Kombi-Zertifizierung von Risk und Compliance – Wesentlicher Nachweis für Nachhaltigkeits-Managementsystem und ESG-Due Diligence

Josef Scherer

Seit wenigen Monaten gibt es neue zertifizierbare (ISO-)Normen für Risk (ÖNORM 4900 ff.:2021) und Compliance (ISO 37301:2021). Diese Systeme sind generell aufgrund des Legalitätsprinzips sowie weiterer neuer Anforderungen aus Gesetzgebung und Rechtsprechung Pflicht. Zugleich aber auch sind dies die wesentlichen Pfeiler für Nachhaltigkeit (ESG/CSR), dem Megatrend neben wachsender Regulierung und Digitalisierung. Ebenso bilden sie die Basis für eine ESG-Due-Diligence.

Neue Anforderungen
2021 traten die zertifizierbaren Standards ISO 37301 (Compliance-Managementsystem) und die Ö-Norm 4900 ff. für Risiko-Managementsysteme in Kraft.

Im April 2021 publizierte die Europäische Kommission den Entwurf der Corporate Sustainability Reporting Directive (CSRD).[1] Betroffen und damit nachhaltigkeitsberichterstattungspflichtig sind künftig auch große Unternehmen ab 250 Mitarbeitern[2].

Bzgl. Compliance entschied der BGH am 18.11.2020, im „Buchhändler-Urteil", ein Unternehmer habe sich laufend über rechtliche Änderungen zu informieren, diese angemessen zu bewerten und umzusetzen: „Nichtwissen schützt vor Strafe nicht."[3]

Es ist also ratsam, sich gerade bzgl. dieser Neuerungen gut zu informieren.

Diese Aufzählung von neuen[4] regulatorischen Compliance-Anforderungen in Bezug auf Governance, Nachhaltigkeit und Resilienz auf globaler, europäischer und deutscher Ebene ließe sich noch beliebig fortsetzen.

Compliance und Risk auch als Basis für ein Nachhaltigkeits- / Resilienz-Managementsystem
Es zeigt sich, dass bei Nachhaltigkeit (CSR/ESG) insbesondere Compliance- und Risikomanagement die Grundvoraussetzungen sind, um die vielen Anforderungen der einzelnen Themen zu identifizieren und zu erfüllen.

Ökonomische, soziale und ökologische Nachhaltigkeit (ESG / CSR) enthält weitgehend identische Anforderungen wie Governance, Risk & Compliance („GRC") und kann idR nur über ein Integriertes Managementsystem effektiv und effizient gesteuert werden.

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

ESG – Due Diligence
Due Diligence ist eine „gewissenhafte, sorgfältige Prüfung", die i.d.R. vor dem Kauf eines „Investitionsobjektes", z.B. eines Unternehmens oder einer Organisationseinheit zur Identifikation und Bewertung von Risiken und Chancen des Kaufobjektes durchgeführt wird (bzw. werden sollte).

Es können dabei Gesellschaftsanteile („share-deal") oder einzelne Vermögensgegenstände (Patente, Fachkräfte, Anlagen, Good will, etc. „asset-deal") „erworben" werden.

Die Prüfung durch den Käufer (Buyer's Due Diligence) ist fast zwingend, da bei Fehlinvestitionen aufgrund unterlassener Prüfung dem Verantwortlichen der Käuferseite zivil- und strafrechtliche Haftungsgefahren (u.a. wegen Veruntreuung anvertrauter Gelder etc.) und sonstiges Ungemach (Reputationsverlust, Entlassung, etc.) drohen.

Beispiele für wohl vermeidbare, verlustreiche Fehl-Investitionen gibt es genug.[5]

Der Verkäufer (Vendor's Due Diligence) ist umgekehrt an Transparenz interessiert, wenn er „viel Positives" zu bieten hat:

Das Ergebnis der Prüfung beeinflusst Kaufentscheidung (ob oder ob nicht) und Preis.

Die klassischen Unternehmensbewertungsmethoden (z.B. Discounted Cashflow-, Ertragswert-, etc.- Verfahren) sind ohne aussagekräftige Due Diligence-Ergebnisse nicht zielführend, da sie aus Ergebnissen der Vergangenheit Rückschlüsse auf die nachhaltige Existenz und Ertragskraft in der Zukunft zielen wollen, was unter den heutigen volatilen Rahmenbedingungen völlig untauglich ist [vgl. Scherer 2013].

In der Praxis sind (derzeit noch) die Financial-, Legal– (Compliance-) und Tax-Due Diligence üblich.

Aufgrund der Erkenntnis, dass auch andere Themen immer „wichtiger" werden, finden sich vermehrt IT-, HR- und Commercial-Due Diligence-Prüfungen.

