ISSN 2568-6380 Art.-Nr. 74659531

ZInsO 31

31. Juli 2025

Zeitschrift für das gesamte Insolvenz- und Sanierungsrecht

28. Jahrgang · Seite 1489 bis 1548

FOKUS

Transformation und Restrukturierung in der Krise

Josef Scherer/Sascha Seehaus

Pflicht zu Governance mit Risikofrüherkennung, Resilienz und Transformation als Kardinalpflicht von Organen und Führungskräften

Wolters Kluwer

Pflicht zu Governance mit Risikofrüherkennung, Resilienz und Transformation als Kardinalpflicht von Organen und Führungskräften[1]

Geschäftsführer,[2] Vorstände, Aufsichtsratsmitglieder und Führungskräfte „segeln blind in Haftung und Versicherungsverlust“[3]

von Professor Dr. Josef Scherer, Deggendorf* und Dr. Sascha Seehaus, Diez**

Geschäftsführer, Vorstände, Aufsichtsräte, Abschlussprüfer, Revisoren, Compliance- und Risikomanager, IKS-Verantwortliche (sowie weitere Lines of Defense-Funktionen) kümmern sich in Zeiten multipler Krisen und Transformation oft zu wenig um die wirklich wichtigen Dinge. Die aktuelle Lage birgt große Gefahren und Chancen. Diese angemessen zu identifizieren und zu bewerten und daraus angemessene Transformationsmaßnahmen abzuleiten, um langfristig die Existenz bzw. Resilienz der Organisation zu sichern,[4] gehört zu den wesentlichen Governance-Pflichten, die häufig unbekannt sind oder vernachlässigt werden. Dies verursacht bei den betroffenen Organisationen häufig finanzielle Schäden, bringt sie nicht selten in vermeidbare existenzielle Schwierigkeiten und wird zumeist haftungsbewehrtes Missmanagement[5] darstellen.

Neben des nachgewiesen drastisch steigenden Risikos der persönlichen Haftung droht aufgrund des von aktueller Rechtsprechung[6] angenommenen Vorwurfs der „Verletzung von Kardinalpflichten“[7] und der daraus abgeleiteten Indikation einer „wissentlicher Pflichtverletzung“ der Verlust des Versicherungsschutzes für Manager.

Die Untersuchung der Geschäftsberichte von Organisationen indiziert häufig große Versäumnisse bei Governance, Risk und Compliance, also der ökonomischen Nachhaltigkeit. Bspw. existiert bei den Organen (Geschäftsführer, Vorstand, Aufsichtsgremien) und „Lines of Defense“ i.d.R. noch wenig Verständnis bzgl. des Inhalts von sog. „Kardinalpflichten“ und „risikobasierter Governance-Compliance“, obwohl dies aktuell das Top-Risiko nahezu aller Organisationen verkörpert. Wenn das Leitungsorgan Führung und Überwachung (Governance) im Bereich der Resilienz und Transformation delegiert, die Delegationsempfänger jedoch nicht effektiv sind, stellt sich die Frage der Abgrenzung von fehlerhafter Delegation und Mitarbeiterexzess.

Nachfolgende Abhandlung beleuchtet die Rolle der Organe, der „Lines of Defense“-Funktionen inklusive Auditoren[8] und Zertifizierer, die sich zum einen bei auftretenden Problemen in ihrem Scope bzw. Prüfbereich zu rechtfertigen haben.

Zum anderen wird aufgezeigt, dass umgekehrt „gute, risikobasierte Audits“ enorme Wertbeiträge für Resilienz in schwierigen Zeiten bringen können.

Nicht ohne Grund steht das „Governance-G“ im Nachhaltigkeitsakronym ESG für ökonomische Nachhaltigkeit. Diese wiederum ist die Voraussetzung, um auch sozial und ökologisch nachhaltig wirken zu können: „Ohne Moos nichts los.“[9]

---

* Prof. *Dr. Josef Scherer* ist Gründer und Partner der Kanzlei Prof. Dr. Scherer & Partner mbB mit Fokus auf Wirtschaftsrecht, Compliance, Risk und Governance. Seit 1996 lehrt er als Prof. für Unternehmensrecht, Risiko- und Compliancemanagement an der TH Deggendorf. Zuvor war er Staatsanwalt und Zivilrichter. Als Geschäftsführer der Governance Solutions GmbH begleitet er Unternehmen bei der Digitalisierung und rechtskonformen Ausgestaltung ihrer Organisations- und Managementsysteme.

** *Dr. Sascha Seehaus* ist Fachanwalt für Insolvenz- und Sanierungsrecht sowie zertifizierter ESGRC-Manager und Master Risiko- und Compliancemanagement (M.A.). Er begleitet Unternehmer in Transformations- und Übergangsphasen mit besonderem Schwerpunkt auf nachhaltiger Unternehmensführung, strategischer Restrukturierung, haftungsvermeidender Leitungsorganisation sowie wirksamem Personal- und Forderungsmanagement.

1 Hinw.: Teile dieses Beitrags entsprechen dem Artikel *Scherer*: Kardinalpflicht fordert „risikobasierten Ansatz“, veröffentlicht auf RiskNET, abrufbar unter: *https://www.risknet.de/themen/risknews/kardinalpflicht-fordert-risikobasierten-ansatz/.*

2 Gender-Hinw.: Sofern in diesem Artikel bestimmte Gender-Formen Verwendung finden, sind stets alle gemeint.

3 Leicht abgeändertes Zitat aus: OLG Frankfurt/M., Beschl. v. 16.1.2025 – 7 W 20/24, NJW-RR 2025, 731: „blind in die Krise segeln“.; vgl. auch OLG Frankfurt/M., Urt. v. 5.3.2025 – 7 U 134/23, DStR 2025, 917, mit einem ähnlichen Fall (Rev. eingelegt, BGH – IV ZR 66/25).

4 Vgl. ISO 37000:2021-09 „Governance of Organizations“, chap. 6.11 „Viability and performance over time“.

5 Vgl. *Scherer*, Das interessiert Kapitalgeber: Antifragilität und der „Achilleskörper“ des Ordentlichen Kaufmanns, 2019, abrufbar unter: *https://www.scherer-grc.net/publikationen/das-interessiert-kapitalgeber-antifragilitaet-und-der-achilleskoerper-des-ordentlichen-kaufmanns*.

6 OLG Frankfurt/M., Beschl. v. 16.1.2025 – 7 W 20/24, NJW-RR 2025, 731: „blind in die Krise segeln“ und OLG Frankfurt/M., Urt. v. 5.3.2025 – 7 U 134/23, DStR 2025, 917, mit einem ähnlichen Fall (Rev. eingelegt, BGH – IV ZR 66/25).

7 „Kardinalpflichten“ sind nach den aktuellen Urteilen des OLG Frankfurt/M. (OLG Frankfurt/M., Beschl. v. 16.1.2025 – 7 W 20/24, NJW-RR 2025, 731; OLG Frankfurt/M., Urt. v. 5.3.2025 – 7 U 134/23, DStR 2025, 917) „*elementare berufliche Pflichten, deren Kenntnis nach der Lebenserfahrung bei jedem Berufsangehörigen vorausgesetzt werden kann*.“ Es wurden von der aktuellen Rechtsprechung (vgl. oben) auch *Kardinalpflichten im Rahmen der Governance* (gewissenhafte Führung und Überwachung von Organisationen) statuiert. Dabei haben sich in der Rechtsprechung bereits diverse Fallgruppen herausgebildet. Die aktuelle Rechtsprechung erweitert diese Fallgruppen nun auf die „*vielfältigen Pflichten in Bezug auf die Unternehmensleitung, die mit Eintragung als Geschäftsführer einer Kapitalgesellschaft verbunden sind*“. Damit ist die *Governance-Compliance* zu Recht als eine elementare berufliche Pflicht eines Geschäftsführers oder Vorstandes anzusehen.

8 Auditoren werden z.B. als interne Auditoren (vgl. ISO Harmonized Structure Normabschnitt 9.2), Third Party-Auditoren oder Auditoren externer Zertifizierungsstellen tätig.

9 Bayerisches Sprichwort.

I. Aktuelle Lage: Best, real und worst Case – dringender Handlungsbedarf

1. Zuspitzung der Risikolage in Zeiten multipler Transformationen

Die weltweiten geopolitischen, ökonomischen und ökologischen Krisen in Zeiten grundlegender Transformation (technologisch, demografisch, ökologisch, sozial, regulatorisch) spitzen sich allmählich zu.

Ein angemessenes Risikomanagement inklusive Risikofrüherkennung[10] muss auch Worst-Case-Szenarien berücksichtigen, alle Risiken angemessen quantifizieren, aggregieren, steuern und mit der Risikotragfähigkeit in Abgleich bringen.[11]

2. Relevante empirische Befunde: Insolvenzrisiken und Risikowahrnehmung

a) Erhöhte Insolvenzwahrscheinlichkeit in der Breite der Wirtschaft

Nach einer aktuellen Studie zur Finanzlage von Unternehmen in Deutschland haben aktuell ca. 318.000 bzw. jedes zehnte Unternehmen ein erhöhtes Insolvenzrisiko.[12]

Die Insolvenzzahlen stiegen allerdings bereits vor Trumps Zollkapriolen auf Höchstwerte.[13]

b) Risikobewusstsein in kapitalmarktorientierten Unternehmen vorhanden

Eine aktuelle Auswertung[14] der Geschäftsberichte der 134 größten deutschen DAX-, M-DAX und S-DAX-Unternehmen weist auf einen enormen Anstieg der Risiken hin. Die Zahl der benannten Risiken stieg in den Geschäftsberichten gegenüber dem 2023 um 30 %. Jeweils 98 % der Risikoberichte nennen *Regulatorische Veränderungen* und *Cyber-Vorfälle* als Top-Risiken, gefolgt von *Geopolitischen Entwicklungen, Finanzthemen, Wettbewerb* und *Recht und Compliance*.

c) Glaubwürdigkeitsdefizit durch Kommunikationslücke beim Top-Management

Während in Risikoberichten so viele Risiken und Bedrohungen gleichzeitig benannt wurden wie noch nie, schweigen sich über 40 % der CEO-Vorworte hierüber aus. Dies untergräbt die Glaubwürdigkeit der Governance-Funktion. CEOs verfehlen so ihre Führungsverantwortung.[15]

3. Fehlende Risikoorientierung in Leitung und Überwachung

a) Ignoranz gegenüber realistischen Krisenszenarien

Obwohl inzwischen sogar eine Weltwirtschaftskrise vom Chef des Ifo-Instituts für möglich gehalten wird,[16] ist der aktuelle Handlungsdruck offenbar noch nicht bei den Geschäftsführern, Vorständen und Überwachern (Aufsichtsräten, Abschlussprüfern, Lines of Defense mit Interner Revision, Risiko- und Compliance-Management etc.), aber auch bei den diversen Arten von *Auditoren* angekommen.

Worst-Case-Szenarien werden oft bewusst oder aus Ignoranz ausgeblendet.[17]

b) Fehlgeleiteter Ressourceneinsatz und verhaltensökonomische Blockaden

Stattdessen werden häufig die weniger werdenden Ressourcen nicht auf die wichtigen Dinge gebündelt, sondern für reine Bürokratie ohne Wertbeiträge ausgegeben.[18]

Das mag verhaltensökonomische Gründe[19] haben, liegt aber häufig auch daran, dass zum einen in den Aufsichtsratsgremien und Vorstands- und Geschäftsführungsetagen Regularien, wie § 1 StaRUG (Pflicht zur Risikofrüherkennung) oder § 93 Abs. 1 Satz 2 AktG (Business Judgment Rule) nicht angemessen bekannt sind oder verstanden werden.

c) Wissensdefizite und mangelnde GRC-Kompetenz

Oft fehlt auch echte Governance-, Risiko- und Compliancekompetenz und die GRC-Experten werden vor oft intuitiven Entscheidungen der Organe nicht beigezogen oder ernstgenommen.[20] Diese werden vielmehr mit operativen Aufgaben, wie Schulungen und bürokratischem Reporting[21] beschäftigt.

---

10 Vgl. hierzu ausführlich *Scherer/Seehaus*, Governance und Compliance nach § 1 StaRUG, 2024, RiskNET.de, abrufbar unter: *https://www.risknet.de/themen/risknews/kontinuierliche-risikoueberwachung-in-echtzeit/*, und *Romeike*, IDW ES 16 – Krisenfrüherkennung und Krisenmanagement nach § 1 StaRUG, 2025, RiskNET.de, abrufbar unter: *https://www.risknet.de/themen/risknews/krisenfrueherkennung-und-krisenmanagement-nach-1-starug/*.

11 Vgl. *Scherer/Romeike/Gursky*, Mehr Risikokompetenz für eine neue Welt, RiskNET.de, 2021, abrufbar unter: *https://www.risknet.de/themen/risknews/mehr-risikokompetenz-fuer-eine-neue-welt/* und *Pätzold*, ZInsO 2025, 605 ff.

12 Vgl. CRIF, Jedes zehnte Unternehmen in Deutschland ist insolvenzgefährdet, 2025, RiskNET.de, abrufbar unter: *https://www.risknet.de/themen/risknews/jedes-zehnte-unternehmen-in-deutschland-ist-insolvenzgefaehrdet/*.

13 Vgl. Tagesschau, „Zahl der Insolvenzen steigt weiter", 14.3.2025, abrufbar unter: *https://www.tagesschau.de/wirtschaft/insolvenzen-anstieg-100.html*.

14 Vgl. *Romeike*, Was Risikoberichte sagen – und Vorstände verschweigen, 2025, unter Verweis auf Crunchtime Risikomonitor 2025, abrufbar unter: *https://www.risknet.de/themen/risknews/was-risikoberichte-sagen-und-vorstaende-verschweigen/*.

15 Vgl *ders*. ebda.

16 Vgl. n-tv, Ifo-Chef hält neue Weltwirschaftskrise für möglich, ntv news, 12.4.2025, abrufbar unter: *https://www.n-tv.de/wirtschaft/Ifo-Chef-haelt-neue-Weltwirtschaftskrise-fuer-moeglich-article25699556.html*.

17 Vgl. *Scherer/Romeike/Gursky*, Mehr Risikokompetenz für eine neue Welt, RiskNET.de, 2021, abrufbar unter: *https://www.risknet.de/themen/risknews/mehr-risikokompetenz-fuer-eine-neue-welt/*.

18 Vgl. *Scherer*, Investition in Governance im Lichte von Basel IV und Rating, RiskNET.de, 2025, abrufbar unter: *https://www.risknet.de/themen/risknews/der-weg-zu-resilienz-und-rentabilitaet/*.

19 Vgl. *ders*. ebda.

20 Beispiel: Angemessene Business Judgment Rule-Gutachten *vor* relevanten Entscheidungen fehlen häufig. Bayer hat noch immer unter dem Kauf von Monsanto während laufender US-Product-Compliance-Prozessen zu leiden.

21 Z.B. dem LKSG-Bericht, den die BAFA nicht ernsthaft einforderte bzw. dessen Ausbleiben nicht sanktionierte.

d) Unzureichende Umsetzung des risikobasierten Ansatzes

Auch der „*risikobasierte Ansatz*“, nämlich sich nach angemessener Risikobewertung priorisiert um die wichtigen Dinge zu kümmern, ist zu wenig bekannt oder praktiziert:

Wichtig sind primär die Vermeidung von Gefahr für Leib und Leben oder persönlicher Sanktionen Beschäftigter oder Dritter und von erheblichen finanziellen Einbußen, die die Risikotragfähigkeit beeinträchtigen.

4. Fazit: Strategische Fokussierung dringend geboten

„In herausfordernden Zeiten gilt es, den Fokus auf die wichtigen Themen zu legen. (…) Viel Zeit der Geschäftsleitung und Ressourcen werden noch für Themen verwendet, deren strategische Relevanz zumindest fraglich ist.“[22]

II. Das Wichtige richtig machen: Beispiele für Dinge, die viele Ressourcen binden, aber wenig bringen

Nachhaltigkeit und Datenschutz sind natürlich sehr wichtig. Aber auch hier gilt die Anwendung des „risikobasierten Ansatzes“.

1. Beispiel: Nachhaltigkeitsberichterstattung und Lieferkettensorgfaltspflichten-Gesetz

Nachdem sich der Mittelstand bei hohem Ressourcenverbrauch nunmehr Jahre auf die Berichterstattung mit CSRD, ESRS, Taxonomie, CSDDD etc. vorbereitet hat, erkennen die EU und auch die neue Koalition, dass sich in die Regulierung existenziell wichtigen Nachhaltigkeitsthemen sehr viel Bürokratie, Redundanzen und Analogien eingeschlichen hatten und steuern jetzt mit ESG-Omnibuspaketen und Abschaffung von LKSG zurück.[23]

Außer Unberechenbarkeit, Kosten, Bürokratie, Verunsicherung und Verärgerung im Mittelstand wurde nichts erreicht.

2. Beispiel: Datenschutz und Löschung wichtiger Dokumente

Seit 2018 fielen mit der DSGVO dem oft schon hysterisch umgesetzten Datenschutz mit voreiliger Löschung von Dokumenten viele Informationen zum Opfer, die im Nachgang als entlastende oder positive Dokumentation gegenüber Vertragspartnern, Behörden oder Gerichten benötigt werden würden.

Es ließen sich noch – neben einer komplexen Steuerregulierung, der nicht auszuweichen ist[24] – zahlreiche weitere Bürokratie-Monster aufzählen, die der Mittelstand leidvoll erträgt.

III. Beispielsfälle, in denen evtl. das Risikomanagement, aber u.U. auch Aufsichtsorgane, Abschlussprüfer und Lines of Defense inklusive diverse Auditoren versagt haben

1. Fall BayWa AG: Bilanzprüfung, Informationsversäumnisse und Prüfungsversagen

Am 11.11.2024 meldeten die Medien, die Bafin ordne die Überprüfung der BayWa-Bilanz an. Es gäbe konkrete Anhaltspunkte für Verstoß gegen Rechnungslegungsvorschriften. Die Darstellung der finanziellen Lage und der Risiken aus der Finanzierung des Konzerns sei möglicherweise fehlerhaft. Die international tätige Wirtschaftsprüfungsgesellschaft PricewaterhouseCoopers (PwC) hatte den Geschäftsbericht testiert. Im uneingeschränkten Testat zum Geschäftsbericht 2023 verzichtet PwC auf Hinweise zur angespannten finanziellen Lage des Unternehmens, die allerdings längst bekannt war. Inzwischen seien ca. 1 Mrd. Fresh Money ausgereicht worden, so Presseberichte.[25]

2. Weitere Fälle: Wirecard, Helma AG und Creditshelf AG u.v.m.

Nicht nur bei Wirecard haben nach allg. M. sämtliche Aufsichtsmechanismen kläglich versagt.[26]

Bei den insolventen Unternehmen Helma AG und Creditshelf AG kam eine nachträgliche Überprüfung des Geschäftsberichts zum Schluss, dass u.U. die „*gesetzlich gebotenen Mindestanforderungen an das Risiko- und Krisenfrüherkennungssystem nicht umgesetzt worden waren*.“[27]

„Es ist erschreckend, dass diese von den Abschlussprüfern, die sich am IDW PS 340 orientieren, weiterhin nicht geprüft werden. Dies sollten Vorstand und Aufsichtsräte wissen, weil die Prüfung damit kaum hilfreich ist. (…) ist festzuhalten, dass Verpflichtung für ein leistungsfähiges Krisen- und Risikofrüherkennungssystem selbstverständlich bei Vorstand und Aufsichtsrat liegt und auch den Aufsichtsrat hier in die Haftung nimmt.“[28]

---

22 Zitat aus *Gleißner/Weissmann*, Die strategischen Herausforderungen deutscher Unternehmen, Die Deutsche Wirtschaft, 2024, abrufbar unter: *https://futurevalue.de/wp-content/uploads/2024/12/FA-2344-Strategische-Herausforderungen-deutscher-Unternehmen-2024.pdf*.

