BAVARIAN JOURNAL OF APPLIED SCIENCES®

Integriertes Technical-Product-Compliance-Managementsystem mit GRC – Wesentlicher Baustein für Risikomanagement, Resilienz und Nachhaltigkeit (ESG / CSR)

Josef Scherer* **Wiebke Ketelsen****

ABSTRACT

Durch die Anforderungen zur ordnungsgemäßen und sorgfältigen Geschäftsführung, die sich sowohl in §§ 91, 93 und 116 Aktiengesetz als auch in § 1 Gesetz über den Stabilisierungs- und Restrukturierungsrahmen für Unternehmen (StaRUG), etc. wiederfinden, ist für jedes Unternehmen die Erkennung von Risiken obligatorisch. Compliance-Abweichungen können beispielsweise solche Risiken darstellen, weshalb ein wirksames Compliance Management System (CMS) notwendig ist. Dazu gehören Abweichungen zu *verpflichtenden Anforderungen, die mit den Eigenschaften des Produktes in Beziehung stehen*, also z.B. auch Aspekte des Datenschutzes, des Patentrechts oder sogar des Steuerrechts im Kontext der Produkt-Planung, Entstehung, Verwendung und -Entsorgung, die mit dem gesamten Lebenszyklus in Verbindung stehen, d.h. Risiken aus der (technischen) Produkt-Compliance. Hierzu wird analog ein Technical Product-Compliance Managementsystem (TPCMS) benötigt. In der Ausführung zeigt sich allerdings, dass der einzige Unterschied zwischen TPCMS und CMS in den inhaltlich zu behandelnden Sachverhalten besteht. TPCMS ist dann eine *Teilmenge des CMS* und kann integriert gesteuert werden. Methodisch ist folglich kein Unterscheid erkennbar. Dadurch profitieren alle Prozessbeteiligten: Juristen, die sich heute im Rahmen des CMS häufig im Detail und im Schwerpunkt z.B. vor allem mit Anti-Korruption und Anti-Trust beschäftigen, müssen vor vermeintlich neuen, unbekannten Themen nicht zurückschrecken, und Ingenieure, die die TPCMS-Fragestellungen in ihrer Arbeit identifizieren, können auf ein ausgereiftes „klassisches“ integriertes Risiko- und Compliance-Managementsystem (z.B. gemäß der international – neben COSO – anerkannten Standards ISO 37301:2021, ISO 31000:2018 und ÖNORM 4901:2021) mit angemessen Methoden und Tools zurückgreifen. Governance, Risikomanagement und Compliance sind *generell*, nicht nur in Bezug auf ökologische Themen, die wesentlichen Säulen von Nachhaltigkeit (ESG / CSR). Somit ist das TPCMS für die Erfüllung der ESG- / CSR-Anforderungen und -Ziele unverzichtbar.

Under certain German company laws (Stock Corporation Law [AktG] and Law on the Stabilisation and Restructuring Framework for Enterprises [StaRUG]), the company's management is required to identify risks and establish risk management processes. Such a risk could be created by, for example, potential deviations from regulations or other relevant requirements, thus making the installation of a functioning Compliance Management System (CMS) necessary. In particular, for companies manufacturing and

* Rechtsanwalt und Consulter, 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)

* Ingenieurin in einem deutschen Automobilkonzern; Masterandin im Studiengang Risiko- und Compliancemanagement an der THD

selling products, each decision concerning the lifecycle of the product (including, but not limited to planning, engineering, usage, recycling, data security and intellectual property) can potentially carry a risk, therefore a Technical Product Compliance Management System (TPCMS) should also be introduced to ensure adherence with relevant laws and regulations. However, it is shown in the following article, that the only difference between TPCMS and CMS concerns the facts of the cases. TPCMS is a subset of the CMS and can be controlled simultaneously. The method remains the same. This helps every member involved in the process, e.g. lawyers, who are heavily involved in anti-corruption or anti-trust topics, can adapt easily to new issues; and engineers, who will encounter TPCMS issues during their work, can rely on an already implemented and effective system that is certified and based on internationally recognized standards (ISO 37301:2021, ISO 31000:2018, ÖNORM 4901:2021 and the COSO framework).Governance, risk and compliance management are not only an important pillar of sustainability (ESG / CSR) from an ecological point of view. The TPCMS is essential to guarantee the fulfillment of ESG and CSR requirements and goals.

KEYWORDS

Technical Product Compliance, Nachhaltigkeit, Risikomanagement, unbestimmte Rechtsbegriffe, Standardisierung

Technical Product Compliance, sustainability, risk management, undetermined legal terms, standardization

1. Einführung

Breaking News
Gesamtschuldnerische Schadensersatzhaftung gemäß § 826 BGB für Schädigung aufgrund „sittenwidriger *Herstellung* des manipulierten Motors“ durch den (Motoren-) Komponentenhersteller und „sittenwidriges *Inverkehrbringen* des manipulierten Fahrzeugs“ durch den Endprodukt-Hersteller [1].

Pain
Unfälle oder Nutzungseinschränkungen, die auf Produktfehler zurückzuführen sind, können für die Verantwortlichen bei Komponenten- und Endproduktherstellern sowohl erhebliche strafrechtliche Risiken als auch zivilrechtliche Haftung nach sich ziehen ([2], S.76, 90, 97) und für Unternehmen hohe Bußgelder bewirken [3]. Ein großes Risiko im Hinblick auf Risikotragfähigkeit, Finanzen und Reputation für die Unternehmen [4] und ebenso ein Risiko für die beteiligten Manager, Vorstände Geschäftsführer und sonstigen Mitarbeiter (bspw. die beteiligten Ingenieure), die auch persönliche strafrechtliche Konsequenzen befürchten müssen. [5–7]

Lösungsansatz
Ein integriertes *Technical Product-Compliance-Managementsystem (TPCMS)* ermöglicht, die (Compliance-)Risiken im Zusammenhang mit technischen und rechtlichen Anforderungen angemessen zu steuern. In der Vergangenheit haben solche Systeme bereits bußgeld- und strafmindernd gewirkt oder einen Vergleich begünstigt [3, 8].

