Prof. Dr. Josef Scherer

Rechtsanwalt, Leitung des Internationalen Instituts für Governance, Management, Risk und Compliance und der Stabsstelle ESGRC der Technischen Hochschule Deggendorf. Mitglied diverser ISO- / DIN- / ASI-Normungsausschüsse und Beirat bei FIRM

Kardinalpflicht fordert „risikobasierten Ansatz“

Geschäftsführer, Vorstände, Aufsichtsratsmitglieder und Führungskräfte *„segeln blind in Haftung und Versicherungsverlust“*[1]

Prof. Dr. jur. Josef Scherer, 01.05.2025

Summary

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. Dies verursacht bei den betroffenen Organisationen häufig finanzielle Schäden, bringt sie nicht selten in

---

[1] Abgeändertes Zitat von OLG Frankfurt am Main, Beschluss vom 16.1.2025, Az. 7 W 20 / 24: „blind in die Krise segeln“. Vgl. auch OLG Frankfurt am Main, Urteil vom 5.3.2025, Az. 7 U 134 /23 mit einem ähnlichen Fall: **Hier ist die Revision beim BGH anhängig**: Az. IV ZR 66 / 25.

vermeidbare existenzielle Schwierigkeiten und wird zumeist haftungsbewehrtes Missmanagement[2] darstellen.

Neben des nachgewiesen drastisch steigenden Risikos der persönlichen Haftung droht aufgrund des von aktueller Rechtsprechung[3] angenommenen Vorwurfs der „*Verletzung von Kardinalpflichten*“[4] 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*. Beispielsweise existiert bei den Organen (Geschäftsführer, Vorstand, Aufsichtsgremien) und „Lines of Defense“ in der Regel noch wenig Verständnis bzgl. des Inhalts von sog. „Kardinalpflichten“ und „*risikobasierter Governance-Compliance*“, obwohl dies aktuell das Top-Risiko nahezu aller Organisationen verkörpert.

Nachfolgende Abhandlung beleuchtet die Rolle der Organe, der „Lines of Defense“-Funktionen inkl. Auditoren[5] 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.“[6]

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

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

---

[2] 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

[3] OLG Frankfurt am Main, Beschluss vom 16.1.2025, Az. 7 W 20 / 24: „blind in die Krise segeln“ und OLG Frankfurt am Main, Urteil vom 5.3.2025, Az. 7 U 134 /23 mit einem ähnlichen Fall: Hier ist die Revision beim BGH anhängig: Az. IV ZR 66 / 25.

[4] „Kardinalpflichten“ sind nach den aktuellen Urteilen des OLG Frankfurt am Main (vgl. oben) *„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* zurecht als eine elementare berufliche Pflicht eines Geschäftsführers oder Vorstandes anzusehen.

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

[6] Bayerisches Sprichwort.

Ein angemessenes Risikomanagement inkl. Risikofrüherkennung[7] muss auch Worst-case-Szenarien berücksichtigen, alle Risiken angemessen quantifizieren, aggregieren, steuern und mit der Risikotragfähigkeit in Abgleich bringen.[8]

Die Insolvenzzahlen stiegen bereits vor Trumps Zollkapriolen auf Höchstwerte.[9]

Obwohl inzwischen sogar eine Weltwirtschaftskrise vom Chef des Ifo-Instituts für möglich gehalten wird[10], 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.) und Entscheidern (Vorständen und Geschäftsführern), aber auch bei den diversen Arten von *Auditoren* angekommen.

Worst case-Szenarien werden oft bewusst oder aus Ignoranz ausgeblendet.[11]

Stattdessen werden häufig die weniger werdenden Ressourcen nicht auf die wichtigen Dinge gebündelt, sondern für reine Bürokratie ohne Wertbeiträge ausgegeben.[12]

Das mag verhaltensökonomische Gründe[13] 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 S. 2 AktG (Business Judgment Rule) nicht angemessen bekannt sind oder verstanden werden.

Oft fehlt auch echte Governance-, Risiko- und Compliancekompetenz und die GRC-Experten werden vor oft intuitiven Entscheidungen der Organe nicht beigezogen oder ernstgenommen.[14] Diese werden vielmehr mit operativen Aufgaben, wie Schulungen und bürokratischem Reporting[15] beschäftigt.

---

[7] Vgl. hierzu ausführlich *Scherer, Seehaus,* Governance und Compliance nach § 1 StaRUG, 2024, RiskNET.de, abrufbar unter: https://www.risknet.de/elibrary/kategorien/detailansicht/?tx_hmelibrary_elibrary%5Baction%5D=show&tx_hmelibrary_elibrary%5Bcontroller%5D=Paper&tx_hmelibrary_elibrary%5Bpaper%5D=698&cHash=455f2509571f4b9b92f4f502f1d6af20 und *Romeike*, IDW ES 16 – Krisenfrüherkennung und Krisenmanagement nach § 1 StaRUG, 9.4.2025, RiskNET.de, abrufbar unter: https://www.risknet.de/themen/risknews/krisenfrueherkennung-und-krisenmanagement-nach-1-starug/

[8] 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, Krisenfrüherkennung nach § 1 StaRUG anhand eines exemplarischen Kennzahlensystems, Teile 1 und 2, ZInsO 2025, S. 605 ff..

