagement)] und DIN ISO 37301: 2021 (Compliancemanagement).[2]

Nachhaltigkeits-Berichtspflicht

Der Gesetzgeber wird zum 01.01.2024 für das Geschäftsjahr 2023 die Nachhaltigkeits-Berichtspflicht (vgl. 289 b HGB) auch auf mittelständische Unternehmen ab 250 Mitarbeiter erweitern:

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. € Bilanzsumme oder 40 Mio. € Umsatz (zwei dieser drei Voraussetzungen reichen) für das Geschäftsjahr 2023 über ökonomische, soziale und ökologische Nachhaltigkeit berichten.[3]

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.[4]

Cluster 1

Cluster 1 enthält konzeptionelle Leitfäden zur ***„doppelten Wesentlichkeit"***
(welche Nachhaltigkeits-Risiken wirken einerseits auf Organisation / Unternehmen, aber auch andererseits: welche Nachhaltigkeitsrisiken entstehen durch das Unternehmen / die Organisation für Gesellschaft und Umwelt?)
und zu **Anforderungen an Art und Qualität der einzelnen Informationen** (z. B. über bestimmte Kennzahlen zu bestimmten Themen in digitalem, auswertbarem Format[5]).

Darüber hinaus enthält „Cluster 1" so genannte „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.

---

[2] Verfasser Scherer ist als „Experte" in beiden Arbeitsgruppen tätig.
[3] Vgl. *Richter, Meyer,* Nachhaltigkeitsreporting: Warum die neue EU-Richtlinie wegweisend ist, 03.11.2021, zum Download im Internet.
4 *EFRAG,* Project Task Force on European Sustainbility Report Standards (PTF-ESRS) Status Report, 15.11.2021, zum Download im Internet.
[5] XHTML / ESEF-Datenformat, vgl. *Richter / Meyer*, Sind Unternehmen für die künftigen Anforderungen der Nachhaltigkeitsberichterstattung gewappnet?, 02.06.2021, zum Download im Internet.

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*“.[6]

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: beschäftigt sich mit branchenspezifischen Besonderheiten

Cluster 8: enthält Leitfäden für kleine und mittlere Unternehmen (KMU)

Cluster 9: regelt die Digitalisierung der Berichterstattung.

Darüber hinaus führt bereits jetzt die so genannte **Taxonomie-Verordnung** zu erheblichen Auswirkungen auf Unternehmen / Organisationen.[7]

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 sog. „Frequently Asked Questions (FAQ)“ zu diesen Berichtspflichten.[8]

---

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

[7] Vgl. *Rat für nachhaltige Entwicklung*, EU-Taxonomie: So steht es auf dem Weg zur nachhaltigen Wirtschaft, 22.10.2021, zum kostenlosen Download im Internet.

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

Die Nachhaltigkeits-Berichtspflicht und Nachhaltigkeits-Managementsysteme umfassen als wesentliche Komponenten gerade eben auch Risiko- und Compliance-Management (vgl. unten, 2.).

„ISO Harmonized Structure (HS)"

Die ISO revisionierte 2021 ihre ehemalige „ISO High Level Structure" aus 2012. Nunmehr gibt es den **„Harmonized Approach"** / die **„Harmonisierte Struktur"** (HS) von 2021: ISO / IEC Directives, Part 1, Annex SL, Appendix 2: 2021. Die ISO gibt damit für all ihre Managementsystem-Standards denselben Aufbau mit 10 Punkten und Mustertext vor.

Neue gesetzliche und technische Herausforderungen an Organisationen, wie Unternehmenssanktionsrecht[9], Lieferkettengesetz, Berichterstattung über Nachhaltigkeit in der Lieferkette, Informationssicherheits- und sonstige globale Risiken verstärken den Bedarf der Organisationen an offiziellen Nachweisen[10], auch in den Bereichen Risiko-, Compliance- und Nachhaltigkeitsmanagement (ESG) auf dem Stand der Technik zu sein.

Aufgrund der zahlreichen Redundanzen und Analogien der neuen Risiko- und Compliance-Management-Standards (und auch in Bezug auf Qualitätsmanagement und sonstige nach der „Harmonized Structure" aufgebauten Managementsystem-Standards) bietet es sich an, die Systeme mit einem „Kombizertifikat" als „Integrierte Managementsysteme" zu testieren.

Diese Zertifizierung kann zugleich auch bestätigen, dass bestimmte **wesentliche Komponenten eines Nachhaltigkeits-Managementsystems** beziehungsweise der **Nachhaltigkeits-Berichterstattung** unterliegenden Themen den aktuellen Standards entsprechen.

Zu diesem Themenkomplex gibt es zahlreiche Fragen:

1. Was heißt eigentlich Governance, Risk, Compliance, GRC, Nachhaltigkeit, Managementsystem und Integriertes GRC-Managementsystem?[11]

Corporate Governance heißt in etwa „Angemessene Interaktion zwischen den Organen [Gesellschafter, Leitung (Vorstand / Geschäftsführer) und Aufsichtsgremium (Aufsichtsrat / Beirat)] sowie ordnungsgemäße Unternehmensführung und -überwachung".[12]

Governance ist mehr als Management:

[9] Vgl. *Scherer/Grötsch*, Unternehmenssanktionsrecht, interne Untersuchungen und Whistleblowing als ESG-Elemente im Koalitionsvertrag, 08.12.2021, zum kostenlosen Download auf Scherer-GRC.net

[10] Vgl. *Scherer*, Kombi-Zertifizierung von Risk und Compliance – Wesentlicher Nachweis für Nachhaltigkeits-Managementsystem und ESG – Due Diligence, FIRM Jahrbuch 2022, zum kostenlosen Download im Internet ab 05/2022.

[11] Vgl. *Scherer*, „Management reloaded",2021, zum kostenlosen Download auf Risknet.de

[12] Vgl. *Scherer/Fruth* (Hrsg.), Governance-Management Band I, 2014, S. 9 und Band II, 2015, S. 30, sowie *Scherer*, Good Governance und ganzheitliches strategisches und operatives Management: Die Anreichung des „unternehmerischen Bauchgefühls" mit Risiko-, Chancen- und Compliancemanagement, Corporate Compliance Zeitschrift (CCZ), 6/2012, S. 201, zum kostenlosen Download auf Scherer-GRC.net

Governance soll auch gesellschaftliche Verantwortung (Corporate Social Responsibility (CSR) mit ökonomischer, sozialer und ökologischer Nachhaltigkeit) und Integrität / Ethik umfassen.[13]

Risikomanagement beschäftigt sich mit Unsicherheiten bei Entscheidungen und Zielerreichung. Es hilft, Gefahren (und Chancen) zu identifizieren, zu bewerten und zu steuern.