Es besteht derzeit noch eine *Forschungslücke*, wie ein TPCMS rechtssicher und effektiv aufgebaut und in die Geschäftsprozesse sowie weiterer Management-systeme integriert werden kann. Dabei zeigt sich sowohl in Praxis als auch Wissenschaft, dass zumeist[1] die These vertreten wird, ein TPCMS unterscheide sich wesentlich von einem regulären CMS ([9, 10]; [11], S.1105 ff.).

Daraus entstehen für die Praxis erhebliche Problem- und Fragestellungen, da es sich damit sowohl für Juristen als auch Ingenieure um ein gänzlich neues Aufgabengebiet handeln würde.

[1] Ausnahme: Die *Verfasser* sowie einige Stimmen aus der Praxis, wie z.B. in [8].

Im Gegensatz dazu wird hier und zutreffend z.T. auch in der Industrie [8] die These vertreten, dass das TPCMS lediglich spezielle Inhalte (die mit *Technik und Produkt* im Kontext stehenden [verpflichtenden] Anforderungen) behandelt, im Übrigen aber die gleichen Strukturen, Inhalte und Methoden wie ein „reguläres" CMS aufweist, das ja, um wirksam zu sein, nach Gesetzen, Rechtsprechung [12], Stand von Wissenschaft und Praxis sowie Standards [13–15] und sonstigen regulatorischen Anforderungen ausgerichtet sein muss. Im Fokus stehen – bei beiden Systemen – Identifikation, Bewertung und Steuerung der relevanten Compliance-Risken.

Eine kombinierte Zertifizierung z.B. nach ISO 37301:2021 (Compliance) [vgl. auch COSO Compliance Risk Management 2020] und ISO 31000:2018, ÖNORM 4901:2021 (Risikomanagement) u.v.m. müsste daher das TPCMS in den betroffenen Unternehmen mitbehandeln und würde unter Umständen auch für Organisationen und Entscheider, die nicht bewusst gegen Anforderungen verstoßen, den objektiven Nachweis eines angemessenen und wirksamen TPCMS bringen und enthaftend wirken [16].

2. Definitionen

2.1 Corporate Governance

Corporate Governance kann als *„Angemessene Interaktion zwischen den Organen (Gesellschafter, Leitung […] und Aufsichtsgremium […]) sowie ordnungsgemäße Unternehmensführung und -überwachung"* definiert werden [17]. Governance beinhaltet damit mehr als reines Management und soll auch die gesellschaftliche Verantwortung (Corporate Social Responsibility [CSR] mit ökonomischer, sozialer und ökologischer Nachhaltigkeit), Integrität sowie Ethik umfassen [18].

2.2. Compliance

Eine Legaldefinition für den Begriff Compliance gibt es derzeit noch nicht ([19], S. 65). Der Deutsche Corporate Governance Kodex (DCGK) führt insoweit nicht zum Ziel, da zu sehr auf einen Teil des Ganzen reduziert wird:

„Der Vorstand hat für die Einhaltung der gesetzlichen Bestimmungen und der internen Richtlinien zu sorgen und wirkt auf deren Beachtung im Unternehmen hin (Compliance)". [20]

Es gibt außerhalb „gesetzlicher Bestimmungen" und „interner Richtlinien" zahlreiche andere verbindliche Anforderungen der diversen „interested parties", z.B. die Pflicht, die „Anerkannten Regeln der Technik" und den „Stand der Technik" einzuhalten oder Anforderungen aus behördlichen Auflagen, Verträgen und vielen mehr ([21], S. 68 f.; [22]).

Compliance verlangt also vielmehr die Einhaltung *sämtlicher* externer und interner verpflichtender Anforderungen, insbesondere auch *„technische Entwicklungsstände"* [23].

2.3. Technical Product-Compliance

Auch hier existiert keine Legaldefinition. Bei der Product-Compliance handelt es sich um ein spezielles Themenfeld der Compliance. Obwohl teilweise der Begriff fälschlicherweise (zu eng interpretierend) auf die Produktsicherheit und die Einhaltung des Produktsicherheitsgesetzes (ProdSG) begrenzt wird ([24], S. V), wird vor allem in den USA z.B. auch die Einhaltung von Emissions-Gesetzgebungen und -Anforderungen als eine Disziplin der Product-Compliance gesehen [25].

Die *Product-Compliance* bezieht sich also richtigerweise *auf alle regulatorischen, verpflichtenden Anforderungen, die mit den Eigenschaften des Produktes in Beziehung stehen*, also z.B. auch auf Aspekte des Datenschutzes, des Patentrechts oder sogar des Steuerrechts im Kontext der Produkt-Planung, Entstehung, Verwendung und -Entsorgung, also dem gesamten Lebenszyklus [22].

Technical Product-Compliance würde sich dann sinngemäß einschränkend auf die verbindlichen Anforderungen im Kontext *technischer* (Produkt-)Themen beziehen.

Da es in jedem Prozessthemenfeld einer Organisation, wie z.B. Führungsprozesse (Strategie, Finanzen, Personal, etc.), Kernprozesse (F&E, Beschaffung, Produktion, etc.) und Unterstützungsprozesse (Logistik, QM, etc.), Risiken und Aktivitäten mit Bezug zur (technischen) Product-Compliance gibt und diverse Disziplinen wie Recht, Technik, BWL, Verhaltensökonomie, Branchenspezifika, etc. tangieren, handelt es sich um ein *interdisziplinäres Thema*.

Für Technical Product-Compliance werden in der Praxis eine Reihe von Begriffen synonym verwendet, z.B. technische Compliance [26]

oder technische Konformität [27], wodurch kontraproduktiv divergierende Verständnisse möglich sind.

Bevor also inhaltlich diskutiert wird, muss von den Beteiligten eine präzise, klarstellende Definition des Diskussionsgegenstandes festgelegt werden.