23 Vgl. *Scherer*, CSRD-Umsetzung: Was die Verzögerung für KMU bedeutet, Lexware 2025, abrufbar unter: *https://www.lexware.de/wissen/nachhaltigkeit/csrd-umsetzung/*.

24 Vielmehr ist zu raten, aus Haftungsbegrenzungsgründen ein Tax-Compliance-Managementsystem gem. § 153 AO zu implementieren.

25 Vgl. faz.net, Prüfung des Konzernabschlusses von Baywa, abrufbar unter: *https://www.faz.net/aktuell/wirtschaft/bafin-ordnet-pruefung-des-konzernabschlusses-von-agrarkonzern-baywa-an-110105059.html*.

26 Vgl. *Gleißner*, Wirecard: Schwächen bei Risikomanagement und Abschlussprüfung, RiskNET.de, abrufbar unter: *https://www.risknet.de/themen/risknews/wirecard-schwaechen-bei-risikomanagement-und-abschlusspruefung/* sowie *Glaser*, Und täglich grüßt … Wirecard!, abrufbar unter: *https://www.risknet.de/themen/risknews/und-taeglich-gruesst-wirecard/*.

27 Vgl. *Gleißner/Wolfrum*, ZfRM 2024, 116, 118.

28 Vgl. *Gleißner/Wolfrum*, ZfRM 2024, 116, 118.

3. Empirische Mängellage in Geschäftsberichten und Rolle der Aufsichtsräte

Eine Untersuchung der Angaben zum Risikomanagement in den Geschäftsberichten deutscher DAX- und MDAX-Unternehmen kommt zum Ergebnis, dass die Anforderungen nach § 1 StaRUG und FISG kaum beachtet werden. 83 nach diversen Kriterien bewertete Geschäftsberichte erreichten im Schnitt nur ca. 37 % der möglichen Punkte:[29]

„Viele Vorstände scheinen sich nur mit dem zu befassen, was der Abschlussprüfer sehen möchte und nicht mit den Aspekten, die ökonomisch wichtig und sogar gesetzlich geboten sind. Es besteht großer Handlungsbedarf.

Gefordert sind insbesondere die Aufsichtsräte, die in § 1 StaRUG und § 107 AktG direkt angesprochen werden und denen auch persönliche Haftungsrisiken entstehen könnten (…)"[30]

4. Systemkritik an Rolle, Struktur und Unabhängigkeit der Wirtschaftsprüfer

Die Welt der Überwacher[31] schafft es offenbar trotz des hohen Ressourceneinsatzes nicht, die wirklich wichtigen Dinge effektiv zu steuern und zu überwachen. Die Rolle der Wirtschaftsprüfer als unabhängige Instanz zur Sicherstellung der Verlässlichkeit von Unternehmensabschlüssen gerät zunehmend unter Druck. Fälle wie der der BayWa AG, bei dem die wirtschaftlichen Schwierigkeiten des Unternehmens über einen längeren Zeitraum unzureichend reflektiert wurden, werfen erneut Fragen zur Risikowahrnehmung und Unabhängigkeit von Abschlussprüfern auf. Kritiker bemängeln eine strukturelle Nähe zu den geprüften Unternehmen sowie wirtschaftliche Abhängigkeiten, die die objektive Prüfungsqualität beeinträchtigen könnten.

Zitat.[32]

„(…) Wirtschaftsprüfer sind gemäß § 317 HGB und den Grundsätzen ordnungsmäßiger Abschlussprüfung (IDW PS 200 ff.) verpflichtet, risikoorientiert zu prüfen. Das bedeutet, dass insbesondere bei Unternehmen mit angespannten Bilanzkennzahlen und erhöhter Bestandsgefährdung das Risikomanagementsystem als zentrales Element einer Going Concern-Würdigung in den Fokus der Prüfung rücken muss. (…)

Gerade bei einem Konzern wie BayWa, der hochgradig abhängig ist von externen Einflussfaktoren wie Rohstoffpreisen, Zinssätzen oder regulatorischen Änderungen, ist ein solch vereinfachender Risikoblick grob fahrlässig und führt zu einer kompletten Risikoblindheit.

Es ist daher umso irritierender, dass Wirtschaftsprüfer ein solche Aussage im Risikobericht akzeptieren. Doch leider ist BayWa (PWC) hier keine Ausnahme.

Auch bei Wirecard (Ernst & Young), Lehman Brothers (Ernst & Young), Gerry Weber International (Ebner Stolz), Thomas Cook (Ernst & Young), Prokon Regenerative Energien (BDO), Luckin Coffee (Ernst & Young), Schlecker Drogeriemärkte (Grant Thornton, vormals Baker Tilly Roelfs), NMC Health (Ernst & Young), Greensill Capital (Grant Thornton), Carillion (KPMG), Steinhoff (Deloitte), Hypo Alpe Adria/HETA (KPMG) und vielen weiteren Unternehmenskrisen und -pleiten waren die Wirtschaftsprüfer in einem kompletten Blindflug unterwegs. (…)"

Bereits *Michel Barnier*, ehemaliger EU-Binnenmarktkommissar, hatte im Zuge der Finanzkrise ambitionierte Reformen angestoßen, um die Unabhängigkeit der Wirtschaftsprüfer zu stärken.[33] Vorgesehen waren u.a. eine strikte Trennung von Prüfung und Beratung, eine obligatorische Rotation der Prüfgesellschaften sowie Maßnahmen zur Förderung des Wettbewerbs im stark konzentrierten Prüfungsmarkt. Viele dieser Vorschläge wurden jedoch im weiteren Gesetzgebungsprozess verwässert oder abgeschwächt, auch aufgrund des erheblichen Widerstands großer Marktakteure und nationaler Interessen.

Das Ergebnis ist ein Regulierungsrahmen, der in der Praxis nicht konsequent genug wirkt, um systemische Interessenkonflikte zu vermeiden. Die Diskussion um eine Reform der Wirtschaftsprüfung bleibt damit aktuell – nicht zuletzt vor dem Hintergrund wachsender Anforderungen an Transparenz, Nachhaltigkeit und Risikomanagement in Unternehmen.

Hinweis:

Inzwischen veröffentlichte das Institut Deutscher Wirtschaftsprüfer den IDW ES 16 zur Prüfung der Umsetzung der Anforderungen aus § 1 StaRUG.[34] *Dieser Entwurf beinhaltet noch zahlreiche Schwachstellen und bleibt hinter den Anforderungen des Gesetzgebers und des DIIR Nr. 2 erheblich zurück.*

Aus rechtlicher Perspektive ist anzumerken, dass sich die Verantwortung der Organe (Geschäftsführer/Vorstand/Aufsichtsrat etc.) und exponierter Führungskräfte i.S.v. § 9 Abs. 2 OWiG für eine rechtskonforme und angemessene Risiko- bzw. Krisenfrüherkennung primär nach Gesetz (z.B. § 1 StaRUG, § 91 Abs. 2 und 3 AktG, § 43 GmbHG, §§ 93, 116, 107 AktG), Rechtsprechung und den „Anerkannten Regeln der Technik" zu richten hat und Standards privater (berufsständischer) Organisationen, wie IDW, DIIR, DIN rechtlich nur relevant sind, wenn sie die Anforderungen dieser Quellen widerspiegeln.

Die Aufgabe und Verantwortung der Abschlussprüfer in Hinblick auf deren Prüfung von Risiko- oder Krisenfrüherkennung richtet sich ebenso in erster Linie nach den

29 Vgl. *Jungesblut*, Corporate Finance, 2024, 274.

30 Vgl. *Jungesblut*, Corporate Finance, 2024, 274, 280 (Zitat).

31 Vgl. *Scherer*, FIRM Jahrbuch 2017, 79, abrufbar unter: *https://www.gmrc.de/images/Docs/Publikationen/Scherer_Die_Welt_en_der_Ueberwacher.pdf*.

32 Vgl. *Romeike*, Der Erwartungswert-Irrtum – Selbsttäuschung im Risikobericht der BayWa, 2025, RiskNET.de, abrufbar unter: *https://www.risknet.de/themen/risknews/der-erwartungswert-irrtum/*.

33 Vgl. *Romeike/Hager*, Finanzkrise legt Schwächen bei Wirtschaftsprüfern offen, *abrufbar unter: https://www.risknet.de/themen/risknews/finanzkrise-legt-schwaechen-bei-wirtschaftspruefern-offen/*.

34 Vgl. *Romeike*, IDW ES 16 – Krisenfrüherkennung und Krisenmanagement nach § 1 StaRUG, 2025, RiskNET.de, abrufbar unter: *https://www.risknet.de/themen/risknews/krisenfrueherkennung-und-krisenmanagement-nach-1-starug/*.

Anforderungen aus Gesetz (z.B. HGB) und Rechtsprechung und nicht nach vom eigenen Berufsverband vorgegebenen „Gebrauchsanweisungen" respektive Prüfstandards, sofern diese ein minus hierzu beinhalten. Insofern sollte es ein Anliegen des Berufsstandes sein, nur durch Prüfstandards des Berufsverbandes, die Gesetz, Rechtsprechung und Anerkannten Regeln der Technik entsprechen, unterstützt zu werden. Unkenntnis der Rechtslage unter Verweis auf Befolgung eines hinter der Rechtslage zurückbleibenden Standards würde Abschlussprüfer nicht exkulpieren.

Ein klarstellender Hinweis, dass aktuelle Anforderungen aus Gesetz, Rechtsprechung und Anerkannten Regeln der Technik den Inhalten der Standards stets vorgehen und zu beachten sind, findet sich leider nur vereinzelt und nicht unbedingt plakativ in Standards des DIN und des IDW.

IV. Beispiel für Wichtiges: Risiken bei Governance, Risikofrüherkennung, IT mit KI

1. Aktuelle globale Risikolage und Cyber-Bedrohungsszenarien

Das mittelfristige Top Risiko Nr. 1 des Global Risks Report 2024 war aufgrund der Entwicklungen der Künstlichen Intelligenz (KI) das Thema „Desinformation und Manipulation".[35]

Zu den größten Sorgen der CEOs weltweit gehörten auf Platz 1 die Cyber Risks.[36] Auch 2025 haben sich diese Risikoeinschätzungen kaum verändert.[37]

Die sich weiterhin zuspitzende Cyberbedrohungslage inklusive Bedrohungspotenziale durch die Nutzung von Künstlicher Intelligenz ist die dominierende Sorge der meisten Unternehmen/Organisationen. Im Zusammenhang mit der damit verbundenen stark verschärfenden Regulierung wachsen die Risiken von Streitigkeiten über Versicherungspolicen und Cyber-Compliance in der Wertschöpfungskette.

2. Governance- und Risikoanforderungen im Spannungsfeld regulatorischer Unklarheit

Die sich ausdehnende und vielfältige Risikolandschaft – auch außerhalb von IT und KI – erfordert höchste Aktualität und Qualität bei Risikofrüherkennung und -management sowie der *Governance, also der „nachhaltigen compliance- und risikobasierten, gewissenhaften Führung und Überwachung von Organisationen*".[38]

Erschwerend wirkt sich bei der Erfüllung der Anforderungen aus Governance-Compliance aus, dass bereits mangels Legaldefinition Unklarheit bzgl. der Definition, des Inhalts und der konkreten Anforderungen von Governance in Wissenschaft und Praxis herrscht.

Dadurch interpretieren die o.g. Verantwortlichen inklusive der Auditoren völlig willkürlich und unterschiedlich, was – wie nachfolgend aufgezeigt wird – zu fatalen Ergebnissen führt.

Auch die (Arbeitssicherheits-, Umwelt-, Informationssicherheits-, Qualitäts-, Nachhaltigkeits-, Energieeffizienz- etc.-) Managementsystem-Verantwortlichen nebst deren Auditoren und Zertifizierern müssten längst realisiert haben, dass angemessenes Compliance- und Risikomanagement auch für das von ihnen betreute System die primäre und unverzichtbare Anforderung darstellt.

3. Risikoverständnis und Handlungsnotwendigkeit in Organisationen

I.d.R. sind nicht bestandsgefährdende Einzelrisiken, sondern die kumulierende Wirkung vieler Einzelrisiken fatal; daher ist eine methodisch fundierte Aggregation der Risiken wichtig.[39]

4. Zwischenfazit zur Governance-Kompetenz

Um in den Organisationen für Resilienz zu sorgen, sollten die derzeit nicht angemessen vorhandenen erforderlichen Governance-Kompetenzen bei den Managern und deren Überwachern zeitnah auf angemessenen Stand gebracht und dann auch entsprechend umgesetzt, gesteuert und überwacht werden.

V. Governance-Compliance

1. Begriff und Systematik von Governance

Governance lässt sich juristisch als die *„nachhaltige compliance- und risikobasierte, gewissenhafte Führung und Überwachung von Organisationen inkl. Interaktion mit relevanten Stakeholdern*" definieren.

Das *Governance-Compliance*-Managementsystem ist eine Aufbau- und Ablauforganisation, bestehend aus Komponenten (z.B. Rollen, Zielen, Ressourcen, Prozessabläufen, 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 im Bereich Governance* zu unterstützen.

---

35 Vgl. WEF, Global Risks Report 2024, abrufbar unter: *https://www.weforum.org/publications/global-risks-report-2024/*.

36 Vgl. PWC, CEOs´ Global Survey 2024, abrufbar unter: *https://www.pwc.de/de/ceosurvey.html*.

37 Vgl. WEF, Global Risks Report 2025, abrufbar unter: *https://www.weforum.org/publications/global-risks-report-2025/* und PWC, CEOs´ Global Survey 2025, abrufbar unter: *https://www.pwc.de/de/ceosurvey.html*.

38 Vgl. *Scherer*, Nachhaltige Führung und Überwachung von Organisationen (Governance) nach DIN ISO 37000 - erfolgreich umsetzen, auditieren und reporten, DIN Media, 2025, Kapitel Einl.

39 Vgl. *Romeike*, Qualitative Methoden zur Risikoaggregation sind eine Fiktion, 2019, abrufbar unter: *https://www.risknet.de/themen/risknews/qualitative-methoden-zur-risikoaggregation-sind-eine-fiktion/* sowie *Romeike*, Risikoaggregation wird zur Pflicht, 2025, abrufbar unter: *https://www.risknet.de/themen/risknews/risikoaggregation-wird-zur-pflicht/* und *Scherer*, Nachhaltige Führung und Überwachung von Organisationen (Governance) nach DIN ISO 37000 – erfolgreich umsetzen, auditieren und reporten, DIN Media, 2025, Kap. 6.9.

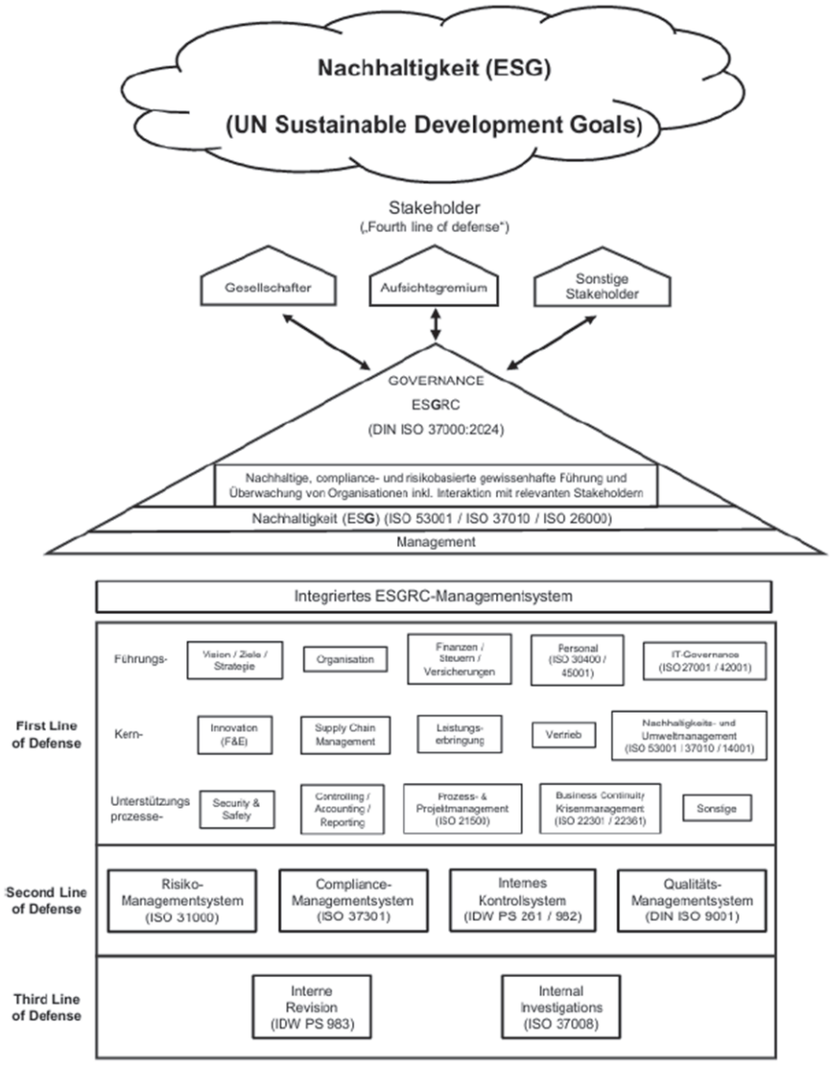

Abb. 1: Das „ESGRC-Haus", eigene Darstellung aus Scherer, Nachhaltige Führung und Überwachung von Organisationen (Governance) nach DIN ISO 37000 – Erfolgreich umsetzen, auditieren und reporten, DIN Media, 2025

Governance umfasst dabei alle relevanten Bereiche/Funktionen/Prozesse einer Organisation.

2. Interdisziplinarität und Beispiel IT-Governance

Jeder einzelne Bereich besteht wiederum aus diversen *interdisziplinären* Komponenten, weshalb bei Governance nicht nur Fachspezialisten, sondern häufiger Generalisten benötigt würden:

Beispiel IT- (KI-) Governance:

IT-(KI-)Governance stellt denjenigen Teil der Aufbau- und Ablauforganisation bzw. des Integrierten IT- (KI-) Governance-Managementsystems dar, der sich u.a. bezieht auf:

IT-Compliance-Management (dies an erster Stelle!), IT-Riskmanagement, IT-Strategie, IT-Planung, IT-Umsetzung, IT-Prozesse, IT-IKS, IT-Revision, IT-Steuerung und -Überwachung, IT-Reporting, IT-Management (das Management [P/D/C/A] der IT, z.B. alles, was mit Hard- und Software zu tun hat), IT-Sicherheitsmanagement, Informationssicherheitsmanagement, Datenschutz, Digitalisierung inklusive Nutzung von KI, IT-Social Engineering etc.

Ob z.B. die Bereichsleitung IT für die Verantwortung von IT-Governance geeignet ist, hängt davon ab, ob sie genügend Affinität und generalistische Kompetenz auch für die vielen nicht-IT-technischen Disziplinen, die IT-Governance umfasst, aufweist. Alternativ käme hier auch eine Komitee-Lösung in Betracht.