[9] Vgl. *Tagesschau*, „Zahl der Insolvenzen steigt weiter", 14.03.2025, abrufbar unter: https://www.tagesschau.de/wirtschaft/insolvenzen-anstieg-100.html

[10] 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

[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/

[12] Vgl. *Scherer,* Investition in Governance im Lichte von Basel IV und Rating, RiskNET.de, 2025, abrufbar unter: https://www.risknet.de/elibrary/kategorien/detailansicht/?tx_hmelibrary_elibrary%5Baction%5D=show&tx_hmelibrary_elibrary%5Bcontroller%5D=Paper&tx_hmelibrary_elibrary%5Bpaper%5D=701&cHash=7e7b1caf47d9b0ca241cb644833d64cf

[13] Vgl. *Scherer*, Investition in Governance im Lichte von Basel IV und Rating, RiskNET.de, 2025, abrufbar unter: https://www.risknet.de/elibrary/kategorien/detailansicht/?tx_hmelibrary_elibrary%5Baction%5D=show&tx_hmelibrary_elibrary%5Bcontroller%5D=Paper&tx_hmelibrary_elibrary%5Bpaper%5D=701&cHash=7e7b1caf47d9b0ca241cb644833d64cf

[14] 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.

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

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.

„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.“[16]

2. 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“.

Beispiel: Nachhaltigkeitsberichterstattung und Lieferkettensorgfaltspflichten-Gesetz:
Nachdem der Mittelstand bei hohem Ressourcenverbrauch sich nunmehr Jahre auf die Berichterstattung mit CSRD, ESRS, Taxonomie, CSDDD etc. vorbereitete, erkannten 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.[17]
Außer Unberechenbarkeit, Kosten, Bürokratie, Verunsicherung und Verärgerung im Mittelstand wurde nichts erreicht.

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[18] – zahlreiche weitere Bürokratie-Monster aufzählen, die der Mittelstand leidvoll erträgt.

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

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.[19]

---

[16] Zitat aus Gleissner, Weissmann, Die strategischen Herausforderungen deutscher Unternehmen, Die Deutsche Wirtschaft, 13.12.24.

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

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

[19] 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

Nicht nur bei Wirecard haben nach allgemeiner Meinung sämtliche Aufsichtsmechanismen kläglich versagt.[20]

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*."[21]

„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."[22]

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:[23]

„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 (…)"[24]

Hinweis:

Inzwischen veröffentlichte das Institut Deutscher Wirtschaftsprüfer den IDW ES 16 zur Prüfung der Umsetzung der Anforderungen aus § 1 StaRUG.[25] Dieser Entwurf beinhaltet noch zahlreiche Schwachstellen und bleibt hinter den Anforderungen des Gesetzgebers und des DIIR Nr. 2 erheblich zurück.

Die Welt der Überwacher[26] 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

---

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

[21] Vgl. *Gleissner, Wolfrum*, Nutzen der Abschlussprüfung, Zeitschrift für Risikomanagement 2024, S. 116, 118.

[22] Zitat aus Gleissner, Wolfrum, ZfR 2024, S. 116, 118.

[23] Vgl. *Jungesblut,* Risikomanagement-Praxis Deutscher DAX- und MDAX-Unternehmen nach StaRUG und FISG, Corporate Finance, 12 / 2024, S. 274 ff..

[24] Zitat aus Jungesblut, Corporate Finance, 12 / 2024, S. 274, 280.

[25] Vgl. *Romeike*, IDW ES 16 – Krisenfrüherkennung und Krisenmanagement nach § 1 StaRUG, 9.4.2025, RiskNET.de, abrufbar unter: https://www.risknet.de/themen/risknews/krisenfrueherkennung-und-krisenmanagement-nach-1-starug/

[26] Vgl. *Scherer*, Die "Welt(en) der Überwacher": Enormes Potenzial für Effektivität, Effizienz und Wertbeiträge bei Governance, Risk & Compliance (GRC), FIRM Jahrbuch 2017, 2017, S. 79-81, abrufbar unter: https://www.gmrc.de/images/Docs/Publikationen/Scherer_Die_Welt_en_der_Ueberwacher.pdf

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.

Bereits *Michel Barnier*, ehemaliger EU-Binnenmarktkommissar, hatte im Zuge der Finanzkrise ambitionierte Reformen angestoßen, um die Unabhängigkeit der Wirtschaftsprüfer zu stärken.[27] Vorgesehen waren unter anderem 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.

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

Das mittelfristige Top Risiko Nr. 1 des Global Risks Report 2024 war aufgrund der Entwicklungen der Künstlichen Intelligenz (KI) das Thema „Desinformation und Manipulation“.[28]

Zu den größten Sorgen der CEOs weltweit gehörten auf Platz 1 die Cyber Risks.[29] Auch 2025 haben sich diese Risikoeinschätzungen kaum verändert.[30]

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.[31]

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*“[32].

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 oben genannten Verantwortlichen inklusive der Auditoren völlig willkürlich und unterschiedlich, was – wie nachfolgend aufgezeigt wird – zu fatalen Ergebnissen führt.

---

[27] Vgl. RiskNET.de, Finanzkrise legt Schwächen bei Wirtschaftsprüfern offen, abrufbar unter: https://www.risknet.de/themen/risknews/finanzkrise-legt-schwaechen-bei-wirtschaftspruefern-offen/

[28] Vgl. *WEF*, Global Risks Report 2024, https://www.weforum.org/publications/global-risks-report-2024/

[29] Vgl. *PWC,* CEOs´ Global Survey 2024, https://www.pwc.de/de/ceosurvey.html

[30] 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

[31] Zitiert aus Scherer, Pothorn, Jones, IT- (KI-) Governance-Compliance-Managementsystem, IT-Governance 2025.