3. Forschungsthese: Die Anforderungen, Inhalte und Methoden des TPCMS unterscheiden sich *nicht* von regulären Compliance-Managementsystemen

3.1 Die Ziele des TPCMS und des regulären CMS (z.B. gemäß ISO 37301:2021) sind identisch

Auf Grund der allgemeinem Legalitätspflicht [28, 29] müssen sich Unternehmen, Management und Mitarbeiter gesetzestreu verhalten ([47], S. 6). Die Rechtsprechung stellte fest, dass Unternehmen ein angemessenes CMS vorhalten müssen [30].

Das Top-Ziel sowohl von TPCMS und CMS ist der Nachweis der Einhaltung von zwingenden (Technical [Product-]) Compliance-Anforderungen[2] und bei Ermessensspielraum die Einhaltung der Business Judgment Rule (§ 93 Abs. 1 Satz 2 AktG) ([19], S. 11).

3.2 Die Zielerreichung wird durch Risiken (Gefahren und Chancen) beeinflusst und kann über den Risikomanagement-Prozess gesteuert werden

Für die Absicherung der Zielerreichung sollte der „klassische" Risikomanagement-Prozess angewendet werden. Die (Technical [Product-])-Compliance-Risiken werden im Rahmen dieses Prozesses identifiziert, bewertet, gesteuert, überwacht und berichtet ([31], S. 248).

Risiko-Identifikation

Während der Identifikation muss sichergestellt werden, dass sämtliche einzuhaltende Anforderungen, auch international, soweit relevant ([32], S. 469 ff.) bekannt sind. Diese Vorgaben lassen sich in einem agilen und sich ständig weiterentwickelnden prozessbezogenen Rechtskataster abbilden ([19], S. 71).

Dabei muss sichergestellt werden, dass alle derzeit geltenden und zukünftigen (neue und sich ändernde) Anforderungen erkannt und nachweisbar eingehalten werden, wenngleich dies eine komplexe Aufgabe darstellt ([33], S. 33):

Beispielsweise entschied der *BGH,* dass ein Händler bei Werbung mit einem Foto eines *Ferrari* die CO_2-Emissionen gemäß PKW-EnVKV angeben muss, selbst wenn dieser gar keine Ferraris verkauft [34].

Grundlegende Methodik hierzu: Zunächst müssen wohl viele der bereits identifizierten und ebenso auf Basis eines entsprechenden Prozesses fortlaufend neu identifizierten Anforderungen aus unterschiedlichsten fachlichen und wissenschaftlichen Disziplinen (Recht, Technik, Ökologie, etc.) in eine (nicht nur für die Juristen und Techniker) verständliche Sprache „übersetzt" werden.

Dabei kommt es zu einer allgemein, also nicht nur bei der Technical Product-Compliance, sondern auch im Gesundheitswesen, in der Immobilien-, Energiewirtschaft etc. auftretenden Schwierigkeit: *„Unbestimmte Rechtsbegriffe"* ([23]; [35], S.105 f.), vgl. hierzu die Exkurse unten.

Wenn nun feststeht oder entschieden wurde, welche *konkrete* Anforderung zu erfüllen ist, müssen noch Prozessschritte, Aktivitäts- und Kompetenzvermittlungs-maßnahmen abgeleitet, in die Prozesse implementiert und zur Wirksamkeit gebracht werden, um sicherzustellen, dass die Anforderung messbar, revisionssicher und dokumentiert erfüllt wird / wurde: Dies gelingt mit führenden Workflows, Automation, digitalen Prozesszwillingen [36] und Kultur, Awareness und Kompetenz (Wissen, Verstehen, Können und Wollen) sowie einem wirksamen „Lines-of-defense"-Steuerungs- und Überwachungssystem.

Dabei kann es im Falle eines Rechtstreits auch zu einer Beweislastumkehr bzw. sekundären Darlegungslast des Unternehmens kommen, nach der nachgewiesen werden muss, unter welchen Bedingungen und von wem Entscheidungen getroffen wurden [37].

[2] Hinweis: Hierbei handelt es sich nicht um fakultative Ziele. Das Management hat lediglich für die Zielerreichung zu sorgen.

Des Weiteren müssen für die Prozessbeteiligten Möglichkeiten geschaffen werden, die angesprochenen „unbestimmten Rechtsbegriffe“ und unverständliche Anforderungen klären und interpretieren zu können ([11], S.1122).

Um sicherzustellen, dass die benötigten Informationen vorliegen, eignet sich ein *Digital Decision Management-Tool*, das den Entscheidungsprozess mit (semi-)künstlicher Intelligenz unterstützt und zur gleichen Zeit getroffene Interpretationen und Definitionen von „unbestimmten Rechtsbegriffen“ revisionssicher dokumentiert [38, 39].

Auch hier kann also mit den „klassischen“ CMS-Methoden die Technical Product-Compliance erfüllt werden.

Risiko-Bewertung
Eine Nichteinhaltung der verpflichtenden Anforderungen kann je nach Ausmaß – z.B. bei Gefahr für Leib und Leben Dritter oder Umweltgefährdung – für die Organisation und die verantwortlichen Mitarbeiter zu existenzvernichtender Wirkung, Freiheitsstrafen, Geldstrafen und Schadensersatzforderungen inkl. Reputationsverlust führen [3, 40]. Außerdem können betroffene Personen im Falle einer Verurteilung für fünf Jahre zur Ausübung einer Organtätigkeit gesperrt sein (§ 76 Abs. 3 Satz 3d AktG bzw. §6 Abs. 3 Satz 2 GmbHG).

Die Risiko-Bewertung hat auch für Compliance-Risiken (!) *angemessen*, also nach anerkanntem Stand von Wissenschaft und Praxis zu erfolgen, also durch Quantifizierung, Aggregation und die Betrachtung der Risikotragfähigkeit [41, 42].

Risiko-Steuerung
Zur Risiko-Steuerung ist es notwendig, die Ausrichtung und Compliance-Kultur des Unternehmens über regelmäßige Schulungen und den „Tone-from-the-Top“ den Mitarbeitern kontinuierlich ins Bewusstsein zu rücken, damit diese stets im Sinne des TPCMS handeln ([31], S. 130).

