

Journal für Medizin- und Gesundheitsrecht

Chefredaktion:

Alois Birklbauer, Markus Grimm,
Wolfgang Kröll und Oliver Neuper

JMG 1|2021

AKTUELLES IN KÜRZE

MARKUS GRIMM | CHRISTOPH WOLF

Aus aktuellem Anlass: Verpflichtende Tests und Impfungen in der COVID-19-Pandemie aus arbeitsrechtlicher Sicht

BERND KLOIBER | OLIVER NEUPER

Blutabnahme und klinische Untersuchung alkohol- und/oder suchtgiftbeeinträchtigter Verkehrsteilnehmer iSd § 5 StVO 1960

KLARA HAIMBERGER

Widerruf oder Widerspruch? Verhinderung einer Datenverarbeitung auf Grundlage des broad consent

JOSEF SCHERER | ANDREAS GRÖTSCH

Gemeinsamkeiten von Nachhaltigkeit (ESG/CSR) und Governance (GRC) im Healthcare- und Pflegebereich

ANDREAS BECKER

Der Blick nach ...: Anforderungen an die Informationssicherheit in deutschen Krankenhäusern (Teil I)

ANDREA POTZ

Der interessante Fall: Der „Chefarzt-Fall“ – eine Kündigung wegen Wiederverheiratung

WERNER HAUSER

Rechtsprechung: Zum Kausalitätsbeweis bei dauerhafter Hirnschädigung

JAHRESREGISTER 2020

ISSN 2415-6868
eISSN 2708-6410





Prof. Dr. Josef Scherer

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



Dipl.-Kfm. Prof. Dr. Andreas Grötsch

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

Gemeinsamkeiten von Nachhaltigkeit (ESG/CSR) und Governance (GRC) im Healthcare- und Pflegebereich¹

- : **Die Verknüpfung von Digitalisierung und Informationssicherheit, Nachhaltigkeit (ESG/CSR)¹ und „Unternehmensführung 4.0“ (GRC)¹ mit Strategie, Zielerreichung und (Nachhaltigkeits-)Berichterstattung⁴**
- : **Thesen: GRC und ESG (CSR) weisen zu fast 100% Redundanzen auf.**
- : **Eine auch lediglich extrinsisch (durch Stakeholder, wie z.B. Gesetzgeber / Kunden / etc.) motivierte**
- : **GRC- bzw. Nachhaltigkeits- (ESG-/CSR-) Berichterstattung nach HGB auf Basis von GRI- bzw. Global**
- : **Compact-Standards führt zu einer messbaren signifikanten Verbesserung des Nachhaltigkeits-Reifegrades und Impacts einer Organisation im Healthcare- und Pflegebereich.**

Nicht erst seit Corona reden alle von Resilienz und Zukunftsfähigkeit, Nachhaltigkeit und Governance. Die Praxis hinkt hier sowohl im Reifegrad der Ablauforganisation als auch bei „Tone from the Top“ und den Kompetenzen von Management und Mitarbeitern noch weit hinterher.

Es stellt sich die Frage, welche Unternehmen resilient und zukunftsfähig – und damit interessant für Stakeholder – sind.⁵

Voraussetzung ist zunächst die Verknüpfung von Digitalisierung, Nachhaltigkeit (ESG/CSR) und „Unternehmensführung 4.0“ (GRC) mit Strategie, Zielerreichung (performance) und (Geschäfts-)Berichterstattung:

„GRC“ bzw. „ESG (CSR)“ müssen dazu aber endlich richtig verstanden, gewünscht und angewandt

werden: Nicht als „lästige Überwachungsfunktion“ oder „Kollektives Greenwashing“, sondern als modernes und unverzichtbares Unternehmensführungs-Instrument.

Ein Vorteil:

Der neue GRC-Ansatz ist nahezu identisch mit dem „Environmental, Social, Governance“-Ansatz (ESG/CSR).

Und noch ein weiteres: Richtig gemacht, erspart dies bereits bei der Umsetzung – und nicht erst Jahre später – Zeit, Geld und Stress!

„GRC & ESG in S & P!“⁶

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.

1 Der Kurzartikel ist ein Auszug aus Scherer, „Management reloaded“ – „GRC & ESG in Strategy & Performance“, 2021,

zum kostenlosen Download auf scherer-grc.net/Publikationen oder Risknet.de.

2 ESG: Environmental, Social, Governance. CSR: Corporate Social Responsibility.

3 Governance, Risk und Compliance.

4 Vgl. ausführlich zum Thema dieser Abhandlung: Scherer in Scherer/Fruth/Grötsch (Hrsg.): Digitalisierung, Nachhaltigkeit und „Unternehmensführung 4.0“, 2021. Leseprobe unter scherer-grc.net/publikationen

5 Vgl. Scherer, Resilienz & Zukunftsfähigkeit, GRC als „Klammer“ diverser Management-Inseln, 9 / 2020, Risknet.de

6 Vgl. Scherer in Scherer/ Fruth / Grötsch (Hrsg.): Digitalisierung, Nachhaltigkeit und „Unternehmensführung 4.0“, 2021, S. III.