3. Pflicht zur Nutzung von KI bei unternehmerischen Entscheidungen

Die ISO 37000 (Governance of Organizations) behandelt in Normabschnitt 6.8 „Daten und Entscheidungen":

Der Einsatz von KI – unter Beachtung rechtlicher (z.B. KI-Compliance mit AI-Act, NIS 2, DORA und Export-Kontrolle)[40] und ethischer Anforderungen sowie Risiken – ist mittlerweile im Rahmen der Risiko-Früherkennung, bei Bewertung der Governance und bei unternehmerischen Entscheidungen (Business Judgment Rule) u.v.m. nicht nur Chance, sondern Pflicht:

(…) „Um Informationspflichten zu genügen, müssen grundsätzlich in der konkreten Entscheidungssituation alle verfügbaren Informationsquellen tatsächlicher und rechtlicher Art ausgeschöpft werden, um auf dieser Grundlage die Vor- und Nachteile der bestehenden Handlungsoptionen sorgfältig abzuschätzen und den erkennbaren Risiken Rechnung zu tragen[41] *(…)“*

Dazu gehört mittlerweile auch KI.[42]

4. OT-Risiken und neue Herausforderungen durch IoT

Anzumerken ist an dieser Stelle, dass eine Risikoanalyse, die ausschließlich die klassische Informationstechnologie (IT) berücksichtigt, nicht mehr ausreicht. Zunehmend muss auch die Operational Technology (OT) einbezogen werden – also jene Systeme, die physische Prozesse steuern, regeln und überwachen, etwa in Industrieanlagen, Energieversorgung oder Verkehrsinfrastruktur. Während IT-Systeme typischerweise auf die Verarbeitung und den Schutz von Daten ausgerichtet sind, betrifft OT unmittelbar die physische Sicherheit, Stabilität und Verfügbarkeit betrieblicher Abläufe.

Diese Trennung verliert jedoch an Bedeutung: Mit der zunehmenden Vernetzung von OT-Systemen über das Internet of Things (IoT) steigt auch die Angriffsfläche. Moderne Sensoren, Steuergeräte und vernetzte Produktionssysteme sind zunehmend direkt oder indirekt mit dem Internet verbunden – häufig ohne den ursprünglich vorgesehenen Schutz gegen externe Bedrohungen. Dadurch entstehen neue, komplexe Risikolagen an der Schnittstelle von IT und OT.

Zur strukturierten Bewertung und Absicherung dieser Systeme hat sich die Normenreihe IEC 62443 als international anerkannter Standard etabliert. Sie bietet einen systematischen Ansatz zur Risikoanalyse, Segmentierung, Zugriffskontrolle und Sicherheitszertifizierung von industriellen Automatisierungs- und Steuerungssystemen. Die Norm richtet sich sowohl an Betreiber als auch an Hersteller und Systemintegratoren und fordert u.a. die Implementierung eines ganzheitlichen Security-Lifecycle-Managements sowie die Einbeziehung von Zonen- und Conduits-Modellen zur Risikobewertung.

VI. Regulierung: Neue Spielregeln – heilsamer Druck statt Bürokratie?

1. Gesetzliche Grundlagen für präventive Unternehmensführung

Die §§ 91 Abs. 2 und Abs. 3, 107 AktG, § 1 StaRUG mit der haftungsbewehrten Pflicht zur Risikofrüherkennung mit Quantifizierung, Aggregation, Steuerung, Abgleich mit Risikotragfähigkeit und Business Continuity- und Krisenmanagement (vgl. IDW ES 16,[43] IDW PS 340 und DIIR Revisionsstandard Nr. 2) beziehen sich ebenso auf Governance-Risiken wie die Rechtsprechung. Diese fordert, ein Geschäftsführer oder Vorstand habe stets die Pflicht zur Kenntnis der finanziellen und wirtschaftlichen Verhältnisse (kontinuierliche Risikofrüherkennung in Echtzeit) und Einleitung angemessener Maßnahmen bei krisenhaften Anzeichen.[44]

Die Pflicht zur Einrichtung eines StaRUG-konformen Frühwarnsystems konkretisiert das Leitbild präventiver Unternehmensführung. § 1 StaRUG verpflichtet zur Einrichtung eines kontinuierlichen, in Echtzeit wirksamen Frühwarnsystems. Maßstab ist nicht die formale Existenz eines Systems, sondern dessen Eignung zur rechtzeitigen Erkennung und Steuerung bestandsgefährdender Entwicklungen. Die zeitliche Dimension der Risikofrüherkennung wird in der Praxis oft unterschätzt. Die Bestimmung des Prognosezeitraums für die Insolvenzwahrscheinlichkeit (p1) i.S.d. § 1 StaRUG orientiert sich an der insolvenzrechtlichen *Fortbestehensprognose*, nicht an der handelsrechtlichen *Fortführungsprognose*. InsO und StaRUG adressieren beide das *Fortbestehen des Rechtsträgers*, während es beim „going concern“ (Fortführungsprognose) des HGB um die *Fortführung des Geschäftsmodells* geht.

Der InsO-Gesetzgeber hat uns (leider) gleich zwei Prognosezeiträume mit auf den Weg gegeben:

- Bei der Überschuldungsprüfung nach § 19 Abs. 2 Satz 1 InsO muss die Zahlungsfähigkeit für 12 Monate prognostiziert werden. Zahlungsfähigkeit deshalb, da eine eingetretene Zahlungsunfähigkeit nach aktuellem Gesetzesstand die Überschuldung determiniert. D.h., wird zum Zeitpunkt der Überschuldungsprüfung die Zahlungsunfähigkeit innerhalb der nächsten 12 Monate prognostiziert, ist die Gesellschaft i.d.R. überschuldet.
- Bei Prüfung der drohenden Zahlungsunfähigkeit ist zu beachten, dass § 18 Abs. 2 Satz 1 durch das SanInsFoG dahin gefasst worden ist, dass i.d.R. auf einen Prognosezeitraum von 24 Monaten abzustellen ist. In insolvenzrechtlicher Hinsicht kann die Gesellschaft wegen drohender Zahlungsunfähigkeit Insolvenzantrag stellen, wenn

40 Vgl. *Scherer*, KI-Verantwortung und enthaftende Wirkung eines KI-Compliance-Managementsystems für Leitung (Vorstand, Geschäftsführer, Officers), Aufsichtsgremium und sonstige Führungskräfte, 2023, abrufbar unter: *https://www.risknet.de/themen/risknews/ki-verantwortung-und-enthaftende-wirkung-eines-ki-compliance-managementsystems/*.

41 Vgl. BGH, Urt. v. 12.10.2016 – 5 StR 134/15, Rn. 34, ZInsO 2017, 25, 30 – HSH Nordbank.

42 Vgl. *Scherer*, Die haftungsbewehrte Pflicht zur Verwendung von KI bei unternehmerischen Entscheidungen – auch im Rahmen des Transformations-, Risiko- und Krisenmanagements, 2024, abrufbar unter: *https://www.risknet.de/themen/risknews/ki-verantwortung-und-enthaftende-wirkung-eines-ki-compliance-managementsystems/*.

43 Vgl. *Romeike*, IDW ES 16 – Krisenfrüherkennung und Krisenmanagement nach § 1 StaRUG, 2025, RiskNET.de, abrufbar unter: *https://www.risknet.de/themen/risknews/krisenfrueherkennung-und-krisenmanagement-nach-1-starug/*.

44 Vgl. z.B.: BGH, Versäumnisurt. v. 19.6.2012 – II ZR 243/11, ZInsO 2012, 1536 und BGH, Urt. v. 23.7.2024 – II ZR 206/22, ZInsO 2024, 1980.

deren Eintreten für einen Zeitpunkt innerhalb der nächsten 24 Monate prognostiziert wird.

Da die Zahlungsunfähigkeit und damit das Eintreten der materiellen Insolvenz im Hinblick auf § 60 Abs. 1 Nr. 4, 5 GmbHG und § 262 Abs. 1 Nr. 3, 4 AktG das Bestehen des Rechtsträgers determiniert, und die Pflicht zur Einleitung von Gegenmaßnahmen nach § 1 Abs. 1 Satz 2, 1. Alt. StaRUG spätestens mit Eintritt der drohenden Zahlungsunfähigkeit greift und ein Frühwarnsystem demnach spätestens zu diesem Zeitpunkt Alarm schlagen muss, ist in Anlehnung an § 18 Abs. 2 InsO der Prognosezeitraum grds. mit 24 Monaten zu bemessen.

„Grundsätzlich" deshalb, da das Gesetz selbst von „in aller Regel" spricht. Damit kann den Besonderheiten des Unternehmens Rechnung getragen werden: z.B. ob das Unternehmen einen kurzfristigen (z.B. Saisongeschäft) oder langfristigen (z.B. Herstellung und Handel in einem Zementwerk) Warenumschlag hat. Bei einem kurzfristigen/langfristigen Umschlag endet der Prognosezeitraum regelmäßig am Ende des Umschlags.[45] Nach zutreffender Auffassung kann demnach nicht auf einen starren Prognosezeitraum abgestellt werden. Mangels besonderer Anhaltspunkte ist jedoch entsprechend der gesetzlichen Vorgabe grds. ein Prognosezeitraum von 24 Monaten zugrunde zu legen.[46]

Zusammenfassend kann somit festgehalten werden: Ausgehend von §§ 18, 19 InsO ist die Planung auf mindestens 12, längstens auf 24 Monate zu erstrecken.[47] Der Planungshorizont sollte sich innerhalb dieses Zeitrahmens befinden und sich nach der Größe und Komplexität des Unternehmens richten, da sich hieraus im Einzelnen die relevanten Stellgrößen und Einflüsse ergeben, die in der Planung zu berücksichtigen sind.

2. Maßstab der Rechtsprechung: Kontinuierliche Echtzeitüberwachung

Das OLG Nürnberg entschied im Fall eines kleinen Unternehmens und ergänzte noch, der Geschäftsführer habe die Pflicht, für ein angemessenes und wirksames Compliance-, Risiko-Management- und Internes Kontroll-System zu sorgen.[48]

In diesem Fall ging es um den Angestellten bei einer kleinen Tankstelle mit wenigen Mitarbeitern, der offenbar die den Geschäftskunden gesetzten Kreditlimits z.T. ignorierte bzw. umging, wodurch es zu Zahlungsausfällen kam.

Als dies bekannt wurde, war ein Schaden von ca. einer 3 3/4 Mio. € entstanden. Der Geschäftsführer (Pächter der Tankstelle) wurde persönlich wegen Pflichtverletzung zu Schadensersatz an die Gesellschaft in dieser Höhe verurteilt.

Das OLG Nürnberg führte aus, er habe es pflichtwidrig unterlassen, für ein angemessenes und wirksames Compliance- und Internes Kontroll-Managementsystem zu sorgen.

Ein Geschäftsführer habe stets die Pflicht zur Kenntnis der finanziellen und wirtschaftlichen Verhältnisse (kontinuierliche Risikofrüherkennung in Echtzeit) und Einleitung angemessener Maßnahmen bei krisenhaften Anzeichen.

Die Entschuldigung des Geschäftsführers, er habe ja gerade eine Stelle für einen Controller ausgeschrieben, der sich genau darum hätte kümmern sollen, aber in Zeiten von Fachkräftemangel habe er niemanden gefunden, erkannte das Gericht nicht an: Dann müsse er sich als Geschäftsführer halt persönlich darum kümmern.

Wichtig: In diesem Fall ging es nicht um Insolvenz- oder Krisenvermeidung, sondern um die Pflicht zur generellen Schadensvermeidung.[49]

VII. Haftungsrisiken steigen proportional zu wachsender Regulierung

1. Zunehmende persönliche Haftung von Geschäftsleitern und Funktionsträgern

Proportional zu den regulatorischen Anforderungen steigen die Haftungsrisiken für Organe (Aufsichtsräte, Vorstände, Geschäftsführer), exponierte Funktionen, wie Abteilungsleiter, Risiko- oder Compliance-Officer und Unternehmen enorm:

Im Zeitraum von 1986 – 1995 wurden in Deutschland ebenso viele Verurteilungen zur Managerhaftung registriert wie in den gesamten 100 Jahren zuvor. In den folgenden Dekaden, 1996 – 2005 und 2006 – 2015, verdoppelte sich diese Zahl jeweils erneut, wie aus aktuellen Analysen hervorgeht. Für den Zeitraum 2016 – 2025 liegen derzeit keine vollständigen Daten vor. Allerdings deuten Trends wie die Zunahme von ESG-bezogenen Klagen und verschärfte regulatorische Anforderungen darauf hin, dass die Zahl der Managerhaftungsfälle weiterhin steigt.

2. Internationale Trends und steigende Vergleichssummen

Die durchschnittliche Vergleichssumme der 50 größten US-Haftungs-Gerichtsurteile von 2014 – 2018 von 28 auf 54 Mio. $ fast verdoppelt.[50]

„Chefposten werden riskanter – mehr Klagen werden erwartet"

„Spitzenpositionen sind auch mit einem wachsenden Risiko verbunden, Ziel eine Klage zu werden."

[…]

45 Vgl. Schwerdtfeger/*Scheuffele*, 4. Aufl. 2025, § 18 InsO Rn. 14 f.

46 Vgl. AG Köln, Beschl. v. 3.3.2021 – 83 RES 1/21, ZInsO 2021, 868.

47 Vgl. a.A. *Bea/Dressler*, NZI 2021, 67, 70 – diese generell für eine Planung über 24 Monate.

48 Vgl. OLG Nürnberg, Urt. v. 30.3.2022 – 12 U 1520/19, NZG 2022, 1058.

49 Vgl. hierzu ausführlich: *Scherer/Seehaus*, Governance und Compliance nach § 1 StaRUG, 2024, RiskNET.de, abrufbar unter: *https://www.risknet.de/themen/risknews/kontinuierliche-risikoueberwachung-in-echtzeit/*.

50 Vgl. beck-aktuell, Allianz: Haftungsrisiken für Unternehmen steigen, 2020, abrufbar unter: *https://rsw.beck.de/aktuell/daily/meldung/detail/allianz-haftungsrisiken-fuer-unternehmen-steigen*.

„Wir beobachten, dass Aufsichtsbehörden auf der ganzen Welt das Unternehmensverhalten schärfer überprüfen, wodurch Unternehmenslenker anfälliger für Untersuchungen, Strafen und Klagen werden."[51]

3. Entwicklungen bei der D&O-Versicherung

„D&O-Versicherung: Manager werden öfter zur Kasse gebeten

(…) Die Versicherer rechnen damit, dass Schadenersatzforderungen gegen Manager künftig zunehmen werden. Dies ist auf die konjunkturelle Lage und höhere gesetzliche Anforderungen zurückzuführen. Nach der aktuellen D&O-Statistik des GDV stieg die Zahl der Schäden bereits das zweite Jahr in Folge. Dabei steigen die Schäden schneller als die Beitragseinnahmen.

Die in Deutschland tätigen Managerhaftpflicht-Versicherer haben 2023 erneut mehr Schäden regulieren müssen. Die Zahl der Fälle ist auf 2.200 gestiegen, fast sieben Prozent mehr als im Vorjahr. Eine D&O- bzw. Managerhaftpflichtversicherung zahlt Schadenersatzforderungen gegen Manager-/innen, wenn diese gegen ihre Pflichten verstoßen haben. Jeder Schaden kostete die Versicherer im Schnitt fast 100.000 Euro.

Die Entwicklung führen die Versicherer auf die konjunkturelle Lage und höhere gesetzliche Anforderungen zurück. Die Zahl der Insolvenzen ist zuletzt deutlich gestiegen. Das zieht oft hohe Schadenersatzforderungen von Insolvenzverwaltern gegen die Verantwortlichen nach sich.

Dazu kommen stetig wachsende Compliance-Anforderungen. Manager haften persönlich, wenn sie kein funktionierendes Compliance-System eingerichtet haben. (…)"[52]

4. Anforderungen an die persönliche Eignung

BFH statuierte eine „Geschäftsführerhaftung wegen Unfähigkeit":

„[…] wer den Anforderungen an einen gewissenhaften Geschäftsführer nicht entsprechen kann, muss von der Übernahme des Geschäftsführeramtes absehen, bzw. dieses Amt niederlegen. […]"[53]

Hinweis:

Die neue DIN ISO 37301:2021(CMS) enthält rd. 60 BGH-Entscheidungen zur rechtssicheren Organisation.[54]

VIII. Haftungsverschärfung durch jüngste „Kardinalpflicht"-Rechtsprechung: „Blind in Haftung und Versicherungsverlust segeln"

1. Haftungsrisiko: Kardinalpflicht

Neben des nachgewiesen drastisch steigenden Risikos der persönlichen Haftung droht aufgrund des von aktuellster Rechtsprechung des OLG Frankfurt/M.[55] angenommenen Vorwurfs der „*Verletzung von Kardinalpflichten*" und der daraus abgeleiteten Indikation einer „*wissentlicher Pflichtverletzung*" der Verlust des Versicherungsschutzes für Manager.

„Kardinalpflichten" sind nach den aktuellen Urteilen des OLG Frankfurt/M. „elementare berufliche Pflichten, deren Kenntnis nach der Lebenserfahrung bei jedem Berufsangehörigen vorausgesetzt werden kann."

2. Ausprägungen der Kardinalpflichten und Rechtsprechung

a) Kardinalpflichten in Vertragsverhältnissen

Diese Pflichten beziehen sich zum einen auf Vertragsbeziehungen („*Pflichten, deren Erfüllung die ordnungsgemäße Durchführung des Vertrages erst ermöglicht und auf deren Einhaltung der Vertragspartner regelmäßig vertrauen darf*")[56]

b) Kardinalpflichten im Bereich Governance

Zum anderen werden von der aktuellen Rechtsprechung auch *Kardinalpflichten im Rahmen der Governance (gewissenhafte Führung und Überwachung von Organisationen*) statuiert.

Dabei haben sich in der Rechtsprechung bereits diverse Fallgruppen herausgebildet.

Fallgruppen:[57]

„(…) Für eine geschäftsführende Person (Vorstand einer Aktiengesellschaft, Geschäftsführer einer GmbH oder sonstigen Gesellschaft, leitender Angestellter) sollen zu diesen Kardinalpflichten gehören:

- *weder sich noch Dritten aus dem Unternehmensvermögen Vorteile zu gewähren, auf die kein Anspruch besteht,*[58]

---

51 Zitat aus: beck-aktuell, Allianz: Chefposten werden riskanter – mehr Klagen erwartet, 2024, *https://rsw.beck.de/aktuell/daily/meldung/detail/allianz-chefposten-risiko-klagen-versicherung-manager*.

52 Zitat aus: GDV-Gesamtverband der Deutschen Versicherer, D&O-Versicherung: Manager werden öfter zur Kasse gebeten, 2024, abrufbar unter: *https://www.gdv.de/gdv/themen/schaden-unfall/d-and-o-versicherung-manager-kosten-182564*.

53 Zitat aus: BFH, Beschl. v. 15.11.2022 – VIII R 23/19, LS, Rn. 35, BFHE 278, 392.

54 Vgl. *Scherer*, Compliance-Managementsystem nach DIN/ ISO 37301 erfolgreich, implementieren, integrieren, auditieren, zertifizieren, DIN Media Verlag, 2022, 40, Fn. 96 mit Verweis auf *Rack*, CB 2021, 433.

55 Vgl. OLG Frankfurt/M., Beschl. v. 16.1.2025 – 7 W 20/24, NJW-RR 2025, 731: „blind in die Krise segeln".; vgl. auch OLG Frankfurt/M., Urt. v. 5.3.2025 – 7 U 134/23, DStR 2025, 917, mit einem ähnlichen Fall (Rev. eingelegt, BGH – IV ZR 66/25).

56 Zitat aus: BGHZ 164, 11 (BGH, Urt. v. 20.1.2005 – V III ZR 121/04).

57 Zitat aus: Wikipedia, Kardinalpflicht/Kardinalpfichten bei der Geschäftsführung, abrufbar unter: *https://de.wikipedia.org/wiki/Kardinalpflicht*.