Durch das „Lines-of-Defense“-Modell mit Compliance, Risikomanagement, Internem Kontrollsystem (IKS) und Revision ([1], S. 188f), die Einrichtung von (KI-gestützten) Monitoring-Prozessen ([43], S. 956), neutralen Ombudspersonen ([44], S. 186) und Zertifizierung des TPCMS als Bestandteil eines Integrierten Risiko- und Compliance-Managementsystems, sollte die Überwachung und Reifegradbewertung des Compliance-Prozesses und der Komponenten des CMS gewährleistet werden. Dadurch werden auch Risiken der Abweichungen von Vorgaben identifiziert und Aktivitäten zu Verbesserungen des Prozesses und der Komponenten abgeleitet.

Exkurs 1: Unbestimmte Rechtsbegriffe
Um der Fortentwicklung von Wissenschaft, Technik, Recht, BWL, etc. den erforderlichen Raum zu lassen, arbeiten Gesetzgeber, Policy-Autoren, etc. vernünftigerweise mit abstrakten Begriffen, die in ihrer „Übersetzung“ auf einen konkreten Anwendungsfall (Subsumption) einem Wandel unterliegen.

Begriffe wie „sicher“, „gewissenhaft“, „sorgfältig“, „angemessen“, „effektiv“, „wirksam“, etc. sind eben nicht im Detail definiert, sondern werden fall- und umfeldbezogen von der Judikative (und der Wissenschaft) geprägt.

Ein Gericht wird bei der Entscheidung, ob z.B. Produkt, System, Software, die ebenfalls in den Anwendungsbereich der Technical Product-Compliance fällt [45], etc. „sicher“ ist oder war, auf der *„Erkenntnisebene“* bei fehlendem eigenen (fachlichen) Sachverstand auf Gutachter, evidenzbasierte wissenschaftliche Literatur und Rechtsprechung, etc., aber auch *„Standards“* als sogenannte *„antizipierte Sachverständigengutachten“* zurückgreifen [22].

Natürlich spielen *unbestimmte Rechtsbegriffe* gerade im Bereich von technischen Innovationen eine bedeutsame Rolle – zum Leidwesen von Anwendern, Ingenieuren und Unternehmensjuristen oder Compliance-Verantwortlichen, aber auch von Auditoren, Zertifizierern, Revisoren, Wirtschaftsprüfern, etc.

Jedes neue Thema bringt nicht nur neue Gefahren und Chancen (Risiken), sondern insbesondere auch neue Compliance-Anforderungen mit sich, z.B. die *„Anforderungen zur Lautstärke der Warnsignale von batterieelektrischen Fahrzeugen“*, die *„Einhaltung der StVO für autonom fahrende Fahrzeuge“* oder auch bereits frühere Beispiele, wie die Einführung von Airbags. So sprechen technische Regularien für Automobile von *„erwartbaren Situationen“* oder Fahrten *„unter normalen Bedingungen“* [46]. Hierbei handelt es sich wiederum um „unbestimmte Rechtsbegriffe“, die im Einzelfall zu definieren sind.

Ende Exkurs 1

Exkurs 2: Entscheidungen und Konkretisierung unbestimmter Rechtsbegriffe

Im Zusammenhang mit unbestimmten (technischen) Rechtsbegriffen treten mindestens zwei Problemkreise auf:

E2.1. Gute und rechtssichere Entscheidungen treffen

Bei „echten" Innovationen wird es häufig noch keine einschlägige Rechtsprechung oder einschlägige Dokumentation geben, wie ein relevanter unbestimmter Rechtsbegriff (z.B. „*die angemessene Lautstärke von Warnsignalen bei elektroangetriebenen Fahrzeugen*") zu interpretieren ist. Die Verantwortlichen in den Organisationen *müssen* dann entscheiden, wie zu verfahren ist, um (technisch) sicherzustellen, dass die Anforderungen erfüllt werden.

Bei solchen Fragen handelt es sich um *gebundene* Entscheidungen:

Das heißt, bzgl. der Antwort auf die Frage, ob z.B. die tatsächliche Lautstärke für Warngeräusche *„angemessen"*, ob das Fahrzeug oder die Steuersoftware *„sicher"* oder was *„erwartbare Situationen"* sind, etc., besteht *kein* (!) Entscheidungsspielraum ([38]; [44], S. 65).

Es empfiehlt sich, in dieser Art „Dilemma-Entscheidungssituation" (gebundene Entscheidung ohne Kenntnis der konkreten, einzelfallbezogenen Anforderungen aufgrund der Formulierung als „unbestimmter Rechtsbegriff") die *Methodik* (!) der sog. „Business Judgement Rule" (§ 93 Abs. 1 Satz 2 AktG) als allgemeine Regel, wie Entscheidungen gewissenhaft zu treffen sind, entsprechend heranzuziehen ([44], S. 71):

Zunächst muss eine „angemessene" Informationsgrundlage geschaffen werden, d.h. gemäß Rechtsprechung des BGH, *alle derzeit verfügbaren, relevanten Informationen* zur anliegenden Entscheidung heranzuziehen [47]. Diese Informationen sind zu bewerten: Nicht intuitiv mit Bauchgefühl oder auf Basis von Heuristiken, die auf die neuen Situationen nicht passen, sondern mit den passenden (angemessenen!) Risikobewertungsmethoden (Szenarioanalysen, Quantifizierungen, Monte-Carlo-Simulationen etc.) [42, 48].

Auf Basis dieser Bewertung soll dann *pro Sicherheit* (nicht: „pro Ergebnis-[Bonus]-Optimierung", etc.) entschieden werden. Bei Risikobewertung und Entscheidung muss sichergestellt sein, dass die Entscheidung frei von Manipulationen und Verzerrungen des Gehirns erfolgt [42]. Der Entscheidungsprozess und das Ergebnis sollten dokumentiert werden, um im Streitfall beweisen zu können, in welchem zuständigen Gremium (?) wann (?), welche (angemessene und bestmögliche) Entscheidung (?) getroffen wurde ([49]; [44], S. 105).