1. Definitionen

Was heißt GRC bzw. ESG/CSR und Integriertes GRC/ ESG – (CSR-) -Managementsystem?⁷

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

Ein Managementsystem⁸, das mehrere Unternehmensfunktionen bzw. Prozesse (z.B. Risiko-, Qualitäts-, Umwelt-, Arbeitssicherheits- und Compliance-management) digitalisiert und zu einem „Unternehmensführungs-System“ integriert, kann „**Digitalisiertes Integriertes GRC/ ESG – (CSR-) -Managementsystem genannt werden.**⁹

Social
<ul style="list-style-type: none"> • Occupational safety • Health protection • Compliance with labor law • Fair working conditions • Prohibition of child labor • No forced labor • Compliance with ESG criteria for service providers and suppliers

Environmental
<ul style="list-style-type: none"> • Environmental protection • Climate protection • Renewable energies • Reduction of emissions • Careful use of raw materials and energy • Environmental Risk und Compliance

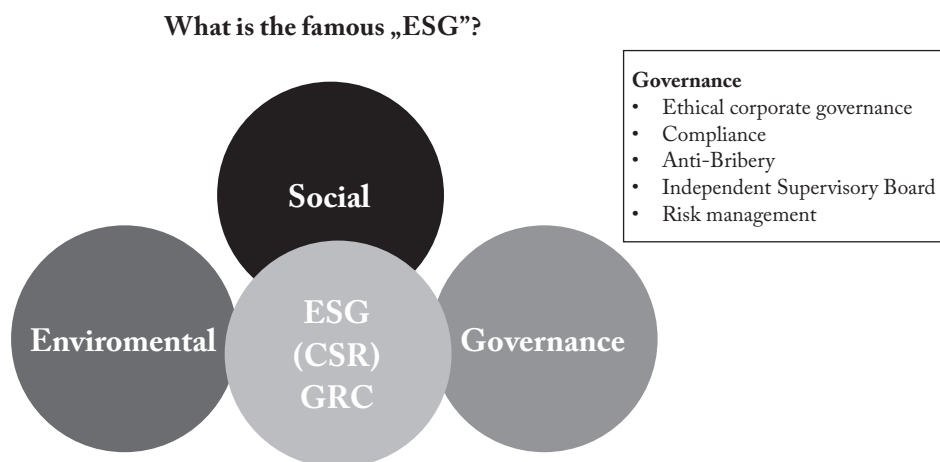


Abb. 01: Environmental-Social-Governance-ESG¹⁸

2. Weltweite Trends: Governance (GRC), Nachhaltigkeit (ESG/CSR) und Cyber-Risikomanagement

Der Normenausschuss 175-00-01 AA der DIN erarbeitet derzeit die **ISO 37000: 2021 Guidance for the Governance of Organizations.**¹⁰

Danach wird der **Kernbereich von Governance** folgende Punkte umfassen:

1. Mission, Werte, Kultur
2. Nachhaltige Wertschöpfung
3. Strategie
4. Rechtlicher Rahmen¹¹
5. Verantwortungsbewusstsein¹²
6. Stakeholder-Relationship
7. Führung und Werte¹³
8. Daten und Entscheidungen¹⁴
9. Risikobasierte Unternehmensführung¹⁵
10. Soziale Verantwortung¹⁶
11. Nachhaltigkeit¹⁷

Wichtig: Diese im ISO-Standard 37000: Governance of Organizations genannten GRC-Punkte sind die gleichen Punkte, die auch ESG/CSR ansprechen:

⁷ Vgl. *Scherer/Fruth* (Hrsg.), *Governance-Management* Band I, 2014, S. 9 und Band II, 2015, S. 30, sowie Scherer, *Good Governance und ganzheitliches strategisches und operatives Management. – Die Anreicherung des „unternehmerischen Bauchgefühls“ mit Risiko-, Chancen- und Compliance Management*, *Corporate Compliance Zeitschrift (CCZ)*, 6/2012, S. 201, zum kostenlosen Download auf Scherer-grc.net/Publicationen.

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

⁸ Governance ist mehr als Management. Governance soll auch gesellschaftliche Verantwortung (Corporate Social Responsibility (CSR) mit ökonomischer, sozialer und ökologischer Nachhaltigkeit) und Integrität / Ethik umfassen. vgl. ISO/DIS 37000:2020 *Governance of organizations*. **Nachhaltigkeit**

(ESG/CSR) könnte mit „bei Fortschritt bewahrend ausgerichtetes Entscheiden und Handeln“ beschrieben werden.

⁹ Vgl. *Scherer / Fruth / Grötsch* (Hrsg.), *Digitalisierung, Nachhaltigkeit und „Unternehmensführung 4.0“ (GRC)*, 2021, S. 23.

¹⁰ Der Verfasser ist als „Experte“ Mitglied der einschlägigen Arbeitsgruppe von DIN/ISO WG 309.

¹¹ Compliance: Gesetze, Normen, Regeln, Richtlinien.

¹² „Fit & proper“-Kompetenzen, Transparenz und Vertrauen schaffen.

¹³ Werte definieren und die Organisation nachhaltig, ethisch und effektiv führen.

¹⁴ Daten als wertvolle Ressource für Entscheidungsvorbereitung und -fällung.

