

# LEITARTIKEL

Josef Scherer\*

Andreas Grötsch\*\*

Frank Romeike\*\*\*

## Forschungsbedarf bei Nachhaltigkeit (CSR / ESG), Governance und Digitalisierung / KI<sup>1</sup>:

*„...I hope someday you'll join us  
And the world will be as one...”*

Imagine (John Lennon)

Die vorliegende Ausgabe des Bavarian Journal of Applied Sciences (BJAS) legt den Schwerpunkt auf den Forschungsbedarf bei Nachhaltigkeit (ESG / CSR), Governance, Digitalisierung / KI und Unternehmensführung 4.0.

Der Herausgeber bedankt sich bei den AutorInnen für die Einreichung der Beiträge, sowie den Reviewern aller eingereichten Beiträge für ihre wertvolle Arbeit. Wir wünschen Ihnen aufschlussreiche Einblicke und eine anregende Lektüre.

\* Rechtsanwalt und Consultant, 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).

\*\* Rechtsanwalt, Steuerberater, Fachanwalt für Steuerrecht  
Professor für Corporate Social Responsibility und Tax Compliance an der THD Deggendorf. Mitglied des Vorstands des GMRC-Institut der THD.

\*\*\* 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-Institut der THD.

**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.

**Gender-Hinweis:** In diesem Artikel wird aus Gründen der besseren Lesbarkeit das generische Maskulinum verwendet. Weibliche und anderweitige Geschlechteridentitäten werden dabei ausdrücklich mitgemeint.

<sup>1</sup> Vgl. Scherer, Romeike, Grötsch, Unternehmensführung 4.0: CSR/ESG, GRC & Digitalisierung integrieren, 2021, zum kostenlosen Download auf risknet.de.

Josef Scherer\*

Andreas Grötsch\*\*

Frank Romeike\*\*\*

## Need for Research in Sustainability (CSR / ESG), Governance and Digitalization / AI<sup>1</sup>:

*“...I hope someday you’ll join us  
And the world will be as one...”*

Imagine (John Lennon)

This issue of the Bavarian Journal of Applied Sciences (BJAS) focuses on the need for research in sustainability (ESG / CSR), governance, digitalization / AI and corporate governance 4.0.

The editor would like to thank the authors for submitting their contributions, as well as the reviewers of all submitted contributions for their valuable work. We wish you interesting insights and many inspirations while reading.

\* Lawyer and consultant, board member of the International Institute for Governance, Management, Risk and Compliance Management at the Technical University of Deggendorf. Member of various ISO / DIN standards committees (governance, compliance, human resources management) and of Austrian Standards International (risk management system).

\*\* Lawyer, tax advisor, tax law specialist  
Professor for Corporate Social Responsibility and Tax Compliance at the THD Deggendorf. Member of the board of the GMRC Institute of the THD.

\*\*\* Founder of the Competence Centre RiskNET – The Risk Management  
Managing Director and owner of RiskNET GmbH, as well as founder and partner of RiskNET Advisory & Partner.  
Member of the Board of the GMRC Institute of the DIT.

**Note:** This article contains links to external websites of third parties over whose content we have no influence. Therefore, we cannot assume any liability for these external contents. The respective provider or operator of the pages is always responsible for the content of the linked pages. The linked pages were checked for possible legal violations at the time of linking. Illegal contents were not recognisable at the time of linking.

However, a permanent control of the contents of the linked pages is not reasonable without concrete evidence of a violation of the law. If we become aware of any infringements of the law, we will remove such links immediately.

**Gender note:** In this article, the generic masculine is used for better readability. Female and other gender identities are explicitly included.

<sup>1</sup> Cf. *Scherer, Romeike, Grötsch*, Unternehmensführung 4.0: CSR/ESG, GRC & Digitalisierung integrieren, 2021, available for free download at risknet.de.

# LEITARTIKEL

## **1. Messbare und zwingende Anforderungen an GRC, Nachhaltigkeit (CSR / ESG) und Digitalisierung / KI: Der Ausgangspunkt jeglicher Forschung**

*„Ab jetzt fordern wir alle Nachhaltigkeit, Governance und Digitalisierung.“*

So einfach ist das aber nicht.

Zuerst sind Definitionen zu recherchieren und festzulegen, um nicht „Äpfel mit Birnen oder Erdäpfeln“ zu vergleichen.

Im Anschluss sind die (international) zwingend zu beachtenden Vorgaben zu identifizieren und – soweit relevant – in die Forschungsarbeiten einzubeziehen.

Sofern in einem Forschungsfeld noch nichts oder nur wenig reguliert ist, wird die Regulierung der Technik folgen.<sup>2</sup>

Egal, ob privatwirtschaftliche Unternehmen (AG, GmbH, etc.) oder die Öffentliche Hand (Regierungen, Kommunen, kommunale Unternehmen, Parteien etc.), profitorientierte oder nicht-profitorientierte Organisationen, alle setzen sich derzeit mit den Zielen Nachhaltigkeit, Compliance, Risikosteuerung, Resilienz, Digitalisierung, KI 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 reduziert vor allem den Aufwand bei der Erforschung dieser überlappenden Gebiete.

Jede Komponente aus Governance bzw. GRC (z.B. Qualitäts-, Risiko- oder Compliancemanagement) 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>3</sup>

Und „größere“ Kunden verlangen in diesem Trend<sup>4</sup> von ihren Lieferanten / Suppliern verstärkt und ernsthaft Nachweise über wirksame Nachhaltigkeits-(CSR- / ESG-) und GRC-Systeme.

### **Definitionen**

**Management** nach der Plan- / Do- / Check- / Act-Methode umfasst Unternehmens-, Umfeld-, Stakeholder-Analysen (auch bzgl. Geschäftsmodell und -prozessen), 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*“.

<sup>2</sup> Vgl. Digitalisierungsgesetze, KI-Verordnung der EU, CSRD der EU, zahlreiche Urteile des BVerfG, des EUGH, etc.

<sup>3</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.

<sup>4</sup> Vgl. hierzu das Lieferkettengesetz sowie die Berichtspflichten bzgl. Nachhaltigkeit in der Supply Chain: *Huth, Romeike*, Supply Chain Risk Management: ESG-Risiken in der Lieferkette erkennen, in: *Zukunftssicher: So geht Innovation an der Schnittstelle von Wirtschaft und Versicherung*, 2021.

## **1. Measurable and mandatory requirements for GRC, sustainability (CSR / ESG) and digitalization / AI: The starting point of any research**

*“From now on, we shall demand sustainability, governance and digitalization. “*

But it is not that simple.

First, definitions must be researched and established so as not to compare “*apples with pears or potatoes*”.

Subsequently, the mandatory (international) requirements are to be identified and – as far as relevant – included in the research work.

If nothing or only little is regulated in a research field, regulation of the technology will follow.<sup>2</sup>

Be they private companies (stock corporation [AG], limited liability company [GmbH], etc.) or bodies of the public sector (governments, municipalities, municipal companies, political parties, etc.), profit-oriented or non-profit organizations, all are currently addressing the goals of sustainability, compliance, risk management, resilience, digitalization, AI and information security.

