



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



Frank Romeike  
Gründer des Kompetenzzentrums RiskNET – The Risk Management Geschäftsführer und Eigentümer der RiskNET GmbH, sowie Gründer und Gesellschafter von RiskNET Advisory & Partner  
Mitglied des Vorstands des GMRC-Instituts der THD.



Dipl.-Kfm. Prof. Dr. Andreas Grötsch  
Rechtsanwalt, Steuerberater, Fachanwalt für Steuerrecht  
Professor für Corporate Social Responsibility und Tax Compliance an der THD Deggendorf.  
Mitglied des Vorstands des GMRC-Instituts der THD.

Scherer / Romeike / Grötsch

## **Unternehmensführung 4.0: CSR/ESG, GRC & Digitalisierung integrieren**

„...I hope someday you'll join us  
And the world will be as one...“ Imagine (John Lennon)

### **1. Messbare Anforderungen an Nachhaltigkeit (CSR / ESG) und GRC einfach und effizient mit Integriertem Managementsystem erfüllen**

„Ab jetzt sind wir alle nachhaltig, compliant, risikoorientiert und digital!“

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 Zielen Nachhaltigkeit, Compliance, Risikoorientierung und 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)*. Dies erleichtert und reduziert vor allem den Aufwand bei der Einführung und der operativen Umsetzung eines Nachhaltigkeits- bzw. GRC-Managementsystems enorm.

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

Der enorme Nachholbedarf vor allem in öffentlich-rechtlichen aber auch privatrechtlichen Organisationen bei Nachhaltigkeit, GRC und Digitalisierung wurde mittlerweile umfänglich öffentlich bekannt.<sup>1</sup>

---

Hinweis: 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.

Eine permanente inhaltliche Kontrolle der verlinkten Seiten ist jedoch ohne konkrete Anhaltspunkte einer Rechtsverletzung nicht zumutbar. Bei Bekanntwerden von Rechtsverletzungen werden wir derartige Links umgehend entfernen.

<sup>1</sup> Vgl. die aktuellen und oft leider schon wieder viel zu schnell vergessenen Korruptionsskandale und Complianceverstöße bei Staatsregierungen, in Politik, Religionsgemeinschaften, im Management größerer und kleinerer Unternehmen/Organisationen/Verbände. Aufgabe: Sammeln Sie bitte aus den aktuellen Nachrichten die Skandalfälle: Prüfen Sie, ob wirksam gelebtes und kontrolliertes GRC/ESG/CSR diese verhindert hätte.

Und „größere“ Kunden verlangen in diesem Trend<sup>2</sup> von ihren Lieferanten / Supplier verstärkt und ernsthaft Nachweise über wirksame Nachhaltigkeits-(CSR-/ESG-) und GRC-Systeme.

In ► Infobox 01 finden Sie einige relevante Definitionen zum Thema.

### **Info-Box 01: Definitionen**

**Management** nach der Plan-/Do-/Check-/Act-Methode umfasst Unternehmens-, Umfeld-, Stakeholder-Analysen (auch bzgl. Geschäftsmodell und -prozesse), Zielsetzung, Strategieentwicklung, Planung, Umsetzung, Steuerung und Überwachung, Reporting.

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

**Risikomanagement** beschäftigt sich mit Unsicherheiten bei Entscheidungen und Zielerreichung. Unternehmerische Tätigkeit ist 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 daher als Streuung um einen Erwartungswert definiert. Nach dieser Definition werden sowohl positive Abweichungen (Chancen) als auch negative Abweichungen (Gefahren) berücksichtigt.<sup>4</sup>

**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].

**Nachhaltigkeit<sup>5</sup> (ESG<sup>6</sup>/CSR<sup>7</sup>)** 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*“<sup>8</sup> beschrieben werden.

---

<sup>2</sup> Vgl. hierzu das Lieferkettengesetz sowie die Berichtspflichten bzgl. Nachhaltigkeit in der Supply Chain. Vgl. zum Lieferkettengesetz: *Huth, Romeike*, Supply Chain Risk Management: ESG-Risiken in der Lieferkette erkennen, in: Zukunftssicher: So geht Innovation an der Schnittstelle von Wirtschaft und Versicherung, Murmann Verlag, Hamburg 2021.