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].

Governance, Risk und Compliance „zusammen", also „GRC" ist u.U. etwas anderes als die Summe dieser drei Komponenten. Eine Legal-Definition gibt es hier nicht. GRC könnte (leider etwas komplex) mit „Integre, nachhaltige, complianceorientierte und risikobasierte Interaktion der Organe und Unternehmensführung und -überwachung" übersetzt werden.

Die Begründung, weshalb Governance compliance-orientiert sein muss: Compliance bildet generell den rechtlichen, zwingenden Rahmen für unternehmerisches Handeln.

Risikobasiert muss Unternehmensführung sein, weil andernfalls nicht wie ein „gewissenhafter" Unternehmer, Vorstand, Geschäftsführer agiert werden würde: Gefahren (und Chancen) zu identifizieren, bewerten und steuern, ist Voraussetzung für die Erreichung der Ziele.

Ein Managementsystem besteht aus Komponenten[14], wie Aufbau- und Ablauforganisation mit dem Zweck, eine Organisation bei Entscheidungen, Zielsetzung und Planung, Umsetzung sowie Steuerung und Überwachung zur Erreichung zwingender und fakultativ gesetzter Ziele zu unterstützen.

Integriertes Managementsystem heißt, dass Komponenten / Prozessschritte zur Erüllung der Anforderungen aus diversen Themenbereichen (z.B. Compliance, Risiko-, Qualitäts-, Informationssicherheits-Management, etc.) in ein **einziges** Managementsystem, also in die ja nur *einmalig* existierende *Aufbau- und Ablauforganisation (End-to-end-Prozess)* implementiert werden. Dadurch werden Redundanzen vermieden und Analogien für mehr Effizient genutzt.

Nachhaltigkeit könnte mit „bei Fortschritt bewahrend ausgerichtetes Entscheiden und Handeln" beschrieben werden.

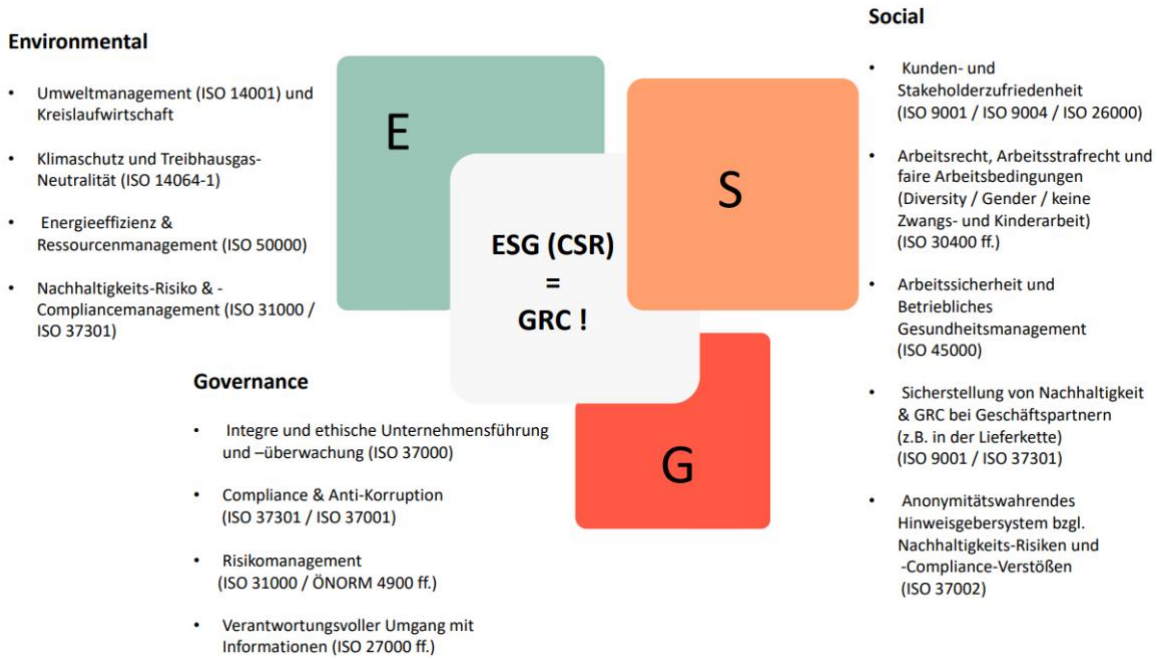
[13] Vgl. ISO 37000:2021 (Governance of Organizations)

[14] Zuständigkeiten, Aufgaben- und Verantwortungsbereiche, beispielsweise abgebildet in Organigrammen, Stellenbeschreibungen, etc. sowie Prozessabläufe, Delegationen und Interaktionen.

2. Was umfasst alles ein Risiko-, Compliance- und Nachhaltigkeits-Managementsystem in der Praxis?

Auch hier gibt es bisher noch keine Legaldefinition, so dass die Definitionsfreiheit viele Vorschläge ermöglicht:

Ein Nachhaltigkeits-, aber auch ein GRC-Managementsystem enthält in der Regel folgende Komponenten[15]:



Damit stellt sich die Frage, wie Organisationen / Unternehmen ein *Integriertes Risiko- und Compliance- bzw. Nachhaltigkeits-Managementsystem* aufbauen können:

Für die konkrete Umsetzung eines entsprechenden Systems gab es für Unternehmen und sonstige Organisationen (public / private / profit / non profit) bis vor kurzem noch keine international akzeptierten *und zertifizierbaren* Standards.

Diese Lücke schlossen nun die **zertifizierbaren** Standards DIN ISO 37301: 2021 und die ÖNORM 4900 ff.: 2021.

[15] Vgl. auch oben, Einleitung

3. Weisen die diversen Systeme (Risk, Compliance, Nachhaltigkeit etc.) nicht erhebliche Redundanzen und Analogien auf und drängt sich dadurch nicht der Ansatz eines Integrierten Managementsystems (IMS) mit z.B. Risk und Compliance „in einem Paket" auf?