If one now compares the – little known – *specific and, above all, measurable (!) requirements* from legal regulations and standards, it is striking that there are *many redundancies of governance or GRC and sustainability (ESG / CSR)*. This reduces the effort in researching these overlapping areas.

Each component of governance or GRC (e.g. quality, risk or compliance management) equally constitutes an essential component of sustainability.

The enormous need to catch up in sustainability, GRC and digitalization, especially in public but also private organizations, has now become widely publicized.<sup>3</sup>

And alongside this trend, “larger” customers are increasingly and seriously demanding evidence of effective sustainability (CSR / ESG) and GRC systems from their suppliers.<sup>4</sup>

### **Definitions**

**Management** according to the Plan / Do / Check / Act method includes company, environment and stakeholder analyses (also regarding business model and processes), goal setting, strategy development, planning, implementation, control and monitoring, reporting.

**Corporate governance** roughly means “*appropriate interaction between the bodies* (shareholder, management [executive board / managing director]) and supervisory body [supervisory board / advisory board / administrative board]) *as well as proper corporate management and supervision*”.

<sup>2</sup> Cf. digitalization laws, the EU’s AI Regulation, the EU’s CSRD, numerous rulings by the German Federal Constitutional Court (BVerfG), the European Court of Justice (ECJ), etc.

<sup>3</sup> Cf. the current corruption scandals and compliance violations in state governments, in politics, religious communities, in the management of larger and smaller companies / organisations / associations, which are unfortunately often forgotten about far too quickly. Task: Please collect the scandal cases from the current news: Check whether effectively implemented and controlled GRC / ESG / CSR would have prevented them.

<sup>4</sup> Cf. the Supply Chain Act and the reporting obligations regarding sustainability in the supply chain: *Huth, Romeike, Supply Chain Risk Management: Identifying ESG risks in the supply chain*, in: *Zukunftssicher: So geht Innovation an der Schnittstelle von Wirtschaft und Versicherung*, 2021.

# LEITARTIKEL

Governance<sup>5</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 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 die Organisation 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>6</sup>

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

**Nachhaltigkeit<sup>7</sup> (ESG<sup>8</sup> / CSR<sup>9</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<sup>10</sup> Generationen die Möglichkeit zur Deckung ihres eigenen Bedarfs zu nehmen“<sup>11</sup> beschrieben werden:

„Lebe nicht auf Kosten anderer!“

**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, Compliance-orientierte und risikobasierte Unternehmensführung und -überwachung“ übersetzt werden.

<sup>5</sup> Vgl. Grötsch, Andreas, Erklärung zum Deutschen Corporate Governance Kodex, 2021, aufrufbar unter: [www.risknet.de](http://www.risknet.de).

<sup>6</sup> Zu den Zielen und positiven Effekten eines Risikomanagements, vgl. <https://www.risknet.de/wissen/risk-management-prozess/>.

<sup>7</sup> Vgl. Scherer, Kollmann, Birker, Integriertes Nachhaltigkeits-Managementsystem, 2019, zum kostenlosen Download auf [scherer-grc.net/Publikationen](http://scherer-grc.net/Publikationen).

<sup>8</sup> ESG ist ein Akronym und steht für Environmental, Social, Governance (zu Deutsch: Umwelt, Soziales und Unternehmensführung).

<sup>9</sup> CSR ist ein Akronym und steht für „Corporate Social Responsibility“, d.h. eine unternehmerische Gesellschaftsverantwortung bzw. unternehmerische Sozialverantwortung.

<sup>10</sup> Anmerkung Scherer: „... und gegenwärtigen...“

<sup>11</sup> World Commission on Environment and Development; Our Common Future; Oxford University Press, Oxford 1987, S. 43

Governance<sup>5</sup> is more than management. Governance should also include social responsibility (Corporate Social Responsibility [CSR] with economic, social and ecological sustainability) and integrity / ethics, see ISO 37000:2021 (Governance of organizations).

**Risk management** deals with uncertainties in decision-making and the achievement of goals. (Entrepreneurial) Activity is always associated with uncertainties. The mission of risk management is to systematically identify opportunities and risks and to evaluate them in terms of potential impact on the organization. The term risk is therefore defined as dispersion around an expected value. According to this definition, both positive deviations (opportunities) and negative deviations (threats) are taken into account.<sup>6</sup>

**Compliance** means dutiful conduct with regard to generally binding rules (laws, jurisdiction), but also with regard to (internally) declared binding requirements (e.g. regulations from the company-specific code of conduct or employment contract).

**Sustainability<sup>7</sup> (ESG<sup>8</sup> / CSR<sup>9</sup>)** could be described as “*making decisions and acting in a manner that preserves progress*” or, according to the World Commission on Environment and Development, as “*development that meets present needs without compromising the ability of future<sup>10</sup> generations to meet their own needs*”.<sup>11</sup>

“Do not live at the expense of others!”

**Governance, risk, compliance and sustainability “together”,** i.e. “**GRC**” or **ESG / CSR** may be something other than the sum of the four components. There is no legal definition here. GRC or ESG / CSR could be translated as “*Integral, sustainable, compliance-oriented and risk-based corporate governance and monitoring*”.

<sup>5</sup> Cf. Grötsch, Andreas, Declaration on the German Corporate Governance Code, 2021, available at: [www.risknet.de](http://www.risknet.de).

<sup>6</sup> On the objectives and positive effects of risk management, cf. <https://www.risknet.de/wissen/risk-management-prozess/>.

<sup>7</sup> Cf. Scherer, Kollmann, Birker, Integriertes Nachhaltigkeits-Managementsystem, 2019, available for free download at [scherer-grc.net/publications](http://scherer-grc.net/publications).

<sup>8</sup> ESG is an acronym that stands for Environmental, Social, Governance.

<sup>9</sup> CSR is an acronym that stands for Corporate Social Responsibility, i.e. a corporate social responsibility.

<sup>10</sup> Comment by Scherer: „... and present...”

<sup>11</sup> World Commission on Environment and Development; Our Common Future; Oxford University Press, Oxford 1987, p. 43

# LEITARTIKEL

## Nachhaltigkeits-Berichterstattung<sup>12</sup>

Nachdem die „großen“ Unternehmen<sup>13</sup> nachhaltigkeitsberichtsspflichtig 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 ausgeweitet<sup>14</sup> werden.

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 Sustainability 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. EUR Bilanzsumme oder 40 Mio. EUR Umsatz (zwei dieser drei Voraussetzungen reichen) für das

Geschäftsjahr 2023 über ökonomische, soziale und ökologische Nachhaltigkeit berichten.<sup>15</sup>

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

Diese Standards werden in 9 Cluster aufgeteilt (vgl. unten Punkt 2.2).<sup>16</sup>

## EU-Taxonomie-Verordnung

Darüber hinaus führt bereits jetzt die so genannte **Taxonomie-Verordnung** zu erheblichen Auswirkungen auf Unternehmen / Organisationen.<sup>17</sup>

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.

<sup>12</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):

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 nicht-finanzielle 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 nicht-finanziellen Erklärungen, um die Reputation für ihr Unternehmen zu verbessern.

<sup>13</sup> BMW erstellte 2019 erstmals einen (*kombinierten*) Nachhaltigkeits- und Geschäftsbericht.