<sup>3</sup> Vgl. *Grötsch, Andreas*, Erklärung zum Deutschen Corporate Governance Kodex, 2021, aufrufbar unter: [www.risknet.de](http://www.risknet.de)

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

<sup>5</sup> Vgl. *Scherer, Kollmann, Birker*, Integriertes Nachhaltigkeits-Managementsystem, 2019, zum kostenlosen Download auf [scherer-grc.net/Publikationen](http://scherer-grc.net/Publikationen).

<sup>6</sup> ESG ist ein Akronym und steht für Environmental, Social, Governance (zu Deutsch: Umwelt, Soziales und Unternehmensführung)

<sup>7</sup> CSR ist ein Akronym und steht für „Corporate Social Responsibility“, d.h. eine unternehmerische Gesellschaftsverantwortung bzw. unternehmerische Sozialverantwortung

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

**Governance, Risk, Compliance und Nachhaltigkeit „zusammen“**, also „GRC“ bzw. ESG/CSR ist u.U. 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<sup>9</sup>**

Nachdem die „großen“ Unternehmen<sup>10</sup> nachhaltigkeitsberichtspflichtig wurden und der Bericht auch verpflichtet, die Business Partner (insbesondere Lieferanten / Supplier) auf Nachhaltigkeit zu prüfen, setzt sich auch im Mittelstand der kombinierte Nachhaltigkeits- und Geschäftsbericht durch. Außerdem soll die CSR-Berichtspflicht künftig auch *gesetzlich* auf den Mittelstand<sup>11</sup> ausgeweitet<sup>12</sup> werden.

**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 auf die digitale Transformation ausgerichtet, sofern sinnvoll.

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

---

<sup>9</sup> 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.

Zitat aus [www.globalreporting.org/standards](http://www.globalreporting.org/standards):

„Der Standard „Global Reporting Initiative wird vom Global Sustainability Standards Board (GSSB) herausgegeben. Die einzelnen GRI-Standards stehen unter [www.globalreporting.org/standards](http://www.globalreporting.org/standards) komplett zum Download bereit. GRI 101: Grundlagen gilt für alle Organisationen, die ihre Berichte zu ökonomischen, ökologischen und/oder sozialen Auswirkungen auf Grundlage der GRI-Standards erstellen möchten.

Mit den GRI-Standards wird für Organisationen und Stakeholder eine gemeinsame Sprache geschaffen, auf deren Grundlage die ökonomischen, ökologischen und sozialen Auswirkungen von Organisationen vermittelt und verstanden werden können.

Die in den Nachhaltigkeitsberichten enthaltenen Informationen erlauben es internen und externen Stakeholdern, sich eine Meinung zu bilden und angesichts der Beiträge der betreffenden Organisation zum Ziel einer nachhaltigen Entwicklung fundierte Entscheidung zu treffen.“

Durch die Verweisung in § 264a Abs. 1 HGB sind auch haftungsbeschränkte offene Handelsgesellschaften und Kommanditgesellschaften sowie durch die Verweisung in § 336 Abs. 2 S. 1 Nr. 2 HGB Genossenschaften bei Erfüllung der oben aufgeführten Kriterien verpflichtet, solch eine nichtfinanzielle Erklärung zu erstellen. Dieser Bericht muss gem. § 289c Abs. 2 HGB zumindest die Umweltbelange, Arbeitnehmerbelange, Sozialbelange, die Achtung der Menschenrechte sowie die Bekämpfung von Korruption und Bestechung umfassen. Viele Unternehmen, die diese Kriterien nicht erfüllen, erstellen trotzdem freiwillig solche nichtfinanziellen Erklärungen, um die Reputation für ihr Unternehmen zu verbessern.

<sup>10</sup> BMW erstellte 2019 einen (*kombinierten*) Nachhaltigkeits- und Geschäftsbericht.