Extrem ungünstig in Bezug auf diese Art *gebundener Entscheidungen,* ebenso wie bei *Entscheidungen unter Unsicherheit* oder *unter Risiko,* wirkt es sich aus, wenn – wie leider in der Praxis aufgrund der Last des operativen Tagesgeschäftes nicht selten anzutreffen – relevante Entscheidungen, egal in welcher Hierarchiestufe, *gar nicht oder nicht reflektiert* getroffen werden, wie sogar in Gerichtsverhandlungen teilweise bestätigt wird.

„(...) Bis zu 200 E-Mails täglich seien bei seinem Sekretariat eingegangen, einen großen Teil davon habe er nie gesehen. Wesentliche Entscheidungen seien im Zehnminutentakt gefallen, Termine ständig verschoben, gekürzt oder abgesagt worden, in seinem Büro [...] sei er bestenfalls ein paar Stunden pro Woche gewesen. Im Jahr hätten ihn höchstens zehn „blaue Meldungen" über Probleme persönlich erreicht. (...)" [50]. Eine ähnliche Situation tritt auch an anderer Stelle in der Praxis -*messbar*- häufig auf [51].

Daraus ergibt sich dann aber die Frage, wie oft dieses Risiko angemessen gesteuert wird oder sogar, ob es überhaupt in der Risiko-Identifikationen zur Sprache kommt. Bei derartigen „Nicht-„ oder oberflächlichen Entscheidungen in allen Hierarchien könnte, im Falle einer strafrechtlichen Verfolgung, sogar der Tatbestand eines bedingten Vorsatzes begründet sein (eine negative Folge der Entscheidung für möglich halten und sich damit abfinden). Hierbei handelt es sich um ein extremes (Compliance-)Risiko für die Organisation und den betroffenen Manager oder Mitarbeiter, aber auch für Vorstand, Gesellschafter, Aufsichtsgremium, da eine Organisationspflichtverletzung vorliegen dürfte.

E2.2. Konkretisierung unbestimmter Rechtsbegriffe durch Standards, Normungsarbeit versus technische Kartelle
Um die oben beschriebenen „Dilemma-ähnlichen" Entscheidungen zu erleichtern, besteht natürlich die Möglichkeit, neue (technische) Anforderungen und die (technischen) Vorgaben zur Erfüllung dieser Anforderungen nach „Anerkanntem Stand der Wissenschaft und Praxis" bzw. „Anerkannten Regeln der Technik" oder besser noch „Stand der Technik" [22] in einem Leitfaden / Standard, etc., wie ISO-, VDI-, VDA-, -etc., Norm zu dokumentieren.

Bei Beachtung diverser Regularien bzgl. der Qualitätssicherung beim Erstellen der Norm zeigten diese nach ständiger *BGH-* und *BVerwG*-Rechtsprechung eine (widerlegbare) Vermutungswirkung, dass ein Vorgehen entsprechend der Norm pflichtgemäß war [22].

Die Standards haben insofern einerseits zwar u.U. strafbarkeitskonstituierende Wirkung, falls die Anforderungen *nicht* eingehalten waren, andererseits aber bei der rechtlichen Beurteilung durch die Judikative u.U. die Wirkung eines „*antizipierten Sachverständigengutachtens*", mit der Aussage, dass die beschriebene Vorgehensweise „good practice" entspricht.

Selbstverständlich müssen solche Standards ausschließlich (und nachweisbar) das Ziel verfolgen, einen den „Stand der Technik" bzw. die „Anerkannten Regeln der Technik" widerspiegelnden Stand zur bestmöglichen Sicherheit aufzuzeigen.

Sofern dagegen durch entsprechende technische Normierungen ausschließlich oder auch nebenbei versucht wird, den Wettbewerb horizontal oder vertikal zu verzerren oder den Verbraucher- (oder Umwelt-!!)Schutz aufzuweichen, drohen erhebliche Sanktionen [52].

Ende Exkurs 2

3.3. Menschliches Versagen in der Risikofrüherkennung als größte Gefahr für das (Technical [Product])-Compliance-Managementsystem
Die frühzeitige Identifikation der (Technical [Product-]) Compliance-Risiken und das Erkennen der tatsächlich größten Risikofelder des Unternehmens mit objektivem, nicht kognitiv-verzerrtem Blick stellt den ersten Schritt dar [15, 42].

Oft werden in der Praxis naheliegende Worst-Case-Szenarien ignoriert. Dabei handelt es sich fast nie um *„schwarze Schwäne"*, noch nicht einmal um *„schmutzige weiße Schwäne"*, sondern um *„graue Nashörner"*,[3] also offensichtliche Risiken, die aus psychologischen Gründen und / oder aus Kalkül seitens der Verantwortlichen einer kaschierenden *(„Potemkinsche Dörfer")* Risiko-Behandlung zum Opfer fallen [53].

Im Falle des Versagens der Risikofrüherkennung werden dann diese Abweichungen meist dem Umfeld, wie Wettbewerbern oder der Politik zugeschrieben [54].

Um ein *wirksames* TPCMS sicherzustellen, sollte demnach größten Wert auf eine frühzeitige und umfängliche, faktenbasierte und von kognitivem Versagen befreite, fachmännische Risiko-Identifikation nach Stand der Technik gelegt werden.

4. Ausblick

Es zeigt sich, dass der einzige Unterschied zwischen TPCMS und CMS in den inhaltlich zu behandelnden Sachverhalten besteht. TPCMS stellt dann eine *Teilmenge des CMS* dar und kann integriert gesteuert werden. In der Methodik ergibt sich folglich kein Unterschied.