58 Vgl. hierzu BGH, Urt. v. 10.1.2023 – 6 StR 133/22, BGHSt 67, 225, (*„Vergütung VW-Betriebsräte"*) und BGH, Urt. v. 10.2.2022 – 3 StR 329/21, ZInsO 2022, 765 (*„Haftung von Vorständen wegen Untreue bei Entscheidungen bei mangelhafter Informationsgrundlage"*). Beide Entscheidungen beschäftigen sich mit der strafrechtlichen Haftung von Vorständen wegen Untreue (§ 266 StGB), wenn diese *unberechtigte oder nicht in der konkreten Höhe berechtigte Zahlungen* veranlassen/leisten. Steuer(straf)rechtlich steht dabei häufig auch *Steuerhinterziehung* im Raum. Bei einer Verurteilung droht dem Vorstand/Geschäftsführer Geld- oder Freiheitsstrafe und als weitere Konsequenz natürlich zivilrechtliche Schadensersatzhaftung, Kündigung etc. und persönlicher/beruflicher Reputationsverlust ➔

- *das Unternehmensvermögen nicht für unternehmensfremde Zwecke zu verwenden,*[59]
- *bei Insolvenzreife rechtzeitig Insolvenzantrag zu stellen,*
- *sich jederzeit über die wirtschaftliche Lage der Gesellschaft zu vergewissern*[60] *und eingehend zu prüfen, ob Insolvenzreife vorliegt: wer erkennt, dass die Gesellschaft zu einem bestimmten Stichtag nicht in der Lage ist, ihre fälligen und eingeforderten Verbindlichkeiten vollständig zu bedienen, hat die Zahlungsfähigkeit anhand einer Liquiditätsbilanz zu überprüfen (OLG Frankfurt, Urteil vom 5.3.2025 – 7 U 134/ 23 (…)".*

c) Erweiterung der Fallgruppen der Kardinalpflichtverletzung auf Governance-Compliance

Die aktuelle Rechtsprechung erweitert diese Fallgruppen nun

- auf die Pflicht zur Risiko- bzw. Krisenfrüherkennung und zum
- Krisenmanagement und
- auf die „*vielfältigen Pflichten in Bezug auf die Unternehmensleitung, die mit Eintragung als Geschäftsführer einer Kapitalgesellschaft verbunden sind*".

Zitat des OLG Frankfurt/M.:[61]

„Grundsätzlich setzt die Annahme einer Kardinalpflichtverletzung voraus, dass die (…) verletzte

Rechtsnorm zu den zentralen, fundamentalen Grundregeln einer bestimmten Regelungsmaterie gehört."

„Die allgemein anerkannte (…) Pflicht zur Krisenfrüherkennung und zum Krisenmanagement bei haftungsbeschränkten Unternehmensträgern bestand schon vor Inkrafttreten des § 1 Abs. 1 StaRUG aus § 43 Abs. 1 GmbHG."

d) Exkurs: Risikofrüherkennung als notwendiger Bestandteil der Krisenfrüherkennung

Soweit § 1 StaRUG und die aktuelle Rechtsprechung von „*Krisenfrüherkennung*" und nicht „*Risikofrüherkennung*" sprechen, ist anzumerken, dass Risikofrüherkennung die unverzichtbare Vorstufe der Krisenfrüherkennung ist.

Die Risikofrüherkennung als zwingendes Element eines Überwachungssystems, um „bestandsgefährdende Entwicklungen frühzeitig zu erkennen", wurde bereits 1998 mit dem KonTraG in § 91 AktG als gesetzliche Pflicht für AG und (analog) für große GmbHs statuiert (vgl. die Gesetzgebungsmaterialien zum KonTraG und zum FiSG).

- Nichtige Vorstandsentlastung wegen nicht angemessenen Risiko-Managementsystems

Die Rechtsprechung zog schnell nach und erweiterte die Pflicht auf nicht bestandsgefährdende Risiken:[62]

Das LG München I[63] entschied bereits 2007, die Entlastung des Vorstands eines Münchener Unternehmens sei nichtig (unwirksam), weil die Dokumentation der Prozessabläufe und der Verantwortlichkeit des Risiko-Managementsystems unterlassen wurde. Da Entlastungsbeschlüsse aufgrund von materiellen Mängeln nur bei schwerwiegenden Gesetzes- oder Satzungsverstößen erfolgreich angefochten werden können, lässt sich folgern, dass das Gericht hier eine entsprechend schwere Verletzung annahm.

Die Entscheidung des LG enthält auch Ausführungen, die sich dahin gehend interpretieren lassen, dass das einzurichtende und zu dokumentierende (!) Risiko-Managementsystem nicht ausschließlich bestandsgefährdende Risiken, sondern auch allgemeine Risiken zu behandeln habe.[64] Das Gericht verlangte laut seiner Urteilsbegründung, dass nicht nur die Geschäftsleitung, sondern alle einschlägigen Stellen wie die betroffenen Bereiche und Hierarchieebenen bis hinunter zum Sachbearbeiter über die existierenden – nicht lediglich bestandsgefährdenden – Risiken im betroffenen Bereich und Aufgabenfeld informiert sein müssen, um diese Gefahren „in den Griff zu bekommen".

---

u.v.m. Hinw.: Sofern der *Aufsichtsrat* solche unberechtigten Zahlungen zu verantworten hätte, träfe die Aufsichtsratsmitglieder der Vorwurf, gegen § 116 AktG verstoßen zu haben, da dieser auf § 93 Abs. 1 Satz 2 AktG verweist. Unberechtigte (Über-)Zahlungen kommen *in der Praxis* häufig vor, um sich anstelle einer gerichtlichen Auseinandersetzung auf Basis eines Aufhebungsvertrages/Vergleiches/etc. „geräuschlos" zu trennen oder sich durch überhöhte Vergütungen/Bonuszahlungen wohlwollendes Verhalten (z.B. von Betriebsräten) zu „erkaufen". Oft wird auch in der Praxis nicht geprüft, ob überhaupt Bedarf für die zu beauftragende Leistung besteht oder die erbrachte Leistung ihren Preis rechtfertigt oder es werden – ohne BJR-Anwendung – verlustbringende Investments getätigt oder aufrechterhalten. Die Fallgruppen „unberechtigte Zahlungen" sind in der Praxis unheimlich zahlreich und stellen damit für Vorstände/Geschäftsführer und Aufsichtsräte erhebliches Haftungspotenzial dar, wenn sie die BJR entweder nicht kennen oder trotz Kenntnis nicht beachten. Der 6. Senat des *BGH* (v. 6.1.2023 – 6 StR 133/22) betont, „*es komme für die Strafbarkeit wegen Untreue nicht darauf an, ob dieser Verstoß gravierend oder evident sei*". Auch das „*Einverständnis der Vermögensinhaber*" (z.B. Gesellschafter der AG oder GmbH) „*stehe der Pflichtverletzung nicht entgegen*" und der u.U. durch die nichtberechtigte Leistung erlangte Vorteil könne mit den unberechtigten Vermögensabflüssen nicht kompensiert werden. Auch ein *Rückforderungs-Erlass* ist strafrechtlich problematisch. Vgl. hierzu ausführlich *Scherer*, Nachhaltige Führung und Überwachung von Organisationen (Governance) nach DIN ISO 37000 – erfolgreich umsetzen, auditieren und reporten, DIN Media, 2025, Kap. 6.8.

59 Vgl. BGH, Urt. v. 10.7.2018 – II ZR 24/17, BB 2018, 2369: Gerade auch bzgl. der in Governance-Standards genannten Gemeinwohlbelange, wie Nachhaltigkeit und Social Responsibility, sind im Spannungsfeld „Integrität und Ethik" Compliance-Vorgaben zu beachten. Bspw. können Geschäftsführer, Vorstand und Aufsichtsrat nicht einfach Stakeholder- oder Gemeinwohlinteressen, wie Nachhaltigkeit (ESG) oder soziale Verantwortung (CSR) in ihre den Transformationsanforderungen anzupassenden strategischen Ziele einbeziehen. Vielmehr müssen sie sich, um nicht sanktioniert zu werden, an zahlreiche rechtliche Vorgaben halten.

60 Vgl. BGH, Versäumnisurt. v. 19.6.2012 – II ZR 243/11, ZInsO 2012, 1536, und BGH, Urt. v. 23.7.2024 – II ZR 206/22, ZInsO 2024, 1980, und OLG Nürnberg, Urt. v. 30.3.2022 – 12 U 1520/19, NZG 2022, 1058.

61 Vgl. OLG Frankfurt/M., Urt. v. 5.3.2025 – 7 U 134/23, DStR 2025, 917, mit einem ähnlichen Fall (Rev. eingelegt, BGH – IV ZR 66/25).

62 Vgl. *Scherer*, Nachhaltige Führung und Überwachung von Organisationen (Governance) nach DIN ISO 37000 – erfolgreich umsetzen, auditieren und reporten, DIN Media, 2025, Kap. 6.9.

63 Vgl. LG München I v. 5.4.2007 – 5 HK O 15964/06, NZG 2008, 319; *Theusinger/Liese*, NZG 2008, 289; LG Berlin v. 3.7.2002 – 2 O 358/01, AG 2002, 682: dieses sah bereits 2002 ein mangelhaftes Risikomanagement als wichtigen Grund für eine außerordentliche Kündigung eines Vorstandes an.

64 Vgl. *Theusinger/Liese*, NZG 2008, 290.

Da zumeist nicht ein einziges Risiko sich als bestandsgefährdend auswirkt, sondern viele sich aggregierende Einzelrisiken, ist auch im Rahmen der Krisenfrüherkennung zunächst auf Risikofrüherkennung mit Quantifizierung und Aggregation und Abgleich mit der Risikotragfähigkeit zu achten (was dazu führt, dass aufgrund der allgemeinen Pflicht zur gewissenhaften Geschäftsführung – § 43 GmbHG, § 93 AktG – auch bei Risiken unterhalb der Schwelle der Bestandsgefährdung angemessen gesteuert werden muss).[65]

- *Unzureichendes Risikomanagement und Aggregation zahlreicher Einzelrisiken als Hauptursache für Insolvenz*

In dem von einer anerkannten Wirtschaftsprüfungsgesellschaft testierten Lagebericht für eine vom Verfasser verwaltete Insolvenz heißt es:

„Darstellung der Lage: […] Ein Hauptgrund ist im fehlenden Risikomanagement zu sehen, was in einer unkontrollierten Häufung zahlreicher und für die Unternehmensgröße in Summe zu vieler Unternehmensrisiken führte.“[66]

Durch ein funktionierendes Risiko-Managementsystem wäre hier großer Schaden vermieden worden: Ca. 73 Mio. € angemeldete Forderungen seitens der Gläubiger der Gruppe, ca. 50 Mio. davon wurden durch den Insolvenzverwalter festgestellt. Über Unternehmensfortführung, übertragende Sanierung, Absonderungen, Verwertung etc. konnten bisher an die Gläubiger ca. 17 Mio. € zurückfließen. Der Rest bleibt wohl unwiederbringlich verloren.

Zitat des OLG Frankfurt/M.:[67]

„Grundsätzlich setzt die Annahme einer Kardinalpflichtverletzung voraus, dass die (…) verletzte Rechtsnorm zu den zentralen, fundamentalen Grundregeln einer bestimmten Regelungsmaterie gehört.“

„Die allgemein anerkannte (…) Pflicht zur Krisenfrüherkennung und zum Krisenmanagement bei haftungsbeschränkten Unternehmensträgern bestand schon vor Inkrafttreten des § 1 Abs. 1 StaRUG aus § 43 Abs. 1 GmbHG.“

Die aktuelle Gerichtsentscheidung sieht hier – wohl zu Recht – § 43 GmbHG (Pflicht des GmbH-Geschäftsführers zur gewissenhaften Geschäftsführung) als Rechtsnorm an, die „*zu den zentralen, fundamentalen Grundregeln einer bestimmten Regelungsmaterie gehört*“.

Damit ist konsequenterweise für Vorstände § 93 AktG (Pflicht des Vorstands einer AG zur gewissenhaften Geschäftsführung) inklusive § 93 Abs. 1 Satz 2 mit der Obliegenheit zur Einhaltung der sog. Business Judgment Rule) eine entsprechende Rechtsnorm, die zu den Kardinalpflichten zählt.

Und für Aufsichtsräte ist § 116 AktG, der auf § 93 AktG verweist, einschlägig.

Somit ist die Governance-Compliance[68] zu Recht als eine elementare berufliche Pflicht eines Geschäftsführers, Vorstandes oder Aufsichtsrats anzusehen.

Sicher wird bei jeder einzelnen Pflichtverletzung i.S.d. § 43 GmbHG bzw. §§ 93, 116 AktG zu prüfen sein, ob die jeweils fundamentalen Grundregeln der Regelungsmaterie verletzt wurden. Dies wird wieder eng mit der jeweiligen Risikolage bzgl. dieser Regelungsmaterie in Bezug auf die konkrete Organisation zusammenhängen.

So ist Risiko- und Krisenfrüherkennung und -management sicher für alle Organisationen fundamental, weil damit die Existenz der Organisation geschützt werden soll. Aktuell ähnlich wichtig für alle Organisationen dürften die Themen IT-Governance inklusive Informationssicherheit sein. Auch Nachhaltigkeitsrisiken dürften immer mehr zu diesen Risikobereichen gehören.

Generell würde eine angemessene (Compliance-)Risikoanalyse[69] in der individuellen Organisation Aufschluss darüber geben, welche (Rechts-)Bereiche mit den zugehörigen Pflichten zu den Kardinalpflichten zu zählen sind. Der risikobasierte Ansatz sieht Anforderungen mit dem Ziel der Vermeidung von Gefahr von Leib und Leben, erheblichen zivil- oder strafrechtlichen Sanktionen oder erheblicher finanzieller Einbußen, die die Risikotragfähigkeit beeinträchtigen, als besonders wichtig an.

3. Legalitätspflicht als Kardinalpflicht

Das Legalitätsprinzip,[70] bzw. die Pflicht zur Compliance, also die Pflicht aller, sich an verbindliche Regeln, wie Gesetze oder Rechtsprechung zu halten, hat sich in den letzten Jahren auch in der Rechtsprechung manifestiert:

Beginnend mit dem „berühmten“ „Neubürger“-Urteil des LG München v. 10.12.2013[71] im Siemens-Compliance-Skandal,

65 Vgl. *Scherer/Seehaus*, Governance und Compliance nach § 1 StaRUG, 2024, RiskNET.de, abrufbar unter: *https://www.risknet.de/themen/risknews/kontinuierliche-risikoueberwachung-in-echtzeit/*.

66 Vgl. den veröffentlichten Lagebericht der N.N. Raumexklusiv GmbH für das Geschäftsjahr v. 1.1. bis zum 31.12.2012.

67 Vgl. OLG Frankfurt/M., Urt. v. 5.3.2025 – 7 U 134/23, DStR 2025, 917, mit einem ähnlichen Fall (Rev. eingelegt, BGH – IV ZR 66/25).

68 Vgl. zu den Inhalten von Governance-Compliance: *Scherer*, Nachhaltige Führung und Überwachung von Organisationen (Governance) nach DIN ISO 37000 – erfolgreich umsetzen, auditieren und reporten, DIN Media, 2025.

69 Vgl. DIN ISO 37301 Normabschnitt 4.6 Compliance-Riskoanalyse und ISO IEC 31010 Risk Assessment.

70 Vgl. BGH, Urt. v. 27.8.2010 – 2 StR 111/09, ZCG 2010, 285 (RWE-Tochter: Müllentsorgung und schwarze Kassen“), kommentiert in *Scherer*, Das interessiert Kapitalgeber: Antifragilität und der „Achilleskörper“ des Ordentlichen Kaufmanns, 2019, abrufbar unter: *https://www.scherer-grc.net/publikationen/das-interessiert-kapitalgeber-antifragilitaet-und-der-achilleskoerper-des-ordentlichen-kaufmanns*.

71 Das sog. „Siemens/Neubürger-Urt.“ des LG München I, Urt. v. 10.12.2013 – 5 HK O 1387/10, NZG 2014, 345, gilt als richtungsweisendes Urteil zur organisationsbezogenen Haftung von Vorständen in AG. Im Zentrum stand die Frage, ob der ehemalige Siemens-Vorstand *Dr. Uriel J. Neubürger* gegen seine Sorgfaltspflichten gem. § 93 Abs. 1 AktG verstoßen habe, indem er defizitäre Compliance-Strukturen im Konzern nicht angemessen verbessert habe. Das Gericht bejahte die persönliche Haftung und stellte klar, dass Vorstandsmitglieder auch dann haften, wenn sie Organisationspflichten verletzen, insbesondere bei unzureichender Kontrolle von Korruptionsrisiken und internen Kontrollsystemen. Dabei wurde betont, dass die Pflicht zur Etablierung eines funktionierenden Compliance- ➔

führten das LAG Düsseldorf,[72] das ArbG Frankfurt,[73] der BGH[74] und aktuell das OLG Nürnberg[75] aus, das es Obliegenheit des Geschäftsführers oder Vorstands sei, ein angemessenes und wirksames Compliance-Managementsystem einzurichten.[76]

Flankierend dazu entschied der BGH im „Buchhändler-Urteil",[77] ein beruflich Tätiger habe das erforderliche Wissen bzgl. der für seine Tätigkeit relevanten Compliance-Anforderungen zu haben oder es sich über Experten zu besorgen. Darüber hinaus müsse er diese Anforderungen auch erfüllen. Die Befolgung der Empfehlung des Experten kann gemäß BGH in den „ISION-Entscheidungen" enthaftend wirken.[78]

Aus der jahrelang kontinuierlichen Wiederholung der Rechtsprechung lässt sich schlussfolgern, dass Compliance- und Legalitätspflicht eine selbstverständliche Kardinalpflicht der Organe ist:

Wer wissentlich (dolus eventualis, also das „Für-möglich-halten und sich-damit-abfinden" reicht) gesetzliche Vorgaben missachtet, verstößt also gegen grundlegende Berufspflichten.

Dass vorsätzliche Gesetzesverstöße in nahezu allen Rechtsgebieten (Strafrecht, Versicherungsrecht, Vertragsrecht etc.) streng sanktioniert werden, dürfte nicht überraschen.

Gegenmeinungen, die mittelbar argumentieren, Vorstand oder Geschäftsführer sei kein Beruf, der eine bestimmte Qualifikation voraussetzt wurde, wird durch den Hinweis des BGH,[79] ein Geschäftsführer, der sich haftungsbefreiend von der Gesellschaft trennen möchte, müsse sein Amt niederlegen, der Boden entzogen.

Ebenso sieht es der BFH, der ausführte:

„[…] wer den Anforderungen an einen gewissenhaften Geschäftsführer nicht entsprechen kann, muss von der Übernahme des Geschäftsführeramtes absehen, bzw. dieses Amt niederlegen. […]"[80]

Es ist sicher nicht einfach, stets alle Compliance-Anforderungen zu erfüllen. Es wird aber bzgl. der Kardinalpflichten nicht die umfassende Compliance gefordert, sondern nur, dass nicht vorsätzlich Compliance-Pflichten verletzt werden.

Flankierend dazu entwickelte die Rechtsprechung[81] das *Korrektiv der enthaftenden Wirkung eines Compliance-Managementsystems*: Bei Pflichtverstößen unterhalb der Leitungsebene kann bei Existenz eines Compliance-Managementsystems der Vorwurf des Organisationsverschuldens im Sinne einer Aufsichtspflichtverletzung entfallen.