[32] Vgl. *Scherer*, Nachhaltige Führung und Überwachung von Organisationen (Governance) nach DIN ISO 37000 - erfolgreich umsetzen, auditieren und reporten, Herausgeber DIN, DIN Media Verlag, 2025, Kapitel Einleitung.

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.

In der Regel sind nicht bestandsgefährdende Einzelrisiken, sondern die kumulierende Wirkung vieler Einzelrisiken fatal; daher ist eine methodisch fundierte Aggregation der Risiken wichtig[33].

Zwischenfazit: 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.

5. Governance-Compliance

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.

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

---

[33] Vgl. RiskNET.de, Qualitative Methoden zur Risikoaggregation sind eine Fiktion, abrufbar unter: https://www.risknet.de/themen/risknews/qualitative-methoden-zur-risikoaggregation-sind-eine-fiktion/ sowie RiskNET.de, Risikoaggregation wird zur Pflicht, 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, Herausgeber DIN, DIN Media Verlag, 2025, Kapitel 6.9 Risiko-Governance.

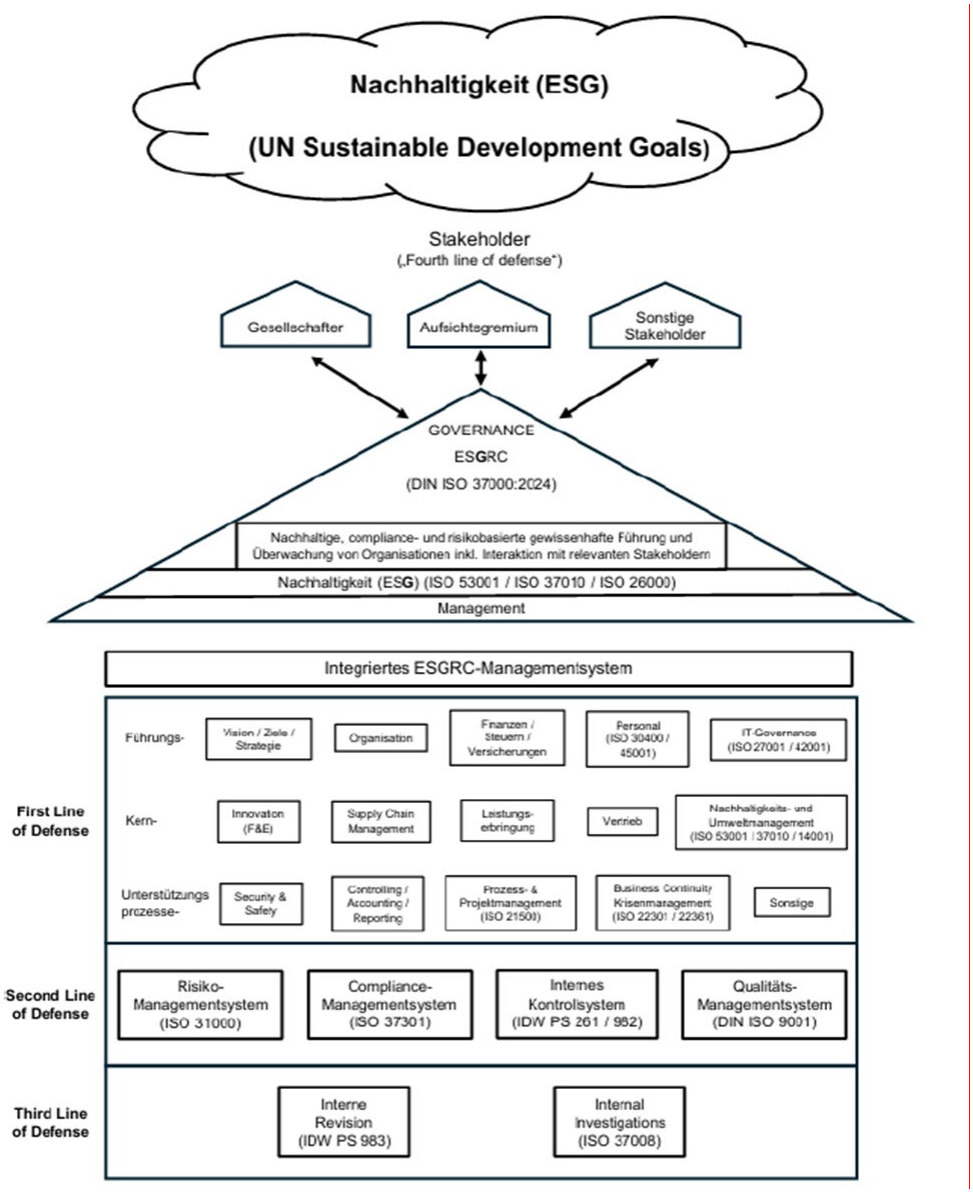

Abbildung 1: Das „ESGRC-Haus“, eigene Darstellung aus *Scherer*, Nachhaltige Führung und Überwachung von Organisationen (Governance) nach DIN ISO 37000 – Erfolgreich umsetzen, auditieren und reporten, DIN Media, 2025

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 inkl. 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.

Beispiel: Die 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[34]) 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[35] *(…)“*

Dazu gehört mittlerweile auch KI.[36]

Anzumerken sei 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 unter anderem die Implementierung eines ganzheitlichen Security-Lifecycle-Managements sowie die Einbeziehung von Zonen- und Conduits-Modellen zur Risikobewertung.