<sup>14</sup> Vgl. *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>15</sup> Vgl. *Richter, Meyer*, Nachhaltigkeitsreporting: Warum die neue EU-Richtlinie wegweisend ist, 03.11.2021, zum Download im Internet.

<sup>16</sup> *EFRAG*, Project Task Force on European Sustainability Report Standards (PTF-ESRS) Status Report, 15.11.2021, zum Download im Internet.

<sup>17</sup> Vgl. *Rat für nachhaltige Entwicklung*, EU-Taxonomie: So steht es auf dem Weg zur nachhaltigen Wirtschaft, 22.10.2021, zum kostenlosen Download im Internet.

### Sustainability reporting<sup>12</sup>

After the “big” companies<sup>13</sup> became obliged to report on sustainability and since the report also obliges them to check the business partners (especially suppliers) for sustainability, the combined sustainability and annual report is also gaining ground in the SME sector. In addition, the CSR reporting obligation is to be *legally* extended<sup>14</sup> to SMEs in the future.

The legislator will extend the sustainability reporting obligation (cf. 289 b HGB [*Handelsgesetzbuch*, German Code of Commercial Law]) to medium-sized companies with 250 or more employees as of 1 January 2024 for the 2023 financial year:

According to the draft of the *Corporate Sustainability Reporting Directive (CSRD)*, which will probably be finally adopted as an EU directive by June 2022 at the latest, large corporations and partnerships with limited liability with more than 250 employees, a balance sheet total of € 20 million or a turnover of € 40 million (two of these three conditions are sufficient) must report on economic, social and ecological sustainability for the financial<sup>15</sup> year 2023.

The *European Financial Reporting Advisory Group (EFRAG)* intends to propose standards for this reporting in June 2022 and make the first part of the standards mandatory in October 2022 and the second part mandatory in October 2023.

These standards are divided into 9 clusters (cf. point 2.2 below).<sup>16</sup>

### EU Taxonomy Regulation

Furthermore, the so-called **Taxonomy Regulation** is already leading to significant impacts on companies / organizations.<sup>17</sup>

Financial, insurance, but also certain non-financial companies will have to report on (currently still primarily environmental) sustainability as early as 2022 (!) due to the Delegated Act on Art. 8 of the EU Taxonomy Regulation.

With regard to (environmentally) sustainable activities, for example, non-financial companies must also report on their respective shares in operating (“OpEx”) and capital expenditure (“CapEx”), but also in turnover.

<sup>12</sup> Mandatory sustainability reporting – the so-called CSR reporting obligation, based on the EU Directive 2014/95/EU – was introduced in Germany in 2017 for capital market-oriented companies with more than 500 employees, 40 million EUR turnover and/or a balance sheet total of 20 million EUR (§ 289b HGB).

This non-financial corporate reporting is based on the guidelines of the *Global Reporting Initiative (GRI)* and must be included in the management report.

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

By reference in § 264a para. 1 HGB, limited partnerships and limited partnerships with limited liability as well as cooperatives by reference in § 336 para. 2 p. 1 no. 2 HGB are also obliged to prepare such a non-financial statement if the criteria listed above are met. According to § 289c para. 2 HGB, this report must at least cover environmental concerns, employee concerns, social concerns, respect for human rights and the fight against corruption and bribery. Many companies that do not meet these criteria nevertheless voluntarily prepare such non-financial statements in order to improve the reputation of their company.

<sup>13</sup> BMW prepared a (*combined*) sustainability and annual report for the first time in 2019.

<sup>14</sup> Cf. *Grötsch, Andreas*, Corporate Social Responsibility-Berichtspflicht und die Folgen von Rechtsverstößen, KoR (Zeitschrift für internationale und kapitalmarktorientierte Rechnungslegung), 2021 and Sustainable Finance-Beirat der Bundesregierung, Zwischenbericht, 2020, 33 f., available at: [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), last accessed 13 Apr 2021.

<sup>15</sup> Cf. *Richter, Meyer*, Nachhaltigkeitsreporting: Warum die neue EU-Richtlinie groundbreaking ist, 03 Nov 2021, for download on the internet.

<sup>16</sup> *EFRAG*, Project Task Force on European Sustainability Report Standards (PTF-ESRS) Status Report, 15 Nov 2021, available for download on the internet.

<sup>17</sup> Cf. *Council for Sustainable Development*, EU Taxonomy: How we are doing on the road to a sustainable economy, 22 Oct 2021, available for free download on the internet.

# LEITARTIKEL

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.<sup>18</sup>

**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.

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>19</sup> ersetzt bzw. unterstützt werden.

Ein „**Digitalisiertes Integriertes GRC- / ESG- (CSR-) Managementsystem**“<sup>20</sup> ist ein Managementsystem<sup>21</sup>, das mehrere Unternehmensfunktionen bzw. Prozesse (z.B. Nachhaltigkeits-, Risiko-, Qualitäts-, Umwelt-, Arbeitssicherheits- und Compliancemanagement) digitalisiert und zu einem „Unternehmensführungs-System“ integriert.

<sup>18</sup> Vgl. *Flick*, Art. 8 Taxonomie-Verordnung: FAQ und weiteres Informationsmaterial zu den neuen Berichtspflichten veröffentlicht, Artikel vom 22.12.2021, zum Download im Internet.

<sup>19</sup> Der englische Begriff „Artificial Intelligence“ (AI) wird nur allzu häufig mit „Künstliche Intelligenz“ übersetzt. Dabei bedeutet „Intelligence“ vielmehr Informationsverarbeitung. „Die Central Intelligence Agency heißt ja auch nicht so, weil die so geschickt sind“, sagt der österreichische Kybernetiker, Artificial-Intelligence-Experte und Wissenschaftler Robert Trapp. 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>20</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>21</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.

On 20 December 2021, the European Commission published “Frequently Asked Questions (FAQ)” on these reporting obligations that are worth reading and paying attention to.<sup>18</sup>

**Digitalization** means first examining whether the previous business model should be replaced or supplemented in whole or in part by a digital model (e.g. platform solution).

Provided that the previous processes remain in place, the result is an increased “intellectual property” (digital assets) consisting of knowledge and information in the form of processes with associated components (roles, goals, resources), IT systems and IT tools, algorithms, robots and, in many remaining places, people with appropriate competencies and attitudes. These different components of a company are aligned to the digital transformation, if sensible.

Most entrepreneurial activities are to be modelled as processes in such a way that they fulfil the various requirements from technology, business management, compliance, risk, sustainability, etc. and ensure that the set goals are achieved.

At the same time, it must be analyzed which activities will still be<sup>19</sup> replaced or supported by humans or (partially) automated by applications, IT systems, robots, algorithms or other tools from digitalization and artificial intelligence (AI).

A “**Digitized Integrated GRC / ESG (CSR) Management System**”<sup>20</sup> is a management<sup>21</sup> system that digitizes several corporate functions or processes (e.g. sustainability, risk, quality, environmental, occupational safety and compliance management) and integrates them into a “corporate governance system”.

<sup>18</sup> Cf. *Flick*, Art. 8 Taxonomy Regulation: FAQ and further information material on the new reporting obligations published, article dated 22 Dec 2021, available for download on the internet.