Diese Entwicklung der Rechtsprechung und zumindest das *Risiko* der Annahme einer Kardinalpflichtverletzung bei vorsätzlichen Complianceverstößen (bereits bei dolus eventualis) kann enorme Auswirkungen auf Organe und Führungskräfte haben und sollte im Risiko- und Compliancemanagement angemessen reflektiert werden.

IX. Korrektiv der enthaftenden Wirkung eines angemessenen Compliance-Managementsystems, Aufsichtspflichtverletzung und Mitarbeiter-Exzess

1. Verantwortung trotz Delegation – Geschäftsherrenhaftung und strukturelle Anforderungen an Governance

Wenn Organe ihre Governance-Aufgaben auf Führungskräfte delegieren, verbleiben nach gefestigter Rechtsprechung zumindest Überwachungspflichten und Letztverantwortung beim Organ.

Dies gilt auch im Lichte der sog. Geschäftsherrenhaftung, die – obwohl das deutsche Gesellschaftsrecht keine generelle Erfolgshaftung kennt – eine straf-, ordnungswidrigkeiten- und zivilrechtliche Verantwortlichkeit für betriebsbezogene Pflichtverletzungen von Mitarbeitern begründet. Die Grundlage bildet eine Garantenstellung i.S.d. § 13 StGB, konkretisiert durch § 43 GmbHG, § 93 AktG sowie § 130 OWiG.[82]

Die Aufgaben der Risiko- und Krisenfrüherkennung, Compliance, Informationssicherheit und Business Continuity, aber auch relevante Transformationsbereiche, wie Digitalisierung und Organisationsentwicklung werden häufig auf die entsprechenden Stabsstellen bzw. Lines of Defense-Funktionen delegiert.

Diese arbeitsteilige Struktur ist betriebswirtschaftlich sinnvoll – sie ändert jedoch nichts an der originären Verantwortung der Geschäftsleitung (Geschäftsherrenverantwortung).

---

oder Risikomanagementsystems nicht delegierbar sei und zu den zentralen Leitungsaufgaben eines Vorstands gehört. Ein bloßes Vertrauen auf nachgeordnete Stellen entlaste nicht von der Verantwortung.

72 Vgl. LAG Düsseldorf, Urt. v. 27.11.2015 – 14 Sa 800/15, Rn. 242 (Schienenkartell-Urteil).

73 Vgl. ArbG Frankfurt, Urt. v. 11.9.2013 – 9 Ca 1541/13 (Libor-Manipulation).

74 Vgl. BGH, Urt. v. 15.1.2013 – II ZR 90/11, NJW 2013, 1958 Rn. 22 (unternehmenszweckwidrige Derivatgeschäfte) und BGH, Urt. v. 9.5.2017 – 1 StR 265/16, NJW 2017, 3798 (Panzerhaubitzenfall).

75 Vgl. OLG Nürnberg, Urt. v. 30.3.2022 – 12 U 1520/19, NZG 2022, 1058.

76 Vgl. *Scherer*, Compliance-Managementsystem nach DIN/ISO 37301 erfolgreich, implementieren, integrieren, auditieren, zertifizieren, DIN Media Verlag, 2022, 39.

77 Vgl. BGH, Urt. v. 18.11.2020 – 2 StR 246 /20, wistra 2021, 355.

78 Vgl. *Scherer*, Compliance-Managementsystem nach DIN/ISO 37301 erfolgreich, implementieren, integrieren, auditieren, zertifizieren, DIN Media, 2022, 233: „Wer soll das alles wissen?".

79 Beschl. v. 21.5.2019 – II ZR 337/17.

80 Vgl. BFH, Beschl. v. 15.11.2022 – VIII R 23/19, LS Rn. 35, BFHE 278, 392.

81 BGH 2017: (KMW), Urt. v. 9.5.2017; BGH 2022: (Selbstreinigung), Urt. v. 27.4.2022; BGH 2023 (Geschäftsverteilung), Urt. v. 9.11.2023; EuGH 2023: (Deutsche Wohnen), Urt. v. 5.12.2023; EuGH 2023: (Hackerangriff), Urt. v. 14.12.2023; EuGH 2024: (USt-Betrug), Urt. v. 30.1.2024; EuGH 2024: Urt. v. 11.4.2024 – C-741/21, NJW 2024, 1561; OLG Stuttgart 2025: (Mitarbeiterexzess), Beschl. v. 25.2.2025 – 2 ORbs 16 Ss 336/24, NJW 2025, 1279.

82 Vgl. BGH, Urt. v. 17.7.2009 – 5 StR 394/08 (2), NJW 2009, 3173; BGH, Urt. v. 20.10.2011 – 4 StR 71/11, BGHSt 57, 43.

Nach § 43 GmbHG und § 93 Abs. 1 AktG ist die Geschäftsleitung verpflichtet, dafür zu sorgen, dass delegierte Funktionen:

- methodisch geeignet,
- personell und organisatorisch ausgestattet,
- systemisch eingebunden und
- laufend überwacht sind.

Diese Anforderungen spiegeln sich auch in den internationalen Standards wider: ISO 37301 (Nr. 5.3) fordert eine kontinuierliche Überprüfung der Integrität, Angemessenheit und Wirksamkeit des Compliance-Managementsystems,[83] ISO 37000 (Nr. 5.1) betont die Verantwortung der Leitung für Governance-Strukturen.[84]

Fehlt eines dieser Elemente, entfällt die Möglichkeit zur Exkulpation – insbesondere, wenn Hinweise auf Überlastung, Unterbesetzung oder strukturelle Mängel vorlagen.

Sofern die Delegationsempfänger, also die jeweils qua delegatione verantwortlichen Führungskräfte ihre Aufgaben nicht oder nicht ordnungsgemäß erfüllen und dadurch die Organisation oder Dritte zu Schaden kommen, stellt sich die Frage nach der (Haftungs-)Verantwortung der Organe und Delegationsempfänger.

Bei pflichtwidrigem Handeln oder Unterlassen der Delegationsempfänger im Rahmen ihrer betrieblichen Tätigkeit kann ein Aufsichtsverschulden der Organe vorliegen, jedoch ein angemessenes Compliance-Managementsystem enthaftend wirken.[85]

2. Mitarbeiterexzess – Definition, Zurechnung und Grenzen der Haftungsverlagerung

Sofern die Delegationsempfänger aufgrund der Verfolgung eigener, unternehmensfremder Ziele nicht pflichtgemäß agieren, stellt sich die Frage, ob die Organe auch für einen sog. „Mitarbeiterexzess" verantwortlich sind.

> ***Beispiel im Kontext der Erfüllung der Überwachungspflichten***
>
> *Bspw. wäre diese „Entlastungs-Argumentation Mitarbeiter-Exzess" denkbar, wenn trotz ordnungsgemäßer Delegation an eine grds. ordnungsgemäß ausgewählte, kompetente, instruierte, mit angemessenen Ressourcen versehene und auch überwachte Lines of Defense-Funktion ihre Meta-Überwachungs-Aufgaben nicht angemessen erfüllt, um Dritte, bspw. primär verantwortliche Kollegen nicht zu kompromittieren.*
>
> *Oder mit anderen Worten: Liegt Mitarbeiter-Exzess vor, wenn trotz Kenntnis der relevanten und riskanten Schwachstellen in der Organisation die Lines of Defense-Funktion ohne Kenntnis oder gar Weisung durch die Organe bewusst andere Themen prüft und reported?*

Mitarbeiterexzess stellt ein Verhalten dar, bei dem sich ein Beschäftigter außerhalb seines arbeitsvertraglichen Pflichtenkreises bewegt und objektiv nicht mehr für den Arbeitgeber tätig ist. Es fehlt jeder funktionale Bezug zur betrieblichen Aufgabe. Typisch sind Handlungen, die ausschließlich privat oder betriebsfremd motiviert sind, etwa zur persönlichen Bereicherung oder zum Vorteil Dritter.

Der BGH stellt klar, dass solche Exzesse grds. nicht der Organisation zugerechnet werden können, da sie außerhalb des betrieblichen Einflussbereichs liegen. Aus der Stellung als Betriebsinhaber bzw. Vorgesetzter kann sich zwar eine Garantenpflicht zur Verhinderung von Straftaten nachgeordneter Mitarbeiter ergeben; diese beschränkt sich jedoch – so der amtliche Leitsatz – auf betriebsbezogene Straftaten und umfasst nicht solche Taten, die Mitarbeiter lediglich bei Gelegenheit ihrer Tätigkeit im Betrieb begehe.[86]

Dogmatisch liegt in Fällen des Mitarbeiterexzesses ein Verhalten außerhalb des Weisungsrechts und der arbeitsvertraglichen Bindung vor. Das Unternehmen und dessen Geschäftsleiter haftet dann grds. nicht als „Verantwortlicher" i.S.v. Art. 4 Nr. 7 DSGVO, § 831 oder § 278 BGB.

Maßgeblich für die Zurechnung ist, ob die Handlung noch innerhalb des vom Arbeitgeber übertragenen Aufgabenbereichs liegt – was sich regelmäßig aus Stellenbeschreibungen, Arbeitsverträgen, Dienstanweisungen oder konkreten Einzelaufträgen ergibt. Handelt ein Mitarbeiter innerhalb dieses Rahmens – selbst weisungswidrig –, bleibt das Verhalten grds. dem Unternehmen zurechenbar. Erst wenn der Handlungsrahmen objektiv überschritten und der Bezug zum Unternehmenszweck vollständig verloren ist, liegt ein echter Exzess vor. Die Schwelle zum Exzess ist also dort überschritten, wo die formale Aufgabenbindung verlassen und durch subjektiv-egoistische Interessen ersetzt wird.

Ein Blick in die Rechtsprechung zeigt: Der Exzess führt grds. zur Eigenverantwortlichkeit des Mitarbeiters.

> ***Beispielsfall (1) des OLG Stuttgart: Polizist als Datendieb – Keine Zurechnung beim Geschäftsherrn bei vollständiger Zweckumkehr:***[87]
>
> *Ein Polizeibeamter nutzte in der Nacht aus reiner Neugier seinen dienstlichen Zugang zum polizeilichen Informationssystem, um ohne jeglichen dienstlichen Anlass personenbezogene Daten eines inhaftierten Kollegen abzurufen. Handelt der Mitarbeiter bewusst zweckentfrem-*

83 Vgl. *Scherer*, Compliance-Managementsystem nach DIN ISO 37301 erfolgreich, implementieren, integrieren, auditieren, zertifizieren, DIN Media, 2022, Kap. 5.1, 5.2.

84 Vgl. *Scherer*, Nachhaltige Führung und Überwachung von Organisationen (Governance) nach DIN ISO 37000 – erfolgreich umsetzen, auditieren und reporten, DIN Media, 2025, Kap. 5.2.

85 Vgl. *Scherer*, Nachhaltige Führung und Überwachung von Organisationen (Governance) nach DIN ISO 37000 – erfolgreich umsetzen, auditieren und reporten, DIN Media, 2025, Kap. 4.2 „Governance und Delegation".

86 BGH, Urt. v. 20.10.2011 – 4 StR 71/11, BGHSt 57, 42.

87 Vgl. OLG Stuttgart, Beschl. v. 25.2.2025 – 2 ORbs 16 Ss 336/24, NJW 2025, 1279.

dend, also ohne dienstliche Veranlassung, agiert er nicht mehr als weisungsgebundener Erfüllungsgehilfe (§ 278 BGB), sondern eigenverantwortlich (hier i.S.d. Art. 4 Nr. 7 DSGVO). Er wird damit selbst zum „Verantwortlichen" mit allen sich daraus ergebenden haftungs- und bußgeldrechtlichen Konsequenzen Die private Nutzung dienstlicher Zugriffsrechte stellt einen sog. „Mitarbeiterexzess" dar – also ein Verhalten, das vollständig außerhalb der dienstlich legitimierten Aufgabenstellung erfolgt und so nur dem Mitarbeiter und nicht dem Geschäftsherrn zugerechnet werden kann.

Beispielsfall (2) des SG Schwerin: Kriminelle Energie der Praxismitarbeiterin – Mitarbeiterexzess entlastet Vertragsarzt:[88]

In einer ärztlichen Praxis manipulierte eine medizinische Fachangestellte gemeinsam mit einer pharmazeutischen Angestellten das Rezeptwesen. Ohne Wissen des Arztes stellten sie Verordnungen aus, bestellten Arzneimittel zulasten der gesetzlichen Krankenkassen und veräußerten die Ware anschließend in der Bodybuilderszene. Eine Krankenkasse machte daraufhin einen Regressanspruch i.H.v. rd. 68.000 € gegen den Vertragsarzt geltend. Das SG wies die Klage ab: Dem Arzt könne kein eigenes Verschulden nachgewiesen werden. Insbesondere sei nicht belegt worden, dass die verwendeten Verordnungen auf von ihm unterzeichneten Blankorezepten beruhten. Der Missbrauch durch die Mitarbeiterinnen stellte damit einen eigenverantwortlichen Exzess außerhalb des dienstlichen Pflichtenkreises dar – mit der Folge, dass der Arzt nicht für das Verhalten seiner Mitarbeiterinnen einzustehen hatte.

Merksatz für die Praxis:

Verlässt ein Mitarbeiter mit krimineller Energie bewusst den dienstlichen Rahmen und verschleiert sein Handeln gezielt, spricht vieles für einen eigenverantwortlichen Exzess – und gegen eine Zurechnung zur Leitung. Die Enthaftung setzt voraus, dass die Pflichtverletzung für die Führungskraft objektiv nicht erkennbar und organisatorisch nicht beherrschbar war.

Anmerkung zum Mitarbeiterexzess bei krimineller Energie:

Der Apothekenfall des SG Schwerin veranschaulicht, dass bei erheblicher krimineller Energie, gezielter Verschleierung und fehlender Kontrollzugänglichkeit ein schädigendes Mitarbeiterverhalten als eigenverantwortlicher Exzess einzustufen ist. Ob ein pflichtwidriges Verhalten eines Mitarbeitenden der Organisation oder Geschäftsleitung zurechenbar ist, hängt maßgeblich von zwei Kriterien ab: dem funktionalen Zusammenhang mit dem betrieblichen Aufgabenbereich und der objektiven Kontrollierbarkeit durch die Leitungsebene. Wird ein Verhalten zwar formal im Rahmen dienstlicher Zugriffsrechte ausgeführt, dient jedoch ausschließlich sachfremden, eigennützigen Zwecken – etwa zur eigenen Bereicherung oder der Dritter – und ist zudem bewusst auf Täuschung und Verschleierung angelegt, spricht vieles für einen eigenverantwortlichen Mitarbeiterexzess. Bei hoher krimineller Energie und geringer Kontrollmöglichkeit steigt Wahrscheinlichkeit der Enthaftung. Diese steigt insbesondere dann, wenn der Mitarbeiter ein Kontrollumfeld schafft, das eine Entdeckung seines Handelns systematisch erschwert – etwa durch Umgehung interner Abläufe, Manipulation von Dokumenten, Missbrauch besonderer Vertrauensstellungen oder gezielte Informationsverknappung gegenüber Kontrollinstanzen. In solchen Konstellationen löst sich der innere Betriebszusammenhang so weit, dass eine Zurechnung zur Organisation regelmäßig ausscheidet– selbst dann, wenn der Mitarbeiter formal innerhalb bestehender Befugnisse gehandelt hat.

Ein kontroverser Beispielsfall (3): VW-Abgasskandal – Mitarbeiterexzess oder strukturelles Kontrollversagen?

Im Jahr 2018 verhängte die Staatsanwaltschaft Braunschweig gegen die Volkswagen AG eine Geldbuße i.H.v. 1 Mrd. € wegen einer Verletzung der Aufsichtspflicht gem. § 130 OWiG, nachdem die US-Umweltbehörde EPA im September 2015 aufgedeckt hatte, dass VW die Abgaswerte von Dieselfahrzeugen durch eine Software manipulierte (Abschalteinrichtungen). Der Vorwurf: Das Unterlassen hinreichender organisatorischer Vorkehrungen zur Verhinderung rechtswidriges Verhalten. Die Bußgeldverfügung bestand aus einer formellen Geldbuße von 5 Mio. € und einer Abschöpfung wirtschaftlicher Vorteile i.H.v. 995 Mio. €. Da Volkswagen akzeptierte, kam es zu keiner gerichtlichen Überprüfung. – Die Abschalteinrichtungen wurden von VW-Mitarbeitern entwickelt, die im Rahmen ihrer betrieblichen Funktionen handelten. Ob dieses Verhalten als eigenmächtiger Mitarbeiterexzess einzuordnen ist oder ob vielmehr strukturelle Ursachen, unterlassene Aufsicht oder gar Mitverantwortung auf Führungsebene vorlagen, ist bis heute nicht geklärt.[89]

Anmerkung:

Der VW-Abgasskandal stellt einen noch ungeklärten Fall dar, der exemplarisch zeigt, wie anspruchsvoll und schwer im Einzelfall die tatsächliche und rechtliche Klärung von Sachverhalten in komplexen Organisationen sein kann. Der Fall wurde in zahlreichen Verfahren, Untersuchungsausschüssen und Veröffentlichungen aufgearbeitet; eine rechtlich gesicherte Einordnung als Exzessverhalten einzelner Mitarbeiter, bei dem die Schwelle zur Eigenverantwortlichkeit überschritten wurde, oder als ein Mitarbeiterverhalten, welches (noch) der Organisation zuzurechnen ist, liegt aufgrund der Komplexität des Falles und der Vielzahl ungeklärter Aspekte auch nach

88 Vgl. SG Schwerin, Urt. v. 14.6.2023 – S 6 KA 15/20.

89 Vgl. LG München II, Urt. v. 27.6.2023 – W5 KLs 64 Js 22724/19 (s. hierzu Pressemitteilung 38/20, abrufbar unter: *https://www.justiz.bayern.de/gerichte-und-behoerden/oberlandesgerichte/muenchen/presse/2023/38.php*); vgl. tagesschau, Frühere VW-Manager in Dieselaffäre zu Haft verurteilt, 2025, abrufbar unter: *https://www.tagesschau.de/wirtschaft/volkswagen-dieselaffaere-urteil-100.htm*; WirtschaftsWoche, Frühere VW-Manager wegen Dieselskandal zu Haft verurteilt, 2025, abrufbar unter: *https://www.wiwo.de/unternehmen/auto/betrugsprozess-fruehere-vw-manager-wegen-dieselskandal-zu-haft-verurteilt/100130305.html*.

10 Jahren „Dieselgate“ nicht vor. Der Fall regt somit zu weiteren Diskussionen an.

3. Haftungsfolgen bei Kontrollversagen und Anforderungen an wirksames CMS

a) Delegation und Organisationspflicht

Im Unternehmensrecht ist haftungsrechtlich entscheidend, ob die Geschäftsleitung ihrer Steuerungs-, Kontroll- und Interventionsverantwortung hinreichend nachkommt. So hat das OLG Frankfurt/M. klargestellt, dass ein Geschäftsführer persönlich haftet, wenn er Vollmachten erteilt, ohne für eine wirksame Kontrolle zu sorgen.[90] In solchen Fällen kann selbst ein ursprünglich eigenmächtiger Mitarbeiterexzess in ein strukturell bedingtes Organisationsversagen umschlagen – mit voller Zurechnung zur Leitungsebene.