Aus den Auswertungen zahlreicher Insolvenzverfahren und den

Erkenntnissen des Risikomanagements zeigt sich jedoch, dass die Ursachen für Krisen oder hohe Verluste in nahezu jedem denkbaren internen oder externen Ereignis liegen können.

Aus diesem Grund verlangt seit 1.1.2021 §1 des StaRUG[6], dass Vorstände oder Geschäftsführer kontinuierlich Risikofrüherkennung zu betreiben hätten.

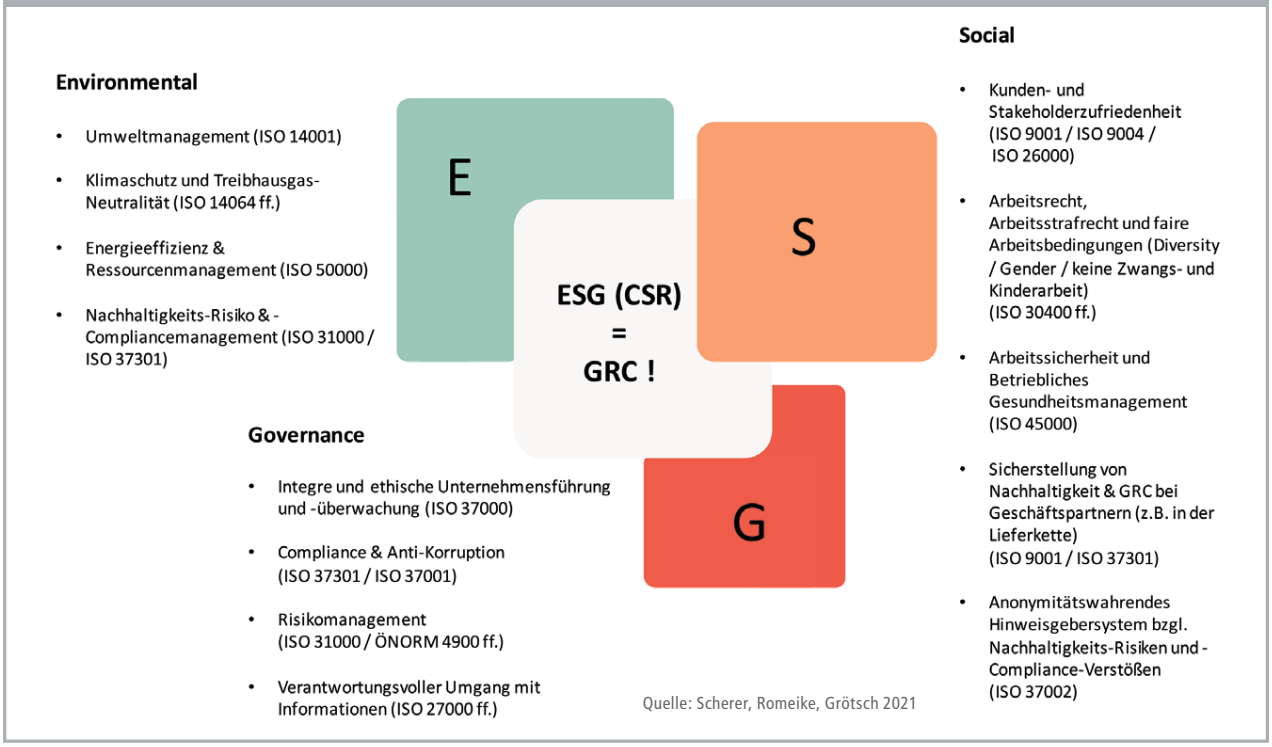
Um also eine Informationsbasis zur Bewertung der nachhaltigen Existenz und Ertragskraft (Risikotragfähigkeit und „Resilienz") eines Investitionsobjektes zu bekommen, ist eine risikobasierte (!) Due Diligence erforderlich.

Mit anderen Worten: Eine umfassende Risikoanalyse bestimmt, welche Bereiche nochmals vertieft durch klassische Due Diligence-Prüfungen bewertet werden müssen.

Eine Nachhaltigkeits- (ESG-) Due Diligence hat nicht nur zum Ziel, Informationen bzgl. Risikotragfähigkeit, also Existenzsicherung oder Resilienz und künftiger Ertragskraft zu bekommen, sondern darüber hinaus auch bzgl. weiterer ökonomischer, sozialer und ökologischer Nachhaltigkeits-Faktoren.

Die zu prüfenden Bereiche einer ESG-Due Diligence ergeben sich aus den in diversen internationalen Standards (Global Reporting Initiative, Global Compact etc.) genannten Themen und finden sich in ▶ Abb. 01.