Ja, da sämtliche ISO-Managementsystem-Standards einen „harmonisierten Aufbau" mit fast zu 70% redundanten / analogen Elemente aufweisen, empfiehlt es sich, *ein einziges* „Integriertes Managementsystem" anstelle vieler „Insel-Systeme" vorzuhalten..

4. Was ist der Kernbereich eines *Compliance-*, Risiko- und Nachhaltigkeits-Managementsystems?

Der Kernbereich eines *Compliance*-Risiko-Management-Systems besteht in der Planung, Umsetzung, Steuerung mit Überwachung und Anpassung / Verbesserung (P/D/C/A) von folgenden Komponenten:

Identifikation und Bewertung der zwingenden und fakultativ gesetzten Ziele und Risiken des *Compliance*-Management-Systems sowie die Ermittlung von Anforderungen und Handlungsbedarf für Maßnahmen sowie deren Umsetzung zur Erreichung dieser Ziele.

Außerdem allgemeine Prophylaxe- und Reaktionsmaßnahmen, wie beispielsweise Erlass von fehlenden beziehungsweise ergänzenden Regelungen (unter Berücksichtigung von internen und Umfeld-Veränderungen), der Installation eines *Compliance-Risikomanagement*-Prozesses mit Eruierung und Analyse, Bewertung und Steuerung von *Compliance*-Risiken sowie der Installation eines wirksamen Complianceverstoß-Erkennungs- und -Sanktionsprozesses.

Weitere Themen im Bereich Compliance-Managementsystem sind Compliance-Beauftragte, Hinweisgebersystem mit Ombudsmann (vgl. ISO 37002 :2021), Risikomanagement, Internal Investigations-Prozess und die Anreicherung der Prozess-Schritte mit Komponenten zur Erfüllung der Anforderung aller relevanten rechtlichen Regelungen (Gesetze, Rechtsprechung, Behördliche Auflagen, Technikstände, etc. und interner, verpflichtender Regelungen (z.B. Richtlinien).

5. Gab es Umfeldveränderungen, die die Bedeutung von *Risiko- und Compliance*-Management-Systemen steigern? Ist die Entstehungsgefahr, Entdeckungsgefahr, Sanktionsgefahr beziehungsweise das Haftungsrisiko bei *Compliance-Verstößen* und *nicht gesteuerten Risiken* in den letzten Jahren gestiegen?

Die Gefahr, dass *Compliance*-Verstöße häufiger als früher entstehen, geht unter anderem mit der Globalisierung einher: Die meisten mittelständischen Unternehmen weisen mittlerweile auch Auslandsbezüge auf. Gerade in den neuen Märkten Asien und Osteuropa bestehen noch erhebliche Gefahren und Möglichkeiten, in *Compliance*-Problematiken verwickelt zu werden.

Eine weitere neue Erscheinung stellen die Forderungen und Anforderungen der Großunternehmen gegenüber ihren Kunden und Lieferanten dar: Sie verlangen mittlerweile verpflichtend von ihren Geschäftspartnern die Vorhaltung von entsprechenden *Compliance*-Risikomanagement und Nachhaltigkeits-Systemen und lassen sich dies unter anderem auch vertragsstrafenbewehrt versichern.

Die Einhaltung entsprechender Anforderungen wird mittlerweile mittels ausführlichster Fragenkataloge oder sogar Audits vor Ort überprüft. Im Grunde werden die Anforderungen der Großunternehmen teilweise direkt in den Lieferketten von Unternehmen zu Unternehmen durch- und weitergereicht, so dass schließlich auch kleinere Unternehmen von diesem Trend betroffen sind. Als Sanktion für die Verweigerung entsprechender Anforderungen ist der Wegfall der Geschäftsbeziehung keine Ausnahme.

Nicht nur das neue Lieferkettengesetz verpflichtet die Unternehmen zur Überprüfung ihrer Supply Chain auf Risiko-, Compliance- und Nachhaltigkeitsmanagement.

Die großen nachhaltigkeitsberichtspflichtigen Unternehmen (vgl. 289 b ff. HGB) und ab 01.01.2024 auch Unternehmen ab 250 Mitarbeiter (für das Geschäftsjahr 2023) müssen auch dezidiert über ihre Maßnahmen zur Sicherstellung von Nachhaltigkeit, Compliance und Risikomanagement in ihrer Lieferkette berichten:

Deshalb werden diese Anforderungen verstärkt auf den Mittelstand durchgereicht. Gerade deshalb geht der Mittelstand verstärkt zur Implementierung von Nachhaltigkeits-, Risiko- und Compliance- Managementsystemen über.

Das *Entdeckungsrisiko* ist ebenfalls gestiegen, wofür es diverse Gründe gibt: Die eingerichteten Hinweisgebersysteme, wie Whistleblowing- oder Ombudsmannsysteme, funktionieren laut diverser wissenschaftlicher Aufsätze und Erfahrungen in der Praxis besser als Revision und *Controlling*, um entsprechende *Compliance*-Vorfälle aufzudecken.

Vgl. hierzu die aktuellen Trends: EU-Vorgabe zum Schutz von Whistleblowern mit den entsprechenden nationalen Umsetzungsgesetzen.[16]

Kronzeugenregelungen im Strafrecht aber auch vor allem „Bonusregelungen“ für den Erstmelder im Kartellrecht führen dazu, dass zum einen mehr Kartellverfahren eingeleitet werden, zum anderen aber die Informationen für die Behörden über den Hinweisgeber griffiger werden.

Eine weitere Erscheinung ist die verstärkte Professionalisierung der Staatsanwaltschaften und Wirtschaftsstrafkammern, die auf dem Gebiet des Compliancemanagements schon sehr eifrig arbeiten.

Auch die Möglichkeit der digitalen Datenanalyse im Zeitalter von *Big Data* kombiniert mit dem Einsatz von IT-Experten auf dem Gebiet der Forensik und entsprechender Spezialsoftware

[16] Vgl. *Scherer/Grötsch*, Unternehmenssanktionsrecht und Whistleblowing, 2021, zum kostenlosen Download auf Scherer-GRC.net/Publikationen

ermöglicht es, Verstöße aufzudecken, die mit herkömmlichen Methoden sehr häufig der Flut der Masseninformationen zum Opfer gefallen wäre.

