06.25

Juli 2025
Seiten 284–296

www.ZIRdigital.de

ZIR

Zeitschrift Interne Revision

Fachzeitschrift für Wissenschaft und Praxis

Herausgeber:
DIIR Deutsches Institut für Interne Revision e.V.

Wissenschaft - Forschung

PROF. DR. JOSEF SCHERER · GÜLSAH ATAY · ANNA KLINGER

Interne Revision, risikobasierter Ansatz und Kardinalpflicht zur Governance-Compliance

Das Wichtige richtig machen, statt blind in Haftung und Versicherungsverlust zu segeln[1]

Prof. Dr. Josef Scherer *ist Rechtsanwalt und Leiter des Internationalen Instituts für Governance, Management, Risk und Compliance und der Stabsstelle ESGRC der Technischen Hochschule Deggendorf.*
Gülsah Atay, *Cand. M.A. Risiko- und Compliance-Management, ist Mitarbeiterin der Stabsstelle ESGRC der Technischen Hochschule Deggendorf.*
Anna Klinger, *Cand. M.A. Risiko- und Compliance-Management, ist Mitarbeiterin im Referat Compliance und der Stabsstelle ESGRC der Technischen Hochschule Deggendorf.*

Die Interne Revision gehört zur Third Line of Defense.[2] Revisoren[3] kümmern sich, ebenso wie Geschäftsführer, Vorstände, Aufsichtsräte, Abschlussprüfer, Compliance- und Risikomanager, IKS-Verantwortliche sowie weitere Lines-of-Defense-Funktionen, in Zeiten multipler Krisen und Transformation unter Umständen oft zu wenig um die wirklich wichtigen Dinge. Dies verursacht bei den betroffenen Organisationen häufig finanzielle Schäden, bringt sie nicht selten in vermeidbare existenzielle Schwierigkeiten und wird zumeist haftungsbewehrtes Missmanagement[4] der Organe darstellen.

Die nachfolgende Abhandlung beleuchtet die Rolle der Revisoren und der Organe der weiteren Lines-of-Defense-Funktionen. Diese haben sich zum einen bei auftretenden Problemen in ihrem Scope beziehungsweise Prüfbereich zu rechtfertigen. Zum anderen wird aufgezeigt, dass umgekehrt gute, risikobasierte (Revisions-)Prüfungen 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."[5]

1. Einleitung

Neben dem nachgewiesen drastisch steigenden Risiko der persönlichen Haftung[6] droht aufgrund des von aktueller Rechtsprechung[7] angenommenen Vorwurfs der „Verletzung von Kardinalpflichten"[8] und der daraus abgeleiteten Indikation einer

1 Abgeändertes Zitat von OLG Frankfurt am Main, Beschluss vom 16. Januar 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. Vgl. zur ausführlichen Langversion dieser Abhandlung Scherer, J. (2025), Kardinalpflichten und risikobasierter Ansatz, Risknet.de, 5/2025, zum kostenlosen Download im Internet.

2 Vgl. Scherer, J., Nachhaltige Governance, Kapitel 6.4 Aufsicht, III.2 Das Lines-of-Defense-Modell, Third Line of Defense: Assurance/Revision/Internal Investigation.

3 Gender-Hinweis: Zur besseren Lesbarkeit wird in diesem Text das generische Maskulinum verwendet. Es bezieht sich selbstverständlich auf Personen aller Geschlechter und impliziert keine Benachteiligung oder Ausschließung.

4 Vgl. Scherer, J. (2019), Kapitalgeber.

5 Bayerisches Sprichwort.

6 Vgl. neben Spezialvorschriften aus dem Strafrecht und anderen Rechtsgebieten § 9 Abs. 2 OWiG.

7 OLG Frankfurt am Main, Beschluss vom 16. Januar 2025, Az. 7 W 20/24: „blind in die Krise segeln" und OLG Frankfurt am Main, Urteil vom 5. März 2025, Az. 7 U 134/23 mit einem ähnlichen Fall: Hier ist die Revision beim BGH anhängig: Az. IV ZR 66/25.

8 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 als eine elementare berufliche Pflicht eines Geschäftsführers oder Vorstandes anzusehen.

„wissentlicher Pflichtverletzung" der Verlust des Versicherungsschutzes für Manager und exponierte Funktionen, wie zum Beispiel Revisoren.