¹⁵ Steuerung der Unsicherheiten bzgl. strategischer Ziele.

¹⁶ Gesellschaftliche Verantwortung (CSR / ESG).

¹⁷ Ökonomische, soziale und ökologische Wertschöpfung.

¹⁸ Vgl. Euramco, zuletzt abgerufen am 14.01.2021, unter <https://www.euramco-asset.de/glossar/environmental-social-governance-esh/>

Nachhaltigkeitsberichterstattung¹⁹

Auch im Bereich **Nachhaltigkeit bzw. Corporate Social Responsibility (CSR/ESG)** gibt es zahlreiche äußerst aktuelle Standards (z.B. Global Reporting Initiative) auf UN-, OECD- und nationaler Ebene.²⁰

Nachdem die „großen“ Unternehmen nachhaltigkeitsberichtspflichtig wurden und der Bericht auch verpflichtet, die Business Partner auf Nachhaltigkeit zu prüfen, setzt sich auch im Mittelstand der kombinierte Nachhaltigkeits- und Geschäftsbericht durch.²¹

Cyber-Risikomanagement und Informationssicherheit

Einhergehend mit exponentieller Digitalisierung sind auch die Themen „Cyber-Risikomanagement“ und „Informationssicherheit“ (ISO 27000 ff.) derzeit zwingende Ziele einer pflichtgemäßen Unternehmensführung.

3. Pain / Problemstellung

„**Wer spielt schon gern mit Schmuttelkindern?**“ – **Gründe für negative Stimmung gegenüber „GRC“ bzw. ESG (CSR):**

Ineffektive, aber aufwendige GRC- / ESG- (CSR-) Systeme, IT-Tools und Methoden

Häufig werden in der Praxis noch (IT-) Tools, Systeme und Methoden eingesetzt, die nur zusätzliche Bürokratie, Zeit- und Finanzaufwand bedeuten und keinerlei Wertbeitrag bringen (Beispiel: „Risikobuchhaltung“ mit Excel, Powerpoint und Word ...).²²

Abhaken von „Regulierungs-Checklisten“ anstelle von guten unternehmerischen Entscheidungen („Governance“)

Ein weiterer Aspekt: Oft werden unkritisch von „Jugendforscht-Beratern“ empfohlene (IT-) Lösungen

implementiert, die zwar geeignet sind, in Checklisten festgehaltene, Mindestanforderungen für Audits, Testate, Zertifizierungen zu erfüllen.

Kultur, Bewusstsein, Kompetenzen, Prozesse werden dadurch jedoch nicht verbessert, („a fool with a tool is still a fool...“).²³

Fehlende messbare Wertbeiträge (Impact / Performance) von GRC bzw. ESG (CSR)

Schließlich sind die meisten Manager, aber auch Berater, nicht in der Lage, überzeugend und motivierend zu erklären, welche nachweisbaren, messbaren Wertbeiträge GRC bzw. ESG (CSR) bringt. Die Argumentation, dass GRC bzw. ESG (CSR) - unternehmerische Tätigkeit überhaupt erst ermöglicht,

- Problemfälle, die eventuell mal eintreten könnten, vermeiden hilft,
- Anforderungen von Regulieren erfüllt,
- Haftungsgefahren reduziert,
- die Erreichung unternehmerischer Ziele fördert,
- etc.,

klingt abgedroschen und beinhaltet nicht den *Beweis*, dass GRC bzw. ESG (CSR) in überschaubarer Zeit finanziell die Performance (P) verbessert.²⁴

Auch *Achleitner*, eine Koryphäe im Bereich „private equity und investment“, ist der Ansicht, dass „Corporate Governance ein wichtiger Werttreiber“ wird/ist:

„*Wenn man sich die Hebel der Wertschöpfung in den vergangenen 30 Jahren anschaut, dann war die Verbesserung der operativen Wertschöpfung der wichtigste. (...) Die operative Wertschöpfung wird die größte Herausforderung für die Unternehmen (...) in Zukunft sein. (...) In den vergangenen Jahren stand Corporate Governance oft unter dem Überwachungsaspekt. Der wertschöpfende Aspekt fehlte dagegen. Es geht um bessere unternehmerische Entscheidungen durch funktionierende und gelebte Governance (...). Eine gute Corporate-Governance-Praxis wird ein entscheidender Wettbewerbsfaktor in der Zukunft*

19 Eine verpflichtende Nachhaltigkeitsberichterstattung – die sogenannte CSR-Berichtspflicht, basierend auf der EU-Richtlinie 2014/95/EU - wurde 2017 eingeführt (§ 289 HGB ff.).

Diese nicht-finanzielle Unternehmensberichterstattung beruht auf den Leitlinien der Global Reporting Initiative (GRI) und muss in den Lagebericht eingebunden werden, vgl. *Scherer / Fruth / Grötsch* (Hrsg.), Digitalisierung, Nachhaltigkeit und „Unternehmensführung 4.0“ (GRC), 2021.