Ähnlich wird es auch zum Teil in der Praxis unter Diskussion der Ergebnisse der „Product Compliance Studie 2020" durch Experten diverser Industriezweige gesehen, u.a. *Uhlig: „(...) sollte die Technische Compliance so weit wie möglich in die vorhandenen Governance-Strukturen des Unternehmens, wie insbesondere ein vorhandenes Compliance-Managementsystem, angepasst werden, um Synergieeffekte zu nutzen [...] Deshalb ist daneben die regelmäßige präventive Überwachung der Angemessenheit und Wirksamkeit des Systems und seiner einzelnen Elemente erforderlich (...)"* ([55], S. 42)

Dadurch profitieren alle Prozessbeteiligten: Juristen, die sich heute im Rahmen des CMS häufig im Detail und im Schwerpunkt z.B. vor allem mit Anti-Korruption und Anti-Trust beschäftigen, müssen vor vermeintlich neuen, unbekannten Themen nicht zurückschrecken, und Ingenieure, die die TPCMS-Fragestellungen in ihrer Arbeit identifizieren, können auf

[3] Vor der Entdeckung „schwarzer Schwäne" in Australien waren die Europäer der Meinung, dass es solche Tiere nicht gäbe. Ein „Schwarzer Schwan" als Risiko ist heute gänzlich unbekannt. „Schmutzige weiße Schwäne" sind die Risiken, die bekannt sein könnten, aber nicht identifiziert werden können. „Graue Nashörner" sind offensichtliche Risiken, die bei Eintritt „tödlich", d.h. existenzgefährdend für das Unternehmen, wären. [51]

ein ausgereiftes „klassisches“ integriertes Risiko- und Compliance-Managementsystem (z.B. gemäß der international – neben COSO – anerkannten Standards ISO 37301:2021, ISO 31000:2018 und ÖNORM 4901:2021) mit angemessen Methoden und Tools zurückgreifen. Die Auditierung und Zertifizierung eines klassischen Risiko- und Compliance-Managementsystems sollte somit auch wertvolle Hinweise auf den Reifegrad des TPCMS inkl. Handlungsempfehlungen bringen und zugleich enthaftende Wirkung für „rechtschaffene“ Organisationen, Manager und Mitarbeiter zeigen.

Governance, Risikomanagement und Compliance sind *generell*, nicht nur in Bezug auf ökologische Themen, die wesentlichen Säulen von Nachhaltigkeit (ESG / CSR), im Detail siehe hierzu auch die Abbildung 1 [56]. Das TPCMS ist damit für die Erfüllung der ESG- / CSR-Anforderungen und -Ziele unverzichtbar.

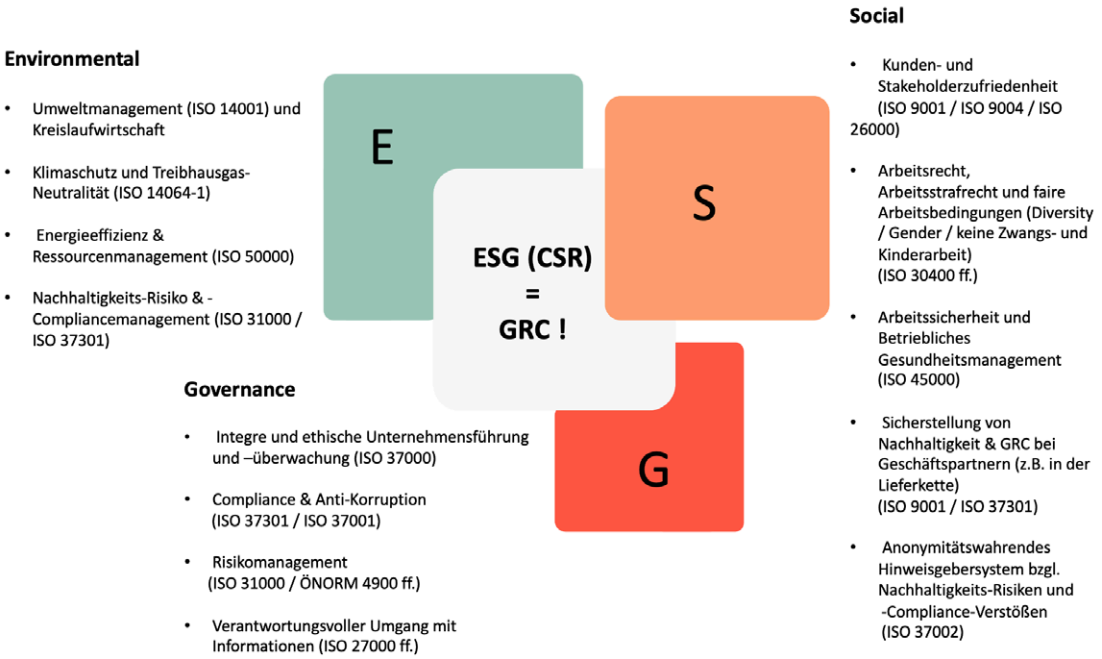

Abbildung 1 ESG = CRC! [40]

Literatur

[1] OLG Köln, Urteil vom 7.7.2021, Az. 11 U 68/20: Beck Aktuell – Heute im Recht, 20. Juli 2021, Online verfügbar unter: https://rsw.beck.de/aktuell/daily/meldung/detail/vw-und-audi-haften-gesamtschuldnerisch-fuer-vw-touareg (zuletzt geprüft: 25.09.2021).

[2] Scherer / Fruth (Hrsg.), Handbuch: Einführung in Product-Compliance, Vertragsmanagement und Qualitätsmanagement, 1. Auflage, 2018.

[3] United States District Court for the District of Columbia, Consent Decree Civil Action Nos. 1:20-cv-2564, 1:20-cv-2565, 14. September 2020, S. 41f, Online verfügbar unter: https://www.epa.gov/enforcement/daimler-ag-and-mercedes-benz-usa-llc-clean-air-act-civil-settlement-consent-decree (zuletzt geprüft: 25.09.2021).

[4] Hahne, „Dieselgate“ und die Folgen, Deutschlandfunk, 19.04.2021, Online verfügbar unter: https://www.deutschlandfunk.de/dieselgate-und-die-folgen-die-schleppende-aufarbeitung-des.724.de.html?dram:article_id=495928 (zuletzt geprüft: 25.09.2021).

[5] Beck Aktuell - Heute im Recht, Diesel Skandal: Führende Volkswagen Manager wegen Marktmanipulation angeklagt, im Internet unter: https://rsw.beck.de/aktuell/daily/meldung/detail/diesel-skandal-fuehrende-volkswagen-manager-wegen-marktmanipulation-angeklagt (zuletzt geprüft: 25.09.2021).