<sup>11</sup> Sämtliche Kapitalgesellschaften mit mehr als 500 Mitarbeitern (auch ohne die Voraussetzungen der Kapitalmarktorientierung) sowie sämtliche Unternehmen aus nachhaltigkeitssensiblen Branchen (sog. High-Impact-Sektoren).

<sup>12</sup> Grötsch, Andreas, Corporate Social Responsibility-Berichtspflicht und die Folgen von Rechtsverstößen, KOR (Zeitschrift für internationale und kapitalmarktorientierte Rechnungslegung), 2021 und Sustainable Finance-Beirat der Bundesregierung, Zwischenbericht, 2020, 33 f., aufrufbar unter: [https://sustainable-finance-beirat.de/wp-content/uploads/2020/200306\\_SFB-Zwischenbericht\\_DE.pdf](https://sustainable-finance-beirat.de/wp-content/uploads/2020/200306_SFB-Zwischenbericht_DE.pdf), zuletzt aufgerufen am 13.04.2021.

Zugleich ist zu analysieren, welche Aktivitäten künftig noch von Menschen oder (teil-), automatisiert durch Anwendungen, IT-Systeme, Roboter, Algorithmen oder sonstigen Tools aus Digitalisierung und Artificial Intelligence (AI)<sup>13</sup> ersetzt bzw. unterstützt werden.

Ein „**Digitalisiertes Integriertes GRC- / ESG- (CSR-) Managementsystem**“<sup>14</sup> ist ein Managementsystem<sup>15</sup>, das mehrere Unternehmensfunktionen bzw. Prozesse (z.B. Nachhaltigkeits-, Risiko-, Qualitäts-, Umwelt-, Arbeitssicherheits- und Compliancemanagement) digitalisiert und zu einem „Unternehmensführungs-System“ integriert.

## **2. Messbare und verbindliche Soll-Größen / Komponenten von Nachhaltigkeit und Governance / GRC**

### **2.1 Zwingende rechtliche Rahmenbedingungen für Nachhaltigkeit (CSR / ESG), Unternehmensführung mit Governance, Risk & Compliance (GRC) und Digitalisierung**

Geschäftsleitung und sonstige Verantwortliche *müssen* die jeweiligen von ihnen betreuten (GRC) (Prozess-) Themenfelder / Bereiche und auch die nachfolgend dargestellten 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.

Zahlreiche Einzelgesetze und Rechtsprechung beschäftigen sich mit zwingend zu beachtenden Teilgebieten von GRC und Nachhaltigkeit (ESG / CSR), wie zum Beispiel das gesamte öffentlich- und privat-rechtliche Umweltrecht, Arbeitsrecht, Arbeitssicherheit- und Gesundheitsschutzrecht, Straf- und Ordnungswidrigkeitenrecht, u.v.m.

Aufgrund der „Legalitätspflicht“ der Geschäftsleitung und der Anforderungen an einen „gewissenhaften“ Geschäftsführer, Vorstand, Aufsichtsrat, Kaufmann (§§ 43 GmbHG, 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.

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, Abschlussprüfung oder Zertifizierung gut vorbereitet zu sein. Standards können laut dem Vorsitzenden Richter des 1. Strafsenats des BGH „strafbarkeitskonstituierend“ sein.<sup>16</sup>

---

<sup>13</sup> Der englische Begriff „Artificial Intelligence“ (AI) wird nur allzu häufig mit „Künstlicher Intelligenz“ übersetzt. Dabei bedeutet „Intelligence“ viel mehr Informationsverarbeitung. „Die Central Intelligence Agency heißt ja auch nicht so, weil die so gescheit sind“, sagt der österreichische Kybernetiker, Artificial-Intelligence-Experte und Wissenschaftler Robert Trappl. AI beschäftigt sich im Kern mit der Nachbildung menschenähnlicher Entscheidungsstrukturen durch Algorithmen. Vgl. hierzu *Romeike, Frank*, Predictive Analytics im Risikomanagement - Daten als Rohstoff für den Erkenntnisprozess, in: CFO aktuell, März 2017.