Zahlreiche Einzelgesetze und Rechtsprechung beschäftigen sich mit zwingend zu beachtenden Teilgebieten von CSR und Nachhaltigkeit, zum Beispiel: Umweltrecht, Arbeitsrecht, Arbeitssicherheits- und Gesundheitsschutzrecht, Straf- und Ordnungswidrigkeitenrecht, u.v.m.

Damit stellt ein GRC-Managementsystem bereits einen erheblichen und wesentlichen Teil von CSR/ESG und Nachhaltigkeit dar.

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

21 BMW ging 2019 mit gutem Beispiel (kombinierter Nachhaltigkeits- und Geschäftsbericht) voran.

22 Vgl. *Lie-Bjelland*, Das fehlende P in GRC, 9 / 2020, Risknet.de.

23 Vgl. *Lie-Bjelland*, Das fehlende P in GRC, 9 / 2020, Risknet.de.

24 Vgl. *Lie-Bjelland*, Das fehlende P in GRC, 9 / 2020, Risknet.de.

(...) aus der Beteiligungspraxis hören sie, dass es Fälle gibt, in denen die Corporate Governance zwei Drittel der Wertsteigerung der Firmen beisteuert. (...)“²⁵

Leider fehlt auch hier das konkrete Beispiel mit Angabe von Euros, Dollars oder bit coins, dass nach- bzw. beweist, worauf die Wertsteigerung konkret beruht.

Regulierungsanforderungen und Haftungsgefahren verdrängt der Mensch und Manager gerne ...

Aufgrund einiger prominenter Fälle (nicht erst „Wirrecard“) spricht sich mittlerweile sehr schnell herum, dass vieles, was früher noch toleriert oder nicht konsequent verfolgt wurde, nun jedoch empfindlich geahndet wird.²⁶

Die „gefühlte“ Verschärfung von Haftungs- und Sanktionsgefahren für Vorstände, Geschäftsführer, Aufsichtsräte und sogar Gesellschafter und Mitarbeiter mit dem Vorwurf, pflichtwidrig gehandelt zu haben, ist objektiv messbar: Im 10-Jahreszeitraum 1986-1995 gab es genauso viele Verurteilungen im Bereich der Managerhaftung, wie in den letzten 100 Jahren zuvor.

Für die nachfolgenden 10-Jahreszeiträume 1996-2005 und 2006–2015 wurde eine nochmalige Verdoppelung gemessen bzw. geschätzt!²⁷

Jüngst²⁸ wies ein großer Versicherer auf enorm steigende Haftungsrisiken für Unternehmen, nicht nur wegen einer Vielzahl von Produktrückrufen, hin.

Aktuell sorgen *Lieferketten-Gesetz und Unternehmenssanktionsrecht* in der gesetzgeberischen Pipeline für weitere Unruhe bei Unternehmenskernen.

Aufgrund der verhaltensökonomisch angelegten kognitiven Verzerrungen bei Managern führt dieses „Bewusstsein im Hinterkopf“ zwar zu Unbehagen, Angst vor Verantwortungsübernahme und „Lähmungserscheinungen vor anstehenden Entscheidungen“, nicht jedoch zur Implementierung einer enthaftenden rechtssicheren Organisation, die Management und Mitarbeiter für „unternehmerisches Verhalten den Rücken freihält“.

Obwohl in jüngster Zeit Rechtsprechung²⁹ und Gesetzgeber (vgl. z.B. BMF-Schreiben vom 23.5.2016³⁰ zu § 153 Abgabenordnung: „Tax Compliance“), die

allgemein anzuerkennende Rechtsfigur bestätigten, dass organisatorische Vorkehrungen zur Vermeidung von Pflichtverstößen u.U. im Einzelfall den Vorwurf vorsätzlichen Handelns entfallen lassen.

Auch der Gesetzesentwurf des Bundesjustizministeriums³¹ zur Unternehmenssanktion bei Compliance-Verstößen geht in diese Richtung.³²

Überforderung von Management und Mitarbeitern bei Digitalisierung, Informationssicherheit und GRC bzw ESG (CSR) wegen geringen Reifegrads des Prozessmanagements

Der in den diversen Organisationen / Unternehmen, aber auch in einzelnen Abteilungen vorzufindende Reifegrad des Prozessmanagements ist höchst unterschiedlich. Ein gutes Prozessmanagement ist jedoch die Basis für Digitalisierung, Informationssicherheit, Nachhaltigkeit im Integrierten GRC-Managementsystem:

„Stand der Technik“ (z.B. im IT-Sicherheitsgesetz, im Datenschutz oder im Arbeitsschutz) sind nicht mehr Excel, E-Mail-Flut, Datenfriedhöfe, sondern (teil-) automatisierte Prozesse und Human Workflow-Management.

Wenn lediglich „nicht gelebte analoge Dokumente“ digitalisiert werden, gibt es am Ende nur „nicht gelebte digitalisierte Dokumente“, aber keine gelebte Vernetzung, Automatisierung und digitale Transformation im Sinne von „4.0“.