[6] Beck Aktuell - Heute im Recht, Anklage gegen Ex-VW-Chef Winterkorn wegen Verdachts der Marktmanipulation zugelassen, 24.09.2020, Online verfügbar unter: https://rsw.beck.de/aktuell/daily/meldung/detail/lg-braunschweig-anklage-gegen-ex-vw-chef-winterkorn-wegen-verdachts-der-marktmanipulation-zugelassen (zuletzt geprüft: 25.09.2021).

[7] Beck Aktuell - Heute im Recht, Kündigung einer Führungskraft wegen Dieselskandal unwirksam, 20.04.2021, Online verfügbar unter: https://rsw.beck.de/aktuell/daily/meldung/detail/lag-niedersachsen-kuendigung-fuehrungskraft-dieselskandal-vw-unwirksam (zuletzt geprüft: 25.09.2021).

[8] Scherer, Managerenthaftung, Transparenz, Wertbeiträge, Zielerreichung, digitale Transformation, Nachhaltigkeit: trotz menschlicher Schwächen mancher Manager und Mitarbeiter?, 2018, Online verfügbar unter: https://www.gmrc.de/images/Docs/Publikationen/Managerenthaftung_durch_Human_Workflow_Management_2018.pdf (zuletzt geprüft: 25.09.2021).

[9] Krubasik / Mehl / Römer, Technical Compliance White Paper, 2020, S.2., Online verfügbar unter: https://www.de.kearney.com/automotive/article/?/a/an-technical-compliance-kommt-niemand-mehr-vorbei (zuletzt geprüft: 25.09.2021).

[10] United States Environmental Protection Agency (EPA), Technical Compliance Rate (TCR) Performance Measures, 2015, https://www.epa.gov/ust/technical-compliance-rate-tcr-performance-measures (zuletzt geprüft: 25.09.2021).

[11] Wieland/ Steinmeyer/ Grüninger (Hrsg.), Handbuch Compliance-Management, 3. Auflage, 2020.

[12] Krenek, Interview zum Neubürger-Urteil, 2015, im Internet unter compliance-manager.net/fachartikel/zum-neubuerger-urteil-022015 (zuletzt geprüft: 25.09.2021).

[13] COSO Enterprise Risk Management – Integrated Framework, 2017.

[14] Institut Deutsche Wirtschaftsprüfer, Prüfungsstandard 980:2011.

[15] ISO 37301:2021 (Compliance Management).

[16] BGH, Urteil vom 9.5.2017, 1 StR 265/16.

[17] Scherer / Romeike / Grötsch, Unternehmensführung 4.0: CSR/ESG, GRC & Digitalisierung integrieren, 2021, Online verfügbar unter: https://www.risknet.de/elibrary/paper/unternehmensfuehrung-40-csr-esg-grc-digitalisierung-integrieren/ (zuletzt geprüft: 25.09.2021).

[18] ISO/DIS 37000:2021 (Governance of organizations).

[19] Scherer / Fruth (Hrsg.), Integriertes Compliance-Managementsystem mit GRC (4.0), 2. Auflage, 2017.

[20] Deutscher Corporate Governance Kodex 2019, im Internet unter https://www.dcgk.de/de/kodex/aktuelle-fassung/praeambel.html.

[21] Achenbach, Handbuch Wirtschaftsstrafrecht, 5. Auflage, 2019.

[22] Scherer, Technik-Governance - Die untrennbare Verzahnung von Recht, Technik, Wirtschaft und Psychologie – in BCM Sonderdruckheft, 2016.

[23] BVerfG, Beschluss vom 08.08.1978 – 2 BvL 8/77.

[24] Lach/ Polly, Produkt-Compliance, Leitfaden zum ProdSG, 3. Auflage, 2017.

[25] United States Environmental Protection Agency (EPA), Next Generation Compliance, Online verfügbar unter: https://www.epa.gov/compliance/next-generation-compliance (zuletzt geprüft: 25.09.2021).

[26] Schumacher/ Richter, Die Bedeutung von Technical Compliance, 10. Dezember 2020, Online verfügbar unter: https://www.deutscheranwaltspiegel.de/compliancebusiness/compliance/die-bedeutung-von-technical-compliance-22356/ (zuletzt geprüft: 25.09.2021).

[27] Porsche AG, Geschäfts- und Nachhaltigkeitsbericht 2020, S.49, Online verfügbar unter: https://newsroom.porsche.com/de/unternehmen/porsche-geschaefts-und-nachhaltigkeitsbericht-2020.html (zuletzt geprüft: 25.09.2021).

[28] BGH, Urteil vom 27.08.2010, 2 StR1 11/09.

[29] Scherer / Fruth (Hrsg.), Das interessiert Kapitalgeber: Antifragilität und der „Achilleskörper“ des Ordentlichen Kaufmanns, 1. Auflage, 2019, Online verfügbar unter: https://www.scherer-grc.net/files/fil/kapitalgeber.pdf (zuletzt geprüft: 25.09.2021).

[30] Scherer / Fruth (Hrsg.), Einführung in ein integriertes Compliance-Managementsystem mit GRC, 1. Auflage, 2018.

[31] Scherer / Fruth (Hrsg.), Governance- Management Band II (Standard & Audit), 1. Auflage, 2015.

[32] Scherer/ Butt/ Reimertshofer, Risiken der internationalen Produkthaftung aus der Sicht eines Unternehmers in Der Betrieb, Heft 9 vom 5.3.1993 S.469–474.

[33] Raum, Artikel „Compliance im Zusammenhang straf- und bußgeldrechtlicher Pflichten“, in Hastenrath (Hrsg.), Compliance-Kommunikation, 2017.

[34] BGH, Urteil vom 30.04.2020 - I ZR 115/16.

[35] Detterbeck, Allgemeines Verwaltungsrecht mit Verwaltungsprozessrecht, 18. Auflage, 2020.