Die Gefahr, bei *Compliance*-Verstößen verschärft sanktioniert zu werden, hat sich ebenfalls erhöht: Gewinnabschöpfungen, Geldbußen und Geldstrafen, entsprechende Nachforderungen von Sozialversicherungsbeiträgen und Steuern sowie Schadensersatzansprüche gegen unterschiedlichste Mitwirkende gehören zum Repertoire der Verfolger. Eine weitere, ganz erhebliche, existenzbedrohende Sanktion stellt der Wegfall von Geschäftsbeziehungen oder der Ausschluss von Märkten oder Auftragsvergaben dar. Auch bei einem finanziell weniger scharf sanktionierten Complianceverstoß kann das einhergehende sich verwirklichende Reputationsrisiko existenzbedrohende Züge annehmen.

Auch das Haftungsrisiko ist gestiegen, wenngleich nicht unbedingt neue Haftungstatbestände dazukamen. Lediglich die Pflichten wurden durch Literatur und Rechtsprechung ausgeweitet. Neu ist, dass sogar Mitglieder von Aufsichtsgremien auch tatsächlich regressiert werden**.** Im Übrigen gab es laut Bachmann[17] in den Jahren 1986 bis 1995 genauso viele Urteile zur Managerhaftung wie in den letzten 100 Jahren zuvor. In den nachfolgenden 10-Jahres-Zeiträumen habe sich diese Zahl nochmals verdoppelt.

Auch in den Medien ist das Thema „Verantwortung von Managern und Aufsichtsräten" ein Dauerbrennerthema, so dass die Wahrnehmung, aber auch die öffentliche Berichterstattung über die Betroffenen zugenommen hat.

Gemäß §§ 116, 107 AktG ist der Aufsichtsrat *persönlich* für die *Wirksamkeit* von Compliance-, Risiko-Managementsystem, Internes Kontrollsystem und Revision verantwortlich.

6. Welchen Mehrwert bietet ein *Compliance*-Risiko-Management-System einem Unternehmen?

Die Vorteile eines wirksamen (gelebten) *Compliance*-Risiko-Managementsystems liegen nicht nur in der Einsparung von Bußgeldern und Schadensersatzzahlungen.

Vielmehr soll es die Identifikation der Mitarbeiter mit dem Unternehmen stärken und hohe Fluktuationsraten vermeiden.

Bezüglich der Akquise von Fachkräften könne ein *Compliance*-, Risiko- und Nachhaltigkeits-Managementsystem ein Differenzierungsmerkmal darstellen.

Auch bei Kreditratings und Versicherungen (und aufgrund der Taxonomie-Verordnung) werden im Hinblick auf Risikobewertung und Prämienfestsetzung erhebliche Vorteile festgestellt.

[17] Vgl. Gutachten zum 70. Deutschen Juristentag 2014, Seite 13

Es lassen sich aber noch viele weitere Vorteile finden, wie beispielsweise die Erfüllung von zwingenden Kundenanforderungen oder das Überwinden von Markteintrittsbarrieren.

Ebenso die Vermeidung persönlicher zivil- und strafrechtlicher Sanktionen mit der Folge des persönlichen und beruflichen Existenzverlustes.

7. Was sind die Vorteile eines *zertifizierten* Risiko- und Compliance-Managementsystems?

Nach erfolgreicher Prüfung erhält in der Regel das Unternehmen ein *Zertifikat*, welches gegenüber den „Interested Parties / Stakeholdern" eine Beurteilung des *Compliance*-Risiko-Managementsystems ermöglichen soll.

Der Nutzen einer entsprechenden Dokumentation kann in einem unabhängigen und objektivierten Nachweis liegen, dass die *Compliance*-Strukturen angemessen und möglicherweise auch wirksam sind.

Dieser Nachweis lässt sich dann im positiven Sinn gegenüber Kunden, Versicherungen, Banken, Aufsichtsbehörden und Mitarbeitern und bei öffentlichen Ausschreibungen verwenden.

Intern könne so eine Prüfung auch als *Stresstest* für das Unternehmen zu verstehen sein, um den Verantwortlichen Schwächen im System aufzuzeigen und im eigenen Interesse die Möglichkeit zur Verbesserung zu geben. Dies mag häufig einen sogenannten „heilsamen Druck" erzeugen.

Unter Umständen könne eine erfolgreiche Wirksamkeitsprüfung auch eine haftungsmindernde Wirkung entfalten: Die Gerichte und Staatsanwaltschaften betonen in Fachvorträgen jedoch kontinuierlich, dass die Exculpation nicht lediglich in Dokumenten zu sehen, sondern vielmehr die Vorbildfunktion der Geschäftsleitung („Tone from the top") und das „Leben" der Vorgaben durch alle Mitarbeiter ausschlaggebend sei.

Erstmalige (!) Rechtsprechung des Bundesgerichtshofes zum Nutzen eines Compliance-Managementsystems

BGH, Urteil vom 09.05.2017 – 1 StR 265/16 (Krauss Maffei Wegmann „KMW"):

„Erstmals hat der Bundesgerichtshof (BGH) im Urteil vom 9.5.2017 festgestellt, dass *bei der Bußgeldbemessung gegen juristische Personen und Personenvereinigungen (§ 30 OWiG)* ***sowohl die Existenz eines Compliance-Management-Systems (CMS), als auch die das CMS betreffenden Optimierungsmaßnahmen, welche nach Einleitung eines staatlichen Sanktionsverfahrens ergriffen wurden, von Bedeutung*** *sind."*

*„**Unternehmen, insbesondere mittelständischen, die auch international tätig sind, ist daher dringend zu empfehlen, sich um die Einführung eines risikobasierten CMS bereits in Zeiten zu kümmern, in denen im Unternehmen aus Compliance-Sicht „die Welt noch in Ordnung ist**“, d.h. sie sollten besser Vorsorge als Nachsorge betreiben.“* [18]

Zitat *Raum*: zu: **Bedeutung und Auswirkung von Standards (ISO / IDW / etc.) und Zertifizierungen auf die Manager- und Unternehmenshaftung:**[19]

*„Ebenso stellt **der kommunikative Prozess**, der mit der Zertifizierung verbunden ist, **einen Wert an sich** dar. Hierdurch wird **Problembewusstsein geschaffen** und regelmäßig auch eine **Verbesserung der vorhandenen Strukturen** herbeigeführt. Jedenfalls können die auf dem Markt befindlichen **Richtlinien** gerade im unternehmerischen Bereich ein **wichtiger Leitfaden für den Aufbau und die Weiterentwicklung eines Compliance-Systems** sein.“*

„*Derartige Leitlinien können* deshalb *faktisch strafbarkeitskonstituierend sein*.“

8. Was kann "geprüft" bzw. "zertifiziert" werden?

Im Grunde lässt sich alles prüfen, beziehungsweise zertifizieren, also Personen, Produkte, aber natürlich auch Systeme. Weitere Infos hierzu finden sich im Akkreditierungsstellen-Gesetz.