Angesichts der Unternehmensgröße und arbeitsteiligen Prozesse sind Geschäftsleiter regelmäßig nicht in der Lage, sämtliche Pflichten – insbesondere Auswahl-, Aufsichts- und Verkehrssicherungspflichten – persönlich wahrzunehmen. Daher besteht eine rechtlich zwingende Pflicht zur Delegation, insbesondere auf Fachabteilungen wie Personal, Compliance oder Revision.[91] Diese Delegation ist jedoch nur dann entlastend, wenn sie ordnungsgemäß strukturiert, risikoadäquat ausgestaltet und wirksam kontrolliert wird. Über die Zeit hat die Rechtsprechung unter dem Stichwort des „dezentralisierten Entlastungsbeweises“[92] ein gestuftes System von Organisationspflichten entwickelt. Dieses umfasst insbesondere die Pflicht zur systematischen Ermittlung aller betrieblichen Rechtspflichten, deren risikoadäquate Delegation an fachlich geeignete Mitarbeitende, die klare Instruktion über Aufgaben und Risiken, die Einrichtung wirksamer Kontroll- und Überwachungsmechanismen sowie ein aktives Eingreifen bei erkannten Pflichtverstößen. Hinzu tritt die fortlaufende Überprüfung und Anpassung der Organisationsstruktur an veränderte rechtliche und betriebliche Rahmenbedingungen.

Dass eine bloße Delegation ohne wirksame Kontroll- und Überwachungsstruktur keine haftungsbefreiende Wirkung entfaltet, zeigt exemplarisch der folgende

> ***Beispielsfall (4) – OLG Nürnberg:***[93]
>
> *Ein langjähriger Mitarbeiter konnte Tankkartenabrechnungen in erheblichem Umfang manipulieren, weil weder ein funktionierendes Vier-Augen-Prinzip noch stichprobenartige Kontrollen existierten. Obwohl die Aufgaben formal an das Controlling delegiert waren, versagte die Überwachung faktisch vollständig.*

Anmerkung:

Das OLG Nürnberg sah hierin ein Organisations- und Aufsichtsversagen der Geschäftsleitung. Es stellte klar: Es besteht eine Rechtspflicht zur Einrichtung eines wirksamen Compliance-Systems. Delegation entbindet nicht von der Pflicht zur Kontrolle und sofortigen Intervention. Ein bloß formales CMS genügt nicht – erforderlich ist strukturierte, risikoadäquate Aufsicht. Das Urteil betont, dass ohne systemische Einbindung und laufende Überwachung selbst gut gemeinte Delegationen haftungsbegründend wirken können.

b) Pflichten zur Prävention und Kontrolle

Delegation ist zulässig – aber nicht enthaftend. Wer delegiert, muss kontrollieren, dokumentieren und korrigieren, wenn Abweichungen auftreten. Gerade im Kontext von Mitarbeiterexzessen ist zu prüfen, ob die Organisation Exzesse hätte verhindern können, etwa durch:

- definierte Verhaltensrichtlinien (Code of Conduct),
- Schulungen zur Pflichtengrenze,
- wirksame Meldesysteme und Hinweisgeberschutz,
- und eine dokumentierte Überwachung der Exzesseingriffsgrenze.

c) Exzess und Kontrollversagen: Grenzen der Enthaftung bei Systemmängeln

Die Enthaftung bei Mitarbeiterexzess ist nicht grenzenlos. Sie setzt voraus, dass die Unternehmensleitung ihren Organisations-, Auswahl- und Überwachungspflichten wirksam nachgekommen ist. Fehlen funktionierende Kontroll- oder Compliance-Strukturen oder bleiben sie bloß formaler Natur, kann das exzessive Verhalten dennoch zugerechnet werden – weil dann ein strukturelles Organisationsversagen vorliegt.

Allerdings gilt im Umkehrschluss: Das geltende Haftungsrecht verlangt keine lückenlose Allmacht der Kontrolle. Es besteht keine Pflicht zur Unmöglichkeit (impossibilium nulla obligatio est). Eine Aufsichtspflicht kann nur dort verletzt sein, wo eine solche im konkreten Fall auch realisierbar gewesen wäre (vgl. § 130 OWiG), denn der Aufsichtspflichtige muss die Zuwiderhandlung schuldhaft (vorwerfbar) begangen haben.[94] Diese von der Rechtsprechung bestätigte Grundregel trägt dem praktischen Umstand Rechnung, dass ein Unternehmen nicht alle denkbaren Pflichtverstöße einzelner Mitarbeitender verhindern kann – insbesondere dann nicht, wenn diese mit hoher krimineller Energie und gezielter Täuschung agieren.

Die Grenze der Enthaftung ist daher dort erreicht, wo ein Unternehmen kein gelebtes und wirksames Kontrollsystem nachweisen kann. In solchen Fällen tritt der individuelle Exzess hinter einem zurechenbaren Systemmangel zurück. Entscheidend ist die dogmatische Trennlinie zwischen subjektiver Eigenmächtigkeit des Täters und objektiver Organisationsverantwortung. Gleichzeitig schützt ein strukturell funktionieren-

90 Vgl. OLG Frankfurt/M., Urt. v. 23.5.2019 – 5 U 21/18, ZIP 2018, 1132; ebenso OLG Nürnberg, Urt. v. 30.3.2022 – 12 U 1520/19 (Tankkartenfall), DB 2022, 2153.

91 Vgl. *Rack*, CB 2013, 231.

92 S. MünchKomm-BGB/*Wagner*, 9. Aufl. 2024, § 831 Rn. 56 ff.

93 Vgl. OLG Nürnberg, Urt. v. 30.3.2022 – 12 U 1520/19, NZG 2022, 1058.

94 Vgl. OLG Jena, Beschl. v. 2.11.2005 – 1 Ss 242/05, NStZ 2006, 533.

des System nicht in jedem Fall – etwa dann nicht, wenn Frühindikatoren ignoriert, Whistleblower übergangen oder Kontrollmechanismen lückenhaft implementiert wurden. Dann schlägt der Exzess in ein Organisationsverschulden um.

Beispielfall (4) des EuGH: Gefälschte Rechnungen durch Mitarbeitenden – Exzess entlastet bei gelebtem Kontrollsystem[95]

Eine Tankstellenmitarbeiterin in Polen stellte über einen längeren Zeitraum hinweg mehr als 1.600 gefälschte Rechnungen im Volumen von insgesamt rd. 320.000 € im Namen ihres Arbeitgebers aus – ohne dessen Wissen und ohne tatsächliche Warenbewegung. Die fingierten Rechnungen wurden nicht im System verbucht. Die Empfänger nutzten diese Rechnungen, um sich unrechtmäßig die USt erstatten zu lassen. Die Steuerbehörde forderte die USt vom Unternehmen, denn dieses habe die Aufsichtspflichten verletzt.

Der EuGH (Urt. v. 30.1.2024 – C-442/22) entschied, dass ein solches Verhalten als eigenverantwortlicher Mitarbeiterexzess zu werten sein kann – jedoch nur dann, wenn der Arbeitgeber nachweisen kann, dass er alle zumutbaren Maßnahmen zur Prävention, Kontrolle und Aufdeckung solcher Verstöße getroffen hat. Die Entscheidung betont: Ein formal vorhandenes Compliance- oder Kontrollsystem genügt nicht. Entscheidend sei, ob das System im konkreten Fall lebendig, wirksam und überprüfbar funktioniert hat. Diese Anforderung bedeutet allerdings nicht, dass ein über Jahre hinweg verdeckt gebliebenes Fehlverhalten das gesamte System automatisch disqualifiziert und die Verantwortung des Geschäftsherrn zuzurechnen ist. Vielmehr kann selbst ein strukturiertes und gelebte Kontrollsystem umgangen werden – etwa durch besondere kriminelle Energie, gezielte Täuschung und Ausnutzung von Vertrauensstrukturen. In einem solchen Ausnahmefall liegt der Schwerpunkt der Pflichtverletzung nicht mehr im organisatorischen Bereich, sondern ausschließlich beim handelnden Mitarbeiter – und entlastet damit das Unternehmen und dessen Geschäftsherrn von der Zurechnung.

Beispielfall (5) – OLG Jena: Keine Pflicht zur Allmacht – Aufsichtspflicht endet am Exzess mit krimineller Energie[96]

In einem Unternehmen wurde ohne Genehmigung Abfallmaterial in der Nähe eines Flusslaufs abgelagert. Ob dies vorsätzlich weisungswidrig durch Mitarbeitende geschah, blieb durch die Behörde und die Vorinstanzen ungeklärt. Eine Anweisung der Geschäftsleitung lag jedenfalls nicht vor. Wegen angeblich unzureichender Aufsichtsmaßnahmen wurde gegen die GmbH und ihren Geschäftsführer ein Bußgeldbescheid nach § 130 OWiG erlassen.

Das OLG Jena (Beschl. v. 2.11.2005 – 1 Ss 242/05, NStZ 2006, 533) hob den Bescheid auf und stellte klar: § 130 OWiG begründet keine Garantiehaftung der Unternehmensleitung. Die bloße Stellung als Geschäftsführer reicht für eine Zurechnung nicht aus. Vielmehr setzt der Vorwurf einer Aufsichtspflichtverletzung voraus, dass konkrete, realisierbare Kontrollmaßnahmen unterlassen wurden – und zwar schuldhaft. Eine Verantwortlichkeit entsteht nur dann, wenn der Aufsichtspflichtige tatsächlich in der Lage gewesen wäre, das Verhalten zu erkennen, zu unterbinden oder zu verhindern.

Anmerkung:

Damit bestätigt das Gericht einen grundlegenden Haftungsmaßstab: Es besteht keine Pflicht zur Unmöglichkeit – „impossibilium nulla obligatio est". Wichtig ist dies zu beachten in Fällen, in denen Mitarbeiter mit erheblicher krimineller Energie tätig werden und gezielt interne Strukturen umgehen oder ihr Verhalten verschleiern. In diesen Fällen kann die Erfüllung der Aufsichtspflicht im Einzelfall objektiv unmöglich sein. In solchen Konstellationen – etwa im Fall eines Mitarbeiterexzesses – endet die Zurechenbarkeit dort, wo das Leitungshandeln seine strukturell-realisierbaren Grenzen erreicht hat.

Beispielfall (6) – Vodafone-Datenskandal: Exzess oder strukturelles Kontrollversagen?[97]

Anfang Juni 2025 wurde gegen Vodafone ein Bußgeld i.H.v. 45 Mio. € verhängt – das bislang höchste, welches die Bundesbeauftragte für den Datenschutz und Informationsfreiheit in Bonn je verhängt hat. Der Vorwurf: unzureichende Kontrolle von Partnerunternehmen, lückenhafte IT-Sicherheit und fehlende Aufsicht über Prozesse, die den Missbrauch von Kundendaten ermöglichten. U.a. hatten Mitarbeitende in Partnershops systematisch Mobilfunkverträge manipuliert und interne IT-Strukturen unbefugt genutzt.

Auch wenn einzelne Handlungen auf eigenmächtiges Verhalten mit erheblicher krimineller Energie hindeuten, sah die Behörde im Bereich der DSGVO-Bußgeldsanktionierung offenbar die Voraussetzungen eines haftungsausschließenden Exzesses nicht als gegeben an. Entscheidend war wohl, dass Vodafone grundlegende Kontrollmechanismen – etwa zur Überwachung der Auftragsverarbeiter – strukturell nicht wirksam etabliert haben soll. In einem solchen Fall sind Pflichtverletzungen nicht nur ein individueller Fehltritt, sondern Folge eines systemischen Versagens der Aufsicht.

Bei der Frage der (strafrechtlichen) Verantwortlichkeit der Organe und Führungskräfte wurden die Verfahren eingestellt.[98] Unklar ist, ob hier zugunsten (in dubio pro reo) der Organe

95 Vgl. EuGH, Urt. v. 30.1.2024 – C-442/22, abrufbar unter: *https://curia.europa.eu/juris/document/document.jsf?text=&docid=282265 &pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1*.

96 Vgl. OLG Jena, Besch. v. 2.11.2005 – 1 Ss 242/05, NStZ 2006, 53.

97 Vgl. Bundesbeauftragte für den Datenschutz und Informationsfreiheit, BfDI verhängt Geldbußen gegen Vodafone, Pressemitteilung 6/2025, abrufbar unter: *https://www.bfdi.bund.de/SharedDocs/Pressemitteilungen/DE/2025/06_Geldbu%C3%9Fe-Vodafone.html*.

98 Vgl. InvestmentWeek, 45 Mio. für den Mantel des Schweigens – was Vodafone lieber verschweigen würde, 2025, abrufbar unter: *https://www.investmentweek.com/45-millionen-fur-den-mantel-des-schweigens-was-vodafone-lieber-verschweigen-wurde/*.

und Führungskräfte von einem Mitarbeiter-Exzess ausgegangen wurde.

d) Kriterien für haftungsrelevantes Kontrollversagen

Gerade im Fall eines Mitarbeiterexzesses ist – wie bereits dargelegt – entscheidend, ob dieser für die Unternehmensleitung vorhersehbar war und ob vorhandene Risikosignale unbeachtet blieben. Die bloße formale Existenz eines CMS genügt nicht, wenn das System in der betrieblichen Realität nicht wirksam umgesetzt wurde oder strukturelle Schwächen aufweist. Maßgeblich ist, ob sich aus konkreten Anhaltspunkten eine Pflicht zur Reaktion ergab – etwa durch systematische Abweichungen, Hinweise aus der Belegschaft oder kritische Risikoberichte.

Kritisch ist insbesondere zu prüfen:

- Gab es Frühindikatoren, die ignoriert oder bagatellisiert wurden?
- War das eingerichtete Compliance-Management-System (CMS) realitätsfern, personell oder sachlich unterausgestattet oder methodisch ungeeignet?
- Wurde auf aggregierte Risikoberichte oder positive Selbstauskünfte vertraut, ohne deren Validität zu hinterfragen oder auf Plausibilität zu prüfen?

Wird auch nur eine dieser Fragen bejaht, entfällt die Enthaftung. Denn in diesem Fall liegt ein kontrollpflichtiges Warnsignal vor, auf das nicht angemessen reagiert wurde – mit der Folge, dass der Exzess nicht mehr isoliert dem Mitarbeiter zugerechnet werden kann, sondern haftungsrechtlich auf ein strukturelles Kontrollversagen der Organisation zurückzuführen ist. Die zentrale Frage lautet dann nicht mehr, ob das CMS vorhanden war, sondern wie es konkret gelebt und auf seine Wirksamkeit hin überprüft wurde.[99]

e) Exzess als Führungspflichtversagen? Oftmals ja, aber nicht immer!

Unkenntnis entlastet nicht – sie belastet: Geschäftsleiter, die sich auf fehlende Information berufen, müssen sich fragen lassen, warum sie ihre Erkundigungs- und Informationspflichten nicht erfüllt haben. Es kommt nicht nur darauf an, was bekannt war, sondern was hätte bekannt sein müssen. Die Leitung ist verpflichtet, ein funktionierendes Meldesystem zu etablieren und durchzusetzen. Dazu gehört, Beschäftigte zur Mitteilung von Risiken und Pflichtverstößen im jeweiligen Verantwortungsbereich zu verpflichten. Nur wer ein solches Berichtswesen aktiv steuert, erfüllt seine Legalitätspflicht.[100]

Die dargestellte Rechtsprechung verdeutlicht: Ein fehlgeleiteter Glaube an Schutz durch Delegation oder Berichte führt nicht zur Entlastung, sondern zur Durchgriffshaftung – gerade im Fall vorhersehbarer Verhaltensabweichungen und mangelnden systemischen Strukturen.

Rack bringt es (eigentlich) auf den Punkt, wenn er schreibt: „Wer delegiert, muss kontrollieren oder haften."[101] Mitarbeiter mit besonderer krimineller Energie, die sich gezielt der Kontrolle entziehen, führen diese an sich zutreffende Maxime jedoch an ihre dogmatische Grenze.

Daher gilt: Der Exzess ist kein Entlastungsargument, sondern zunächst ein Brennglas für systemisches Führungsversagen – insbesondere, wenn:

- kein wirksames CMS bestand,
- Whistleblower unbeachtet blieben,
- Sanktionssysteme fehlten,
- Risiken nicht aggregiert oder validiert wurden,
- Delegation ohne Steuerung erfolgte,
- die Zweckbestimmung der Handlung nicht mit dem durch die Stellenbeschreibung definierten Pflichtenkreis des Mitarbeiters übereinstimmte und
- keine systematische Abgrenzung zwischen weisungswidrigem und exzessivem Verhalten vorgenommen wurde.

Beispielfall (7): Der etwas andere Fall aus der Praxis – Zurechnung trotz Exzess eines (ehemaligen) Erfüllungsgehilfen mit krimineller Energie[102]

Das LG München I verurteilte einen Finanzdienstleister zur Zahlung von immateriellem Schadensersatz nach Art. 82 DSGVO und stellte klar: Der Exzess eines (ehemaligen) Erfüllungsgehilfen entlastet nicht, wenn Kontrollpflichten verletzt werden. Über einen IT-Dienstleister wurden nach der Vertragsbeendigung über Monate hinweg nicht gesperrte Zugangsdaten genutzt, um sich unberechtigt Zugriff auf sensible Kundendaten eines Finanzdienstleisters zu verschaffen – darunter Steuer-ID, Ausweiskopien und Depotdaten. Die Geschäftsleitung hatte es versäumt, die Rechte dem ehemaligen IT-Dienstleister zeitnah zu entziehen. Der Zugriff erfolgte vollständig außerhalb der betrieblichen Weisungsstruktur, wie bei einem Mitarbeiterexzess. Gleichwohl haftete der Finanzdienstleister, da keine wirksame Zugriffskontrolle und keine revisionssichere Berechtigungspflege implementiert war. Zwar bestand formal ein Compliance-System – dieses wurde vom Gericht jedoch als strukturell unzureichend und faktisch funktionslos eingestuft.

---

99 In der Fachliteratur wird dies unter dem Begriff der strafrechtlich relevanten Organisationsverantwortung behandelt, vgl. *Momsen/Grützner*, Wirtschafts- und Steuerstrafrecht, 2. Aufl. 2020, § 16 Rn. 42 ff.

100 Ausführlich hierzu: OLG Stuttgart, Urt. v. 19.2.2012 – 20 U 3/11, ZCG 2012, 167, zur sog. „Sardinien-Äußerung" des Aufsichtsrats; BGH, Urt. v. 19.6.2012 – II ZR 243/11, ZInsO 2012, 1536, 1538 [Insolvenzreife – Unkenntnis schützt nicht].

101 Lesenswert: *Rack*, Manfred: Wer delegiert, muss kontrollieren oder haften – Die Haftung der Betriebsleiter, Abteilungsleiter und Führungskräfte des mittleren Managements mit ausdrücklichem Auftrag, Download unter: *https://xn--rack-rechtsanwlte-3qb.de/upload/downloads/aufsaetze/Wer_delegiert.pdf*.

102 Vgl. LG München I, Urt. v. 9.12.2021 – 31 O 16606/20, openJur 2021, 46734.

Das Besondere an diesem Fall: Es ging nicht um ein aktives Fehlverhalten aktueller Mitarbeiter, sondern um eine unterlassene Entziehung von Berechtigungen nach Ausscheiden eines externen Dienstleisters – also um einen exzessiven Zugriff durch einen ehemaligen Erfüllungsgehilfen. Gleichwohl wurde dem Unternehmen die Pflichtverletzung des Dritten zugerechnet. Die Entscheidung zeigt, dass der Exzess (hier eines Dritten) – anders als vielfach angenommen – nicht automatisch zur Enthaftung führt, wenn das Unternehmen seine Kontroll-, Überwachungs- und Organisationspflichten verletzt.