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

Die §§ 91 Abs. 2 AktG und Abs. 3 AktG, 107 AktG, § 1 StaRUG mit der haftungsbewehrten Pflicht zur Risikofrüherkennung mit Quantifizierung, Aggregation, Steuerung, Abgleich mit Risikotragfähigkeit und

---

[34] Vgl. *Scherer*, KI-Verantwortung und enthaftende Wirkung eines KI-Compliance-Managementsystems für Leitung (Vorstand, Geschäftsführer, Officers), Aufsichtsgremium und sonstige Führungskräfte, 2023, zum kostenlosen Download im Internet.

[35] Vgl. *BGH*, Urteil vom 12.10.2016, Az. 5 StR 134 / 15 „HSH Nordbank“.

[36] Vgl. *Scherer*, Die haftungsbewehrte *Pflicht* zur Verwendung von KI bei unternehmerischen Entscheidungen – auch im Rahmen des Transformations-, Risiko- und Krisenmanagements, 31.10.2024, zum kostenlosen Download im Internet.

Business Continuity- und Krisenmanagement (vgl. IDW ES 16[37], 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.[38]

Ebenso entschied das OLG Nürnberg[39] 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.

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 dreiviertel Million Euro 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*.[40]

7. Haftungsrisiken steigen proportional zu wachsender Regulierung

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 bis 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 bis 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.

---

[37] Vgl. *Romeike*, IDW ES 16 – Krisenfrüherkennung und Krisenmanagement nach § 1 StaRUG, 9.4.2025, RiskNET.de, abrufbar unter: https://www.risknet.de/themen/risknews/krisenfrueherkennung-und-krisenmanagement-nach-1-starug/

[38] Z.B. BGH vom 19.06.2012, II ZR 243 /11 und BGH vom 23.07.2024, II ZR 206 / 22.

[39] *OLG Nürnberg*, Urteil vom 30.3.2022, Az. 12 U 1520 / 19 „Tankstellenpächter".

[40] Vgl. hierzu ausführlich *Scherer, Seehaus,* Governance und Compliance nach § 1 StaRUG, 2024, RiskNET.de, abrufbar unter: https://www.risknet.de/elibrary/kategorien/detailansicht/?tx_hmelibrary_elibrary%5Baction%5D=show&tx_hmelibrary_elibrary%5Bcontroller%5D=Paper&tx_hmelibrary_elibrary%5Bpaper%5D=698&cHash=455f2509571f4b9b92f4f502f1d6af20

Die durchschnittliche Vergleichssumme der 50 größten US-Haftungs-Gerichtsurteile von 2014 bis 2018 von 28 auf 54 Millionen US-Dollar fast verdoppelt.[41]

„Chefposten werden riskanter - mehr Klagen werden erwartet“

„Spitzenpositionen sind auch mit einem wachsenden Risiko verbunden, Ziel eine Klage zu werden.“ […]

„Wir beobachten, dass Aufsichtsbehörden auf der ganzen Welt das Unternehmensverhalten schärfer überprüfen, wodurch Unternehmenslenker anfälliger für Untersuchungen, Strafen und Klagen werden.“[42]

„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.** (…)“*[43]

Der Bundesfinanzhof 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. […]“[44]

Hinweis:

Die neue DIN ISO 37301:2021(CMS) enthält ca. 60 BGH-Entscheidungen zur rechtssicheren Organisation.[45]

---

[41] Vgl. *Beck* aktuell, Allianz: Haftungsrisiken für Unternehmen steigen, 09.09.2020, abrufbar unter: https://rsw.beck.de/aktuell/daily/meldung/detail/allianz-haftungsrisiken-fuer-unternehmen-steigen

[42] Zitat aus beck-aktuell, Allianz: Chefposten werden riskanter - mehr Klagen erwartet, vom 05.12.2024.

[43] Zitat aus Gesamtverband der Deutschen Versicherer, D&O-Versicherung: Manager werden öfter zur Kasse gebeten, 1.10.2024.

[44] Vgl. *Bundesfinanzhof*, Beschluss vom 15.11.2022, VIII R 23/19 und Dürr, „Geschäftsführerhaftung wegen Unfähigkeit“, 20.03.2023.

[45] Vgl. *Scherer*, Compliance-Managementsystem nach DIN / ISO 37301 erfolgreich, implementieren, integrieren, auditieren, zertifizieren, DIN Media Verlag, 2022, S. 40, Fn. 96 mit Verweis auf Rack.

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

Neben des nachgewiesen drastisch steigenden Risikos der persönlichen Haftung droht aufgrund des von aktuellster Rechtsprechung des OLG Frankfurt am Main[46] 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 am Main „*elementare berufliche Pflichten, deren Kenntnis nach der Lebenserfahrung bei jedem Berufsangehörigen vorausgesetzt werden kann.*"

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*", vgl. BGH, Urteil vom 20.1.2005, Az. VIII ZR 121 / 04).

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[47]:

„(…) *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*[48]*,*

---

[46] OLG Frankfurt am Main, Beschluss vom 16.1.2025, Az. 7 W 20 / 24: „blind in die Krise segeln" und OLG Frankfurt am Main, Urteil vom 5.3.2025, Az. 7 U 134 /23 mit einem ähnlichen Fall: Hier ist die Revision beim BGH anhängig: Az. IV ZR 66 / 25.