9. Welche Arten von Prüfungen sieht der *IDW PS 980* vor?

Der Prüfungsstandard für Wirtschaftsprüfer zur Prüfung von *Compliance*-Management-Systemen *IDW PS 980* sieht zunächst eine *Konzeptionsprüfung* vor. Dabei wird geprüft, ob die Konzeption des CMS in wesentlichen Belangen zutreffend dargestellt ist und eine Beschreibung sämtliche Grundelemente eines CMS umfasst.

Des weiteren ist eine *Angemessenheitsprüfung* vorgesehen. Dabei wird geprüft, ob die Grundsätze und Maßnahmen des CMS in allen wesentlichen Belangen zutreffend dargestellt sowie angemessen sind. Darüber hinaus, ob die Grundsätze und Maßnahmen zu einem bestimmten Zeitpunkt auch (in Aufbau- und *Ablauforganisation*) implementiert sind.

---

[18] *Malik*, BGH: Berücksichtigung Compliance-Management-System bei Bußgeldbemessung, www.haufe.de/compliance/recht-politik/vorteile-durch-compliance-management-system-bei-bussgeldbemessung; vgl. auch Jenne/Martins, Compliance-Managementsysteme sind bei der Bußgeldbemessung zu berücksichtigen – Anmerkung zu BGH, Urteil vom 09.05.2017, CCZ 2017, S. 285 ff..

[19] *Raum* (Vorsitzender Richter des 1. Strafsenats des Bundesgerichtshofes), „Compliance im Zusammenhang straf- und bußgeldrechtlicher Pflichten“, S. 48 ff., Rn. 56 ff., in: *Hastenrath* (Hrsg.), Compliance-Kommunikation, 2017.

Als „letzte Stufe“ ist eine *Wirksamkeitsprüfung* vorgesehen. Bei der Wirksamkeitsprüfung wird festgestellt, ob Grundsätze und Maßnahmen des CMS in allen wesentlichen Belangen zutreffend dargestellt und angemessen sind sowie zu einem Zeitpunkt implementiert und in einem bestimmten Zeitraum wirksam sind.

10. Worauf ist bei der Vertrags-, Testats- und Urkundengestaltung zu achten?

Hierbei sind vielfältige Überlegungen anzustellen:

Über den entsprechenden Auftrag, aber auch das erteilte Testat oder eine ausgestellte Urkunde werden Informationen unter Umständen auch für Dritte mit einem vereinbarten oder sich aufgrund einer Prüfung ergebenden Inhalt erstellt und kommuniziert.

Dies kann, sofern Aussagen nichtzutreffend sind, unter Umständen sogar zu Haftungsansprüchen bei den Beteiligten führen. Es ist deshalb im Vorfeld genau zu überlegen, welche Leistungen erbracht werden sollen („Lasten- und Pflichtenheft“) und welche Ergebnisse erzielbar sind und wie diese letztendlich kommuniziert werden sollen/dürfen.

11. Kann ein Zertifikat oder Testat sogar haftungserhöhende Wirkung entfalten?

Ja, dies kann passieren. Aufgrund entsprechender vertraglicher Vorgaben werden bereits jetzt schon zwischen Unternehmer und Kunden oder sonstigen Akteuren im Hinblick auf Risiko- und Compliancemanagement verbindliche Vereinbarungen getroffen, die oft sogar vertragsstrafenbewehrt sind oder bei Pflichtverstößen Schadensersatzzahlungen auslösen könnten.

Wird durch das Testat Unzutreffendes bestätigt, hat dies unter Umständen Einfluss auf entsprechende Sanktionsmöglichkeiten und kann zu Regressen führen.

Darüber hinaus kann auch das Werben mit einem *Zertifikat*, das den tatsächlichen Zustand nicht realistisch widerspiegelt, zur erhöhten Verantwortung führen[20].

Entscheidend ist also, dass das über Urkunden / Testate / Zertifikate Versprochene auch zutrifft!

[20] *Scherer / Friedrich*, Risikoerhöhung durch Qualitäts- und Risikomanagementsysteme, ZfAW 2007, S. 2 ff.

12. Wie wird in der Praxis auditiert?

Ein Audit erfolgt üblicherweise – nicht abschließend – über Dokumentenprüfung, Interviews, Prozessprüfungen, digitale Datenanalyse und eigene Beobachtungen des Auditors.

13. Ist die ÖNORM 4900 ff: 2021 in Anlehnung an ISO 31 000 : 2018 sowie die DIN ISO 37301:2021 (*Compliance*-Managementsystem) zertifizierbar?

Ja, die ÖNORM 4901 ff. und die DIN ISO 37301 weisen Mussvorschriften auf und sind auf Zertifizierbarkeit angelegt.

14. Wie kann im Hinblick auf die Global Reporting Initiative (GRI) zertifiziert werden?

Hier ist auf alle Fälle eine Zertifizierung *in Anlehnung* an die in diversen zertifizierbaren ISO-Normen enthaltenen Bestimmungen[21] möglich.

15. Besteht bei einer Zertifizierung von *Compliance*-Risiko-Managementsystemen die Voraussetzung der Akkreditierung des Zertifizierers?

Soweit bisher bekannt ist, setzt die Zertifizierung von *Risiko-* oder *Compliance*-Managementsystemen noch keine Akkreditierung des Zertifizierers voraus.

Da die Zertifizierung kein Hoheitsakt ist, würde auch eine Akkreditierung lediglich ein mögliches Qualitätsmerkmal im Hinblick auf Objektivität und Sachkunde des Zertifizierers darstellen.