<sup>14</sup> Vgl. *Scherer / Fruth / Grötsch* (Hrsg.), Digitalisierung, Nachhaltigkeit und „Unternehmensführung 4.0“ (GRC), 2021, S. 23. Leseprobe unter [scherer-grc.net/publikationen](http://scherer-grc.net/publikationen)

<sup>15</sup> 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.

<sup>16</sup> Vgl. Raum, in: Hastenrath, Compliance-Kommunikation, 2018.

**Damit stellt ein *Compliance*-Managementsystem einen grundlegenden und wesentlichen Teil von Nachhaltigkeit (ESG / CSR) sicher.**

## **2.2 Nachhaltigkeits-Komponenten: „Das saubere Dutzend“**

Ein Nachhaltigkeits-Managementsystem bzw. die CSR-Berichterstattung nach GRI beschäftigt sich nach herrschender Meinung in Literatur und Nachhaltigkeits-Standards (GRI / Global Compact / etc.) i.d.R. primär mit den folgenden 12 Themen:

(mit aktuellen themenspezifischen *Spezial*-Standards<sup>17)</sup><sup>18</sup>

1. Governance (Ordnungsgemäße, ethische Unternehmensführung) (ISO 37 000 : 2021: Governance of organizations)<sup>19</sup>
2. Compliance (ISO 37301 : 2021<sup>20</sup> / IDW PS 980) und Anti-Korruption (ISO 37001 : 2021<sup>21</sup>)
3. Kunden- und Stakeholdermanagement (ISO 9001 : 2015 und ISO 9004 : 2018)
4. Risikomanagement (ISO 31000 : 2018 / ÖNORM 4900 ff. : 2021<sup>22</sup> / IDW PS 981)
5. Umweltmanagement (ISO 14000 : 2015)
6. Klimaschutz und Treibhausgas-Neutralität
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, Informationssicherheit (ISO 27000 ff. : 2017), Datenschutz]
11. Sicherstellung von Nachhaltigkeit in Lieferkette und bei Geschäftspartnern
12. Anonymitätsbewahrendes Hinweisgebersystem für Nachhaltigkeits-Risiken und Compliance-Verstöße (ISO 37002 : 2021)

---

<sup>17</sup> Standards sind i.d.R. 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.

<sup>18</sup> Klarstellender Hinweis: Um ein angemessenes Nachhaltigkeits-Managementsystem zu implementieren, ist es nicht erforderlich, die aufgeführten Standards in „Insel-Managementsystemen“ umzusetzen oder zu zertifizieren.

<sup>19-24</sup> Autor *Scherer* ist Mitglied der einschlägigen Arbeitsgruppe.

## 2.3 Governance und GRC

Der Normungsausschuss 175-00-01 AA der DIN erarbeitete jüngst die **ISO FDIS 37000: 2021 (E) Guidance for the Governance of Organizations**.<sup>23</sup> mit folgenden Punkten als **Kernbereich**:

1. Mission, Werte, Kultur
2. Nachhaltige Wertschöpfung
3. Strategie
4. Rechtlicher Rahmen / Compliance: Gesetze, Normen, Regeln, Richtlinien.
5. Verantwortungsbewusstsein<sup>24</sup>
6. Stakeholder-Relationship
7. Führung und Werte<sup>25</sup>
8. Daten und Entscheidungen<sup>26</sup>
9. Risikobasierte Unternehmensführung<sup>27</sup>
10. Soziale Verantwortung<sup>28</sup>
11. Nachhaltigkeit<sup>29</sup>

## 3 Beweis: Nachhaltigkeit (ESG / CSR) = GRC!

Vergleicht man nun die oben unter 2. dargestellten konkreten *und messbaren (!) Anforderungen aus gesetzlichen Regelungen und Standards*, so zeigen sich auffällig die enormen Redundanzen zwischen Governance bzw. GRC und Nachhaltigkeit (ESG/CSR). GRC und Nachhaltigkeit (ESG/CSR) sind weitestgehend identisch.

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

---

<sup>24</sup> „Fit & proper“-Kompetenzen, Transparenz und Vertrauen.