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 bezüglich des Inhalts von sogenannten Kardinalpflichten und risikobasierter Governance-Compliance, obwohl dies aktuell das Toprisiko nahezu aller Organisationen verkörpert.

Für Aufsehen sorgte 2009 ein höchstrichterliches Urteil: Der Bundesgerichtshof (BGH) verurteilte am 17. Juli 2009[9] einen Leiter einer Rechtsabteilung und Internen Revision eines Berliner Entsorgungsbetriebs wegen Beihilfe zum Betrug durch Unterlassen zu einer Geldstrafe von 120 Tagessätzen. Hintergrund war der Vorwurf gegenüber dem Leiter der Innenrevision der Berliner Stadtreinigung, er habe von überhöhten Gebührenfestsetzungen gewusst, ohne sie beim Vorstand zu beanstanden. Dadurch habe er Beihilfe zum Betrug geleistet. Hierbei referenzierte der BGH auf die sogenannte Garantenplicht, wonach für eine Strafbarkeit durch Unterlassen eine Pflicht zum Handeln bestehen muss.[10]

Die Interne Revision stellt eine „prozessunabhängige Institution innerhalb des Unternehmens dar, die Strukturen und Aktivitäten prüft und beurteilt."[11] „Bei der Überwachung der eingerichteten Corporate-Governance-Systeme wird der Vorstand regelmäßig von der Internen Revision unterstützt. Dabei prüft die Interne Revision auch das unternehmensweite Interne Kontrollsystem und Risikomanagementsystem."[12]

2. 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. Eine angemessene Risikofrüherkennung[13] muss auch Worst-Case-Szenarien berücksichtigen, alle Risiken angemessen quantifizieren, aggregieren, steuern und mit der Risikotragfähigkeit in Abgleich bringen.[14] Die Insolvenzzahlen stiegen bereits vor Trumps Zollkapriolen auf Höchstwerte.[15] 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 (Aufsichtsräte, Abschlussprüfer, Lines of Defense mit Interner Revision, Risiko- und Compliance-Management etc.) angekommen.

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

Zudem fehlt oft auch echte Governance-, Risiko- und Compliance-Kompetenz, und die GRC-Experten werden vor oft intuitiven Entscheidungen der Organe nicht hinzugezogen oder ernst genommen.[20] Diese werden vielmehr mit operativen Aufgaben, wie Schulungen und bürokratischem Reporting,[21] beschäftigt. 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 von persönlichen Sanktionen Beschäftigter oder Dritter und von erheblichen finanziellen Einbußen, die die Risikotragfähigkeit beeinträchtigen.

9 BGH, Urteil vom 17. Juli 2009, (Az 5 StR 394/08 – Berliner Stadtreinigung).
10 Vgl. hierzu ausführlich Scherer, J. (2025), Nachhaltige Governance, Kapitel 4.2 Governance und Delegation.
11 Vgl. Bungartz, O. (2021).
12 Vgl. DIIR-Revisionsstandard Nr. 3, Ziffer 9.
13 Vgl. hierzu ausführlich Scherer, J./Seehaus, P. (2024); Romeike, F. (2025).
14 Vgl. Scherer, J./Romeike, F./Gursky, T. (2021); Pätzold, A. (2025).
15 Vgl. Tagesschau (2025), Zahl der Insolvenzen steigt weiter.
16 Vgl. n-tv (2025), Ifo-Chef hält neue Weltwirtschaftskrise für möglich.
17 Vgl. Scherer, J./Romeike, F./Gursky, T. (2021).
18 Vgl. Scherer, J. (2025), Basel IV.
19 Vgl. Scherer, J. (2025), Basel IV.
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 sie nicht sanktionierte.

„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]

3. Eventuelles Versagen von Risikomanagement, Aufsichtsorganen, Prüfern und Lines of Defense

Am 11. November 2024 meldeten die Medien, die BaFin ordne die Überprüfung der BayWa-Bilanz an. Es gäbe konkrete Anhaltspunkte für Verstöße gegen Rechnungslegungsvorschriften. Die Darstellung der finanziellen Lage und der Risiken aus der Finanzierung des Konzerns sei möglicherweise fehlerhaft. Im uneingeschränkten Testat zum Geschäftsbericht 2023 verzichtete die Wirtschaftsprüfungsgesellschaft PwC auf Hinweise zur angespannten finanziellen Lage des Unternehmens, die allerdings längst bekannt war. Inzwischen seien circa eine Milliarde Fresh Money ausgereicht worden, so Presseberichte.[23]