Ob eine existierende Akkreditierung für andere Themen (beispielsweise Qualitätsmanagement, Umweltmanagement) unter Beachtung der Vorgaben des Akkreditierungsstellen-Gesetzes die entsprechende Sachkunde auch für Compliancemanagement verifizieren kann, ist zu diskutieren.

Objektivität und Sachkunde sollte zumindest nachvollziehbar und transparent sein. Dies sollte jedoch nicht nur für die jeweilige Organisation, sondern auch für die handelnden Personen gelten.

[21] Vgl. oben, Frage 1.

16. Welche rechtliche *Qualität* hat ein *Zertifikat* einer privatrechtlichen Organisation?

Ein *Zertifikat* eines privaten Zertifizierers stellt eine Bekundung aufgrund einer privatrechtlichen Vereinbarung dar. Keinesfalls stellt ein entsprechendes *Zertifikat* eine hoheitliche Maßnahme dar, die entsprechenden Vertrauensschutz genießt.

17. Wird von der DIN ISO für Risk, Compliance und Nachhaltigkeit spezielle Sachkunde der Auditoren gefordert und ist bei den herkömmlichen Zertifizierungsgesellschaften bzw. Auditoren bereits die entsprechende Sachkunde bezüglich Risk-, Compliance- und Nachhaltigkeits-Management vorhanden?

Für Compliance gibt es ganz neu die ISO 17021 -13 : 2021: Anforderungen an die Kompetenzen von Auditoren im Bereich Compliance.

Die dort geregelten Grundsätze können analog auch für andere Themenbereiche herangezogen werden.

Die Existenz der angemessenen Sachkunde der Auditoren und im Zertifizierungsprozess Tätigen bei den vielen diversen Zertifizierungsanbietern kann nicht hinreichend beurteilt werden. In der Praxis gibt es hierzu noch wenige Informationen über entsprechende Referenzen.

Klar ist, dass es bisher kaum klassische und wenige berufsbegleitende Hochschulprogramme gibt, die sich interdisziplinär mit *Governance, Risk, Compliance und Nachhaltigkeit* beschäftigen.

Das berufsbegleitende und akkreditierte Masterprogramm *Risiko-* und Compliancemanagement der *Technischen Hochschule Deggendorf* (THD), das gemeinsam mit dem Kompetenzportal RiskNET und dem TÜV konzipiert wurde, stellt hier noch immer eine Ausnahme dar.

Ebenso der ab Herbst 2022 startende berufsbegleitende Bachelor (S.C.) „Nachhaltigkeit (ESG), Governance und Digitalisierung“ und der Zertifikatskurs „Nachhaltigkeit und GRC“ der *Technischen Hochschule Deggendorf.*

18. Welche Rolle spielen Testate nach *IDW PS 980* (Compliance) und 981 (Risk) im Ausland?

Da *IDW PS 980 und 981* von einem *Deutschen Bundesverband* erlassen wurden, mag unter Umständen im internationalen Geschäftsverkehr ein entsprechendes Testat des Instituts *Deutscher* Wirtschaftsprüfer nicht die erwünschte Anerkennung, beziehungsweise Wirkung erzielen.

19. Sieht die ISO 37301:2021 ähnlich wie der *IDW*-Standard Bereichsausnahmen vor?

Die ISO nennt entsprechende Bereichsausnahmen nicht so explizit wie der *IDW*-Standard.

Entsprechende Bereichsausnahmen müssten auf alle Fälle vertraglich sowie im Testat und auch in der entsprechenden Zertifikatsurkunde explizit hervorgehoben werden.

Im Übrigen mögen Bereichsausnahmen bei Compliance der Legalitätspflicht widersprechen.

20. Spielt die zertifizierbare ISO 9001:2015 (Qualitäts-Managementsysteme) möglicherweise im Hinblick auf den Bedarf eines *Compliance*-Risiko-Managementsystems nach DIN ISO 37301 :2021 und ÖNORM 4900 ff.: 2021 eine Rolle?

Die ISO 9001:2015 (Qualitäts-Managementsysteme) sieht als primäres Ziel die Kundenzufriedenheit vor. Gleichwohl ist in diesem Standard an zahlreichen Stellen eingeflochten, die Forderung erkennbar, dass „*gesetzliche und behördliche Anforderungen zu erfüllen sind*".

Dass zur Erfüllung der gesetzlichen und behördlichen Anforderungen (was den weiten Compliancebegriff noch nicht vollständig abdeckt) jedoch auch unter Umständen ein systematisches Vorgehen im Sinne von Compliancemanagement erforderlich ist, nennt die ISO 9001 nicht.

Ebenso erwähnt diese Norm neuerdings den „verstärkten" prozessorientierten und „neuen" risikobasierten Ansatz an zahlreichen Stellen, konstatiert jedoch gleichwohl, dass ein Risikomanagementsystem, insbesondere auch nach *ISO 31000*, nicht erforderlich sei, um die Kundenanforderungen zu erfüllen.

Dies mag den sachkundigen Leser irritieren. Außerdem muss ein „risikobasierter Ansatz" zwingend auch *Compliance*-Risiken umfassen, da angemessenes *Risikomanagement* nicht eine ganz erhebliche Risikogruppe (*Compliance*-Risiken) einfach ausklammern darf.

Somit verlangt auch die ISO 9001:2015 nach *Compliance*- und *Risikomanagement* im Unternehmen.

Diese „Systeme" sollten angemessen und wirksam sein, müssen sich jedoch nicht zwingend nach den einschlägigen ISO-Normen richten.

Belastend für die Praxis ist jedoch der sogar wachsende Trend der Standard-Ersteller, immer mehr zusätzliche Managementsystem-Inseln zu schaffen, statt – was ohne weiteres möglich wäre – der Praxis einen Standard zur Verfügung zu stellen, der diverse Anforderungen integriert.

Cui bono?

Wem nützt das?

Ein positives Beispiel stellt dagegen der PAS 99 : 2012 zum Integrierten Managementsystem und jetzt auch die „Harmonized Structure“ der ISO dar.

21. Wird die ISO 37301:2021 (*Compliance*-Managementsystem) im Ausland Anerkennung finden und welche Rolle spielen COSO-Standards?