Für eine „echte digitale Transformation“ sind Integrierte Human-Workflow-Managementsysteme notwendig.³³

4. „Bauanleitung für Nachhaltigkeitsmanagement (ESG/CSR)“³⁴

Step 1: Fundierte Analysen inkl. „Wesentlichkeitsanalyse“

Der Manager (Vorstand, Geschäftsführer, Aufsichtsrat) hat über diverse (Risiko-)Analysen und eine „Wesentlichkeitsanalyse“ (nach GRI) die derzeitigen Megatrends, die wirtschaftliche und finanzielle Lage, die

25 Vgl. *Lie-Bjelland*, Das fehlende P in GRC, 9 / 2020, Risknet.de.

26 Vgl. *Lie-Bjelland*, Das fehlende P in GRC, 9 / 2020, Risknet.de.

27 Vgl. *Scherer*, Resilienz und Zukunftsfähigkeit – GRC als „Klammer“ diverser Management-Inseln, 9 / 2020, Risknet.de.

28 Vgl. dpa vom 9.9.2020, Allianz: Haftungsrisiken für Unternehmen steigen.

29 Vgl. die erste Entscheidung des Bundesgerichtshofs zur enthaftenden Wirkung und zum Nutzen eines (zertifizierten) Com-

pliance-Managementsystems, vgl. Bundesgerichtshof vom 09.05.2017 Az. 1 StR 265/16, „*KMW*“ Rn. 110

30 BMF Schreiben v. 23.5.2016, DStR 21/2016, 1218.

31 Referentenentwurf: Gesetz zur Förderung der Integrität in der Wirtschaft vom Juni 2020

32 Vgl. *Scherer*, Resilienz und Zukunftsfähigkeit – GRC als „Klammer“ diverser Management-Inseln, 9 / 2020, Risknet.de

33 Vgl. *Scherer*, Resilienz und Zukunftsfähigkeit – GRC als „Klammer“ diverser Management-Inseln, 9 / 2020, Risknet.de.

Resilienz und Zukunftsfähigkeit seiner Organisation zu beurteilen und vor allem angemessene Ziele und Strategien abzuleiten.

Die Zielerreichung kann mithilfe eines digitalisierten und integrierten GRC-Managementsystems erfolgen, das überwiegend aus Zielen, Prozessen, Tools und Methoden sowie Kultur und Kompetenzen von Managern und Mitarbeitern besteht.

Die meisten unternehmerischen Aktivitäten laufen in Zukunft als überwiegend oder zum Teil digitalisierte Prozesse ab. Prozesse und ein digitalisiertes sowie integriertes GRC-Managementsystem stellen das **zentrale Nervensystem der Organisation** dar.

Es ist darauf zu achten, dass Digitalisierung, Nachhaltigkeit und „Unternehmensführung 4.0“ im integrierten GRC-Managementsystem konzeptionell und „ganzheitlich“ („aus einem Guss“) eingeführt werden.

Reiner Aktivismus hat oft gegenläufige, nicht harmonisierende Abläufe und Systembrüche zur Folge.

Auch, um auf der „Prozessebene“ das Richtige richtig zu tun, ist für Management und Mitarbeiter die angemessene Einstellung auf der kognitiven und emotionalen Ebene enorm wichtig: Tone from the top, Kultur, Awareness, Kompetenzen, Motivation u.v.m. ... („Human-Ebene“). Erst dann kann eine Ablauforganisation „wirksam“ („gelebt“) werden.³⁵

Step 2: Ableitung der Top-Ziele, Strategien und Treiber für Resilienz und Zukunftsfähigkeit über „Wesentlichkeitsanalyse“ und „Managementansatz“

Es stellt sich die Frage, auf welche Top-Themen sich ein Unternehmenslenker konzentrieren muss / sollte.³⁶ Dafür werden jährlich die „wesentlichen Themen“ identifiziert.

Bei der „Wesentlichkeitsanalyse“ liegt der Schwerpunkt auf ökonomischen, ökologischen und gesellschaftlichen Themen, die sowohl für die Organisation als auch für die Stakeholder von Interesse sind.

Für die Sicherstellung der Wettbewerbs- und Zukunftsfähigkeit kommt ein „Managementansatz“ zur Anwendung. Dieser zeigt die „Verantwortung und Regelungen“, „Ziele und Kennzahlen“ sowie „Maßnahmen (Projekte und Initiativen) zur Zielerreichung.“

Bei den wesentlichen Themen sind die Mindestanforderungen gem. § 267 a HGB abgedeckt. Ergänzend

hierzu wird der Nachhaltigkeitsbericht auf Basis des Standards *Global Reporting Initiative* (GRI) erstellt.³⁷

Die über eine „Wesentlichkeitsanalyse“ entwickelten *beispielhaft* genannten Top-Ziele

- „1. Nachhaltige Existenzsicherung und Unternehmenswertsteigerung“,
 - „2. Kunden- und Stakeholder- Zufriedenheit“,
 - „3. Compliance und rechtssichere Organisation“,
 - „4. (Projektbezogenes) Risikomanagement“,
 - „5. Strategische Personalentwicklung“,
 - „6. Ressourcenschonung“,
 - „7. Digitalisierung und Informationssicherheit“, etc.
- werden anschließend, neben den übrigen Abteilungszielen, auf Prozessziele und Mitarbeiterziele heruntergebrochen.