<sup>19</sup> The term intelligence in Artificial Intelligence (AI) might be slightly misleading. “Intelligence” much more refers to information processing. “The Central Intelligence Agency is not called that because they are so clever,” said the Austrian cyberneticist, artificial intelligence expert and scientist Robert Trapp. At its core, AI deals with the replication of human-like decision-making structures by algorithms. Cf. *Romeike, Frank*, Predictive Analytics im Risikomanagement – Daten als Rohstoff für den Erkenntnisprozess (Predictive Analytics in risk management – data as a raw material for the knowledge process), in: CFO aktuell, March 2017.

<sup>20</sup> Cf. *Scherer / Fruth / Grötsch* (eds.), Digitalization, Sustainability and “Corporate Governance 4.0” (GRC), 2021, p. 23. Reading sample at [scherer-grc.net/publikationen](http://scherer-grc.net/publikationen).

<sup>21</sup> Organizational structure and process organization consisting of components (e.g. roles, process flows, delegations and interactions, etc.) with the purpose of supporting an organization in decision-making, goal-setting and planning, implementation, and control and monitoring to achieve mandatory and optional goals set.

# LEITARTIKEL

## 2. Messbare und verbindliche Soll-Größen / Komponenten von Nachhaltigkeit (ESG), Governance (GRC), Digitalisierung und KI

### 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 Nachhaltigkeit (ESG / CSR), GRC und Digitalisierung, wie zum Beispiel Spezialgesetze (z.B. IT-Sicherheitsgesetz, Digitalisierungs-Gesetze, KI-Verordnung...), das gesamte öffentlich- und privat-rechtliche Umweltrecht, Arbeitsrecht, Arbeitssicherheits- und Gesundheitsschutzrecht, Straf- und Ordnungswidrigkeitenrecht, u.v.m.

#### Exkurs: Anwendungsbeispiel:<sup>22</sup>

Eine KI-Anwendung ist *rechtlich* zu beurteilen, ob sie zulässig? sicher? dem „Stand der Technik“ entsprechend? ist:

Als Informationsgrundlage dienen zu beachtende fixe Sollgrößen / Referenzgrößen / Pflichtenmaßstäbe, z.B. Gesetze, Rechtsprechung „Technikklauseln“ (nach BVerfG), etc.:

Hier hat z.B. die EU-Kommission den „Entwurf einer Verordnung zur Regulierung von KI („KI-Verordnung“ vom April 2021)<sup>23</sup> verfasst mit Inhalten, wie z.B.

- Verbot des Einsatzes von KI in bestimmten Anwendungsszenarien,
- Technisch-organisatorische Voraussetzungen für den Einsatz von KI,
- etc.

Kernstück der KI-Verordnung ist eine „(Compliance-) Risiko-Analyse<sup>24\*</sup>“ mit folgenden Inhalten:

#### 1. KI-Systemtransparenz:

Kategorisierung der eingesetzten / geplanten KI-Systeme und KI-Compliance-Relevanz

#### 2. Technische Risiko-Folgenabschätzung

bzgl. des konkret geplanten Systems mit „angemessenen“ und „wirksamen“ Risikobewertungs-Methoden nach „Stand der Technik“

#### 3. „Ethics by Design“ (systemimmanente Ethik) als zwingende Verpflichtung

#### 4. Assessments / Freigaben / Kontrollpunkte in den beteiligten Prozessen

<sup>22</sup> Vgl. Scherer, Resilient – Integriertes GRC- / Resilient-Managementsystem – Risknet.de, 2021.

<sup>23</sup> Vgl. Mackert / Makowicz, Nachhaltige menschenzentrierte Implementierung neuer Technologien – KI Compliance, *Comply* 3, 2021.

<sup>24</sup> Vgl. TÜV-Verband fordert Risikoanalyse von KI-Anwendungen, Redaktion Risknet, 03.09.2021, Risknet.de und Vgl. Scherer, Nachhaltigkeits- (ESG-/CSR-) Compliance- und -Risikomanagement – die wesentlichen Pfeiler, auch für Resilienz, 2021, zum kostenlosen Download auf scherer-grc.net.

\* Autor Scherer ist Mitglied der einschlägigen Arbeitsgruppe.

## 2. Measurable and binding target values / components of sustainability (ESG), governance (GRC), digitalization and AI

### 2.1 Mandatory legal framework for sustainability (CSR / ESG), corporate governance with Governance, Risk & Compliance (GRC) and digitalization

The management and other responsible persons *must* align the respective (GRC) [process] topics / areas they are in charge of and also the components of sustainability (CSR / ESG) and GRC presented below *with current requirements from legislation and case law as well as the “recognized state of science and practice”* (“hard law”).

Numerous individual laws and case law deal with mandatory sub-areas of sustainability (ESG / CSR), GRC and digitalization, such as special laws (e.g. IT security law, digitalization laws, AI ordinance...), the entire public and private environmental law, labor law, occupational health and safety law, criminal and administrative offences law, and much more.

#### Excursus: Application example:<sup>22</sup>

An AI application is to be *legally* assessed as to whether it is permissible, safe and, in line with the state of the art:

**Fixed target values / reference values / obligatory standards to be observed, e.g. laws, case law “technology clauses” (according to the German Federal Constitutional Court [BVerfG]), etc., serve as a basis of information:**

In this context, for example, the EU Commission has published the Draft AI Regulation (Artificial Intelligence Act of April 2021)<sup>23</sup> with contents such as

- Prohibition of the use of AI in certain application scenarios,
- Technical and organizational requirements for the use of AI,
- etc.

**The core of the AI Act is a “(Compliance) Risk Analysis<sup>24\*</sup>” with the following contents:**

#### 1. AI system transparency:

Categorization of deployed / planned AI systems and AI compliance relevance

#### 2. Technical risk impact assessment

with regard to the specifically planned system with “appropriate” and “effective” risk assessment methods according to the state of the art

#### 3. “Ethics by Design” (ethics inherent in the system) as a mandatory obligation

#### 4. Assessments / approvals / checkpoints in the processes involved

#### 5. AI - System - Testing

for adequacy and effectiveness, risk assessment under simulations, penetration test procedures (state of the art)

<sup>22</sup> Cf. Scherer, Resiliency – Integrated GRC / Resiliency Management System – Risknet.de, 2021.

<sup>23</sup> See Mackert / Makowicz, Sustainable human-centred implementation of new technologies – AI compliance, *Comply 3*, 2021.

<sup>24</sup> Cf. TÜV association calls for risk analysis of AI applications, Redaktion Risknet, 03.09.2021, Risknet.de and Cf. Scherer, Sustainability (ESG / CSR) compliance and risk management – the essential pillars, also for resilience, 2021, download free at scherer-grc.net.

\* Author Scherer is a member of the relevant working group.

# LEITARTIKEL

## 5. KI – System – Testing

auf Angemessenheit und Wirksamkeit, Risikobewertung unter Simulationen, Penetration-Test-Verfahren (nach Stand der Technik)

## 6. Ein Nachweis durch Audits / Zertifikate

(z.B. „AIC 4 Zertifikat“ / Fraunhofer „KI-Prüfsiegel“, TÜV? etc.) ist bisher nicht im Entwurf der EU-Kommission enthalten, aber u.a. vom TÜV-Verband gefordert.