Abb. 01: ESG (CSR) = GRC



Quelle: Scherer, Romeike, Grötsch 2021

Praxisrelevanz

Da Nachhaltigkeit (ESG / CSR) neben Digitalisierung die beiden Top-Megatrends darstellen und eine ESG-Due Diligence selbstverständlich auch das Thema Risiken und Chancen im Bereich Digitalisierung, Informationssicherheit und Cyber umfasst, ist die Nachfrage entsprechend hoch:

Laut Deloitte [vgl. Delotte 2021] analysieren bereits 94 % institutioneller Investoren auch Nachhaltigkeitsaspekte vor einer Transaktion. 30 Prozent von ihnen ändern ihre Entscheidung über die Investition nach dieser ESG-Analyse. Ebenfalls bemerkenswert: 54 Prozent der institutionellen Akteure reduzieren außerdem den gebotenen Preis für das Target auf der Grundlage der Ergebnisse ihrer Nachhaltigkeitsanalysen.

Effiziente Lösung durch belastbare Zertifikate

Wie u.a. oben dargestellt, ist ein Risk- und Compliance-Managementsystem der „wesentliche Pfeiler" für ein Nachhaltigkeits- (ESG-/CSR-) System, respektive eine entsprechende ESG-Due Diligence, zumal es die von Nachhaltigkeit / ESG betroffenen Bereiche bzgl. (Compliance-) Risiko-Identifikation, -Bewertung und -Steuerung behandeln sollte.

Sofern eine entsprechende Zertifizierung auf Basis der neuen, internationalen Standards nicht „Potemkinsche Risk- und Compliance-Dörfer", also nicht gelebte „(Compliance-) Risikobuchhaltung" akzeptiert, sondern prüft, ob tatsächlich „Wissen, Verstehen, Können und Wollen" in Hinblick auf (Compliance-) Risiko-Identifikation, -Bewertung und -Steuerung bei Management und Mitarbeitern mit entsprechenden Tools und Systemen existiert, ist die Vorlage entsprechender (Kombi-) Zertifikate ein zielführender Bestandteil einer ESG-Due Diligence.

Fazit

Vergleicht man die – wenig bekannten – konkreten und messbaren (!) Anforderungen aus gesetzlichen Regelungen und Standards, so zeigen sich auffällig die vielfältigen Redundanzen von GRC und Nachhaltigkeit (ESG/CSR).

Dies erleichtert die Implementierung eines Nachhaltigkeits- bzw. GRC-Managementsystems enorm. Jede Komponente aus GRC (beispielsweise Stakeholder- oder HR-Management) stellt bereits zugleich eine wesentliche Komponente von Nachhaltigkeit dar.

Compliance und Risk und entsprechende fachlich fundierte Zertifikate spielen bei jeder dieser Komponenten und damit auch für eine ESG-Due Diligence eine wesentliche Rolle.

[1] *Die CSRD löst die Non-financial Reporting Directive ab. Auf nationaler Ebene sind die Regeln und Umsetzung durch die jeweiligen Staaten, z.B. Änderung des HGB, für Unternehmen, Banken, Versicherungen ab 01.01.2024 für das Geschäftsjahr 2023 zu befolgen. Vgl. csr-berichtspflicht, Die EU liefert. Vorgaben für das Nachhaltigkeitsreporting von morgen., zuletzt aufgerufen am 03.06.2021 und BMJ, Richtlinienvorschlag zur Nachhaltigkeitsberichterstattung der Unternehmen (Corporate Sustainbility Reporting Directive CSRD), zuletzt aufgerufen am 16.08.2021.*

[2] *Und Umsatz über 40 Millionen € oder Bilanzsumme über 20 Millionen €.*

[3] *Vgl. Beck-aktuell, Kein Verbotsirrtum nach Schmiergeldzahlungen für Schulbücher, 2021, zuletzt aufgerufen am 16.08.2021.*

[4] *überwiegend im 1. Halbjahr 2021 beschlossenen*

[5] *Vgl. Hypo Alpe Adria, Stahlwerke in Südamerika, „Omega 55", amerikanischer Hersteller von Pflanzenschutzmitteln.*

[6] *Gesetz über den Stabilisierungs- und Restrukturierungsrahmen (Unternehmensstabilisierungs- und -restrukturierungsgesetz, StaRUG)*

Literatur

Deloitte (2021): ESG Due Diligence als inkrementeller Bestandteil von M&A Deals, zuletzt aufgerufen am 23.08.2021 unter www.2deloitte.com

Scherer, J. (2013): Governance-Management, Band 1, 2013.

Scherer, J./Romeike, F./Grötsch, A. (2021): Unternehmensführung 4.0: CSR/ESG, GRC & Digitalisierung integrieren, 2021, zum kostenlosen Download unter www.scherer-grc.net/publikationen

Autor

Prof. Dr. jur. Josef Scherer

Rechtsanwalt, vormals Richter am Landgericht a.D.

Internationales Institut für Governance, Management, Risk- und Compliancemanagement der Technischen Hochschule Deggendorf sowie Mitglied des FIRM-Beirats