4. Zusammenfassung

Der Blick in die Rechtsprechung zeigt: Der Mitarbeiterexzess wirft grundlegende haftungsrechtliche Fragen auf – seine dogmatische Einordnung ist bislang nur ansatzweise erfolgt. Weder die Rechtsprechung noch die Literatur haben bislang ein konsistentes Kriteriensystem entwickelt, das die dogmatischen Voraussetzungen, Reichweiten und Grenzen der Zurechnung bei Überschreitungen des Pflichtenkreises einzelner Mitarbeitender hinreichend konturiert. Ob die Schwelle zur Enthaftung erreicht ist, bedarf daher stets einer sorgfältigen und differenzierten Einzelfallanalyse. Die dogmatische Trennlinie verläuft zwischen delegierter Verantwortlichkeit und strukturellem Versagen – nicht zwischen formaler Zuständigkeit und tatsächlicher Kontrolle.

Nach der Auffassung der Autoren steht die Dogmatik des Mitarbeiterexzesses in engem Zusammenhang mit den Anforderungen an moderne Governance, präventive Risikoüberwachung und funktionale Compliance-Strukturen. Der Mitarbeiterexzess beendet die Zurechnung – nicht aber die Pflicht zur strukturellen Beherrschung durch Governance, CMS und präventive Systemaufsicht. Es bedarf mithin immer einer Einzelfallbetrachtung, ob der Exzess tatsächlich nur Enthaftung führt. Ein wirksames CMS schützt nicht absolut, aber es begründet die Möglichkeit zur Enthaftung. Fehlt es an Mechanismen zur Erfüllung der Aufsichtspflicht, verbleibt die Verantwortung im Unternehmen – selbst bei individualisiertem Fehlverhalten, es sei denn, der Mitarbeiter unterläuft das System mit krimineller Energie durch Manipulationen oder Täuschung.

Die bloße Einrichtung von Rollen, Befugnissen und Zuständigkeiten innerhalb einer Organisation führt nicht automatisch zur Enthaftung bei Fehlverhalten einzelner Mitarbeiter. Entscheidend ist, ob ein funktionierendes Kontroll- und Überwachungssystem etabliert wurde, das geeignet ist, missbräuchliche Nutzung von Rechten, Systemen oder Befugnissen zu erkennen und wirksam zu unterbinden. Fehlende Kontrolle, unterlassene Reaktion auf Warnsignale oder eine „Vertrauensorganisation ohne Überprüfung“ können haftungsrechtlich zur Feststellung eines strukturellen Organisationsversagens bei der Erfüllung der Aufsichtspflicht und damit zu einer Zurechnung trotz Mitarbeiterexzess führen. Dies gilt es durch entsprechende Strukturen zu verhindern. Unterläuft der Mitarbeiter wiederum diese Strukturen, wird zu untersuchen sein, mit welcher Intention und in welcher Art und Weise dies erfolgte, denn das Haftungsrecht kennt weder eine Garantiehaftung aufgrund Geschäftsleiterstellung noch eine Pflicht zur Unmöglichkeit. Gerade in Fällen erheblicher krimineller Energie und gezielter Systemunterlaufung kann die Erfüllung der Aufsichtspflicht objektiv unmöglich sein – mit der Folge, dass eine Zurechnung ausscheidet.

Seine haftungsrechtliche Entlastungswirkung entfaltet der Mitarbeiterexzess dort, wo nicht nur formale, sondern inhaltlich wirksame Mechanismen zur Aufsicht, Kontrolle und Prävention etabliert und überprüfbar praktiziert werden (CMS), aber wiederum auch dort, wo diese Mechanismen mit krimineller Energie manipuliert oder umgangen werden – in allen anderen Fällen droht persönliche Haftung.

X. Basel IV: Neue An- und Herausforderungen für Banken und finanzierte Organisationen

Die Überarbeitung der Capital Requirements Regulation III (CRR III) trat am 1.1.2025 in Kraft.[103] Ziel ist die Stärkung der Widerstandsfähigkeit und Stabilität des Bankensektors durch strengere Regeln für Bewertung von Kreditrisiken und Kapitalunterlegung. Dies zeitigt Auswirkungen auf finanzierte Unternehmen und erhöht die Bedeutung eines seriösen Ratings: Organisationen mit seriösem externen (guten) Rating erhalten i.d.R. bessere Konditionen. Ein gutes Rating sollte als strategisches Ziel verankert werden, wobei es noch Nachholbedarf gibt: Nur jedes zehnte Großunternehmen (mindestens 500 Mio. €) verfügt über externes Rating.

XI. Neue Ansätze für „Ratings“/Bewertungen aufgrund von Angaben in Nachhaltigkeits-, Governance- oder Geschäftsberichten[104]

1. Indikatoren gestützte Bewertung von Governance, Resilienz und Insolvenzrisiko durch KI

Ansätze zur Bewertung von Insolvenzwahrscheinlichkeit, Resilienz, Zukunftsfähigkeit u.v.m. finden sich in den Z-, O- und Q-Score-Konzepten der Wissenschaft.[105]

Die künftig u.U. über Nachhaltigkeitsberichte umfassendere Governance-Berichterstattung in einem einheitlichen digitalen Format macht Organisationen transparenter und erlaubt neue Arten von *Indikatoren-basiertem Governance-Rating oder -Scoring* mithilfe von KI.

---

103 Vgl. Redaktion Risknet, Die Rolle des Risikomanagements unter Basel IV, 2024, RiskNET.de, abrufbar unter: *https://www.risknet.de/themen/risknews/die-rolle-des-risikomanagements-unter-basel-iv/*.

104 Vgl. *Gleissner/Wolfrum/Moecke*, Der Aufsichtsrat, 2024, 110.

105 Vgl. Wikipedia – Die freie Enzyklopädie, Altmann Z-score, 28.5.2024, Wikipedia.de, abrufbar unter: *https://en.wikipedia.org/w/index.php?title=-Altman_Z-score&oldid=1226107836* und Wikipedia – Die freie Enzyklopädie, Ohlsen O-score, 8.12.2024, Wikipedia.de, abrufbar unter: *https://en.wikipedia.org/w/index.php?title=Ohlson_O-score&oldid=1261889479*. Vgl. *Gleissner/Weissmann*, Das zukunftsfähige Familienunternehmen, Sringer 2024, abrufbar unter: *https://link.springer.com/content/pdf/10.1007/978-3-658-42787-0.pdf*.

Gezielte Fragen bzw. Aufträge („Prompts“) an die zur Problemstellung passenden KI-Tools helfen, zentrale Themen, Anforderungen, Kennzahlen etc., die sich in den Angaben der untersuchten Dokumente (z.B. Geschäftsbericht) finden, qualitativ und/oder (semi-)quantitativ zu bewerten.

Diese Ergebnisse können Indikatoren liefern, die eine vertiefte, revisionssichere Untersuchung veranlasst. Für ein Governance-Scoring sollten quantitative Bewertungen – auch der Geschäftsberichte der Geschäftspartner – gegenüber qualitativen Ausführungen bevorzugt werden: „If you can’t meassure it, you can’t manage it.“[106]

2. Wahrhaftigkeit und Widerspruchsprüfung im Reporting als Risikoindikator

Auch die Ehrlichkeit der Aussagen in den untersuchten Dokumenten/Reports sollten überprüft werden: Stimmen die qualitativen Aussagen mit den quantitativen Daten überein? Gibt es widersprüchliche Stellen?

Durch entsprechende KI-gestützte Bewertungen lassen sich Risiken frühzeitig erkennen.

Dies ist – gerade in Zeiten von Krisen und Transformation – Pflicht eines gewissenhaften Organs (§ 43 GmbHG, §§ 91, 93, 116 AktG, § 347 HGB) und auch Kardinalpflicht, deren Verletzung zum Verlust des (D&O-)Versicherungsschutzes führt.

3. Wahrheit in den Geschäftsberichten

Dabei sind an die Wahrheit der Geschäftsberichte ebenfalls strenge Compliance-Maßstäbe anzulegen:

Die neue Green Claims Directive, deren Abschaffung bereits wieder diskutiert wird, verschärft bereits bestehende viele alte Anforderungen.

Reporting – auch mithilfe von KI – ist Bilanzrecht und Compliance, nicht Marketing.

Parallel dazu nimmt die Eintrittswahrscheinlichkeit der Entdeckung von Compliance-Verstößen bei Reporting im Kontext Green-, White- und Pink-Washing aufgrund der Etablierung von Whistleblowing zu.[107]

a) Bestandsgefährdende Risiken und fehlende Prüfung

In Lageberichten wird häufig sinngemäß ausgeführt:

„Als Ergebnis der Analysen von Chancen und Risiken, Gegenmaßnahmen, Absicherungen und Vorsorgen sowie nach Einschätzung des Vorstands sind auf Basis der gegenwärtigen Risikobewertung und unserer Mittelfristplanung keine Risiken vorhanden, die einzeln oder in ihrer Gesamtheit die Vermögens-, Finanz- und Ertragslage des …-Konzerns bestandsgefährdend beeinträchtigen könnten.“

Diese Aussage sei jedoch nach Ansicht renommierter Risikomanagement-Experten nachweislich bei vielen Unternehmen bspw. mithilfe von Stressszenarien o.ä. überhaupt nicht verprobt, damit eine u.U. unrichtige – und oft folgenschwere – Aussage im Lagebericht. Kein Unternehmen ist per se vor bestandsbedrohenden Risiken geschützt. Unabhängig von Branche, Größe oder Markterfahrung besteht für jede Organisation die Möglichkeit, durch den Eintritt schwerwiegender Risiken – etwa Marktverwerfungen, regulatorische Veränderungen, Reputationsschäden oder operative Krisen – in eine existenzbedrohende Lage zu geraten.

b) Strukturkrisen und latente Bestandsgefährdung

Selbst hochprofitable Unternehmen können durch externe Schocks oder interne Fehlsteuerung kurzfristig in Schieflage geraten, wenn keine ausreichenden Risikopuffer, Frühwarnsysteme oder Resilienzmechanismen vorhanden sind.

Besonders deutlich wird dies bei Unternehmen, die regelmäßig auf staatliche Subventionen oder Hilfen angewiesen sind (s. Meyer Werft, gesetzliche Krankenkassen etc.), um ihren operativen Fortbestand zu sichern. Diese Unternehmen weisen strukturell eine anhaltend latente Bestandsgefährdung auf, da ihr Geschäftsmodell unter Marktbedingungen nicht eigenständig tragfähig ist.

Auch dies angemessen zu hinterfragen, gehört nach Ansicht der Autoren zu den Aufgaben der vielen Überwachungsfunktionen, inklusive der Auditoren *von Governance-Compliance*.[108]

> ***Tipp:***
>
> *Versuchen Sie Ihre Governance-Strukturen zu optimieren, um die verpflichtenden Anforderungen Ihrer relevanten Stakeholder, die Sie bewerten, zu erfüllen.*
>
> *Bewerten Sie Ihre relevanten Stakeholder/Business Partner, um frühzeitig deren Risiken zu erkennen.*

---

106 Das oft Peter Drucker oder W. Edwards Deming zugeschriebene findet sich bei keinem von beiden. W. Edwards Deming warnte vor einer rein zahlengetriebenen Steuerung und zählte reines Management „nach sichtbaren Zahlen“ zu den „sieben tödlichen Krankheiten“. Auch Peter Drucker sah in der Messung zwar ein wichtiges Instrument, betonte jedoch, dass gutes Management immer auch auf Urteilsvermögen, Erfahrung und Intuition angewiesen. Nicht alles, was zähle, sei messbar. Nach Auffassung der Autoren bedarf es vor allem auch Good Governance als das Zentrum von ESGRC. Aber ohne Datenerhebung und Auswertung geht es natürlich auch nicht, was aber ohnehin wiederum Teil von ESGRC ist.

107 Vgl. Tagesschau, die Verurteilungen der DWS aufgrund von Greenwashing-Vorwürfen in der Fondsbeschreibung, abrufbar unter: *https://www.tagesschau.de/wirtschaft/finanzen/dws-millionenstrafe-greenwashing-100.html* und FuW, Beschwerde gegen Shell wegen möglicher Irreführung der Aktionäre, 2023, abrufbar unter: *https://www.fuw.ch/beschwerde-gegen-shell-wegen-moeglicher-irrefuehrung-der-aktionaere-445996836231*.

108 Vgl. *Romeike*, IDW ES 16 – Krisenfrüherkennung und Krisenmanagement nach § 1 StaRUG, 2025, RiskNET.de, abrufbar unter: *https://www.risknet.de/themen/risknews/krisenfrueherkennung-und-krisenmanagement-nach-1-starug/*.

4. Regulierung von ESG-Ratings

Zu beachten ist, dass ESG-Rating/-Scoring/-Zertifizierung immer wichtiger und strenger reguliert wird:

Am 19.11.2024 beschloss die EU die *ESG-Rating-Verordnung*,[109] die 20 Tage nach Veröffentlichung in Kraft trat und 18 Monate, also *Mitte 2026* Rechtswirkung auf betroffene Organisationen (Ratinganbieter, Versicherer, Fondsgesellschaften und Kreditinstitute, die ihren Kunden kostenlose Ratings anbieten), entfaltet.

Geregelt ist für in der EU ansässige Ratinganbieter eine Zulassungspflicht bei der ESMA,[110] Transparenz, Interessenkonflikte, Beschwerdemechanismen und Drittländerzulassung.

XII. Exkurs: Prüfungsausschüsse in Unternehmen von Öffentlichem Interesse i.S. § 316a Satz 2 HGB (kapitalmarktorientierte Unternehmen, Kreditinstitute und Versicherer)

1. Auskunftsrechte und risikobasierte Auskunftspflichten

Nach § 107 Abs. 4 Satz 4 AktG kann jedes Mitglied des Prüfungsausschusses in Unternehmen von Öffentlichem Interesse über den Vorsitzenden unmittelbar bei den Leitern der Zentralbereiche der Gesellschaft, wie Risiko-, Compliancemanagement, Rechnungslegung, Abschlussprüfung, Internes Kontrollsystem und Interne Revision Auskünfte einholen.

Dieses Recht mag sich aufgrund der Aufsichtspflicht des Aufsichtsrats über den Vorstand zu einer *Auskunftseinholungspflicht* verdichten, wobei auch hier risikobasiert die *wichtigen* Auskünfte einzuholen sind.

Auch dies setzt wiederum eine angemessene Risikobewertung voraus bzw. dient als Grundlage für die Risikobewertung.

2. Compliance-Aufgaben des Prüfungsausschusses

„(…) Die Compliance-bezogenen Aufgaben des Prüfungsausschusses sind in den vergangenen Jahren stark gewachsen. Dies ist auf eine zunehmende Verrechtlichung im Bereich der ESG- und Cyberthemen, aber auch durch ein gestiegenes Bewusstsein für die Compliance-Relevanz dieser ‚Trendthemen' innerhalb des Unternehmens zurückzuführen. Die Bandbreite der Compliance-Themen, mit denen sich Prüfungsausschüsse intensiv beschäftigen, ist heute weitaus größer als bei Einführung des Prüfungsausschusses.

Mit dem Befragungsrecht gegenüber Führungskräften nachgeordneter Ebenen gewinnt der Prüfungsausschuss eine ‚Untersuchungskompetenz' in Compliance-Sachverhalten dazu. (…)

(…) Den Geschäftsberichten der DAX-40-Unternehmen aus dem Jahre 2023 lassen sich einige Hinweise darauf entnehmen, dass Prüfungsausschussmitglieder von diesem neuen Auskunftsrecht hinsichtlich der Compliance in praxi Gebrauch machen. (…)"[111]

3. Ausweitung der Überwachungspflichten

Durch die messbare „Verschärfung der Compliance-Pflichten des Vorstands durch externe und interne Entwicklungen" würden sich auch die Überwachungspflichten des Aufsichtsrats und der Prüfungsausschüsse verschärfen.

Dabei geht es zum einen um eine Zunahme von neuen Regularien in bekannten Rechtsfeldern. Zum anderen würden immer mehr neue Themen, die bisher nicht reguliert waren, „verrechtlicht". Damit werden z.B. aus den technischen Themen KI und Informationssicherheit die Rechtsthemen KI- und Informationssicherheits-*Compliance*. Ebenso war vor Jahrzehnten der Bereich der Unternehmensführung und Überwachung im Wesentlichen betriebswirtschaftlich geprägt und einer juristischen Bewertung, sowie einer Standardisierung entzogen.[112] Mittlerweile hat sich das grundlegend geändert und die *Governance-Compliance*[113] wurde zu einem der relevantesten Rechtsgebiete für Organe und Führungskräfte.

4. Trendthemen, Legalitätspflicht und Kompetenzbedarf

„(…) Auch allgemeine Trends wie Cybersecurity, Datenschutz, Klimarisiken, Pandemien und geopolitische Unwägbarkeiten müssen kraft Verantwortung für die Compliance-relevante System- und Strukturüberwachung nunmehr im Blick des Prüfungsausschusses sein.

Viele der genannten Handlungsfelder erfuhren in den vergangenen Jahren eine zunehmende Verrechtlichung, durch die die Legalitätspflicht des Vorstands im Rahmen der Leitungsverantwortung für das Unternehmen neu konturiert wird. (…)"[114]

Positiv ist, wenn in Geschäftsberichten vermehrt berichtet wird, dass Aufsichtsräte direkt Informationen bei den Lines of Defense-Funktionen einholen, um ihrer Überwachungsaufgabe gerecht zu werden.

Anzumerken ist hier aber, dass sich Vorstand und Aufsichtsrat nicht um „Trendthemen" zu kümmern haben, sondern um Themen mit relevanten Chancen und Risiken bzgl. ihrer Organisation. Zutreffend wird ausgeführt, dass dies Bedarf bei Aus- und Weiterbildung und fundierter Compliance-Kompetenzen bei den Organen bedingt.

---

109 Die „Verordnung (EU) 2024/3005 des Europäischen Parlaments und des Rates v. 27.11.2024 über die Transparenz und Integrität von Rating-Tätigkeiten in den Bereichen Umwelt, Soziales und Unternehmensführung (ESG) und zur Änderung der Verordnungen (EU) 2019/2088 und (EU) 2023/2859ist im EU-Amtsblatt v. 12.12.2024 veröffentlicht worden, abrufbar unter: *https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202403005*.

110 ESMA ist die Europäische Wertpapier- und Marktaufsichtsbehörde.

111 Vgl. *Arnold/Reinhardt*, CCZ 2025, 60.

112 Vgl. *Scherer/Fruth*, Governance-Management, Bd. I, 2015, 134: „Compliance beherrscht BWL".

113 Die Inhalte zur Governance-Compliance finden sich bei *Scherer*, Nachhaltige Führung und Überwachung von Organisationen (Governance) nach DIN ISO 37000 – erfolgreich umsetzen, auditieren und reporten, DIN Media, 2025.

114 Vgl. *Arnold/Reinhardt*, CCZ 2025, 60.

XIII. Sonderfall: Qualifikationsmatrix für Vorstands- und Aufsichtsratskompetenz in Geschäftsberichten

1. Bedeutung und Defizite der Qualifikationsmatrix

Die Qualifikationsmatrix im Geschäftsbericht soll die Kompetenzen der einzelnen Vorstands- und Aufsichtsratsmitglieder widerspiegeln.

Dabei werden immer öfter die Kompetenzen in Nachhaltigkeit, Governance, Digitalisierung und KI kommuniziert.

Bei der Analyse der Qualifikationsmatrizen aus den Geschäftsberichten 2023 aller in den Börsenindizes DAX, MDAX und SDAX gelisteten Unternehmen wurden jedoch Schwachstellen erkannt:[115]

Es kann sich hier um reine Selbsteinschätzungen handeln und es fehlt i.d.R. die Angabe zur Methodik der Ermittlung der Ergebnisse, ebenso wie eine externe Validierung nach „Fit & Proper".

Auch Kompetenzlevel, wie „Grundkenntnisse, gute Kenntnisse, Expertenkenntnisse" und Benchmarks/Branchen-Vergleichsanalysen fehlen meist.