ISO-Standards sind im Ausland bereits sehr verbreitet und anerkannt.

Es gibt auch Regionen, die auf *COSO*-Standards aufbauen. Der Nachteil von *COSO*-Standards gegenüber den ISO-Standards: Die vielen ISO-Standards für diverse Themen (vgl. oben die Grafik unter Frage 2) ermöglichen Integrierten Ansatz.

COSO deckt nicht so viele Themenfelder ab und weist *keinen* Integrierten Ansatz auf.

22. Welche rechtliche Bedeutung haben Standards?

Standards können unter Umständen einen bestimmten technischen Stand, wie beispielsweise den „Stand der Technik“ oder die „Anerkannten Regeln der Technik“ (den „Anerkannten Stand von Wissenschaft und Praxis“) widerspiegeln.

Nach Rechtsprechung von *Bundesgerichtshof* oder *Bundesverwaltungsgericht* besteht bei idealtypisch zu Stande gekommenen Standards eine entsprechende Vermutungswirkung, dass der Standard die „Anerkannten Regeln der Technik“ widerspiegelt.

Es muss aber bezweifelt werden, dass bei den derzeit inflationär produzierten Standards immer von einem „idealtypischen“ Zustandekommen in Transparenz, Fach- und Sachkunde bezüglich der maßgeblichen Disziplinen und Beteiligung der Öffentlichkeit und ohne Beeinflussung von Lolly-Gruppierungen auszugehen ist.

23. Wie ist das Thema „pflichtgemäßes Verhalten von Geschäftsführung, Vorstand, Aufsichtsrat“ in Hinblick auf §§ 43 GmbHG, 91, 93, 107, 116 Aktiengesetz, 130 OWiG, etc. und auf den „Anerkannten Stand von Wissenschaft und Praxis“ und bezüglich des Standards DIN ISO 37301:2021 abzugrenzen?

Die Pflichten zur gewissenhaften Geschäftsführung richten sich primär nach dem aktuellen Stand von Gesetzgebung und Rechtsprechung.

Dabei wird häufig auf den „Anerkannten Stand von Wissenschaft und Praxis“ als Messlatte für den einzuhaltenden Pflichtmaßstab Bezug genommen.

Entsprechende Standards wie DIN ISO 37301:2021 spiegeln diesen „Stand von Wissenschaft und Praxis“ im Sinne einer Vermutungswirkung dann wider, wenn sie idealtypisch zustande gekommen sind. Dies wäre zu verifizieren. Ebenso kann auch eine Vermutung natürlich widerlegt werden.

Die DIN ISO 37301 : 2021 enthält jedoch darüber hinaus sehr viele Anforderungen, die die Rechtsprechung bereits bezüglich der „Pflicht zur rechtssicheren Organisation“ aufstellte.

24. Besteht eine Vermutung, dass *ISO*- oder *IDW*-Standards generell idealtypisch zustande kommen?

Dies müsste im Detail überprüft werden, da hierzu oft die nötige Transparenz fehlt.

Bisweilen wird argumentiert, dass in diesen Institutionen Standards durch zahlreiche einzugehende Kompromisse, aber auch sogar durch Lobbyismus und der bisweilen fehlenden vertieften Darstellung des maßgeblichen Kernbereichs nicht optimiert gefasst seien.

Dennoch können die positiven Elemente des Standards Hinweise auf vernünftiges und pflichtgemäßes Verhalten geben und sind zumindest diesbezüglich begrüßenswert.

Die in einem genormten Verfahren erarbeiteten *ISO*-Normen sind im Gegensatz zu berufsgruppenspezifischen IDW-Standards Normen, die von den Beteiligten der Öffentlichkeit zur Diskussion und Kritik noch vor Erlass nahegebracht werden.

25. Enthält der Kernbereich eines *Compliance*-Managementsystems auch *Risikomanagement*-Komponenten wie beispielsweise die Erkennung, Analyse, Bewertung und Steuerung von *Compliance*-Risiken?

Ja, diese zentrale Anforderung findet sich in Punkt 4.6 Compliance-Risikoanalyse.

Im Kern geht es bei einer *Compliance*-Risikoanalyse um nichts anderes als die Analyse einer spezifischen Risikoart, eben von *Compliance*-Risiken.

Die Methoden, die sich im *Risikomanagement* als „Stand von Wissenschaft und Praxis“ entwickelt haben, können auch bei *Compliance*-Risiken angewendet werden.

So unter anderem gemäß IDW PS 340: 2020 die Quantifizierung und Aggregation, sowie die Ermittlung der Risikotragfähigkeit.

Zudem bestehen aus einer unternehmensweiten Sicht auf die Risikolandkarte vielfältige Abhängigkeiten zwischen *Compliance*-Risiken und anderen Risikoarten, etwa Reputationsrisiken oder Finanzrisiken.

26. Sind aufgrund der in einem CMS vorhandenen Risikomanagementkomponenten Kompetenzen von Standarderstellern und Auditoren nicht nur im Bereich *Compliancemanagement*, sondern auch im Bereich *Risikomanagement* gefragt?

Auch dies ist eindeutig zu bejahen.

Sowohl Standardersteller als auch Berater, Auditoren oder Zertifizierer müssen Kenntnis bezüglich der nach „Anerkanntem Stand von Wissenschaft und Praxis“ anzuwendenden Methoden des Risikomanagements, aber auch der Prozessmanagement-Methoden haben.

27. Gibt es Anbieter für die kombinierte Zertifizierung eines Integrierten Risiko- und Compliance- bzw. Nachhaltigkeits-Managementsystems?

Ja, es werden monatlich mehr:

Erfolgreiche Compliance-Managementsystem Auditierung[22]

Das Unternehmen Bayern Innovativ / Bayerische Gesellschaft für Innovation und Wissenstransfer mbH (Bayern Innovativ GmbH) hat sich als erstes Unternehmen im Jahr 2021 erfolgreich der Auditierung des Compliance-Managementsystems nach den Anforderungen der neuen ISO 37301 durch die TÜV SÜD Management Service GmbH gestellt.

Bei Einführung im Unternehmen wurde insbesondere Wert auf die *Verknüpfung des Compliance-Managementsystems mit den Prozessen des bereits bestehenden Qualitäts-Managementsystems* nach der ISO 9001 gelegt.