[36] Scherer/ Rieger, Der Digitale Prozesszwilling im Gesundheitswesen - auch als Beitrag zu Nachhaltigkeit (ESG, CSR), systemische Existenzsicherung (Resilienz) und Governance in Journal für Medizin- und Gesundheitsrecht, Ausgabe 2-2021.

[37] Beck Aktuell - Heute im Recht, Dieselklagen – Sekundäre Darlegungslast und Prognose über die Gesamtlaufleistung, 17. August 2021, https://rsw.beck.de/aktuell/daily/meldung/detail/bgh-dieselklagen-sekundaere-darlegungslast-und-prognose-ueber-die-gesamtlaufleistung (zuletzt geprüft: 25.09.2021).

[38] Scherer, Digital Decision Management - die Verknüpfung von Digitalisierung, Nachhaltigkeit und GRC mit Entscheidungsmanagement, Strategieentwicklung, Zielerreichung und Berichterstattung „Aligning GRC with S (Strategy) & P (Performance)“, 25.11.2020 Online verfügbar unter: https://www.scherer-grc.net/publikationen/digital-decision-management (zuletzt geprüft: 25.09.2021).

[39] Taylor, Digital Decisioning: Using Decision Management to Deliver Business Impact from AI, 2. Auflage, 2019.

[40] BAG, Urteil vom 29.04.2021 (Az.: 8 AZR 246/20).

[41] Institut Deutscher Wirtschaftsprüfer, Prüfungsstandard 340:2020.

[42] Scherer/ Romeike/ Gursky, Mehr Risikokompetenz für eine Neue Welt in Journal für Medizin- und Gesundheitrsecht Ausgabe, 3-2021.

[43] Noack, Künstliche Intelligenz und die Unternehmensleitung in Festschrift für Christine Windbichler zum 70. Geburtstag am 8. Dezember 2020.

[44] Scherer/ Fruth (Hrsg.), Governance- Management Band I, 1. Auflage, 2015.

[45] Müller, Software als "Gegenstand" der Produkthaftung: Zugleich eine Betrachtung des Verhältnisses von § 823 Abs. 1 BGB zum Produkthaftungsgesetz, 1. Auflage, 2019.

[46] UNECE, Regelung Nr. 83, Online verfügbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A42015X0703%2801%29, (zuletzt geprüft: 25.09.2021).

[47] BGH, Urteil vom 12.10.2016 - 5StR 134/15.

[48] ISO 31010:2018 (Risikomanagement).

[49] Kahneman/ Sibony/ Sunstein, Noise, 1. Auflage, 2021.

[50] Handelsblatt, "Täuschen war lange Teil einer Arbeitskultur" - Ex-Audi-Chef Stadler sagt erstmals vor Gericht, 12.01.2021, aus im Internet unter: https://www.handelsblatt.com/unternehmen/industrie/dieselskandal-taeuschen-war-lange-teil-einer-arbeitskultur-ex-audi-chef-stadler-sagt-erstmals-vor-gericht-aus/26790318.html (zuletzt geprüft: 25.09.2021).

[51] Porter/ Nohria, How CEOs manage time, Harvard Business Review, 2018, im Internet unter: https://www.toimistosissit.fi/img/uploads/liitteet/leaders_calendar.pdf (zuletzt geprüft:25.09.2021).

[52] Beck Aktuell - Heute im Recht, Millionengeldbußen gegen Autohersteller wegen Absprachen bei Abgasreinigung neuer Diesel-Pkw, 8.Juli 2021 https://rsw.beck.de/aktuell/daily/meldung/detail/eu-kommission-millionengeldbussen-gegen-autohersteller-wegen-absprachen-zu-abgasreinigung-neuer-diesel-pkw (zuletzt geprüft: 25.09.2021).

[53] Romeike, Die Entmystifizierung der Quantifizierung, 8. April, 2021, Online verfügbar unter: https://www.risknet.de/themen/risknews/die-entmystifizierung-der-quantifizierung/ (zuletzt geprüft: 25.09.2021).

[54] Romeike/ Gleißner, Risikofrüherkennung und Erkennen von Krisensignalen, 17. Juni 2021, Online verfügbar unter: https://www.risknet.de/themen/risknews/risikofrueherkennung-und-erkennen-von-krisensignalen/ (zuletzt geprüft: 25.09.2021).

[55] Behrend, Product Compliance Management - Je früher, desto besser - in Zeitschrift unternehmensjurist, Ausgabe 5 - 2021, S. 40–43.

[56] Scherer, Nachhaltigkeits- (ESG-/CSR-) Compliance- und -Risikomanagement– die wesentlichen Pfeiler, auch für Resilienz, 2021, Online verfügbar unter: https://www.scherer-grc.net/files/fil/kurzversion-nachhaltigkeits--esg-csr--compliance--und-risiko.pdf (zuletzt geprüft: 25.09.2021).

Prof. Dr. jur. Josef Scherer*

Kontakt / *Contact*
✉ **josef.scherer@th-deg.de**

Wiebke Ketelsen (B.Eng.)

Wiebke Ketelsen ist seit 2011 in verschiedenen Positionen in einem deutschen Automobilkonzern beschäftigt. Im Rahmen ihrer Tätigkeit in der Konzernrevision und im Bereich Internal Investigations entdeckte sie ihre Faszination für die Schnittstelle zwischen Jura und Technik und speziell das Thema (Technical) Product Compliance. Zur Anreicherung ihres praktischen Wissens mit wissenschaftlichen Grundlagen absolviert sie derzeit den Masterstudiengang „Risiko- und Compliancemanagement“ an der Technischen Hochschule Deggendorf.

Wiebke Ketelsen has held various positions in a German automobile company since 2011. Her work in Group Auditing and Internal Investigations, made her discover her fascination for the interface between law and technology, especially for (technical) product compliance. In order to fortify her practical knowledge by scientific basics, she is currently completing the master's programme "Risk and Compliance Management" at the Deggendorf Institute of Technology.

Kontakt / *Contact*
✉ **wiebke.ketelsen@web.de**

* Profil s. S. 30 / *Personal profile see p. 30*