Diese *Top-Ziele* haben i. d. R. Bezug zu vielen Abteilungen / Prozessen und beeinflussen deren Zielsetzung. In Organisationen werden diese Querschnittsthemen daher oft durch Stabsstellen oder über eine Balanced Scorecard gesteuert.

Bereits beim Ermitteln und Beschließen / Entscheiden der Top-Themen liefert GRC mit Risiko- und Compliancemanagement wertvolle Informationen durch Aufzeigen rechtlicher Anforderungen / Grenzen sowie von Gefahren und Chancen.

Für jedes der oben dargestellten strategischen Ziele gibt es eine passende „Managementsystem-Insel“, die für Erreichung der Ziele sorgt. Idealerweise werden diese als Integriertes (GRC-) Managementsystem zusammengeführt.

Wie wichtig Daten, Risiko- und Compliancemanagement-Methoden für gute unternehmerische Entscheidungen sind, betont auch der neue internationale ISO-Standard **ISO DIS 37 000: 2020** für „Governance of organizations“: **7.8 Information and decisions**.³⁸

Digitale bzw. teilautomatisierte Entscheidungsunterstützung mit GRC und den Regeln der Business Judgment Rule (91 Abs. 1 Satz 2. AktG) hält gerade in allen Branchen Einzug.³⁹

Step 3: Regelung der Verantwortlichkeiten

Ebenso wie im Prozessmanagement empfiehlt sich auch im Rahmen des „Managementansatzes“ für die jeweiligen Top-Ziele „via RACI“ die Festlegung von Ausführungsverantwortung (Responsible), Inhaltliche

34 Nach dem für die Nachhaltigkeits-Berichterstattung zu verwendenden Standard / Global Reporting Initiative (GRI).

35 Vgl. Scherer, Resilienz und Zukunftsfähigkeit – GRC als „Klammer“ diverser Management-Inseln, 9 / 2020, Risknet.de.

36 Vgl. Scherer, Resilienz und Zukunftsfähigkeit – GRC als „Klammer“ diverser Management-Inseln, 9 / 2020, Risknet.de.

37 Vgl. Scherer / Fruth / Grötsch (Hrsg.), Digitalisierung, Nachhaltigkeit und „Unternehmensführung 4.0“, 2021, S. 150.

38 Vgl. ISO/TC 309/WG 1 “Guidance for the governance of organizations”, 2020, S. 34 ff. (eigene Übersetzung aus dem Englischen).

39 Vgl. Scherer, Digital Decision Management, 12/2020 zum kostenlosen Download auf gmrc.de / Publikationen.

Verantwortung (Accountable), Zuziehung von Expertenwissen (Consulted) und Reportinglinien (Informed).

Step 4: Identifikation von Anforderungen bzgl. des jeweiligen Top-Zieles

Compliancemanagement kümmert sich um Identifikation, Bewertung und Maßnahmen zur Erfüllung diverser Anforderungen aus Gesetzen, Rechtsprechung, Technik Klauseln, Verträgen, Standards, etc. bzgl. des jeweiligen Top-Zieles.

Step 5: Strategien entwickeln / Planen

Risk: Ziele und die Wege (Strategien) zum Ziel sind mit Unsicherheit belastet: Risiko- und Chancenmanagement hilft mit modernen Methoden wie z.B. Szenarioanalysen und Bandbreitensimulation, den richtigen Weg einzuschlagen.

Step 6: Ableitung von Projekten / Maßnahmen mit Steuerung und Überwachung

Die „lines of defense“ sorgen vor allem mit (projektbezogenem) Risikomanagement durch Steuern der Unsicherheiten (Gefahren / Chancen) für eine optimierte Zielerreichung in den beschlossenen Projekten / Initiativen.

Step 7: Stakeholder-Kommunikation über Nachhaltigkeits-Berichterstattung

Die Stakeholder werden u.a. über den Nachhaltigkeitsgeschäftsbericht informiert.

Wenig bekannt ist bei Entscheidern / Autoren der Geschäftsberichte, dass Unwahrheiten u. U. sogar strafrechtlich sanktioniert werden.⁴⁰

Dabei verlangt DRS 20 mittlerweile, dass diese Berichte keine nichtssagenden Floskeln, sondern *relevante* Fakten erhalten.

§ 289b HGB sieht vor, dass Kapitalgesellschaften, die die Voraussetzungen des § 267 Abs. 3 S. 1 HGB erfüllen, kapitalmarktorientiert i.S.d. § 264d HGB sind und im Jahresdurchschnitt mehr als 500 Arbeitnehmer beschäftigen, eine sog. nichtfinanzielle Erklärung bzw. einen sog. nichtfinanziellen Bericht⁴¹ für den Bereich CSR erstellen müssen. 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.