Aufgrund der „Legalitätspflicht“ der Geschäftsleitung und der Anforderungen an einen „gewissenhaften“ Geschäftsführer, Vorstand, Aufsichtsrat, Kaufmann (§§ 43 GmbHG, 91, 93, 107, 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- und Digitalisierungs-Governance und -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>25\*</sup>

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

## 2.2 Nachhaltigkeits-Komponenten: *Die Cluster der CSRD*

Ein Nachhaltigkeits-Managementsystem bzw. die CSR-Berichterstattung nach GRI, Global Compact oder dem neuen, in 2022 erscheinenden Berichts-Standard der EU beschäftigt sich primär mit den folgenden Themen<sup>26\*</sup> (Hinweise auf aktuelle themenspezifische Spezial-Standards):

**Governance** (Ordnungsgemäße, ethische Unternehmensführung) [ISO 37 000 : 2021: Governance of organizations]\*

### 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<sup>27</sup>).

<sup>25</sup> Vgl. *Raum*, in: Hastenrath, Compliance-Kommunikation, 2018.

<sup>26</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>27</sup> XHTML / ESEF-Datenformat, vgl. *Richter / Meyer*, Sind Unternehmen für die künftigen Anforderungen der Nachhaltigkeitsberichterstattung gewappnet?, 02.06.2021, zum Download im Internet.

\* Autor *Scherer* ist Mitglied der einschlägigen Arbeitsgruppe.

## 6. Evidence through audits / certifications

(e.g. *AIC 4 Certificate / Fraunhofer Institute Certification for the Trustworthy Use of Artificial Intelligence, TÜV [German Technical Inspection Association]? etc.* ) is not yet included in the EU Commission's draft, but is demanded by the TÜV Association, among others

Due to the management's duty of legality and the requirements on a conscientious managing director, board of directors, supervisory board, businessman (§§ 43 GmbHG [German Law on Limited Liability Companies], 91, 93, 107, 116 AktG [German Stock Corporation Act], 347 HGB [German Code of Commercial Law]), etc., as well as the duty under §§ 130, 30 OWiG (German Law on Administrative Offences) to take precautions against breaches of duty in the company, a corresponding, appropriate organization that enables legally secure, sustainable corporate governance and monitoring, including all relevant *sustainability and digitalization* governance and *compliance*, must be maintained.

In this respect, it can be useful to orientate oneself on current standards (soft law) in order to document the attempt to comply with the "recognized state of science and practice"; also in order to be well prepared for audits, final examinations or certification. According to the presiding judge of the 1st Criminal Division of the *German Federal Court of Justice*, standards can be "constitutive of punishability".<sup>25\*</sup>

**Thus, a compliance management system ensures a fundamental and essential part of governance (GRC) and sustainability (ESG / CSR).**

## 2.2 Sustainability components: The clusters of CSRD

A sustainability management system or CSR reporting according to Global Reporting Initiative (GRI), Global Compact or the new EU reporting standard to be published in 2022 primarily deals with the following topics<sup>26\*</sup> (references to current topic-specific special standards):

**Governance** (Lawful, ethical corporate governance) [ISO 37 000 : 2021: Governance of organizations]\*

### Cluster 1

Cluster 1 contains conceptual guidelines on "*double materiality*"

(Which sustainability risks affect the organization/company on the one hand, and, on the other hand: Which sustainability risks does the company/organization pose on society and the environment)?

and on **requirements on the type and quality of the individual information** (e.g. on specific key figures on certain topics in a digital, evaluable format<sup>27</sup>).

<sup>25</sup> Cf. *Raum*, in: Hastenrath, Compliance-Kommunikation, 2018.

<sup>26</sup> Clarifying note: In order to implement an adequate sustainability management system, it is not necessary to implement or certify the listed standards in insular management systems.

<sup>27</sup> XHTML / ESEF data format, cf. *Richter / Meyer*, Sind Unternehmen für die künftigen Anforderungen der Nachhaltigkeitsberichterstattung gewappnet?, 02.06.2021, for download on the internet.

\* Author *Scherer* is a member of the relevant working group.

# LEITARTIKEL

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.

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*“.<sup>28</sup>

**Cluster 2:** Umwelt: Klimawandel und Anpassung

**Cluster 3:** Umwelt: Wasser- und Meeres-Ressourcen, Umweltverschmutzung, Kreislaufwirtschaft, Biodiversität und Ökosysteme.

**Umweltmanagement** (ISO 14000 : 2015)

**Klimaschutz und Treibhausgas-Neutralität** (ISO 14064 ff.)

**Energieeffizienz / Ressourcenmanagement** (ISO 50001 : 2018)

**Cluster 4:** Soziales: Eigenes Personal / Human Resources

**Cluster 5:** Soziales: Personal in der Wertschöpfungskette, betroffene Gemeinschaften, Verbraucher

**Arbeitssicherheit und Betriebliches Gesundheitsmanagement** (ISO 45001: 2018)

**Arbeitsrecht, Arbeitsstrafrecht und faire Arbeitsbedingungen** (Diversity, Gleichbehandlung der Geschlechter, keine Zwangs- und Kinderarbeit) / (ISO 30400 ff.:2017 ff.)

**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

<sup>28</sup> Vgl. Scherer, Fruth, Grötsch (Hrsg.), Digitalisierung, Nachhaltigkeit und „Unternehmensführung 4.0“ (GRC), 2021, Leseprobe unter [scherer-grc.net/publikationen](http://scherer-grc.net/publikationen).

In addition, “Cluster 1” contains so-called cross-sectional standards on *resilience topics*, such as

1. business model and strategy
2. key sustainability risks, opportunities and impacts
3. sustainable corporate governance and organization / processes
4. principles, guidelines and goals relating to sustainability
5. derived planning of projects / measures and resources required for them.

This corresponds roughly to the analyses of key sustainability issues and strategic goals (“*materiality analysis*”) already known from the *Global Compact* or *Global Reporting Initiative* standards with the associated *management approach*.<sup>28</sup>

**Cluster 2:** Environment: climate change and adaptation

**Cluster 3:** Environment: water and marine resources, pollution, circular economy, biodiversity and ecosystems.

**Environmental management**  
(ISO 14000 :2015 )

**Climate protection and greenhouse gas emission neutrality** (ISO 14064 ff.)

**Energy efficiency / resource management**  
(ISO :500012018 )

**Cluster 4:** Social: own staff / human resources

**Cluster 5:** Social: value chain personnel, affected communities, consumers

**Occupational safety and health management**  
(ISO 45001: 2018)

**Labour law, labour criminal law and fair working conditions** (diversity, gender equality, no forced or child labour) / (ISO 30400 ff. : 2017 ff.)

**Cluster 6:** Governance: Corporate governance and supervision

- with
- a) governance, risk and compliance, internal control and monitoring
  - b) responsible business practices
  - c) products and services, innovation, management and quality of relations with business partners

<sup>28</sup> Cf. Scherer, Fruth, Grötsch (eds.), Digitalization, Sustainability and “Corporate Governance 4.0” (GRC), 2021, reading sample at [scherer-grc.net/publications](http://scherer-grc.net/publications).