[47] Zitat aus Wikipedia, Kardinalpflicht / Kardinalpfichten bei der Geschäftsführung, abrufbar unter: https://de.wikipedia.org/wiki/Kardinalpflicht

[48] Vgl. hierzu *BGH*, Urteil vom 10.01.2023, Az. 6 StR 133 / 22 (*„Vergütung VW-Betriebsräte"*) und *BGH*, Urteil vom 10.02.2022, Az. 3 StR 329 / 21 (*„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 u.v.m.. Hinweis: 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 S. 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* (06.01.2023, 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

- *das Unternehmensvermögen nicht für unternehmensfremde Zwecke zu verwenden[49],*
- *bei Insolvenzreife rechtzeitig Insolvenzantrag zu stellen,*
- *sich jederzeit über die wirtschaftliche Lage der Gesellschaft zu vergewissern[50] 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. März 2025 – 7 U 134 / 23* (...).

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[51]:

„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."

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 Aktiengesellschaften und (analog) für große GmbHs statuiert (vgl. die Gesetzgebungsmaterialien zum KonTraG und zum FiSG).

---

von Organisationen (Governance) nach DIN ISO 37000 - erfolgreich umsetzen, auditieren und reporten, Herausgeber DIN, DIN Media-Verlag, 2025, Kap. 6.8.

[49] Vgl. die BGH-Entscheidung „Schloss Eller" (BGH, Urteil vom 10.7.2018, Az. II ZR 24 /17): Gerade auch bzgl. der in Governance-Standards genannten Gemeinwohlbelange, wie Nachhaltigkeit und Social Responsibility, sind im Spannungsfeld „Integrität und Ethik" Compliance-Vorgaben zu beachten. Beispielsweise 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.

[50] Vgl. BGH vom 19.06.2012, II ZR 243 /11 und BGH vom 23.07.2024, II ZR 206 / 22 und OLG Nürnberg, Urteil vom 30.3.2022, Az. 12 U 1520 / 19 „Tankstellenpächter".

[51] OLG Frankfurt am Main, Urteil vom 5.3.2025, Az. 7 U 134 /23: **Hier ist die Revision beim BGH anhängig**: Az. IV ZR 66 / 25.

Die Rechtsprechung zog schnell nach und erweiterte die Pflicht auf nicht bestandsgefährdende Risiken:[52]

Nichtige Vorstandsentlastung wegen nicht angemessenen Risiko-Managementsystems

Das *Landgericht München I*[53] 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 Landgerichts enthält auch Ausführungen, die sich dahingehend interpretieren lassen, dass das einzurichtende und zu dokumentierende (!) Risiko-Managementsystem nicht ausschließlich bestandsgefährdende Risiken, sondern auch allgemeine Risiken zu behandeln habe.[54] 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".

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):[55]

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."[56]

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

Ende Exkurs

Zitat des OLG Frankfurt am Main[57]:

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

---

[52] Vgl. *Scherer*, Nachhaltige Führung und Überwachung von Organisationen (Governance) nach DIN ISO 37000 - erfolgreich umsetzen, auditieren und reporten, Herausgeber DIN, DIN Media Verlag, 2025, Kapitel 6.9 Risiko-Governance.

[53] Vgl. LG München I, Urteil vom 05.04.2007 (Az. 5 HKO 15964/06 – „Risiko"); BFH, NJW 2008, S. 319; Theusinger/Liese, Besteht eine Rechtspflicht zur Dokumentation von Risikoüberwachungssystemen?, NZG 2008, S. 289 ff.; das LG Berlin (LG Berlin, AG 2002, S. 682) sah bereits 2002 schon ein mangelhaftes Risikomanagement als wichtigen Grund für eine außerordentliche Kündigung eines Vorstandes an.

[54] Theusinger/Liese, Besteht eine Rechtspflicht zur Dokumentation von Risikoüberwachungssystemen? in: NZG 2008, S. 290.

[55] Vgl. Scherer, Seehaus, Governance und Compliance nach § 1 StaRUG, 2024, Risknet.de, abrufbar unter: https://www.risknet.de/elibrary/kategorien/detailansicht/?tx_hmelibrary_elibrary%5Baction%5D=show&tx_hmelibrary_elibrary%5Bcontroller%5D=Paper&tx_hmelibrary_elibrary%5Bpaper%5D=698&cHash=455f2509571f4b9b92f4f502f1d6af20

[56] Vgl. den veröffentlichten Lagebericht der N.N. Raumexklusiv GmbH für das Geschäftsjahr vom 1. Januar bis zum 31. Dezember 2012.

[57] OLG Frankfurt am Main, Urteil vom 5.3.2025, Az. 7 U 134 /23: Hier ist die Revision beim BGH anhängig: Az. IV ZR 66 / 25.

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 Aktiengesellschaft zur gewissenhaften Geschäftsführung) inkl. § 93 Abs. 1 S. 2 mit der Obliegenheit zur Einhaltung der sogenannten 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*[58] zurecht als eine elementare berufliche Pflicht eines Geschäftsführers, Vorstandes oder Aufsichtsrats anzusehen.

Sicher wird bei jeder einzelnen Pflichtverletzung im Sinne der §§ 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 inkl. Informationssicherheit sein. Auch Nachhaltigkeitsrisiken dürften immer mehr zu diesen Risikobereichen gehören.

Generell würde eine angemessene (Compliance-) Risikoanalyse[59] 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.

Legalitätspflicht als Kardinalpflicht

Das Legalitätsprinzip[60], 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:

---

[58] 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.

[59] Vgl. DIN ISO 37301 Normabschnitt 4.6 Compliance-Riskoanalyse und ISO IEC 31010 Risk Assessment.

[60] Vgl. BGH, Urteil vom 27.8.2010, Az. 2 StR 111 / 09 (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.