§ 331 Nr. 1 HGB regelt, dass Organe einer Kapitalgesellschaft 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. Bei § 331 HGB handelt es sich um ein abstraktes Gefährdungsdelikt. Der Tatbestand ist bei einer unrichtigen Wiedergabe oder Verschleierung der Verhältnisse der Gesellschaft verwirklicht, ohne dass eine konkrete Vermögensgefährdung erforderlich ist. Da § 331 Nr. 1 HGB nicht als Einschränkung vorsieht, dass die Kapitalgesellschaften bestimmte Größenmerkmale (die zu einer Berichtspflicht nach § 289b Abs. 1 i.V.m. § 267 Abs. 3 HGB führen) erfüllen müssen, fallen auch Kapitalgesellschaften unter diesen Anwendungsbereich, wenn sie freiwillig eine nichtfinanzielle Erklärung erstellen und darin die Verhältnisse unrichtig wiedergeben oder verschleiern. Der objektive Tatbestand des § 331 Nr. 1 HGB wird jedoch nur dann verletzt sein, wenn sich die unrichtige Wiedergabe bzw. Verschleierung auf für die Gesellschaft wesentliche Angaben i.S.d. § 289c Abs. 3 HGB bezieht. Erstellt eine Gesellschaft trotz der bestehenden Verpflichtung keine nichtfinanzielle Erklärung, so ist nach dem eindeutigen Wortlaut 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. Hintergrund ist, dass der klare Wortlaut des § 331 Nr. 1 HGB nur eine „unrichtige Wiedergabe“ bzw. „Verschleierung“ sanktioniert, während etwa im Falle einer Steuerhinterziehung § 370 AO neben einer „unrichtigen“ auch eine „unvoll-

⁴⁰ Strafbestand der unrichtigen Darstellung im Lagebericht, § 331 HGB und Ordnungswidrigkeiten gemäß § 334 HGB.

⁴¹ Dies wird oft auch als Nachhaltigkeitsbericht bezeichnet.

ständige“ Begehungsweise strafrechtlich sanktioniert. Für die Erfüllung des Tatbestands ist im subjektiven Bereich eine vorsätzliche Begehung notwendig, wobei im Wege eines Eventualvorsatzes ausreichend ist, dass der Täter die Verwirklichung der Merkmale des gesetzlichen Tatbestands für möglich und nicht ganz fernliegend erkennt, und dass er ihn billigt oder sich um das erstrebte Ziel zumindest mit der Tatbestandsverwirklichung abfindet. Zu beachten ist ferner, dass eine Verurteilung wegen § 331 HGB zur Folge hat, 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. Sobald das geplante Gesetz zur Stärkung der Integrität der Wirtschaft in Kraft tritt, kann gegen Unternehmen, in denen eine Leitungsperson eine Verbandstat begangen hat oder wenn die Leitungsperson die Straftat durch angemessene Vorkehrungen hätte verhindern oder wesentlich erschweren können, sogar eine Verbandsgeldsanktion bis zu 10 % des durchschnittlichen Jahresumsatzes festgesetzt werden, sofern der durchschnittliche Jahresumsatz mehr als 100 Mio. Euro betragen hat.

Nach § 334 Abs. 1 Nr. 3 HGB liegt eine Ordnungswidrigkeit vor, wenn gegen die Vorschriften der §§ 289 – 289b Abs. 1, § 289c, § 289d, § 289e Abs. 2 i.V.m. § 289b Abs. 2 und 3 oder § 289f HGB zuwidergehandelt wurde. Insofern sanktioniert § 334 Abs. 1 Nr. 3 HGB sowohl unzutreffende Angaben in einer nichtfinanziellen Erklärung als auch die nicht erfolgte bzw. verspätete Offenlegung der nichtfinanziellen Erklärung bzw. des nichtfinanziellen Berichts. Die Erfüllung des Tatbestands des § 334 Nr. 1 HGB setzt ebenfalls vorsätzliches Handeln voraus, da von dieser Norm eine fahrlässige Begehungsweise nicht ausdrücklich erwähnt wird. Bedauerlicherweise hat sich in den letzten Jahren die Problematik mit dem Themenbereich „Greenwashing“, bei denen dem Verbraucher bewusst vorgetäuscht wird, dass das Unternehmen oder das Produkt besonders nachhaltig oder umweltfreundlich ist, verschärft. Häufig findet sich diese Problematik im Bereich des Marketings. 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.⁴² Werden solche Falschaussagen im Bereich des „Greenwashing“ auch in der nichtfinanziellen Erklärung bzw. den nichtfinanziellen Bericht mit aufgeführt, so kann auch diesbezüglich eine Erfüllung der Tatbestände des § 331 Nr. 1 HGB bzw. § 334 Abs. 1 Nr. 3 HGB vorliegen.

5. Impact / Performance / (finanzielle) Wertbeiträge eines integrierten GRC- / ESG- / CSR- Managementsystems

Nachhaltige und wert(e)-orientierte Investments sind auf dem Finanzmarkt gefragter, denn je. Einige Investoren finanzieren nur noch Unternehmen, die angemessene wirtschaftliche Kennzahlen nachweisen und umfassende Kriterien im sozialen und ökologischen Bereich erfüllen.⁴³

- Nach der Finanz- und Wirtschaftskrise 2008 war die Wertentwicklung von Unternehmen, die stark auf Nachhaltigkeit ausgerichtet waren, im Schnitt 15 % besser als bei der jeweiligen Branche insgesamt.
- Anleger vertrauten in diesem Fall (zu Recht) auf bessere Krisenbewältigungsfähigkeiten und nachhaltigen Erfolg.
- Ebenso wird es in und nach den Corona-Zeiten sein.
- Zugleich wird durch Digitalisierung, Nachhaltigkeit und GRC Transparenz und Struktur erzeugt. Das sorgt für Effektivität und Effizienz und reduziert unnötigen Stress.
- Durch die digitale Optimierung von Abläufen / Methoden kann zugleich auch noch enorm ressourcenschonend gearbeitet werden:⁴⁴