# LEITARTIKEL

**Compliance** (ISO 37301 : 2021\* / IDW PS 980)

**Anti-Korruption** (ISO 37001 : 2021\*)

**Risikomanagement** (ISO 31000 : 2018 / ÖNORM 4900 ff. : 2021\* / IDW PS 98)

**Verantwortungsvoller Umgang mit Informationen** (Digitalisierung, Informationssicherheit [ISO 27000 ff. : 2017], Datenschutz)

**Sicherstellung von Nachhaltigkeit in der Lieferkette und bei Geschäftspartnern**

**Anonymitätsbewahrendes Hinweisgebersystem für Nachhaltigkeits-Risiken und Compliance-Verstöße** (ISO 37002: 2021)\*

## **Cluster 7:**

Cluster 7 beschäftigt sich mit branchenspezifischen Besonderheiten

## **Cluster 8:**

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

## **Cluster 9:**

Cluster 9 regelt die Digitalisierung der Berichterstattung.

## **2.3 Governance und GRC**

Der Normungsausschuss 175-00-01 AA der DIN erarbeitete jüngst 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<sup>29</sup>
6. Stakeholder-Relationship
7. Führung und Werte<sup>30</sup>
8. Daten und Entscheidungen<sup>31</sup>
9. Risikobasierte Unternehmensführung<sup>32</sup>
10. Soziale Verantwortung<sup>33</sup>
11. Nachhaltigkeit<sup>34</sup>

\* Autor *Scherer* ist Mitglied der jeweiligen Arbeitsgruppe bei DIN / ISO.

<sup>29</sup> „Fit & proper“-Kompetenzen, Transparenz und Vertrauen.

<sup>30</sup> Werte definieren und die Organisation nachhaltig, ethisch und effektiv führen.

<sup>31</sup> Daten als wertvolle Ressource für Entscheidungsvorbereitung und -fällung.

<sup>32</sup> Steuerung der Unsicherheiten bzgl. strategischer Ziele.

<sup>33</sup> Gesellschaftliche Verantwortung (CSR / ESG).

<sup>34</sup> Ökonomische, soziale und ökologische Wertschöpfung.

**Compliance** (ISO 37301 : 2021\* / IDW PS 980)

**Anti-corruption** (ISO 37001 : 2021\*)

**Risk management** (ISO 31000 : 2018 / ÖNORM [Austrian Standards Institute] 4900 ff. : 2021\* / IDW PS [Auditing Standards of the Institute of Public Auditors in Germany] 98)

**Responsible handling of information** [digitalization, information security (ISO 27000 ff. : 2017), data protection].

**Ensuring sustainability in the supply chain and with business partners**

**Anonymous whistleblowing system for reporting sustainability risks and compliance violations** (ISO 37002: 2021)\*

**Cluster 7:**

Cluster 7 deals with sector-specific features

**Cluster 8:**

Cluster 8 contains guides for small and medium-sized enterprises (SMEs)

**Cluster 9:**

Cluster 9 regulates the digitalization of reporting.

**2.3. Governance and GRC**

The DIN standardization committee 175-00-01 AA recently developed **ISO 37000: 2021 Guidance for the Governance of Organizations\*** with the following core topics:

1. Mission, values, culture
2. Sustainable value creation
3. Strategy
4. Legal framework / compliance: laws, standards, rules, guidelines.
5. Sense of responsibility<sup>29</sup>
6. Stakeholder relationship
7. Leadership and values<sup>30</sup>
8. Data and decisions<sup>31</sup>
9. Risk-based corporate governance<sup>32</sup>
10. Social responsibility<sup>33</sup>
11. Sustainability<sup>34</sup>

\* Author *Scherer* is a member of the respective working group at DIN (German Institute for Standardisation) / ISO.

<sup>29</sup> “Fit & proper” competencies, transparency and trust.

<sup>30</sup> Define values and lead the organization sustainably, ethically and effectively.

<sup>31</sup> Data as a valuable resource for decision preparation and decision making.

<sup>32</sup> Managing uncertainties about strategic goals.

<sup>33</sup> Social responsibility (CSR / ESG).

<sup>34</sup> Economic, social and ecological value creation.

# LEITARTIKEL

## 3. These: 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 Compliancemanagement) stellt bereits zugleich eine wesentliche Komponente von Nachhaltigkeit dar.

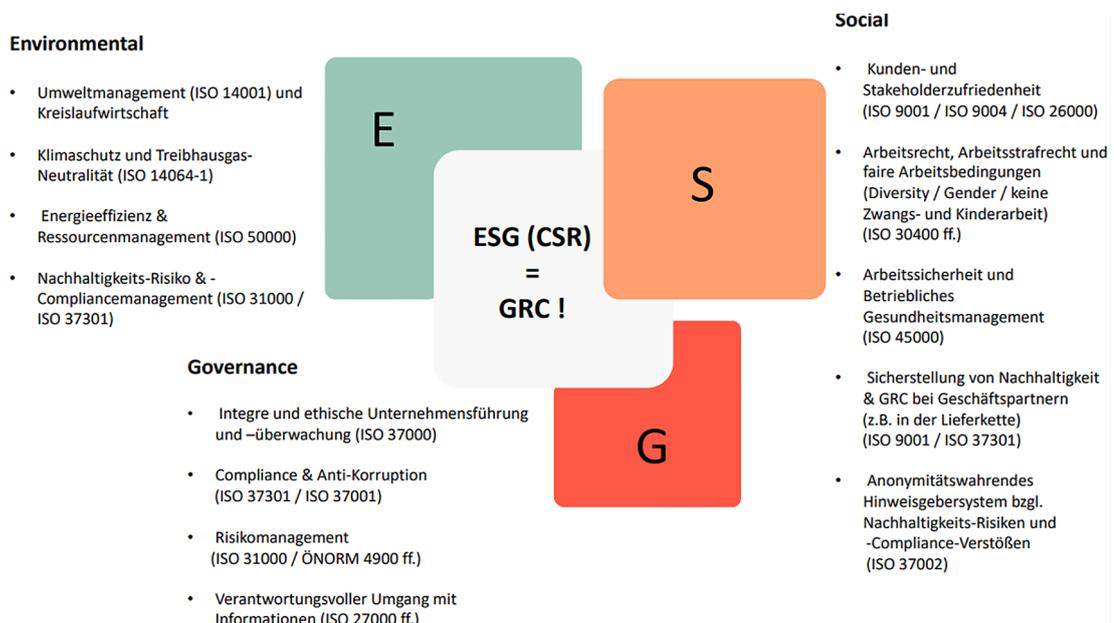


Abb. 1: Environmental, Social, Governance = GRC

### 3. Thesis: Sustainability (ESG / CSR) = GRC!

If we now compare the specific *and measurable (!) requirements from legal regulations and standards* presented above under 2., the enormous redundancies between governance or GRC and sustainability (ESG / CSR) become strikingly apparent. GRC and sustainability (ESG / CSR) are largely identical.

Each component of governance or GRC (e.g. quality or risk or compliance management) is also an essential component of sustainability.