Beginnend mit dem „berühmten“ „Neubürger“-Urteil des LG München vom 10.12.2013[61] im Siemens-Compliance-Skandal, führten das LAG Düsseldorf[62], das ArbG Frankfurt[63], der BGH[64] und aktuell das OLG Nürnberg[65] aus, das es Obliegenheit des Geschäftsführers oder Vorstands sei, ein angemessenes und wirksames Compliance-Managementsystem einzurichten.[66]

Flankierend dazu entschied der BGH im „Buchhändler-Urteil“[67], 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.[68]

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[69], die mittelbar argumentieren, Vorstand oder Geschäftsführer sei kein Beruf, der eine bestimmte Qualifikation voraussetzt wurde, wird durch den Hinweis des BGH (Beschluss vom 21.5.2019, Az. II ZR 337 / 17), ein Geschäftsführer, der sich haftungsbefreiend von der Gesellschaft trennen möchte, müsse sein Amt niederlegen, der Boden entzogen.

Ebenso sieht es der Bundesfinanzhof, der ausführte:

„[…] wer den Anforderungen an einen gewissenhaften Geschäftsführer nicht entsprechen kann, muss von der Übernahme des Geschäftsführeramtes absehen, bzw. dieses Amt niederlegen. […]“[70]

---

[61] Das sogenannte „Neubürger-Urteil“ des Landgerichts München I (Az. 5 HK O 1387/10) vom 10. Dezember 2013 gilt als richtungsweisendes Urteil zur organisationsbezogenen Haftung von Vorständen in Aktiengesellschaften. Im Zentrum stand die Frage, ob der ehemalige Siemens-Vorstand Dr. Uriel J. Neubürger gegen seine Sorgfaltspflichten gemäß § 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- oder Risikomanagementsystems nicht delegierbar sei und zu den zentralen Leitungsaufgaben eines Vorstands gehört. Ein bloßes Vertrauen auf nachgeordnete Stellen entlaste nicht von der Verantwortung.

[62] Urteil vom 27.11.2015 („Schienenkartell“).

[63] Urteil vom 11.9.2013 („Libor-Manipulation“).

[64] Urteil vom 15.1.2013 („unternehmenszweckwidrige Derivate“) und vom 9.5.2017 („Panzerhaubitzenfall“).

[65] *OLG Nürnberg*, Urteil vom 30.3.2022, Az. 12 U 1520 / 19 („Tankstellenpächter“).

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

[67] BGH, Urteil vom 18.11.2020, Az. 2 StR 246 /20.

[68] Vgl. *Scherer*, Compliance-Managementsystem nach DIN / ISO 37301 erfolgreich, implementieren, integrieren, auditieren, zertifizieren, DIN Media Verlag, 2022, S. 233: „Wer soll das alles wissen?“.

[69] Vgl. Herdter, Die Versicherungspraxis, 6 / 2020.

[70] Vgl. Bundesfinanzhof, Beschluss vom 15.11.2022, VIII R 23/19 und *Dürr*, „Geschäftsführerhaftung wegen Unfähigkeit“, 20.03.2023.

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[71] das *Korrektiv der enthaftenden Wirkung eines Compliance-Managementsystems*:
Bei Pflichtverstößen unterhalb der Leitungsebene kann bei Existenz eines Compliance-Managementsystems der Vorwurf des Organisationsverschuldens i.S. einer Aufsichtspflichtverletzung entfallen.

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

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

Die Überarbeitung der Capital Requirements Regulation III (CRR III) trat am 01.01.2025 in Kraft.[72] 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 (mind. 500 Mio. Euro) verfügt über externes Rating.

10. Neue Ansätze für „Ratings" / Bewertungen aufgrund von Angaben in Nachhaltigkeits-, Governance- oder Geschäftsberichten[73]

Ansätze zur Bewertung von Insolvenzwahrscheinlichkeit, Resilienz, Zukunftsfähigkeit u.v.m. finden sich in den Z-, O-, und Q-Score-Konzepten der Wissenschaft.[74]

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.

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.

---

[71] BGH 2017: („KMW"), Urteil vom 09.05.2017; BGH 2022: („Selbstreinigung"), Urteil vom 27.04.2022; BGH 2023 („Geschäftsverteilung"), Urteil vom 09.11.2023; EuGH 2023: („Deutsche Wohnen"), Urteil vom 05.12.2023; EuGH 2023: („Hackerangriff"), Urteil vom 14.12.2023; EuGH 2024: („USt-Betrug"), Urteil vom 30.1.2024; EuGH 2024: („Juris"), Urteil vom 11.04.2024; OLG Stuttgart 2025: („Mitarbeiter-Exzess"), Beschluss vom 25.2.2025.

[72] Vgl. *Redaktion Risknet*, Die Rolle des Risikomanagements unter Basel IV, 28.8.24, RiskNET.de, abrufbar unter: https://www.risknet.de/themen/risknews/die-rolle-des-risikomanagements-unter-basel-iv/

[73] Vgl. *Gleissner, Wolfrum, Moecke*, Risikomanagement nach StaRUG und FISG, Der Aufsichtsrat, 2024, S. 110-112.

[74] Vgl. *Wikipedia – Die freie Enzyklopädie,* Altmann Z-score, 28.05.2024, Wikipedia.de, abrufbar unter: *https://en.wikipedia.org/w/index.php?title=Altman_Z-score&oldid=1226107836*
Vgl. *Wikipedia – Die freie Enzyklopädie,* Ohlsen O-score, 08.12.2024, Wikipedia.de, abrufbar unter: *https://en.wikipedia.org/w/index.php?title=Ohlson_O-score&oldid=1261889479*
Vgl. *Gleissner, Weissmann,* Das zukunftsfähige Familienunternehmen, Mit dem QScore zu Unabhängigkeit, Resilienz und Robustheit, 12/2023, abrufbar unter: https://link.springer.com/content/pdf/10.1007/978-3-658-42787-0.pdf mit einer Checkliste zum Q-Score.