Beispiele für Einsparungen bei Automatisierung lediglich eines einzigen Prozesses:

Elektronik-Unternehmen (ca. 11.000 Mitarbeiter):
26.160 h Zeiteinsparung pro Jahr / 784.800 €
Kosteneinsparung pro Jahr / ca. 66 % Kosteneinsparungen gegenüber anderen Workflowlösungen

42 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

43 Vgl. *Kirchhoff* in: Gazdar, Kaevan et al. (Hrsg.), Erfolgsfaktor Verantwortung, 2006, S. 20 und *PWC*, The growth of tomorrow, ESG-Studie, 10/2020.

44 Vgl. *Scherer / Fruth / Grötsch* (Hrsg.), Digitalisierung, Nachhaltigkeit und „Unternehmensführung 4.0“ Resilienz und Zukunftsfähigkeit, 2021, S. 13.

Automotive OEM: 1 Prozessdurchlauf, um ROI zu erreichen;

Automotive OEM: > 3.000 h Zeiteinsparung pro Jahr⁴⁵

Beispiele für Effizienzsteigerung durch „Digitale Zwillinge“:⁴⁶

- Prozesse, die als „digitaler Zwilling“ abgebildet sind, lassen sich simulieren und auswerten, wodurch die optimale Gestaltung im Vorfeld oder bei Prozessänderungen ermöglicht wird;
- Hersteller für industrielle Computerbauteile (Siemens) steigerte die Produktionsleistung auf derselben Fläche auf das 10-fache seit der Eröffnung, (15 Millionen Einheiten pro Jahr) durch Effizienzgewinne mittels des digitalen Zwillings.
- Sportwagenhersteller Maserati produzierte mithilfe des digitalen Zwillings eine Sportlimousine statt nach 30 bereits nach 16 Monaten.

6. Bleibt nur noch ein Problem: Wie wird GRC bzw. ESG/CSR „sexy“?

Wie schaffen wir es, die neue Bedeutung von GRC bzw. ESG/CSR für Wertbeiträge und Zielerreichung in die Köpfe der Entscheider und sonstigen Mitarbeiter zu bringen?

Bereits auf der *kognitiven* Ebene besteht die Herausforderung, dass Manager und Mitarbeiter es zulassen (Verhaltensökonomie), die neue Bedeutung von

GRC bzw. ESG/CSR zu verstehen und anwenden zu können.

Selbst wenn jedoch das Verständnis für die Vorteile von GRC bzw. ESG/CSR in den Köpfen ist, muss auf der emotionalen Ebene eine (idealerweise intrinsische) Motivation erzeugt werden, „GRC bzw. ESG/CSR auch leben zu wollen.“

Wie schaffen wir es, so, wie *Tom Sawyer* beim Streichen von *Tante Polly's Gartenzaun*⁴⁷, dass aufgrund des durch GRC bzw. ESG/CSR zu erwartenden „*Flow's im Beruf*“ sich jeder freut, GRC bzw. ESG/CSR „leben zu dürfen“?

Die Zielgruppe für das „GRC bzw. ESG/CSR -Marketing“ beschränkt sich dabei nicht nur auf „alte Manager“.

Gerade auch die Top-Führungskräfte von morgen sollten bereits heute an das neue Verständnis von GRC bzw. ESG/CSR und Management herangeführt werden.

Falls Sie auf die Frage:

„*Wer ist unserem Unternehmen für die Nachhaltigkeit, QM, Risk und Compliance verantwortlich?*“

zur Antwort bekommen:

„*Unser Nachhaltigkeits-, QM-, Risk- bzw. Compliance-Beauftragter!*“⁴⁸

gibt es noch viel zu tun:

Die korrekte Antwort könnte lauten:

„*Bei uns ist Jede(r) in seinem Arbeitsumfeld für Nachhaltigkeit, Zielerreichung, Stakeholderzufriedenheit, Risiko- und Compliancemanagement (etc.) verantwortlich.*

Außerdem haben wir kompetente und hilfsbereite Spezialisten / Beauftragte, die uns helfen, auch hier das Richtige richtig zu tun ...“

45 Infos von *TIM Solutions* bzgl. konkreter Praxisfälle zu Einsparungen und Digitalisierung (20.04.2020)

46 *t3n*, Artikel „Was bedeutet digitale Transformation eigentlich konkret?“ vom 15.04.2019.

Hinweis: Der *Verfasser* betreut derzeit die Dissertation von *Rieger, Franz* an der Uni-Klinik Regensburg zur „Modellierung

und Impact-Bewertung eines Digitalen Zwillings eines Prozesses zur Behandlung eines Prostata-Karzinoms.“

47 Vgl. *Keilen*, BMF.

48 Freilich ist es oft schon positiv, wenn im Unternehmen bekannt ist, dass es solche Funktionen überhaupt gibt ...