Nicht nur bei Wirecard haben nach allgemeiner Meinung sämtliche Aufsichtsmechanismen kläglich versagt.[24]

Bei den insolventen Unternehmen Helma AG und Creditshelf AG kam eine nachträgliche Überprüfung des Geschäftsberichts zum Schluss, dass unter Umständen die „gesetzlich gebotenen Mindestanforderungen an das Risiko- und Krisenfrüherkennungssystem nicht umgesetzt worden waren."[25] „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. […] (Es) ist festzuhalten, dass die Verpflichtung für ein leistungsfähiges Krisen- und Risikofrüherkennungssystem selbstverständlich bei Vorstand und Aufsichtsrat liegt und auch den Aufsichtsrat hier in die Haftung nimmt."[26]

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 circa 37 Prozent der möglichen Punkte:[27] „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 […]."[28] Inzwischen veröffentlichte das Institut der Wirtschaftsprüfer den IDW ES 16 zur Prüfung der Umsetzung der Anforderungen aus § 1 StaRUG.[29] Dieser Entwurf beinhaltet noch zahlreiche Schwachstellen und bleibt hinter den Anforderungen des Gesetzgebers und des DIIR-Revisionsstandard Nr. 2 erheblich zurück.

Die Welt der Überwacher[30] 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 bei der BayWa AG, bei denen 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.

Bereits Michel Barnier, ehemaliger EU-Binnenmarktkommissar, hatte im Zuge der Finanzkrise ambitionierte Reformen angestoßen, um die Unabhängigkeit der Wirtschaftsprüfer zu stärken.[31]

22 Zitat aus Gleißner, W./Weissmann, K. (2023), Die strategischen Herausforderungen deutscher Unternehmen, Die Deutsche Wirtschaft, 13. Dezember 2024.
23 Vgl. FAZ (2024), Prüfung des Konzernabschlusses von Baywa.
24 Vgl. Gleißner, W. (2020), Wirecard: Schwächen bei Risikomanagement und Abschlussprüfung; Glaser, C. (2021), Und täglich grüßt… Wirecard.
25 Vgl. Gleißner, W./Wolfrum, A. (2024).
26 Zitat aus Gleißner, W./Wolfrum, A. (2024).
27 Vgl. Jungesblut, S. (2024).
28 Zitat aus Jungesblut, S. (2024).
29 Vgl. Romeike, F. (2025).
30 Vgl. Scherer, J. (2027), Welten.
31 Vgl. Romeike, F./Hager P. (2020), Finanzkrise legt Schwächen bei Wirtschaftsprüfern offen, RiskNET.de, 14. Oktober 2020, 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.

4. Beispiel für Wichtiges: IT/KI-Risiken bei Governance und Risikofrüherkennung

Das mittelfristige Toprisiko Nr. 1 des Global Risks Report 2024 war aufgrund der Entwicklungen der künstlichen Intelligenz (KI) das Thema Desinformation und Manipulation.[32]

Zu den größten Sorgen der CEOs weltweit gehörten auf Platz 1 die Cyber Risks.[33] Auch 2025 haben sich diese Risikoeinschätzungen kaum verändert.[34] Die sich weiterhin zuspitzende Cyberbedrohungslage inklusive Bedrohungspotenziale durch die Nutzung von KI 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.[35]

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."[36]

Erschwerend wirkt sich bei der Erfüllung der Anforderungen aus Governance-Compliance aus, dass bereits mangels Legaldefinition Unklarheit bezüglich 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 existenzgefährdenden Ergebnissen führt. In der Regel sind nicht bestandsgefährdende Einzelrisiken, sondern die kumulierende Wirkung vieler Einzelrisiken fatal. Daher ist eine methodisch fundierte Aggregation der Risiken wichtig.[37]

5. Governance-Compliance

Vor Jahrzehnten war der Bereich der Unternehmensführung und Überwachung im Wesentlichen betriebswirtschaftlich geprägt und einer juristischen Bewertung sowie einer Standardisierung noch entzogen.[38] Mittlerweile hat sich das grundlegend geändert, und die Governance-Compliance[39] wurde zu einem der relevantesten Rechtsgebiete für Organe und Führungskräfte. Governance lässt sich juristisch als die „nachhaltige Compliance- und risikobasierte, gewissenhafte Führung und Überwachung von Organisationen inklusive Interaktion mit relevanten Stakeholdern" definieren. Das Governance-Compliance-Management-System ist eine Aufbau- und Ablauforganisation, bestehend aus Komponenten (zum Beispiel Rollen, Ziele, Ressourcen, Prozessabläufe, Delegationen und Interaktionen), 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. Jeder einzelne Bereich besteht wiederum aus diversen interdisziplinären Komponenten, weshalb bei Governance nicht nur Fachspezialisten, sondern häufiger Generalisten benötigt würden.