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."

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.

Wahrheit in den Geschäftsberichten

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

Die neue Green Claims Directive 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.[75]

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. mit Hilfe 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. 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 (siehe 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.

---

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

Auch dies angemessen zu hinterfragen, gehört nach Ansicht des Autors zu den Aufgaben der vielen Überwachungsfunktionen, inkl. der Auditoren *von Governance-Compliance*.[76]

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.

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*[77], 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[78], Transparenz, Interessenskonflikte, Beschwerdemechanismen und Drittländerzulassung.

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

Nach § 107 Abs. 4, S. 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 Aufsichtrats 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.

Zitat[79]:

„(…) 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-

---

[76] Vgl. *Romeike*, IDW ES 16 – Krisenfrüherkennung und Krisenmanagement nach § 1 StaRUG, 9.4.2025, RiskNET.de, abrufbar unter: https://www.risknet.de/themen/risknews/krisenfrueherkennung-und-krisenmanagement-nach-1-starug/

[77] Vgl. Siethoff, ESG-Rating-Verordnung: Die wichtigsten Fragen und Antworten, 20.1.2025, zum kostenlosen Download im Internet.

[78] Europäische Wertpapier- und Marktaufsichtsbehörde.

[79] Arnold / Reinhardt, Die zunehmende Compliance-Verantwortung des Prüfungsausschusses, Corporate Compliance Zeitschrift 2025, S. 60 ff..

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.* (…)"

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.[80] Mittlerweile hat sich das grundlegend geändert und die *Governance-Compliance*[81] wurde zu einem der relevantesten Rechtsgebiete für Organe und Führungskräfte.

„(…) *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. (…)"[82]

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.

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

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

---

[80] Vgl. Scherer, Fruth, Governance-Management Band I, 2015, S. 134 ff.: Das Ende der klassischen Betriebswirtschaftslehre: „Compliance beherrscht BWL".

[81] 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.

[82] Arnold / Reinhardt, Die zunehmende Compliance-Verantwortung des Prüfungsausschusses, Corporate Compliance Zeitschrift 2025, S. 60 ff..

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:[83]

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.

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

- Eine *Auswahl* von Audit-Checkfragen zum Thema „Governance-Compliance", Resilienz und Kapitalmarktfähigkeit[84]:

Verständnis der (Legal-) Definitionen im Bereich Governance[85]

- 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?[86]

Rechtliche Grundlagen (Compliance) für Governance[87]

- Sind die rechtlichen Grundlagen für Governance (Führung und Überwachung von Organisationen), Digitalisierung und Nachhaltigkeit bekannt und ist deren Einhaltung sichergestellt?[88]
- 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?

---

[83] Vgl. auch *ECBE* (…), Governance Perspectives 2024.

[84] Die Auswahl der Fragen erfolgte in Anlehnung an Anforderungen der BGH-Rechtsprechung, an gesetzliche Anforderungen, an *Achleitner et al*. in: Stiftung Familienunternehmen, Die Kapitalmarktfähigkeit von Familienunternehmen, 2011, S. 59 ff. und ISO Harmonized Structure: 2021.

[85] Vgl. DIN ISO 37000, Normabschnitt 3.

[86] 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.

[87] Vgl. DIN ISO 37000, Normabschnitt 1.

[88] Die Inhalte zur Governance-Compliance finden sich bei *Scherer*, Nachhaltige Führung von Organisationen (Governance) nach DIN ISO 37000 - erfolgreich umsetzen, auditieren und reporten, Herausgeber DIN, Beuth Verlag, 2025.

Relevante Referenzgrößen inkl. Standards für Governance[89]

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

Organe[90]

Organe: 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?

Organe: Interaktion

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

Organe: Kompetenzen

- Wird die Zusammensetzung des Managements (Aufsichtsgremien/Vorstand/Geschäftsführung/erweiterte Geschäftsleitung) 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.

14. Governance-Compliance-Zertifizierungen

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. Vier der vom Autor[91] im Bereich Compliance betreuten Mandanten gehören zu den deutschlandweit ersten sieben Unternehmen, die von der einzigen[92] für ISO 37301- (CMS) bzw. 37001 (Antikorruption)-akkreditierten Zertifizierungsstelle zertifiziert wurden:

---

[89] Vgl. DIN ISO 37000, Normabschnitt 2.

[90] Vgl. DIN ISO 37000, Normabschnitt 4.3.

[91] Über die *Governance Solutions GmbH*.

[92] Stand 05/2025.

Referenzen:

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

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

„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“

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

„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

„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."

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

15. 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)[93] 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 bis 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[94] - *enthaftende Wirkung für Geschäftsführung, Aufsichtsrat, Management, Abteilungsleiter, Compliance- und Risikomanager und sonstige Beschäftigte*.[95]

---

[93] *Gleißner/Günther/Walkshäusl*, Financial sustainability: measurement and empirical evidence, in: Journal of Business Economics, 92, p. 467–516 sowie *Gleißner/Romeike*, Financial sustainability and risk management, in: FIRM Yearbook 2023, S. 125-127.