<sup>25</sup> Werte definieren und die Organisation nachhaltig, ethisch und effektiv führen.

<sup>26</sup> Daten als wertvolle Ressource für Entscheidungsvorbereitung und -fällung.

<sup>27</sup> Steuerung der Unsicherheiten bzgl. strategischer Ziele.

<sup>28</sup> Gesellschaftliche Verantwortung (CSR / ESG).

<sup>29</sup> Ökonomische, soziale und ökologische Wertschöpfung.

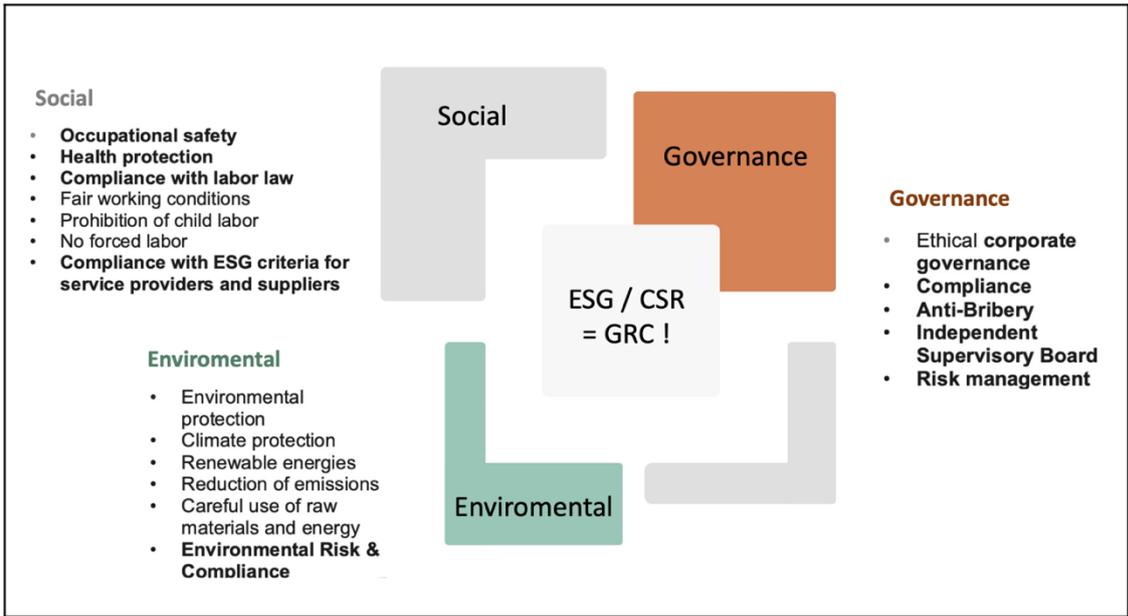


Abb. 02: Environmental, Social, Governance = GRC<sup>30</sup>

<sup>30</sup> Abbildung in Anlehnung an Euramco, zuletzt abgerufen am 30.03.2021, unter <https://www.euramco-asset.de/glossar/environmental-social-governance-esg/>

## 4 Strafbarkeit von Falschinformation bzgl. Nachhaltigkeit (Greenwashing) und Governance<sup>31</sup>

§ 331 Nr. 1 HGB regelt, dass *Organe einer Kapitalgesellschaft* (z.B. Vorstand / Geschäftsführer) mit Freiheitsstrafe bis zu 3 Jahren oder mit Geldstrafe bestraft werden, wenn die Verhältnisse der Kapitalgesellschaft in der nichtfinanziellen Erklärung bzw. im nichtfinanziellen Bericht unrichtig wiedergegeben oder verschleiert dargestellt werden.

Darunter fallen auch Kapitalgesellschaften, die *freiwillig* eine nichtfinanzielle Erklärung erstellen und darin die Verhältnisse unrichtig wiedergeben oder verschleiern. Erstellt eine Gesellschaft trotz bestehender Verpflichtung keine nichtfinanzielle Erklärung, so ist dagegen der Tatbestand des § 331 Nr. 1 HGB nicht erfüllt. Gleiches gilt nach der hier vertretenen Auffassung, wenn eine Gesellschaft zwar eine nichtfinanzielle Erklärung erstattet, in dieser jedoch wesentliche Angaben weglässt.