> In der Regel sind nicht bestandsgefährdende Einzelrisiken, sondern die kumulierende Wirkung vieler Einzelrisiken fatal.

Beispiel IT-(KI-)Governance: IT-(KI-)Governance stellt denjenigen Teil der Aufbau- und Ablauforganisation beziehungsweise des integrierten IT-(KI-)Governance-Management-Systems dar, der sich unter anderem bezieht auf IT-Compliance-Management (dies an erster Stelle!), IT-Risikomanagement, IT-Strategie, IT-Planung, IT-Umsetzung, IT-Prozesse, IT-IKS, IT-Revision, IT-Steuerung und -Überwachung, IT-Reporting, IT-Management, IT-Sicherheitsmanagement, Informationssicherheitsmanagement, Datenschutz, Digitalisierung inklusive Nutzung von KI, IT-Social Engineering etc.

32 Vgl. WEF (2024).
33 Vgl. PwC (2024), PwC's 27. Annual Global CEO Survey.
34 Vgl. WEF (2025); PwC (2025), PwC's 28. Annual Global Survey 2025.
35 Zitiert aus Scherer, J./Pothorn, A./Jones, M. (2025).
36 Vgl. Scherer, J. (2025), Nachhaltige Governance, Kapitel Einleitung.
37 Vgl. Romeike, F. (2025a): Qualitative Methoden zur Risikoaggregation sind eine Fiktion; Scherer, J. (2025), Nachhaltige Governance, Kapitel 6.9 Risiko-Governance.
38 Vgl. Scherer, J./Fruth, K. (2015).
39 Die Inhalte zur Governance-Compliance finden sich bei Scherer, J. (2025), Nachhaltige Governance.

Ob zum Beispiel die Bereichsleitung der 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 Komiteelösung in Betracht.

6. Regulierung: Neue Spielregeln – heilsamer Druck statt Bürokratie

Die §§ 91 Abs. 2 und Abs. 3 AktG, 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,[40] IDW PS 340 und DIIR Revisionsstandard Nr.2) beziehen sich ebenso auf Governance-Risiken wie die BGH-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.[41]

Ebenso entschied das OLG Nürnberg[42] im Fall eines kleinen Unternehmens und ergänzte noch, der Geschäftsführer habe die Pflicht, für ein angemessenes und wirksames Compliance-Management-System, Risikomanagementsystem und Internes Kontrollsystem 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. Wichtig: In diesem Fall ging es nicht um Insolvenz- oder Krisenvermeidung, sondern um die Pflicht zur generellen Schadensvermeidung.[43]

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, Revisoren 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 bis 2005 und 2006 bis 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.

Die durchschnittliche Vergleichssumme der 50 größten US-Haftungs-Gerichtsurteile von 2014 bis 2018 hat sich von 28 auf 54 Millionen US-Dollar fast verdoppelt.[44]

> „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."[45]

> „D&O-Versicherung: Manager werden öfter zur Kasse gebeten: […] Die Versicherer rechnen damit, dass Schadenersatzforderungen gegen Manager künftig zunehmen werden. […] Dabei steigen die Schäden schneller als die Beitragseinnahmen. Die in Deutschland tätigen Managerhaftpflicht-Versicherer haben 2023 erneut mehr Schäden regulieren müssen. […] Die Entwicklung führen die Versicherer auf die konjunkturelle Lage und höhere gesetzliche Anforderungen zurück. […] Dazu kommen stetig wachsende Compliance-Anforderungen. Manager haften persönlich, wenn sie kein funktionierendes Compliance-System eingerichtet haben. […]"[46]

Hinweis: Die neue DIN ISO 37301:2021(CMS) enthält alleine schon circa 60 BGH-Entscheidungen zur rechtssicheren Organisation.[47]