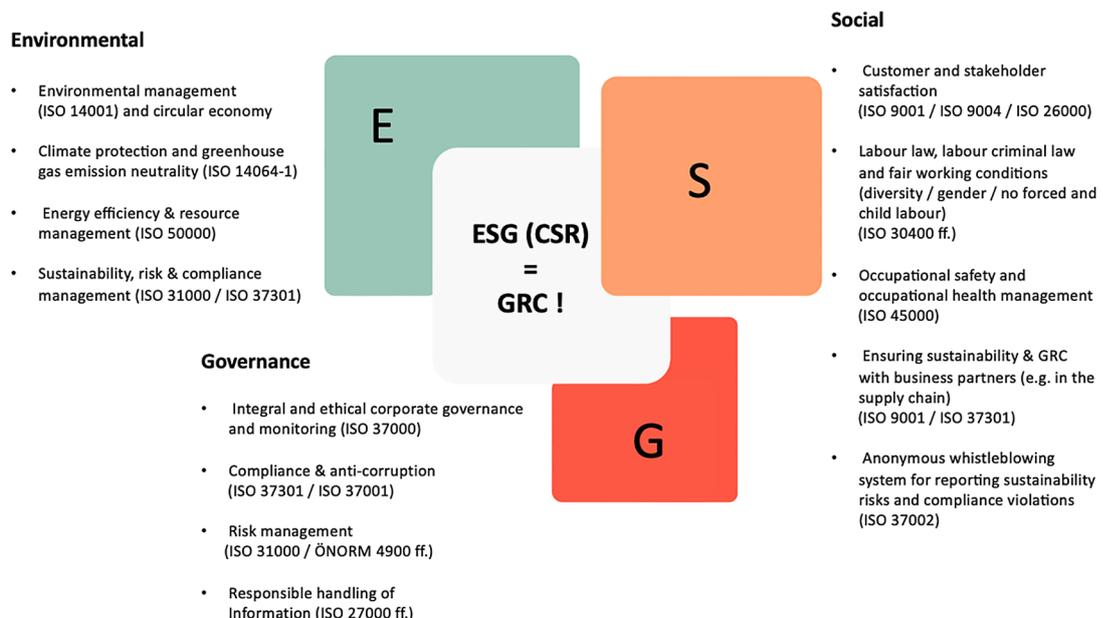


Figure 1: Environmental, Social, Governance = GRC

# LEITARTIKEL

## 4. Strafbarkeit von Falschinformation bzgl. Nachhaltigkeit (Greenwashing) und Governance<sup>35</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 nicht-finanziellen Erklärung bzw. im nicht-finanziellen Bericht unrichtig wiedergegeben oder verschleiert dargestellt werden.

Darunter fallen auch Kapitalgesellschaften, die *freiwillig* eine nicht-finanzielle Erklärung erstellen und darin die Verhältnisse unrichtig wiedergeben oder verschleiern. Erstellt eine Gesellschaft trotz bestehender Verpflichtung keine nicht-finanzielle 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 nicht-finanzielle 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. EUR nach § 30 OWiG festgesetzt werden.<sup>36</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>37</sup>

<sup>35</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>36</sup> Die mögliche Buße nach dem geplanten *Unternehmenssanktionsrecht* könnte weitaus höher ausfallen, vgl. Scherer, Grötsch, Unternehmenssanktionsrecht, interne Untersuchungen und Whistleblowing als ESG-Elemente im Koalitionsvertrag, 2021, zum kostenlosen Download auf [gmrc.net/publikationen](http://gmrc.net/publikationen).

<sup>37</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.

#### 4. Criminal liability for misinformation regarding sustainability (greenwashing) and governance<sup>35</sup>

§ Section 331 No. 1 of the German Code of Commercial Law (HGB) stipulates that executive *bodies of a corporation* (e.g. *board of directors / managing directors*) are punishable by imprisonment of up to 3 years or a fine if the circumstances of the corporation are misrepresented or concealed in the non-financial statement or report.

This also includes corporations that *voluntarily* prepare a non-financial statement and misrepresent or conceal the circumstances therein. If a company does not prepare a non-financial statement in spite of an existing obligation, the offence according to § section 331 no. 1 HGB is not fulfilled. The same applies, according to the opinion expressed here, if a company prepares a non-financial statement but omits essential information from it.

A conviction under section 331 HGB has the consequence that the body concerned may no longer act as managing director of a limited liability company (GmbH) or executive board of a stock corporation for a period of five years after the judgement has become final, pursuant to section 6 para. 2 sentence 2 of the German Law on Limited Liability Companies (GmbHG) or section 76 para. 3 of the German Stock Corporation Act (AktG). Furthermore, an association fine of

up to 10 million EUR may be imposed on the company pursuant to section 30 of the German Law on Administrative Offences (OWiG).<sup>36</sup>

Unfortunately, the problem of *greenwashing*, in which the consumer is deliberately led to believe that the company or product is particularly sustainable or environmentally friendly, has intensified in recent years. This problem, which can be sanctioned under competition law, is often found in the area of marketing.<sup>37</sup>

<sup>35</sup> Grötsch, Andreas, Corporate Social Responsibility-Berichtspflicht und die Folgen von Rechtsverstößen, KoR (Zeitschrift für internationale und kapitalmarktorientierte Rechnungslegung, 2021 and Sustainable Finance-Beirat der Bundesregierung, Zwischenbericht, 2020, 33 f., available at: [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), last accessed 13.04.2021.

<sup>36</sup> The possible fine under the planned *Corporate Sanctions Act* could be much higher, cf. Scherer, Grötsch, Unternehmensanktionsrecht, interne Untersuchungen und Whistleblowing als ESG-Elemente im Koalitionsvertrag, 2021, available for free download at [gmrc.net/publikationen](http://gmrc.net/publikationen).

<sup>37</sup> Cf. Federal Ministry of Justice and Consumer Protection, last accessed on 12.02.2021 at [https://www.bmjjv.de/SharedDocs/Pressemitteilung/DE/2021/0208\\_Greenwashing.html](https://www.bmjjv.de/SharedDocs/Pressemitteilung/DE/2021/0208_Greenwashing.html): An investigation by the European Consumer Protection Cooperation Network (CPC) has recently revealed that in an evaluation of 334 sustainability claims, misleading information on sustainability was found in 42 % of the cases.

# LEITARTIKEL

## 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>38</sup> auditiert und zertifiziert bereits erfolgreich Integrierte GRC- bzw. Nachhaltigkeits-Managementsysteme.

## 6. Ausblick

Obwohl Nachhaltigkeit (ESG / CSR) nahezu deckungsgleich mit dem Themenkomplex Governance / GRC ist, stößt das Thema „Nachhaltigkeit“ auf eine wesentlich größere Sensibilisierung und Offenheit 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>39</sup> und „neues Management“ erfordern, wenn wir als *Homines sapientes* nicht bis zum Jahr 2100 (wie *Harari*<sup>40</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 öffentlich-rechtlichen Organisationen Zeit, sich um Nachhaltigkeit und Governance zu kümmern.

Parallel dazu gibt es aber noch eine ganze Menge zu *erforschen*...

**„We are the world...“<sup>41</sup>**  
(U.S.A. for Africa, 1985)

<sup>38</sup> [www.gmrc.de](http://www.gmrc.de)

<sup>39</sup> Vgl. zur Forderung neuer Rechte in der Menschenrechts-Konvention: *Ferdinand von Schirach*, Jeder Mensch, 2021.

<sup>40</sup> Vgl. *Harari*, Sapiens – Der Aufstieg, Comic, 2021, S.15.