Eine Verurteilung wegen § 331 HGB hat zur Folge, dass das betroffene Organ gem. § 6 Abs. 2 S. 2 GmbHG bzw. § 76 Abs. 3 AktG für die Dauer von fünf Jahren seit der Rechtskraft des Urteils nicht mehr als Geschäftsführer einer GmbH bzw. Vorstand einer Aktiengesellschaft tätig werden darf.

Ferner kann gegen das Unternehmen eine Verbandsgeldbuße bis zu 10 Mio. Euro nach § 30 OWiG festgesetzt werden.<sup>32</sup>

Bedauerlicherweise hat sich in den letzten Jahren die Problematik von „*Greenwashing*“, bei der dem Verbraucher bewusst vorgetäuscht wird, dass das Unternehmen oder das Produkt besonders nachhaltig oder umweltfreundlich ist, verschärft. Häufig findet sich diese unter anderem wettbewerbsrechtlich zu sanktionierende Problematik im Bereich des Marketings.<sup>33</sup>

## 5 Auditierung und Zertifizierung eines (kombinierten) Nachhaltigkeits- / GRC-Managementsystems und eines Nachhaltigkeits-Berichtes

Viele Organisationen haben bereits bemerkt, dass der Ansatz eines *Integrierten* GRC- / ESG-Managementsystems effektiver und zugleich wesentlich kostengünstiger ist, als zahllose „Insel-Systeme“ bürokratisch mit hohen Kosten und wenig Wertbeitrag zu verwalten.

Entsprechend häufen sich Anfragen nach Kombi-Zertifikaten bei den Zertifizierenden.

Das Internationale Institut für Governance, Management, Risk & Compliance der Technischen Hochschule Deggendorf<sup>34</sup> auditert und zertifiziert bereits erfolgreich Integrierte GRC- bzw. Nachhaltigkeits-Managementsysteme.

<sup>31</sup> Grötsch, Andreas, Corporate Social Responsibility-Berichtspflicht und die Folgen von Rechtsverstößen, KOR (Zeitschrift für internationale und kapitalmarktorientierte Rechnungslegung, 2021 und Sustainable Finance-Beirat der Bundesregierung, Zwischenbericht, 2020, 33 f., aufrufbar unter: [https://sustainable-finance-beirat.de/wp-content/uploads/2020/200306\\_SFB-Zwischenbericht\\_DE.pdf](https://sustainable-finance-beirat.de/wp-content/uploads/2020/200306_SFB-Zwischenbericht_DE.pdf), zuletzt aufgerufen am 13.04.2021

<sup>32</sup> Die mögliche Buße nach dem geplanten *Unternehmenssanktionsrecht* könnte weitaus höher ausfallen.

<sup>33</sup>Vgl. Bundesministerium der Justiz und für Verbraucherschutz, zuletzt aufgerufen am 12.02.2021 unter [https://www.bmjv.de/SharedDocs/Pressemitteilung/DE/2021/0208\\_Greenwashing.html](https://www.bmjv.de/SharedDocs/Pressemitteilung/DE/2021/0208_Greenwashing.html): Eine Untersuchung des europäischen Verbraucherschutz-Netzwerks CPC hat aktuell ergeben, dass bei einer Auswertung von 334 Nachhaltigkeitsaussagen in 42 % der Fälle irreführende Angaben zur Nachhaltigkeit festgestellt wurden.

<sup>34</sup> [www.gmrc.de](http://www.gmrc.de)

## 6 Ausblick

Obwohl Nachhaltigkeit (ESG / CSR) nahezu deckungsgleich mit dem Themenkomplex Governance / GRC ist, führt das Thema „Nachhaltigkeit“ auf eine wesentlich größere Sensibilisierung bei Geschäftsleitung und Stakeholder als „GRC“.