40 Vgl. Romeike, F. (2025).
41 Z. B. BGH vom 19. Juni 2012, II ZR 243/11 und BGH vom 23. Juli 2024, II ZR 206/22.
42 OLG Nürnberg, Urteil vom 30. März 2022, Az. 12 U 1520/19 „Tankstellenpächter".
43 Vgl. hierzu ausführlich Scherer, J./Seehaus, P. (2024).
44 Vgl. beck-aktuell (2020), Allianz: Haftungsrisiken für Unternehmer steigen, 9. September 2020.
45 Zitat aus beck-aktuell (2024), Allianz: Chefposten werden riskanter – mehr Klagen erwartet, 5. Dezember 2024.
46 Zitat aus Gesamtverband der Deutschen Versicherer (2024), D&O-Versicherung: Manager werden öfter zur Kasse gebeten, 1. Oktober 2024.
47 Vgl. Scherer, J. (2022), Compliance-Management-System, S. 40, Fn. 96 mit Verweis auf Rack.

8. Haftungsverschärfung durch jüngste Kardinalpflicht-Rechtsprechung

Neben des nachgewiesen drastisch steigenden Risikos der persönlichen Haftung droht aufgrund des von aktueller Rechtsprechung des OLG Frankfurt am Main[48] angenommenen Vorwurfs der „Verletzung von Kardinalpflichten" und der daraus abgeleiteten Indikation einer „wissentlichen 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."

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. Januar 2005, Az. VIII ZR 121/04).

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:[49]

„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,[50]
- das Unternehmensvermögen nicht für unternehmensfremde Zwecke zu verwenden,[51]
- bei Insolvenzreife rechtzeitig einen Insolvenzantrag zu stellen,
- sich jederzeit über die wirtschaftliche Lage der Gesellschaft zu vergewissern[52] und eingehend zu prüfen, ob Insolvenzreife vorliegt."

Die aktuelle Rechtsprechung erweitert diese Fallgruppen nun auf die Pflicht zur Risiko- beziehungsweise Krisenfrüherkennung und zum Krisenmanagement und auf die „vielfältigen Pflichten in Bezug auf die Unternehmensleitung, die mit Eintragung als Geschäftsführer einer Kapitalgesellschaft verbunden sind."

> Kardinalpflichten sind „elementare berufliche Pflichten, deren Kenntnis nach der Lebenserfahrung bei jedem Berufsangehörigen vorausgesetzt werden kann."

Zitat:[53] „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 Aktiengesellschaft zur gewissenhaften Geschäftsführung) inklusive § 93 Abs. 1 S. 2 mit der Obliegenheit zur Einhaltung der sogenannten Business Judgment Rule eine Rechtsnorm, die zu den Kardinalpflichten zählt. Und für Aufsichtsräte ist § 116 AktG, der auf § 93 AktG verweist, einschlägig.

Somit ist die Governance-Compliance[54] zurecht als eine elementare berufliche Pflicht eines

48 OLG Frankfurt am Main, Beschluss vom 16. Januar 2025, Az. 7 W 20/24: „blind in die Krise segeln" und OLG Frankfurt am Main, Urteil vom 5. März 2025, Az. 7 U 134/23 mit einem ähnlichen Fall: Hier ist die Revision beim BGH anhängig: Az. IV ZR 66/25.

49 Zitat aus Wikipedia, Kardinalpflicht/Kardinalpflichten bei der Geschäftsführung, https://de.wikipedia.org/wiki/Kardinalpflicht (Stand: 01.07.2025).

50 Vgl. hierzu BGH, Urteil vom 10. Januar 2023, Az. 6 StR 133/22 („Vergütung VW-Betriebsräte") und BGH, Urteil vom 10. Februar 2022, Az. 3 StR 329/21 („Haftung von Vorständen wegen Untreue bei Entscheidungen bei mangelhafter Informationsgrundlage").

51 Vgl. die BGH-Entscheidung „Schloss Eller" (BGH, Urteil vom 10. Juli 2018, Az. II ZR 24/17).

52 Vgl. BGH vom 19. Juni 2012, II ZR 243/11 und BGH vom 23. Juli 2024, II ZR 206/22 und OLG Nürnberg, Urteil vom 30. März 2022, Az. 12 U 1520/19 „Tankstellenpächter".

53 OLG Frankfurt am Main, Urteil vom 5. März 2025, Az. 7 U 134/23: Hier ist die Revision beim BGH anhängig: Az. IV ZR 66/25.

54 Die Inhalte zur Governance-Compliance finden sich bei Scherer, J. (2025), Nachhaltige Governance.

Geschäftsführers, Vorstandes oder Aufsichtsrats anzusehen.