[94] BGH 2017: („KMW“), Urteil vom 09.05.2017; BGH 2022: („Selbstreinigung“), Urteil vom 27.04.2022; BGH 2023 („Geschäftsverteilung“), Urteil vom 09.11.2023; EuGH 2023: („Deutsche Wohnen“), Urteil vom 05.12.2023; EuGH 2023: („Hackerangriff“), Urteil vom 14.12.2023; EuGH 2024: („USt-Betrug“), Urteil vom 30.1.2024; EuGH 2024: („Juris“), Urteil vom 11.04.2024; OLG Stuttgart, („Mitarbeiter-Exzess“)

[95] Vgl. *Scherer*, Nachhaltige Führung und Überwachung von Organisationen (Governance) nach DIN ISO 37000 - erfolgreich umsetzen, auditieren und reporten, Herausgeber DIN, DIN Media-Verlag, 2025, Kapitel 4.2 Governance und Delegation.

16. Ausblick[96]

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*[97] *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“[98] und typisch menschlicher Beharrungskräfte die Organisation und ihre Menschen erfolgreich durch die Transformation zu führen.

---

[96] Sinngemäß zitiert aus Scherer, Pothorn, Jones, IT- (KI-) Governance-Compliance-Managementsystem, IT-Governance 6/2025.

[97] Vgl. *Scherer*, Nachhaltige Führung und Überwachung von Organisationen (Governance) nach DIN ISO 37000 - erfolgreich umsetzen, auditieren und reporten, Herausgeber DIN, DIN Media-Verlag, 2025, Kapitel 4.2 Governance und Delegation.

[98] Vgl. *beck-aktuell*, „Schrödingers Katze“ - Vorsätzliche Ignoranz, abrufbar unter: https://rsw.beck.de/aktuell/daily/meldung/detail/vorsaetzliche-ignoranz-justiz-behoerden-digitale-transformation-studie

Prof. Dr. jur. Josef Scherer

Rechtsanwalt Prof. Dr. Josef Scherer ist seit 1996 Professor für Unternehmensrecht (Compliance), Risiko- und Krisenmanagement, Sanierungs- und Insolvenzrecht und Leiter der Stabstelle ESGRC an der Technischen Hochschule Deggendorf. Zuvor arbeitete er als Staatsanwalt an diversen Landgerichten und Richter am Landgericht in einer Zivilkammer.

Neben seiner Tätigkeit als Seniorpartner der auf Wirtschaftsrecht und Governance, Risiko- und Compliancemanagement (GRC) spezialisierten Kanzlei Prof. Dr. Scherer & Partner mbB, erstellt er wissenschaftliche Rechtsgutachten und agiert als Richter in Schiedsgerichtsverfahren.

Seit 2001 arbeitet er auch als Insolvenzverwalter in verschiedenen Amtsgerichtsbezirken.

Prof. Dr. Scherer fungiert in diversen Unternehmen / Körperschaften als Compliance-Ombudsmann sowie externer Compliance-Beauftragter und ist gesuchter Referent bei Managementschulungen in namhaften Unternehmen sowie im Weiterbildungsprogramm des Senders BR-alpha und der virtuellen Hochschule Bayern (VHB).

In Kooperation mit TÜV konzipierte er als Studiengangsleiter und Referent den seit über 16 Jahren renommierten und akkreditierten berufsbegleitenden Masterstudiengang Risikomanagement und Compliancemanagement sowie den Zertifikatskurs Nachhaltigkeit und GRC an der Technischen Hochschule Deggendorf und ist als externer Gutachter bei der (System-)Akkreditierung von Weiterbildungsstudiengängen tätig.

Seit 2012 leitet er als Vorstand des Direktoriums das Internationale Institut für Governance, Management, Risk- und Compliancemanagement der Technischen Hochschule Deggendorf als Kompetenzzentrum.

Außerdem ist er seit 2015 Mitglied des Beirates des Instituts für Risikomanagement und Regulierung (FIRM), Frankfurt (www.firm.fm).

Seit 2016 ist er Mitglied des DIN-Normenausschusses Dienstleistungen (Arbeitsausschuss Personalmanagement NA 159-01-19 AA) zur Erarbeitung von ISO/DIN-Standards im Personalmanagement und seit 2017 Mitglied der Delegation ISO TC 309 Governance of organizations (Arbeitsausschuss Governance und Compliance NA 175-00-01-AA zur Erarbeitung von ISO/DIN-Standards im Bereich Unternehmensführung und -überwachung (Corporate Governance), Compliance und Whistleblowing).

Ebenso seit 2016: Fachlicher Leiter der User Group „Nachhaltige Unternehmensführung und Compliance“ der Energieforen Leipzig und seit 2018 Mitglied der Arbeitsgruppe 252.07 von Austrian Standards International zur Erarbeitung einer ÖNORM 4900 ff. (Risiko-Managementsystem-Standards).

Seine Forschungs- und Tätigkeitsschwerpunkte liegen auf den Gebieten Nachhaltigkeit (ESG/CSR), Managerenthaftung, Governance-, Risiko- und Compliancemanagement, Integrierte Human Workflow Managementsysteme und Digitalisierung sowie Vertrags-, Produkthaftungs-, Sanierungs- und Insolvenzrecht, Arbeitsrecht und Personalmanagement.

Prof. Dr. Scherer ist auf dem Gebiet angewandte Forschung und Lösungen / Tools im Bereich ESG/GRC, Digitalisierung und integrierte Workflow-Managementsysteme Gesellschafter-Geschäftsführer der Governance-Solutions GmbH und Aufsichtsrat in diversen Unternehmen und Stiftungen.