Das mag u.a. damit zusammenhängen, dass vor allem die junge Generation erkannt hat, dass die „neuen Zeiten“ auch „neue Sichtweisen“, „neue Menschenrechte“<sup>35</sup> und „neues Management“ erfordern, wenn wir als Homo Sapiens nicht bis zum Jahr 2100 (wie *Harari*<sup>36</sup> statuiert) das Schicksal des Aussterbens mit dem Homo Neanderthaliensis, der vor ca. 30.000 Jahren „verschwand“, teilen wollen.

Es ist für alle privat- und öffentlichrechtlichen Organisationen Zeit, sich um Nachhaltigkeit und Governance zu kümmern.

„We’re gonna move to a better home” – (Elvis Presley)

---

<sup>35</sup> Vgl. zur Forderung der neuen Grundrechte *Ferdinand von Schirach, Jeder Mensch, 2021*

<sup>36</sup> Vgl. *Harari, Sapiens – Der Aufstieg, Comic, 2021, S.15*

## Zu den Autoren:



### **Prof. Dr. jur. Josef Scherer**

Rechtsanwalt

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, Dr. Rieger & Mittag 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 10 Jahren renommierten und akkreditierten berufsbegleitenden Masterstudiengang Risikomanagement und Compliancemanagement an der Technischen Hochschule Deggendorf und ist als externer Gutachter bei der (System-)Akreditierung 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](http://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 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 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 GRC, Digitalisierung und integrierte Workflow-Managementsysteme Gesellschafter-Geschäftsführer der Governance-Solutions GmbH und Aufsichtsrat in diversen Unternehmen und Stiftungen.



### **Frank Romeike**

Gründer des Kompetenzzentrums RiskNET - The Risk Management Network. Er ist Geschäftsführer und Eigentümer der RiskNET GmbH sowie Gründer und Gesellschafter von RiskNET Advisory & Partner.

Er zählt international zu den renommiertesten und führenden Experten für Risiko- und Chancenmanagement und coacht seit rund 20 Jahren Unternehmen aller Branchen und Unternehmensgrößen rund um die Themengebiete Risiko- bzw. Chancenmanagement und Wertorientierte Unternehmenssteuerung. Im Rahmen von Intensiv- und Inhouse-Seminaren der Risk Academy hat er weltweit mehr als 22.000 Risikomanager ausgebildet bzw. gecoacht.

Mit RiskNET ([www.RiskNET.de](http://www.RiskNET.de), [www.risknet.at](http://www.risknet.at) [www.risknet.ch](http://www.risknet.ch)) hat er das mit Abstand führende, deutschsprachige Kompetenz-Portal zum Thema Risk Management und Compliance aufgebaut. In seiner beruflichen Vergangenheit war er Chief Risk Officer bei der IBM Central Europe, wo er u. a. an der Einführung des weltweiten Risk-Management-Prozesses der IBM beteiligt war und mehrere internationale Projekte leitete. Er hat u. a. ein wirtschaftswissenschaftliches Studium (mit Schwerpunkt Versicherungsmathematik) in Köln und Norwich/UK abgeschlossen. Im Anschluss hat er Politikwissenschaften, Psychologie und Philosophie studiert. Außerdem hat er ein exekutives Masterstudium im Bereich Risiko- und Compliancemanagement abgeschlossen.

Er ist Mitglied des Vorstands des International Institute for Governance, Management, Risk & Compliance der Technischen Hochschule Deggendorf (TDH).

#### Forschungs- und Tätigkeitsschwerpunkte:

- Analytische Methoden und Kreativitätsmethoden im Risikomanagement
- Szenarioanalyse und Simulationsmethoden
- Quantitative Methoden im Risikomanagement
- Bandbreitenplanung
- Cash flow at Risk, Ebit at Risk
- Wertorientierte Steuerung
- Enterprise Risk Management
- Projekt-Risikomanagement
- Supply Chain Risk Management (SCRM)

Weitere Informationen unter [www.romeike.info](http://www.romeike.info)



### **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](http://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 Mitarbeitern 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