9. 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). Die Rechtsprechung zog schnell nach und erweiterte die Pflicht auf nicht bestandsgefährdende Risiken:[55]

> Governance-Compliance ist als elementare berufliche Pflicht eines Geschäftsführers, Vorstandes oder Aufsichtsrats anzusehen.

Nichtige Vorstandsentlastung wegen nicht angemessenen Risikomanagementsystems: Das Landgericht München I[56] entschied bereits 2007, die Entlastung des Vorstands eines Münchener Unternehmens sei nichtig (unwirksam), weil die Dokumentation der Prozessabläufe und der Verantwortlichkeit des Risikomanagementsystems unterlassen wurde. Die Entscheidung des Landgerichts enthält auch Ausführungen, die sich dahingehend interpretieren lassen, dass das einzurichtende und zu dokumentierende (!) Risikomanagementsystem nicht ausschließlich bestandsgefährdende Risiken, sondern auch allgemeine Risiken zu behandeln habe.[57] 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 sich zumeist nicht ein einziges Risiko 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).[58]

Unzureichendes Risikomanagement und unzureichende 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."[59] Durch ein funktionierendes Risikomanagementsystem wäre hier großer Schaden vermieden worden (circa 73 Millionen Euro angemeldete Forderungen seitens der Gläubiger der Gruppe, circa 50 Millionen davon wurden durch den Insolvenzverwalter festgestellt). Über Unternehmensfortführung, übertragende Sanierung, Absonderungen, Verwertung etc. konnten bisher an die Gläubiger circa 17 Millionen Euro zurückfließen. Der Rest bleibt wohl unwiederbringlich verloren.

10. Legalitätspflicht als Kardinalpflicht

Das Legalitätsprinzip[60] beziehungsweise 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:

55 Vgl. Scherer, J. (2025), Nachhaltige Governance, Kapitel 6.9 Risiko-Governance.

56 Vgl. LG München I, Urteil vom 5. April 2007 (Az. 5 HKO 15964/06 – „Risiko"); BFH, NJW (2008), S. 319; Theusinger, I./Liese, J. (2008), Besteht eine Rechtspflicht zur Dokumentation von Risikoüberwachungssystemen? NZG, 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.

57 Theusinger, I./Liese, J. (2008), Besteht eine Rechtspflicht zur Dokumentation von Risikoüberwachungssystemen? NZG, S. 290.

58 Vgl. Scherer, J./Seehaus, P. (2024).

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

60 Vgl. BGH, Urteil vom 27. August 2010, Az. 2 StR 111/09 (RWE-Tochter: Müllentsorgung und schwarze Kassen"), kommentiert in Scherer, J. (2019), Kapitalgeber.

Beginnend mit dem berühmten Neubürger-Urteil des LG München vom 10. Dezember 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-Management-System einzurichten.[66]

Flankierend dazu entschied der BGH im Buchhändler-Urteil,[67] ein beruflich Tätiger habe das erforderliche Wissen bezüglich 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 das 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 voraussetzen würde, wird durch den Hinweis des BGH (Beschluss vom 21. Mai 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, beziehungsweise dieses Amt niederlegen. [...]"[70]

Es ist nicht einfach, stets alle Compliance-Anforderungen zu erfüllen. Es wird aber bezüglich 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-Management-Systems: Bei Pflichtverstößen unterhalb der Leitungsebene kann bei Existenz eines Compliance-Management-Systems der Vorwurf des Organisationsverschuldens im Sinne einer Aufsichtspflichtverletzung entfallen.

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

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

61 Im Zentrum stand die Frage, ob der ehemalige Siemens-Vorstand 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. November 2015 („Schienenkartell").
63 Urteil vom 11. September 2013 („Libor-Manipulation").
64 Urteil vom 15. Januar 2013 („unternehmenszweckwidrige Derivate") und vom 9. Mai 2017 („Panzerhaubitzenfall").
65 OLG Nürnberg, Urteil vom 30. März 2022, Az. 12 U 1520/19 („Tankstellenpächter").
66 Vgl. Scherer, J. (2022), Compliance-Management-System, S. 39.
67 BGH, Urteil vom 18. November 2020, Az. 2 StR 246/20.
68 Vgl. Scherer, J. (2022), Compliance-Management-System, „Wer soll das alles wissen?", S. 233.
69 Vgl. Herdter, M. (2020).