<sup>41</sup> U.S.A. for Africa – We are the world, 1985.

## 5. Auditing and certification of a (combined) sustainability / GRC management system and a sustainability report

Many organizations have already realized that the approach of an *Integrated* GRC / ESG Management System is more effective and at the same time much cheaper than bureaucratically managing countless insular systems with high costs and little value added.

Accordingly, requests for combined certificates are accumulating among certifiers.

The International Institute for Governance, Management, Risk & Compliance at the Degendorf<sup>38</sup> University of Applied Sciences already successfully audits and certifies integrated GRC or sustainability management systems.

## 6. Outlook

Although sustainability (ESG / CSR) is almost congruent with governance / GRC, the topic of sustainability meets with much greater awareness and openness among management and stakeholders than GRC.

This may be, among other things, related to the fact that the younger generation in particular has realized that the “new times” also require “new ways of looking at things”, “new human rights”<sup>39</sup> and “new management” if we as *Homines Sapientes* do not want to share the fate of extinction with *Homo neanderthaliensis*, who “disappeared” about 30,000 years ago, by the year 2100 (as *Harari*<sup>40</sup> states).

It is time for all private and public organizations to address sustainability and governance.

In parallel, however, there is still a great deal to explore...

**“We are the world...”**<sup>41</sup>  
(U.S.A. for Africa, 1985)

<sup>38</sup> [www.gmrc.de](http://www.gmrc.de)

<sup>39</sup> Cf. on the demand for new rights in the Human Rights Convention: *Ferdinand von Schirach*, *Jeder Mensch*, 2021.

<sup>40</sup> Cf. *Harari*, *Sapiens – The Rise*, Comic, 2021, p.15.

<sup>41</sup> U.S.A. for Africa – We are the world, 1985.

# LEITARTIKEL

## Gasteditoren / Issue editors:



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

Prof. Dr. jur. Josef Scherer ist Rechtsanwalt, Consultant, Gründer und Leiter des Internationalen Instituts für Governance, Management, Risk- und Compliancemanagement der Technischen Hochschule Degendorf (THD) und seit 1996 Professor an der THD. Zuvor arbeitete er als Staatsanwalt an diversen Landgerichten und als Richter am Landgericht in einer Zivilkammer. Neben seiner Tätigkeit als Seniorpartner der auf Wirtschaftsrecht und Governance, Risiko- und Compliancemanagement (GRC) spezialisierten Kanzlei Prof. Dr. Scherer, Partnerschaft mbB, erstellt er wissenschaftliche Rechtsgutachten. Seit 2001 arbeitet er auch als Insolvenzverwalter in verschiedenen Amtsgerichtsbezirken. Er fungiert in diversen Unternehmen / Körperschaften als Compliance-Ombudsmann sowie externer Compliance-Beauftragter und ist gesuchter Referent bei Managementschulungen. 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. 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 „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). 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.

*Prof. Dr. jur. Josef Scherer is a lawyer and has been a professor at the Deggendorf University of Applied Sciences since 1996. Previously, he worked as a public prosecutor at various regional courts and as a judge at the regional court in a civil chamber. In addition to his work as senior partner of the law firm Prof. Dr. Scherer, Partnerschaft mbB, which specialises in commercial law and governance, risk and compliance management (GRC), he prepares academic legal opinions. Prof. Dr. Scherer acts as compliance ombudsman and external compliance officer in various companies / corporations and is a sought-after speaker at management training courses in well-known companies. In cooperation with TÜV, he designed the renowned and accredited extra-occupational Master's programme in Risk Management and Compliance Management at the Technical University of Deggendorf, which has been running for over 12 years now. He has also been a member of the advisory board of the Institute for Risk Management and Regulation (FIRM), Frankfurt ([www.firm.fm](http://www.firm.fm)) since 2015. Likewise, since 2016, member of the DIN Standards Committee on Services (Working Committee on Human Resources Management NA 159-01-19 AA) for the development of ISO/DIN standards in human resources management and since 2017, member of the delegation ISO TC 309 Governance of organisations (Working Committee Governance and Compliance NA 175-00-01-AA for the development of ISO/DIN standards in the field of corporate governance, compliance and whistle blowing). Also since 2016: Technical leader of the user group "Sustainable Corporate Governance and Compliance" of the Energy Forums Leipzig and since 2018 member of the working group 252.07 of Austrian Standards International for the development of an ÖNORM 4900 ff. (risk management system standards). Prof. Dr. Scherer is a shareholder-managing director of Governance-Solutions GmbH and a member of the supervisory board of various companies and foundations in the field of applied research and solutions/tools in ESG/GRC, digitalization and integrated workflow management systems.*

Kontakt / Contact

✉ [josef.scherer@th-deg.de](mailto:josef.scherer@th-deg.de)

# LEITARTIKEL



## Dipl.-Kfm. Prof. Dr. Andreas Grötsch

Rechtsanwalt Prof. Dr. Grötsch hat in München Betriebswirtschaftslehre und Rechtswissenschaften studiert. Er 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. 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.

*Prof. Dr. Grötsch studied business administration and law in Munich. He has been working as a lawyer and tax consultant at the law firm Wannemacher & Partner ([www.wannemacher-partner.de](http://www.wannemacher-partner.de)) since November 1998 (since 2006 as partner). Wannemacher & Partner is one of the most renowned law firms in the field of criminal tax law and procedural tax law in Germany and is frequently recognized as a leading law firm by the magazines JUVE, FOCUS, Wirtschaftswoche and Handelsblatt. Since 2020, Prof. Dr. Grötsch has been holding the Chair for Tax Compliance, Criminal Tax Law and Corporate Social Responsibility at the Deggendorf Institute of Technology. In the years 2005–2019, he was a lecturer for criminal tax law at the University of Osnabrück.*

Kontakt / Contact

✉ [Andreas.Groetsch@wannemacher-partner.de](mailto:Andreas.Groetsch@wannemacher-partner.de)



## Frank Romeike

Frank Romeike ist geschäftsführender Gesellschafter der RiskNET GmbH und Autor mehrerer Standardwerke im Bereich Risikomanagement. Mit RiskNET betreibt er das führende Kompetenzportal zum Thema Risikomanagement und Corporate Governance. Zuvor war Romeike als Chief Risk Officer bei IBM tätig, wo er an der Implementierung eines globalen Risikomanagementprozesses mitwirkte und mehrere internationale Projekte leitete. Romeike, der auch als Lehrbeauftragter an mehreren nationalen und internationalen Universitäten tätig ist, ist einer der weltweit führenden Experten für Chancen- und Risikomanagement.

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

*Frank Romeike is the Managing Partner at RiskNET GmbH and the author of several standard works in the field of risk management. With RiskNET, he operates the leading competence portal on the subject of risk management and corporate governance. Earlier in his career, Romeike served as Chief Risk Officer at IBM, where he contributed to the implementation of a global risk management process and directed several international projects. Romeike, who also serves as an adjunct professor at several national and international universities, is one of the world's leading experts in opportunity and risk management.*

*Further information at [www.romeike.info](http://www.romeike.info)*

Kontakt/ Contact

✉ [romeike@risknet.de](mailto:romeike@risknet.de)