Damit handelt es sich um ein sinnvolles Instrument, das (noch) nicht angemessen umgesetzt wird, da der Wahrheitsgehalt der Angaben i.d.R. nicht überprüft oder überprüfbar ist.

2. Governance-Compliance-Audits und Resilienz-Score: Erst recht in Krisenzeiten

Hier eine Auswahl von Audit-Checkfragen zum Thema „Governance-Compliance", Resilienz und Kapitalmarktfähigkeit:[116]

a) Verständnis der (Legal-)Definitionen im Bereich Governance[117]

- Sind die relevanten Definitionen für Governance, Risikomanagement und Compliance in Zeiten der Transformation mit Digitalisierung und Nachhaltigkeit (ESG) bei den relevanten Adressaten (Organe, Lines of Defense-Funktionen, Führungskräften etc.) bekannt, verstanden und werden sie einheitlich verwendet?
- Sind angemessene Kenntnisse der „nachhaltigen compliance- und risikobasierten, gewissenhaften Führung und Überwachung von Organisationen (Governance)" bei den relevanten Adressaten (Organe, Lines of Defense-Funktionen, Führungskräften etc.) vorhanden?[118]

b) Rechtliche Grundlagen (Compliance) für Governance[119]

- Sind die rechtlichen Grundlagen für Governance (Führung und Überwachung von Organisationen), Digitalisierung und Nachhaltigkeit bekannt und ist deren Einhaltung sichergestellt?[120]
- Werden die verpflichtenden Bestimmungen (Compliance) der Corporate Governance (ISO 37000:2021) beachtet?
- Sind die *Kardinalpflichten* der Organe und der Leitenden Angestellten bekannt und ist deren Einhaltung sichergestellt?
- Gibt es eine effektive Rechtsabteilung (Legal) und Compliance-Funktion?

c) Relevante Referenzgrößen inklusive Standards für Governance[121]

- Werden neben den regulativ verbindlichen Anforderungen für Governance (vgl. oben) auch relevante Standards für Governance, Risikomanagement, Compliance, Informationssicherheit etc. als Referenzgrößen herangezogen?

d) Organe[122]

aa) Rollen, Aufgaben, Rechte und Pflichten

- Gibt es aktuelle, dokumentierte „Rollenbeschreibungen", Geschäftsverteilungspläne, Geschäftsordnungen für die jeweiligen Gremien etc. und sind sich die jeweiligen Organmitglieder ihrer Aufgaben und (Haftungs-)Verantwortung bewusst und nehmen sie diese auch wahr?
- Werden die Organmitglieder regelmäßig effektiv geschult?

bb) Interaktion

- Sind angemessene Governance-Strukturen (Führung und Überwachung der Organisation)/-Interaktionen zwischen Gesellschafter, Aufsichtsgremium und Leitung sowie zu den Abteilungsleitern sichergestellt?

cc) Kompetenzen

- Wird die Zusammensetzung des Managements (Aufsichtsgremien/Vorstand/Geschäftsführung/erweiterte Ge-

115 Vgl. ECBE Governance Perspectives 2024, Qualifikationsmatrix & Aufsichtsratskompetenz – Eine Analyse der Geschäftsberichte 2023 aus der DAX-Indey-Familie,2024, abrufbar unter: *https://www.ecbe.com/assets/qualifikationsmatrix-und-aufsichtsratskompetenz-ecbe-governance-perspectives-2024.pdf*.

116 Die Auswahl der Fragen erfolgte in Anlehnung an gesetzliche Anforderungen, an Anforderungen der BGH-Rechtsprechung, an *Achleitner/Kaserer/Günther/Volk*, Die Kapitalmarktfähigkeit von Familienunternehmen – Unternehmensfinanzierung über Schuldschein, Anleihe und Börsengang, 2011, 59 ff., abrufbar unter: *https://papers.ssrn.com/sol3/papers.cfm?-abstract_id=1791526*, und ISO Harmonized Structure: 2021.

117 Vgl. DIN ISO 37000, Normabschnitt 3.

118 Die Inhalte zur Governance-Compliance finden sich bei *Scherer*, Nachhaltige Führung und Überwachung von Organisationen (Governance) nach DIN ISO 37000 – erfolgreich umsetzen, auditieren und reporten, Herausgeber DIN, DIN Media-Verlag, 2025.

119 Vgl. DIN ISO 37000, Normabschnitt 1.

120 Vgl. zu den Inhalten der Governance-Compliance: *Scherer*, Nachhaltige Führung und Überwachung von Organisationen (Governance) nach DIN ISO 37000 – erfolgreich umsetzen, auditieren und reporten, DIN Media, 2025.

121 Vgl. DIN ISO 37000, Normabschnitt 2.

122 Vgl. DIN ISO 37000, Normabschnitt 4.3.

schäftsleitung) von fachkundiger und objektiver Seite positiv bewertet?

- Sind die Stellen der Leitungs- und Aufsichtsorgane der Organisation angemessen besetzt?
- Wird die erste Leitungs- und Aufsichtsebene durch die zweite Managementebene (Stabsstellen/Abteilungsleiter) angemessen unterstützt und bei Bedarf vertreten?

Die vollständige Liste enthält noch viele weitere wichtige Governance-Compliance-Audit-Checkfragen.

Die Beantwortung dieser Fragen sollte sich im Idealfall aus den – zutreffenden – Schilderungen im „*Integrierten Corporate Governance-Bericht*" ergeben. Ein Governance-Compliance-Audit könnte dann in Stufe 1 mit wenig Aufwand prüfen, ob der Geschäftsbericht die relevanten Angaben enthält.

Audit-Stufe 2 würde sich dann auf die Verifizierung des Berichteten und auf relevante, aber in den Berichten nicht enthaltene Themen konzentrieren.

XIV. Governance-Compliance-Zertifizierungen

1. Akkreditierte Zertifizierungsstellen und Normenbezug

Eine für Compliance-Managementsysteme akkreditierte Zertifizierungsstelle bietet mittlerweile CMS-Zertifizierungen nach DIN ISO 37301 mit einem besonderem Scope des Audits auf (IT-/KI-)Governance-Compliance in Anlehnung an DIN ISO 37000 und ISO/IEC 38500 an.

2. Zertifizierungserfolge in der Praxis

Vier der im Bereich Compliance betreuten Mandanten[123] gehören zu den deutschlandweit ersten sieben Unternehmen, die von der einzigen[124] für ISO 37301- (CMS) bzw. 37001 (Antikorruption)-akkreditierten Zertifizierungsstelle zertifiziert wurden:

a) Hitzler Ingenieure GmbH & Co. KG

„Durch die fachlich fundierte, praxisorientierte Beratung und Unterstützung konnten wir unser CMS schnell und effizient einführen und zertifizieren – vielen Dank für Ihr Engagement!"

– Ernst Neumann, Geschäftsführer Finanzen, Hitzler Ingenieure GmbH & Co. KG –

b) Congatec GmbH

„Die Vorbereitung auf eine CMS-Zertifizierung durch GovSol war ein bedeutender Schritt für unsere Governance. Die Zusammenarbeit war professionell, effizient und, entgegen den üblichen Standardlösungen großer Beratungen, exakt auf uns abgestimmt. Wir freuen uns über diesen Meilenstein und seine Vorteile für unser Unternehmen. Eine Zertifizierung ist der sicherste Weg die Wirksamkeit eines CMS zu prüfen, ohne erst den Ernstfall abwarten zu müssen"

– Stefan Markovic, Director Global Quality & Compliance Officer, Congatec GmbH –

c) Karl-Gruppe

„Die Zertifizierung zeigte aufgrund der wichtigen Governance-Compliance-Themen den Wertbeitrag der in Bezug auf QM, Umwelt etc. integrativen Funktion eines Compliance-Managementsystems – eine wertvolle Investition."

– Zitat von André Karl, Geschäftsleitung Karl-Gruppe –

d) LASCO Umformtechnik GmbH

„Die Beratung durch GovSol und das von ihr durchgeführte interne Audit hat unsere Mitarbeitenden optimal auf das externe Zertifizierungsaudit vorbereitet. Die fundierte Analyse und praxisorientierten Maßnahmen haben uns dabei unterstützt, die ISO 37001 – Zertifizierung erfolgreich zu erreichen. Ein entscheidender Schritt für unser Unternehmen."

– Lothar Bauersachs, Vorsitzender der Geschäftsführung, LASCO Umformtechnik GmbH –

XV. Wertbeiträge

Investitionen in Digitalisierung mit KI, Governance, Risk und Compliance kosten zunächst Geld. Aber sie verstärken Resilienz und bedeuten nachhaltige Unternehmenswertsteigerung und Zukunftsfähigkeit. Die empirische Studie von Gleißner, Günther und Walkshäusl (2022)[125] belegt, dass Unternehmen mit einer hohen finanziellen Nachhaltigkeit – gemessen an vier zentralen Bedingungen (Wachstum, Überlebenswahrscheinlichkeit, akzeptable Risikobelastung und attraktives Risiko-Rendite-Profil) – signifikant höhere risikoadjustierte Kapitalmarktrenditen erzielen. Dabei erwirtschafteten Unternehmen, die alle vier Kriterien erfüllen, im Zeitraum von 1990 – 2019 monatlich 0,39 % Überrendite im Vergleich zum Marktdurchschnitt – bei gleichzeitig geringerem Risiko.

Ein weiterer derzeit unverzichtbarer Wertbeitrag eines Governance-Compliance-Managementsystems ist die – gemäß ständiger höchstrichterlicher Rechtsprechung[126] – *enthaftende Wirkung für Geschäftsführung, Aufsichtsrat, Management,*

123 Über die *Governance Solutions GmbH*.

124 Stand 05/2025.

125 Vgl. *Gleißner/Günther/Walkshäusl*, Financial sustainability: measurement and empirical evidence, in: Journal of Business Economics, 2022, 467 sowie *Gleißner/Romeike*, FIRM Yearbook 2023, 125.

126 Vgl. u.a. BGH 2017: (KMW), Urt. v. 9.5.2017; BGH 2022: (Selbstreinigung), Urt. v. 27.4.2022; BGH 2023 (Geschäftsverteilung), Urt. v. 9.11.2023; EuGH 2023: (Deutsche Wohnen), Urt. v. 5.12.2023; EuGH 2023: (Hackerangriff), Urt. v. 14.12.2023; EuGH 2024: (USt-Betrug), Urt. v. 30.1.2024; EuGH 2024: (juris), Urt. v. 11.4.2024; OLG Stuttgart, Beschl. v. 25.2.2025 – 2 ORbs 16 Ss 336/24, NJW 2025, 1279 (Mitarbeiter-Exzess).

Abteilungsleiter, Compliance- und Risikomanager und sonstige Beschäftigte.[127]

XVI. Ausblick und Schlussfolgerungen für die Praxis

Die unzähligen schwerwiegenden täglichen Ereignisse mit Gefahren für Leib und Leben, persönlichen Haftungsgefahren für Organe und sämtliche Beschäftigten einer Organisation oder erheblichen finanziellen Schäden bis hin zur Insolvenzverursachung zeigen, dass das Thema Governance nicht sensibel genug behandelt werden kann.

Die aus der Governance abzuleitenden zwingenden Anforderungen und Maßnahmen erscheinen erschlagend, sind es aber nicht. Sofern die Governance als Klammer über dem Integrierten Managementsystems (IMS) geführt wird, ergeben sich zum einen zahlreiche Überschneidungen mit bereits im IMS vorhandenen Elementen, zum anderen werden die korrekt zu erledigenden Aufgaben auf viele Schultern verteilt.

Governance ist primär „Chefsache", also von der Unternehmensleitung (z.B. Geschäftsführer, Vorstand) in Primär- und Letztverantwortung zu übernehmen. Nur durch rechtssichere Pflichtendelegation können Aufgaben und Verantwortung auf kompetente andere Funktionen delegiert werden.

Governance heißt aber auch, dass das Thema in der Überwachungsverantwortung des Aufsichtsgremiums bzgl. der Geschäftsführung und der Weisungsbefugnis des Gesellschafters liegt.

All das, was im Themenfeld Governance getan werden muss, muss (!) getan werden. Das ist reine Compliance ohne Ermessensspielraum bzgl. des „Ob" und damit gebundene Entscheidung und u.U. „*Kardinalpflicht*". Da gibt es auch keinen Risiko-Appetit und kein Pareto-Prinzip.

Da gibt es nur den „risikobasierten Ansatz": Statt alles gleichzeitig – was ja unmöglich ist: Das Wichtigste zuerst!

Um nicht aufgrund des Vorwurfs einer nicht rechtssicheren Organisation in die persönliche Haftungsfalle zu stolpern, ist ein *enthaftendes*[128] *Governance-Compliance-Managementsystem* unverzichtbar.

Neue Umfeld-Entwicklungen erfordern neue Kompetenzen bei Organen und Beschäftigten, aber auch bei den Überwachungsfunktionen.

Aus- und Weiterbildung sollten diesen Megatrend nicht verpassen. Die Darstellung der Bewältigung dieser Transformationsanforderungen findet sich in den nichtfinanziellen Geschäfts- oder Nachhaltigkeitsberichten von immer mehr Organisationen wieder.

Governance heißt nicht zuletzt, im Rahmen eines effektiven Changeprozesses trotz wissenschaftlich nachgewiesener „vorsätzlicher Ignoranz"[129] und typisch menschlicher Beharrungskräfte die Organisation und ihre Menschen erfolgreich durch die Transformation zu führen.

Wirtschaftsbooster und systemischer Fehler: ein bisher kaum hinterfragter Bias:[130]

Die Ursachen für Insolvenzen, Schließungen und strategisches Scheitern liegen häufig nicht im externen Umfeld, sondern in unternehmensinternen Defiziten – insbesondere im Bereich gesetzlich normierter Leitungsverantwortung. Auch Unternehmen, die objektiv vom konjunkturellen „Wirtschaftsbooster" profitieren müssten, geraten ins Straucheln, wenn gravierende Managementfehler übersehen, Missmanagement geduldet oder Frühwarnsysteme gar nicht erst implementiert werden.

Der Glaube, konjunkturelle Impulse wie der vom Bundeskabinett am 4.6.2025 beschlossene „Investitions-, Wachstums- oder auch Wirtschaftsbooster" genannte Gesetzesentwurf für ein steuerliches Investitionssofortprogramm zur Stärkung des Wirtschaftsstandorts Deutschland könnten strukturelle Führungsmängel kompensieren, ist Ausdruck einer gewissen Naivität und eines bislang kaum hinterfragten Bias in Form einer kognitiven Verzerrung: der Stabilitätsillusion. Solange gravierende Managementfehler – etwa im Sinne eines „Management by Blindflug"[131] – fortbestehen und von überwachenden Instanzen wie Aufsichtsräten, Abschlussprüfern oder den Funktionen der Lines of Defense nicht erkannt, nicht hinterfragt oder sogar implizit gedeckt werden, bleibt jeder externe Impuls ohne Wirkung. Eine substanzielle Verbesserung kann nur dort eintreten, wo Governance-Strukturen greifen, Frühwarnsysteme wirksam sind und steuerungsrelevante Informationen nicht nur gesammelt, sondern auch verstanden und genutzt werden.

Unter dem Eindruck der Stabilitätsillusion eines Wirtschaftsboosters besteht die Gefahr, dass Geschäftsleiter weiter ver-

127 Vgl. *Scherer*, Nachhaltige Führung und Überwachung von Organisationen (Governance) nach DIN ISO 37000 – erfolgreich umsetzen, auditieren und reporten, DIN Media, 2025, Kap. 4.2 „Governance und Delegation".

128 Vgl. *Scherer*, Nachhaltige Führung und Überwachung von Organisationen (Governance) nach DIN ISO 37000 – erfolgreich umsetzen, auditieren und reporten, DIN Media, 2025, Kap. 4.2 „Governance und Delegation".

129 Vgl. *Dörr*, Vorsätzliche Ignoranz: Von den Hindernissen digitaler Transformation und Schrödingers Katze, beck-aktuell, 2025, abrufbar unter: *https://rsw.beck.de/aktuell/daily/meldung/detail/vorsaetzliche-ignoranz-justiz-behoerden-digitale-transformation-studie*.

130 Vgl. Die Bundesregierung, Wachstumsbooster zur Stärkung des Standorts Deutschland, 2025, abrufbar unter: *https://www.bundesregierung.de/breg-de/aktuelles/kabinett-beschliesst-wachstumsbooster-2351752*; Vgl. BMF, Wachstumsbooster vom Kabinett beschlossen: Planungssicherheit und Anreize für private Investitionen, Pressemitteilung 5/2025, abrufbar unter: *https://www.bundesfinanzministerium.de/Content/DE/Pressemitteilungen/Finanzpolitik/2025/06/2025-06-04-kabinett-beschliesst-wachstumsbooster.html*; dass., Entwurf eines Gesetzes für ein steuerliches Investitionssofortprogramm zur Stärkung des Wirtschaftsstandorts Deutschland, abrufbar unter: *https://www.bundesfinanzministerium.de/Content/DE/Gesetzestexte/Gesetze_Gesetzesvorhaben/Abteilungen/Abteilung_IV/20_Legislaturperiode/2025-06-04-steuerliches-Investitionssofortprogramm/0-Gesetz.html*.

131 In Anlehnung an: OLG Frankfurt/M., Beschl. v. 16.1.2025 – 7 W 20/24, NJW-RR 2025, 731: „blind in die Krise segeln" und OLG Frankfurt/M., Urt. v. 5.3.2025 – 7 U 134/23, DStR 2025, 917, mit einem ähnlichen Fall (Rev. eingelegt, BGH – IV ZR 66/25).

kennen, dass § 1 StaRUG seit 2021 eine nicht delegierbare Pflicht zur Einrichtung wirksamer Risiko- und Krisenfrüherkennungssysteme statuiert. Diese Pflicht ist Ausprägung der Legalitätspflicht und entfaltet über § 43 GmbHG bzw. § 93 AktG unmittelbare haftungsrechtliche Relevanz. Das OLG Frankfurt/M. hat in seinem Urt. v. 5.3.2025[132] verdeutlicht, dass – wer dieser Pflicht nicht nachkommt – regelmäßig „wissentlich pflichtwidrig" handelt und Gefahr des D&O-Ausschlusses nach § 81 Abs. 2 VVG läuft. Geschäftsleiter, die trotz interner Hinweise, externer Signale oder belastbarer Kennzahlen im Modus des „Management by Blindflug" agieren, handeln außerhalb des Schutzbereichs der Business Judgment Rule.

Governance ohne Steuerung, Compliance ohne Kontrolle und Risikomanagement ohne Aggregation führen nicht zur Resilienz, sondern zur Illusion rechtlicher Absicherung bei tatsächlichem Kontrollversagen. Ohne präventive Unternehmensführung im Sinne eines integrierten ESGRC-Ansatzes bleibt jeder Wirtschaftsbooster ein Strohfeuer – ökonomisch wirkungslos, haftungsrechtlich gefährlich.[133]

---

132 Az. 7 U 134/23.

133 Vgl. *Scherer*, Nachhaltige Führung und Überwachung von Organisationen (Governance) nach ISO 37000, DIN Media 2025, 92 ff.; *ders.*, ESGRC, Gabler Wirtschaftslexikon (Online-Ausgabe), 2024, (Das ESGRC-Modell verbindet ökologische, soziale und rechtlich-normative Anforderungen mit einer unternehmensinternen Führungslogik, bei der Governance die Klammerfunktion übernimmt und als normativer Steuerungsrahmen die Verknüpfung zwischen Risiko, Compliance und nachhaltiger Unternehmensführung sicherstellt), abrufbar unter: *https://wirtschaftslexikon.gabler.de/definition/esgrc-126420/version-390788*.