Diese Kombination der beiden Standards diente somit auch als Basis bei der Auditierung, um die erfolgreiche Einführung und Umsetzung der beiden Grundlagen durch die stichpunktartige Bewertung von Beispielen nachvollziehen zu können.

Besonders *das Zusammenwirken aller Unternehmensprozesse* über die verschiedenen Standorte hinweg stellt eine zusätzliche Herausforderung dar.

Diese Umsetzung konnte durch die externe Auditierung erfolgreich bestätigt werden.

Die im Verlauf der Auditierung befragten Mitarbeiterinnen und Mitarbeiter haben für den jeweiligen Verantwortungsbereich anhand von Beispielen die tägliche Praxis im Umgang mit den definierten Forderungen darstellen können.

[22] Das Unternehmen wurde vom Team „*Scherer*“, der *Governance Solutions GmbH,* bei der Vorbereitung auf die Zertifizierung unterstützt.

28. Bringt das „Kombizertifikat Risiko- und Compliance-Managementsystem“ auch Vorteile auch in Bezug auf Nachhaltigkeit (ESG)?

Ja: Ein kombiniertes Risiko- und Compliance-Managementsystem-Zertifikat kann zugleich auch bestätigen, dass damit auch die *Anforderungen eines Nachhaltigkeits-Managementsystems in Bezug auf Risiko- und Compliance-Management* erfüllt sind.

18.2.2022

Prof. Dr. jur. Josef Scherer

Rechtsanwalt und Consulter
Gründer und Leiter des Internationalen Instituts für Governance, Management, Risk- und Compliancemanagement der Technischen Hochschule Deggendorf THD

Rechtsanwalt Prof. Dr. Josef Scherer ist seit 1996 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, Partnerschaft 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-Ombudsmann 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 TÜV konzipierte er als Studiengangsleiter und Referent den seit 12 Jahren renommierten und akkreditierten berufsbegleitenden Masterstudiengang Risikomanagement und Compliancemanagement an der Technischen Hochschule Deggendorf und ist als externer Gutachter bei der (System-)Akkreditierung von Weiterbildungsstudiengängen tätig.

Seit 2012 leitet er als Vorstand des Direktoriums das Internationale Institut für Governance, Management, Risk- und Compliancemanagement der Technischen Hochschule Deggendorf als Kompetenzzentrum.

Außerdem ist er seit 2015 Mitglied des Beirates des Instituts für Risikomanagement und Regulierung (FIRM), Frankfurt (www.firm.fm).

Ebenso seit 2016 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 whistle blowing).

Ebenso seit 2016: Fachlicher Leiter der User Group *„Nachhaltige Unternehmensführung und Compliance“* der Energieforen Leipzig und seit 2018 Mitglied der Arbeitsgruppe 252.07 von Austrian Standards International zur Erarbeitung einer ÖNORM 4900 ff. (Risiko-Managementsystem-Standards).

Seine Forschungs- und Tätigkeitsschwerpunkte liegen auf den Gebieten Nachhaltigkeit (ESG/CSR), Managerenthaftung, Governance-, Risiko- und Compliancemanagement, 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.

Dipl.-Kfm. Prof. Dr. Andreas Grötsch

Rechtsanwalt, Steuerberater, Fachanwalt für Steuerrecht, Fachberater für internationales Steuerrecht

Rechtsanwalt Prof. Dr. Grötsch hat in München Betriebswirtschaftslehre und Rechtswissenschaften studiert und im Steuerstrafrecht bei Prof. Dr. Joecks promoviert.

Prof. Dr. Grötsch ist seit November 1998 (davon ab 2006 als Partner) bei der Kanzlei Wannemacher & Partner (www.wannemacher-partner.de) als Rechtsanwalt und Steuerberater tätig. Die Kanzlei Wannemacher & Partner zählt im Bereich Steuerstrafrecht und Steuerverfahrensrecht zu den renommiertesten Kanzleien in Deutschland und wird regelmäßig von den Zeitschriften JUVE, FOCUS, Wirtschaftswoche und Handelsblatt als führende Kanzlei ausgezeichnet.

Seine Tätigkeit in der Kanzlei konzentriert sich auf die Beratung von Organen und Mitarbeiten von Unternehmen sowie Privatpersonen im Bereich Steuerstrafrecht, Steuerverfahrensrecht und Tax-Compliance. Er vertritt dabei die ganze Bandbreite von kleinen bzw. einfach strukturierten Unternehmen bzw. deren Organe und Mitarbeiter bis hin zur Begleitung von Mandanten in den derzeit größten Steuerstrafverfahren in Deutschland wie etwa im Cum-Ex - und Goldfinger Verfahren. Seine Beratung umfasst dabei auch den Komplex der präventiven steuerstrafrechtlichen sowie Selbstanzeigeberatung.

Prof. Dr. Grötsch hat begleitend zu seiner Tätigkeit als Rechtsanwalt noch erfolgreich die Prüfungen als Steuerberater, Fachanwalt für Steuerrecht und Berater für internationales Steuerrecht abgelegt.

Seit 2020 leitet Prof. Dr. Grötsch den Lehrstuhl für Tax-Compliance, Steuerstrafrecht und Corporate Social Responsibility an der Technischen Hochschule Deggendorf.

In den Jahren 2005-2019 war er Lehrbeauftragter für Steuerstrafrecht an der Universität Osnabrück.

Seit 2009 ist er zudem Mitglied des Prüfungsausschusses des Staatsministeriums der Finanzen für die mündliche Steuerberaterprüfung.

Er hält seit vielen Jahren diverse Vorträge in den Bereichen Steuern, Steuerstrafrecht und Tax-Compliance.

Forschungs- und Tätigkeitsschwerpunkte:

- Corporate Social Responsibility
- Steuerstrafrecht
- Steuerverfahrensrecht
- Tax-Compliance

Zahlreiche Publikationen auf den Gebieten:

- Steuerstrafrecht
- Corporate Social Responsibility

Die Veröffentlichungen (auch zum kostenlosen Download) finden Sie unter www.gmrc.de/publikationen

Kontakt:
josef.scherer@gmrc.de
www.gmrc.de

Interview: Prof. Dr. Scherer: „GRC in der Praxis – Von der Resilienz und dem nachhaltigen Handeln“ bitte QR-Code scannen: