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

Gülsah Atay

Cand. M. A. Risiko- und Compliancemanagement THD, B.A. Betriebswirtschaft, Mitarbeitende in der Stabsstelle ESGRC der Technischen Hochschule Deggendorf

Anna Klinger

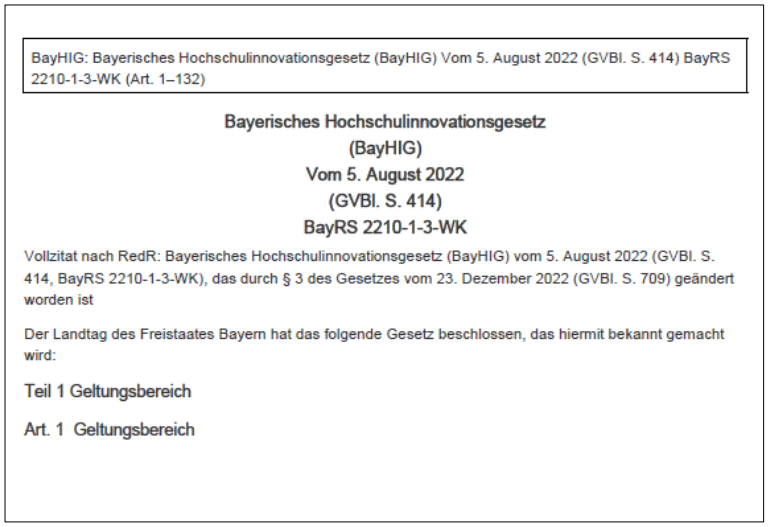
Cand. M. A. Risiko- und Compliancemanagement THD, B.A. Betriebswirtschaft, Mitarbeitende im Referat Compliance und Stabsstelle ESGRC der Technischen Hochschule Deggendorf

Kardinalpflichten und Haftung der Leitung Bayerischer Hochschulen

-das Wichtige richtig machen: Governance-Compliance

Prof. Dr. Josef Scherer, Cand. M.A. Gülsah Atay, Cand. M.A. Anna Klinger,

11.05.2025



BayHIG: Bayerisches Hochschulinnovationsgesetz (BayHIG) Vom 5. August 2022 (GVBl. S. 414) BayRS 2210-1-3-WK (Art. 1–132)

Bayerisches Hochschulinnovationsgesetz
(BayHIG)
Vom 5. August 2022
(GVBl. S. 414)
BayRS 2210-1-3-WK

Vollzitat nach RedR: Bayerisches Hochschulinnovationsgesetz (BayHIG) vom 5. August 2022 (GVBl. S. 414, BayRS 2210-1-3-WK), das durch § 3 des Gesetzes vom 23. Dezember 2022 (GVBl. S. 709) geändert worden ist

Der Landtag des Freistaates Bayern hat das folgende Gesetz beschlossen, das hiermit bekannt gemacht wird:

Teil 1 Geltungsbereich

Art. 1 Geltungsbereich

Summary

Die Abhandlung beleuchtet die Rolle der Organe und der „Lines of Defense“-Funktionen Bayerischer Hochschulen.[1]

Die Mitglieder der Hochschulleitung, Interne Revision und sonstige Lines of Defense-Funktionen (Compliance- und Risikomanager, IKS-Verantwortliche etc). kümmern sich in Zeiten multipler Krisen und Transformation oft zu wenig um die wirklich wichtigen Dinge.

Dies verursacht bei den betroffenen Hochschulen häufig finanzielle Schäden, bringt sie nicht selten in vermeidbare erhebliche Schwierigkeiten und wird zumeist haftungsbewehrtes Missmanagement darstellen. Eine Haftpflichtversicherung existiert für Angehörige des Öffentlichen Dienstes in der Regel nicht.

[1] 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.

Neben des nachgewiesen drastisch steigenden Risikos der persönlichen Haftung droht aufgrund des von aktueller Rechtsprechung angenommenen Vorwurfs der „Verletzung von Kardinalpflichten“ und der daraus abgeleiteten Indikation einer „wissentlicher Pflichtverletzung“ der Verlust des Haftungsprivilegs für Angehörige des Öffentlichen Dienstes.

Die Untersuchung der Geschäftsberichte von Organisationen indiziert häufig große Versäumnisse bei Governance, Risk und Compliance, also der ökonomischen Nachhaltigkeit.

Beispielsweise existiert bei den Organen (Mitglieder der Hochschulleitung), Interner Revision und Lines of Defense meist noch wenig Verständnis bzgl. des Inhalts von sog. „Kardinalpflichten“ und „risikobasierter Governance-Compliance“, obwohl dies aktuell das Top-Risiko nahezu aller Organisationen verkörpert.

Governance ist primär „Chefsache“, also von der Hochschulleitung 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 Ministeriums 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 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.

Governance heißt nicht zuletzt, im Rahmen eines effektiven Changeprozesses trotz wissenschaftlich nachgewiesener typisch menschlicher Beharrungskräfte die Organisation und ihre Menschen erfolgreich durch die Transformation zu führen.

„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.“
(Zitat aus Gleissner, Weissmann, Die strategischen Herausforderungen deutscher Unternehmen, Die Deutsche Wirtschaft, 13.12.24)

1. Breaking News und Top Risks für Hochschulen

Cyber-Angriffe

Weltweit werden Universitäten und Forschungseinrichtungen zunehmend Opfer von Cyberkriminalität. Die Motive der Angreifer reichen von Datendiebstahl über finanzielle Erpressung bis hin zu Sabotageakten. Die zunehmende Digitalisierung und die damit verbundene Vernetzung von Systemen erhöhen die Angriffsflächen und machen Hochschulen zu attraktiven Zielen für Cyberkriminelle.

Die *Universität der Bundeswehr München* wurde im Januar 2025 Ziel eines schweren Cyberangriffs.[2] Die *Hochschule Kempten* „erwischte" es im Februar 2024[3] und die *University of Applied Sciences in Frankfurt* im Juli 2024.[4] Dies sind nicht die einzigen Fälle und viele werden noch folgen.

Spionage und Verstöße gegen Außenwirtschaftsrecht

Ein weiteres Risiko ist in der Zusammenarbeit zwischen deutschen Hochschulen und ausländischen (z.B. chinesischen, indischen oder sonstigen in militärischen oder wirtschaftskriminellen Konflikten auch mittelbar verwickelten Nationen) Forschungs- oder gar Militäreinrichtungen angelegt. Gemäß der internationalen Recherche „*China Science Investigation*" hätten deutsche Universitäten in zahlreichen Fällen mit chinesischen Partnern, die enge Verbindungen zum Militär aufwiesen, kooperiert. Diese Kooperationen beträfen Bereiche wie Künstliche Intelligenz, Robotik und andere Dual-Use[5]-Technologien, die sowohl zivil als auch militärisch genutzt werden können: Die chinesische Führung nutze das aus diesen Kooperationen gewonnene Wissen für die strategische Aufrüstung des Militärs.[6]

Die deutschen Aufsichtsbehörden fordern eine stärkere Sensibilisierung der Wissenschaft in Exportkontrolle und warnten eindringlich vor den Risiken solcher Kooperationen. Es seien klare Richtlinien und Kontrollen notwendig, um Spionage und Missbrauch von Forschungsergebnissen zu verhindern.[7]

Governance-Verstöße, Veruntreuung, Urheberrechtsverletzungen, Steuerhinterziehung u.v.m.

Ein „*Bling-Bling-Professor*"[8] sei wegen Steuerhinterziehung in 32 Fällen sowie Untreue in zwei Fällen zu 18 Monaten Haft verurteilt worden. Der Skandal habe zu weiteren internen Ermittlungen innerhalb der Universität geführt.

An der *Christian-Albrechts-Universität in Kiel* sei die Präsidentin 2024 von ihrem Amt zurückgetreten, nachdem Vorwürfe der Datenmanipulation in wissenschaftlichen Arbeiten erhoben wurden, für die sie als leitende Autorin verantwortlich gewesen sei.

---

[2] Vgl. *Süddeutsche Zeitung*, Cyberkriminalität – Hacker-Angriff auf Universität der Bundeswehr, 2 / 2025, abrufbar unter: https://www.sueddeutsche.de/bayern/cyberkriminalitaet-hacker-angriff-auf-universitaet-der-bundeswehr-dpa.urn-newsml-dpa-com-20090101-250213-930-374666

[3] Vgl. *Hochschule Kempten*, Hacker-Angriff auf die Hochschule Kempten, 3 / 2024, abrufbar unter: https://www.hs-kempten.de/hochschule/aktuelles/artikel/hacker-angriff-auf-die-hochschule-kempten-2598

[4] Vgl. *Tagesschau*, Hacker Attacke auf Frankfurter University of Applied Sciences, 07 / 2024, abrufbar unter: https://www.tagesschau.de/inland/regional/hessen/hr-hacker-attacke-auf-frankfurter-university-of-applied-sciences-100.html

[5] *„„Dual Use" bezeichnet Güter, Software oder Technologien, die sowohl für zivile als auch für militärische Zwecke verwendet werden können. Solche Güter unterliegen in der Europäischen Union besonderen Exportkontrollen, um ihre Nutzung für gefährliche oder unerwünschte Zwecke zu verhindern."* Vgl. Zoll, Außenwirtschaft, Bargeldverkehr, Dual-Use-Güter, abrufbar unter: https://www.zoll.de/DE/Fachthemen/Aussenwirtschaft-Bargeldverkehr/Warenausfuhr/Waren/Dual-Use-Gueter/dual-use-gueter_node.html

[6] Vgl. *Correctiv*, Die Professorin und der Spionagevorwurf, 05.05.2025, abrufbar unter: https://correctiv.org/aktuelles/china-science-investigation/2025/05/05/die-professorin-und-der-spionagevorwurf/

[7] Vgl. *Deutscher Bundestag*, Kurzmitteilung - Sensibilisierung der Wissenschaft im Umgang mit China, vom 16.08.2023, abrufbar unter: https://www.bundestag.de/presse/hib/kurzmeldungen-963004

[8] Vgl. *Correctiv*, Die Bling-Bling Professoren aus Achen, 06 / 2024, abrufbar unter: https://correctiv.org/aktuelles/china-science-investigation/2024/06/18/die-bling-bling-professoren-aus-aachen/

An der *Hochschule für öffentliche Verwaltung und Finanzen Ludwigsburg*[9] hätten sich 2020 Ex-Kanzler und ehemaliger Rektor wegen Untreue vor Gericht verantworten müssen. Strittig sei die Rechtmäßigkeit der an Professoren ausgezahlten Zulagen gewesen.[10]
Die *Fraunhofer-Gesellschaft* sei durch mangelhafte Governance in Negativ-Schlagzeilen geraten. Der neue Präsident habe die Governance-Strukturen reformieren und für Transparenz und Integrität innerhalb der Organisation sorgen müssen.[11]

Das Risiko des Verlustes der wirtschaftlichen Existenz

Gemäß Art. 10 Abs. 5, Satz 2 BayHIG kann (im worst case) das Staatsministerium eine Hochschule ganz oder teilweise vorübergehend schließen, wenn die Ordnung und Sicherheit an der Hochschule in einem Maße gestört sind, dass sie nicht mehr zur Erfüllung ihrer Aufgaben in der Lage ist.
Bei Nichterreichung der Ziele oder finanzieller Überforderung kommen auch u.U. weniger einschneidende Maßnahmen, wie z.B. Fusionen oder Angliederungen von Hochschulen in Betracht.

Wenig Compliance- und Risiko-Managementsysteme an Bayerischen Hochschulen

Nach einer aktuellen Studie sollen ca. drei Viertel der teilnehmenden Bayerischen Hochschulen das Thema Compliance- und Risikomanagement für wichtig einstufen.
Tatsächlich implementiert sei ein Compliance- und Risiko-Managementsystem jedoch nur bei ca. 10 % der befragten Einrichtungen. Unter fünf systematisch geprüften Hochschulen verfüge keine über ein angemessenes Compliance- und Risiko-Managementsystem. Lediglich eine Hochschule habe sich in der aktiven Implementierung befunden. [12]

2. Die Rechtslage

Die Bayerischen Hochschulen unterliegen seit dem 1. Januar 2023[13] dem Bayerischen Hochschulinnovationsgesetz und werden von Präsidien geleitet (Art. 30 BayHIG). Das Präsidium besteht aus dem Präsidenten, den Vizepräsidenten und dem Kanzler und wird auch als Hochschulleitung bezeichnet. Das Präsidium ist für alle Angelegenheiten und Entscheidungen der Hochschule zuständig, sofern nicht im BayHIG andere Zuständigkeiten explizit geregelt sind.
Der Präsident ist dem Hochschulrat und dem Senat bzgl. der Ausführung deren Beschlüssen rechenschaftspflichtig und allgemein auskunftspflichtig. [14] Außerdem ist dem Hochschulrat jährlich ein

---

[9] Vgl. *NDR*, Rücktritt Kieler Uni Präsidentin, Fulda stellt Amt zur Verfügung, 02 / 2024, abrufbar unter: https://www.ndr.de/nachrichten/schleswig-holstein/Ruecktritt-Kieler-Uni-Praesidentin-Fulda-stellt-Amt-zur-Verfuegung,unikiel140.html
[10] Vgl. Stuttgarter *Nachrichten*, Zulagen Affäre in Ludwigsburg, 09 / 2020, abrufbar unter: https://www.stuttgarter-nachrichten.de/inhalt.zulagen-affaere-in-ludwigsburg-strafprozess-wird-neu-aufgerollt.1737f194-e4ed-425c-8ec9-fa21e21f5230.html
[11] Vgl. *Tagesspiegel*, „Es hat ein Versagen gegeben“: Vom Skandalbetrieb zum Vorreiter? Neuer Fraunhofer-Präsident will aufräumen, 06 / 2024, abrufbar unter: https://www.tagesspiegel.de/wissen/vom-eklat-club-zum-vorbild-die-wundersame-wandlung-der-fraunhofer-gesellschaft-11746325.html
[12] Die Zahlen stammen aus einer nicht öffentlichen Prüfmitteilung 2024.
[13] Das Bayerische Hochschulinnovationsgesetz (BayHIG) wurde am 5. August 2022 verabschiedet und trat am 1. Januar 2023 in Kraft.
[14] Art. 31 Abs. 8 BayHIG.

Rechenschaftsbericht der Hochschulleitung über die Erfüllung der Aufgaben der Hochschule zuzuleiten. Das Bayerische Staatsministerium für Wissenschaft und Kunst übt die Rechtsaufsicht über die Hochschulen aus.[15]

Das Präsidium einer seit dem HIG auch *unternehmerisch* tätigen Hochschule hat bei der Wahrnehmung der Leitungsaufgaben zumindest in diesem Bereich die Sorgfalt einer ordentlichen und gewissenhaften Geschäftsleitung bzw. die allgemeinen Sorgfaltspflichten für Kaufleute anzuwenden.[16]

Nach § 130 OWiG hat die Hochschulleitung eine Organisations- und Überwachungspflicht hinsichtlich aller von der Hochschule durchgeführten unternehmerischen Tätigkeiten.[17]

Daraus ergeben sich für die Organe der Hochschule bzw. Mitglieder des Präsidiums die Pflicht zum Vorhalten eines angemessenen und wirksamen Risiko- und Compliance-Managementsystems, das die (Compliance-) Risiken identifiziert, quantifiziert, aggregiert und angemessen steuert.[18]

Auch bei öffentlich-rechtlichem Handeln unterliegen Organe und Beschäftigte von Hochschulen den Strafgesetzen, sogar mit z.T. erheblichen Verschärfungen für Amtsträger. Ebenso kommt hier persönliche zivilrechtliche Haftung mit gewissen Privilegien (z.B. § 839 BGB, Art. 34 GG) in Betracht.

3. Beispiele unternehmerischer Tätigkeit Bayerischer Hochschulen

Neben ihren originären Aufgaben in Forschung und Lehre übernehmen Hochschulen seit Inkrafttreten des HIG zunehmend auch unternehmerische Funktionen, wodurch sich ihre institutionelle Komplexität sowie die Risikolage erheblich erweitern. Dies zeigt sich exemplarisch in folgenden Bereichen:

- Ausgründungen von Start-ups, insbesondere in technologisch oder medizinisch geprägten Disziplinen, bei denen Hochschulen als Mitgesellschafter auftreten, infrastrukturelle Ressourcen bereitstellen oder durch ihr Know-how unterstützen.[19]

- Drittmittelfinanzierte Forschungsvorhaben: In Kooperation mit Industriepartnern, oft im Rahmen öffentlich geförderter Innovationsprogramme, bergen diese das Risiko eines Spannungsverhältnisses zwischen kommerziellen Interessen und wissenschaftlicher Unabhängigkeit mit Fragestellungen im Zusammenhang mit Patenten, Verwertungsrechten oder der wissenschaftlichen Publikationsfreiheit.[20]

---

[15] Art. 10 Abs. 1 Satz 1 BayHIG.
[16] Vgl. *Ellerich/Tüscher* in Handbuch Hochschulmanagement, 2018, S. 90: §§ 43 GmbHG, 93 AktG, 347 HGB, 130, 30, 9 OWiG.
[17] Vgl. *Weber* in Compliance in Hochschulen (Handbuch), 2019, S. 34.
[18] Diese Rechtsansicht wird auch vom Bayerischen Obersten Rechnungshof geteilt.
[19] Vgl. *Forschung und Lehre*, Hochschulen bringen immer mehr Start Ups hervor, abrufbar unter: https://www.forschung-und-lehre.de/management/hochschulen-bringen-immer-mehr-start-ups-hervor-6956
[20] Vgl. *SpringerLink*, Erfindungen und IP-Rechte in F&E-Kooperationen, 2014. S.93-107, abrufbar unter: https://link.springer.com/chapter/10.1007/978-3-642-54994-6_4

- Wirtschaftsnahe Aktivitäten im Rahmen von Betrieben gewerblicher Art (BgA)[21]: Etwa durch An-Institute, Technologie- und Gründerzentren, Beratungs- oder Weiterbildungsangebote, unterliegen diese steuerrechtlichen Pflichten sowie allgemeinen wirtschaftsrechtlichen Rahmenbedingungen.
- Bauvorhaben, Immobilienbewirtschaftung, sowie der Betrieb campusweiter Infrastrukturen: Diese erfordern die rechtskonforme Umsetzung vergaberechtlicher Vorgaben, die Wahrnehmung umfassender Betreiberpflichten sowie die Einhaltung der Verkehrssicherungspflicht.[22]

Im Zuge des gestiegenen unternehmerischen Engagements von Hochschulen, das zunehmend als Merkmal einer modernen und leistungsfähigen Wissenschaftseinrichtung gilt und politisch befürwortet wird, verschwimmen die klassischen Grenzen zwischen öffentlichem Bildungsauftrag und marktorientiertem Handeln. Hieraus resultieren wachsende Anforderungen an eine verantwortungsvolle Governance, effektive Aufsichtsmechanismen sowie an ein systematisch verankertes Compliance-Management.

4. (Compliance-) Risikolandschaft der Hochschulen

ABBILDUNG 1: 6 TYPISCHE COMPLIANCE-RISIKEN IN WISSENSCHAFTSEINRICHTUNGEN[23]

[21] Vgl. *Bundesrechnungshof*, „Betriebe gewerblicher Art der Hochschulen – Anforderungen an Wirtschaftlichkeit und Steuerrecht“, abrufbar unter: https://www.bundesrechnungshof.de/SharedDocs/Downloads/DE/Berichte/2014/2014_Bericht_BgA_Hochschulen.pdf

[22] Vgl. *Wessels et.al.,* Rechtssichere Vergabe an Hochschulen: Risiken, Anforderungen, Handlungsempfehlungen, Hochschule und Recht, 2021/3, S. 127–134.

[23] Vgl. *Friese,* Compliance-Management an Hochschulen – Mehr als Regelkonformität?, 2012, abrufbar unter: https://www.verein-wissenschaftsrecht.de/data/file/friese.pdf

Hochschulen gelten traditionell als Orte der wissenschaftlichen Freiheit[24], der akademischen Lehre und des intellektuellen Austauschs. Weniger präsent im öffentlichen Diskurs ist hingegen, dass sie zugleich hochkomplexe Organisationen darstellen, die neben ihrer Kernaufgabe zunehmend unternehmerische, betriebswirtschaftliche und forschungspraktische Funktionen übernehmen.[25] Aus dieser strukturellen und funktionalen Vielfalt resultiert eine differenzierte (Compliance-) Risikolandschaft, die, bei unzureichender Steuerung, nicht nur Personen- und Sachschäden verursachen, sondern auch zu erheblichen haftungsrechtlichen Konsequenzen für Leitungspersonen führen kann.

Ein systematisierter Blick auf die wesentlichen Risiko- und Gefährdungsbereiche offenbart Parallelen zu industriellen Großbetrieben:

4.1 Gefahren für Leib und Leben Beschäftigter und Dritter: Physische Gefährdungen und Arbeitssicherheitsrisiken in Forschung und Lehre

Insbesondere in Laboren, Werkstätten und klinischen Forschungseinrichtungen bestehen substanzielle Gefahrenquellen. Der Umgang mit chemischen, biologischen oder radioaktiven Substanzen, der Einsatz von Hochdruck- oder Hochspannungstechnologie sowie Lasertechnik erfordert strikte Sicherheitsvorkehrungen. Unzureichende Schutzmaßnahmen oder mangelnde Unterweisungen bergen das Risiko gravierender Unfälle mit potenziell langfristigen gesundheitlichen Folgen für Studierende, Mitarbeitende und externe Dritte.[26]

Auch psychologische Gefährdungslagen mit der Gefahr schwerer Erkrankungen oder Suizid gehören zu diesem Bereich.[27] Psychische Belastungen unter Hochschulangehörigen nehmen in Folge gestiegener Leistungsanforderungen, prekarisierter Beschäftigungsverhältnisse sowie struktureller Unsicherheiten deutlich zu. Chronische Erschöpfung, Burnout oder suizidales Verhalten sind ernstzunehmende Risiken, die, insbesondere bei gravierenden Vorfällen, institutionelle Versäumnisse offenlegen können. Fehlende Präventionsstrategien und unzureichende Unterstützungsangebote berühren dabei auch die arbeitsrechtlich verankerte Fürsorgepflicht der Hochschule.[28]

Fehlende oder unzureichende Präventions- und Interventionsmechanismen im Bereich von Diskriminierung, sexueller Belästigung oder Gleichstellungsfragen[29] können zu nachhaltigen

---

[24] Vgl. *Wikipedia*, Adademische Freiheit, abrufbar unter: https://de.wikipedia.org/wiki/Akademische_Freiheit

[25] Vgl. *Böckler*, Von Humboldt zur unternehmerischen Uni - Hochschulkonzepte im Widerstreit, 09/2010, abrufbar unter: https://www.boeckler.de/de/boeckler-impuls-von-humboldt-zur-unternehmerischen-uni-hochschulkonzepte-im-widerstreit-8120.htm

[26] Vgl. *Haufe*, Sicheres Arbeiten in Laboren/2 Rechtsgrundlagen, abrufbar unter: https://www.haufe.de/id/beitrag/sicheres-arbeiten-in-laboren-2-rechtsgrundlagen-HI2225101.html

[27] Vgl. DIN ISO 45001: Betriebliches Gesundheitsmanagement

[28] Vgl. *Springer*, Gefährdungsbeurteilung psychischer Belastungen an deutschen Hochschulen, abrufbar unter: https://link.springer.com/article/10.1007/s11553-019-00743-2

[29] Vgl. *Antidiskriminierungsstelle des Bundes*, abrufbar unter: https://www.antidiskriminierungsstelle.de/DE/ueber-diskriminierung/lebensbereiche/bildungsbereiche/hochschule/hochschule.html

Vertrauensverlusten, internen Eskalationen sowie medialen Skandalen führen. Auch in diesen Fällen drohen haftungsrechtliche Konsequenzen.

Bzgl. der Einbeziehung der ebenso gefährdeten Studenten und sonstige Stakeholder in die Risikosteuerung bestehen z.T. unterschiedliche Ansichten.
Auch, wenn Studenten und Lehrbeauftrage, wie sonstige Stakeholder nicht zu den Beschäftigten i.S. des Arbeitssicherheitsrechts zählen, besteht eine organisationelle Pflicht, diese vor Gefahren des Betriebes der Hochschule zu sichern, aus §§ 130, 30, 9 OWiG mit persönlicher Haftung der Organe und exponierter Führungskräfte.

4.2 Straf- und zivilrechtliche Haftungsrisiken für Beschäftigte und fehlende Versicherung

Hochschulen sind nicht nur Bildungsstätten, sondern komplexe, risikobehaftete Akteure im Spannungsfeld zwischen Wissenschaft, Politik und Wirtschaft.
In Zeiten grundlegender Transformationen, multipler Krisen, geopolitischer Verwerfungen, finanzieller Engpässe und Fachkräftemangel steht insbesondere die Hochschulleitung zunehmend im Fokus der externen Aufsicht (Ministerien, Staatsanwaltschaft, Zoll, BAFA, Medien u.v.m.).
Schwachstellen bei Governance, insbesondere rechtssicherer Aufbau- und Ablauforganisation, Risiko- und Compliance-Managementsystem steigern die Haftungsrisiken der Mitglieder des Präsidiums, aber auch aller sonstiger Beschäftigten, nicht zuletzt aufgrund der sich verschärfenden Rechtsprechung und wachsender Sensibilität, enorm, vgl. hierzu unten Punkt 13 ff..

Verstöße gegen Strafgesetze und sonstige straf- und bußgeldbewehrte spezialgesetzliche Vorgaben können sowohl individuelle als auch institutionelle Sanktionen nach sich ziehen. Neben Sanktionen für direkte Pflichtverletzungen ist insbesondere die Organisationsverantwortung von Führungspersonen bei Aufsichtspflichtverletzungen haftungsrelevant.[30]
Die Risiken sind mannigfaltig: Vergabe- und Steuer-Verstöße, Haushaltsuntreue oder Zweckentfremdung von Drittmitteln, Scheinselbstständigkeit u.v.m..

Das Haftungsrisiko in bestimmten Bereichen abfedernde Strafrechtsschutz-, Haftpflicht- oder Vermögensschadens-Versicherungen wie in der Privatwirtschaft existieren für Beschäftigte im Öffentlichen Dienst nicht.
Da hilft nur eine rechtssichere Organisation…

4.3 Informationssicherheit, Geheimnis- und Datenschutz[31]

[30] Vgl. *DGUV*, Regelwerk Branche Hochschule, abrufbar unter: https://publikationen.dguv.de/regelwerk/dguv-regeln/4346/branche-hochschule
[31] Vgl. *Forschung und Lehre*, Was Hochschulen beim Datenschutz beachten müssen, 07/2018, abrufbar unter: https://www.forschung-und-lehre.de/management/was-hochschulen-beim-datenschutz-beachten-muessen-772/

Mit dem digitalen Wandel nimmt die Bedrohungslage im Bereich Cybersecurity und Datenschutz kontinuierlich zu. Hochschulen verarbeiten hochsensible geheimhaltungsbedürftige und personenbezogene Daten sowie forschungsrelevante Informationen mit möglicher wirtschaftlicher oder sicherheitskritischer Bedeutung. Sicherheitslücken, unzureichend geschützte Systeme oder Verstöße gegen Datenschutzvorgaben können zu erheblichen Reputationsverlusten, Schadensersatzansprüchen und regulatorischen Sanktionen führen.

Internationale Kooperationen, insbesondere mit Partnern in Drittstaaten, erfordern eine sorgfältige Risikoabwägung im Hinblick auf Exportkontrollvorschriften und sog. „dual-use"-Forschung. Ein unzureichendes Risikomanagement kann zum Abfluss sicherheitsrelevanten Know-hows, zur Unterstützung sicherheitskritischer Technologien und damit zu erheblichen rechtlichen und ethischen Konflikten führen.[32]

5. Persönliche Haftungsrisiken für Hochschulleitungen und die enthaftende Wirkung eines CMS

In diesem komplexen Umfeld trägt die Hochschulleitung, insbesondere das Präsidium, eine rechtlich bedeutsame Gesamtverantwortung für Organisation, Aufsicht und Steuerung, vgl. zur Haftungsverschärfung unten Punkt 13 ff..

Ein angemessenes, dokumentiertes und wirksames Compliance-Managementsystem (CMS) ist deshalb nicht nur ein organisatorisches Hilfsmittel, sondern eine zentrale Enthaftungsstrategie, vgl. hierzu unten Punkt 14..

Nur ein CMS, das tatsächlich gelebt und fortlaufend angepasst wird, kann dazu beitragen, Leitungsverantwortung abzusichern und den Handlungsspielraum der Hochschule rechtssicher auszugestalten.

Zu betonen ist, dass die enthaftende Wirkung bei Pflichtverstößen unterhalb der Leitungsebene nur bei einem angemessenen CMS eintreten kann.

Daran dürfte es bei den meisten Hochschulen noch mangeln, vgl. oben 2..

6. Die Hochschulleitung muss „das Wichtige richtig tun" – insbesondere bei den sogenannten „Kardinalpflichten" und der „Governance-Compliance"[33]

Nachfolgende Abhandlung zeigt, dass Mitglieder des Präsidiums unabhängig von etwaigen sonstigen Zielen aus HIG oder Zielvereinbarungen primär die *Governance-Compliance* inkl. der sog. „*Kardinalpflichten*" zu erfüllen haben.

---

[32] Vgl. *Uni Tübingen*, Exportkontrolle, abrufbar unter: https://uni-tuebingen.de/einrichtungen/verwaltung/i-universitaetsentwicklung-struktur-und-recht/abteilung-4-universitaetsentwicklung-und-compliance/exportkontrolle

[33] Vgl. für die nachfolgenden Abhandlungen ausführlich *Scherer*, Kardinalpflichten und risikobasierter Ansatz, 1.5.25, Risknet.de, abrufbar unter: https://www.risknet.de/themen/risknews/kardinalpflicht-fordert-risikobasierten-ansatz/

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.“[34]

7. 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.
Ein angemessenes Risikomanagement inkl. Risikofrüherkennung[35] muss auch worst case-Szenarien berücksichtigen, alle Risiken angemessen quantifizieren, aggregieren, steuern und mit der Risikotragfähigkeit in Abgleich bringen.[36]
Die Insolvenzzahlen stiegen bereits vor Trumps Zollkapriolen auf Höchstwerte.[37]
Obwohl inzwischen sogar eine Weltwirtschaftskrise vom Chef des Ifo-Instituts für möglich gehalten wird[38], ist der aktuelle Handlungsdruck offenbar noch nicht bei allen Organen und Überwachern (Aufsichtsgremien, Abschlussprüfern, Lines of Defense mit Interner Revision, Risiko- und Compliance-Management etc.) angekommen.
Worst case-Szenarien werden oft bewusst oder aus Ignoranz ausgeblendet.[39]
Stattdessen werden häufig die weniger werdenden Ressourcen nicht auf die wichtigen Dinge gebündelt, sondern für reine Bürokratie ohne Wertbeiträge ausgegeben.[40]
Das mag verhaltensökonomische Gründe[41] haben, liegt aber häufig auch daran, dass zum einen in den Aufsichtsratsgremien und Führungsetagen Regularien, wie § 1 StaRUG (Pflicht für Kapitalgesellschaften zur Risikofrüherkennung) oder § 93 Abs. 1 S. 2 AktG (Business Judgment Rule) nicht angemessen bekannt sind oder verstanden werden.

---

[34] Bayerisches Sprichwort.
[35] 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/
[36] 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..
[37] Vgl. *Tagesschau*, „Zahl der Insolvenzen steigt weiter“, 14.03.2025, abrufbar unter: https://www.tagesschau.de/wirtschaft/insolvenzen-anstieg-100.html
[38] 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
[39] 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/
[40] 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
[41] 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

Diese für Kapitalgesellschaften kodifizierten Rechtsfiguren sind bei unternehmerisch tätigen Hochschulen über die allgemeine Pflicht zur gewissenhaften Leitung entsprechend anzuwenden.
Oft fehlt auch echte Governance-, Risiko- und Compliancekompetenz und die GRC-Experten werden vor oft intuitiven Entscheidungen der Organe nicht beigezogen oder ernstgenommen.[42] Diese werden vielmehr mit operativen Aufgaben, wie Schulungen und bürokratischem Reporting[43] 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 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.“[44]

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

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

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[45] - zahlreiche weitere Bürokratie-Monster aufzählen, die die Administration leidvoll erträgt.

---

[42] 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.
[43] Z.B. dem LKSG-Bericht, den die BAFA nicht ernsthaft einforderte bzw. dessen Ausbleiben nicht sanktionierte.
[44] Zitat aus Gleissner, Weissmann, Die strategischen Herausforderungen deutscher Unternehmen, Die Deutsche Wirtschaft, 13.12.24.
[45] Vielmehr ist zu raten, aus Haftungsbegrenzungsgründen ein Tax-Compliance-Managementsystem gem. § 153 AO zu implementieren.

9. Beispielsfälle aus der Wirtschaft, in denen evtl. das Risikomanagement, aber u.U. auch Aufsichtsorgane, Abschlussprüfer und Lines of Defense 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. Eine renommierte Wirtschaftsprüfungsgesellschaft habe den Geschäftsbericht testiert, also abgenommen. Inzwischen seien ca. 1 Mrd. Fresh Money ausgereicht worden.[46]

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

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*."[47]

„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."[48]

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:[49]

„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 (…)"[50]

---

[46] 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

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

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

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

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

Hinweis:

Inzwischen veröffentlichte das Institut Deutscher Wirtschaftsprüfer den IDW ES 16 zur Prüfung der Umsetzung der Anforderungen aus § 1 StaRUG.[51] Dieser Entwurf beinhaltet noch zahlreiche Schwachstellen und bleibt hinter den Anforderungen des Gesetzgebers und des DIIR Nr. 2 erheblich zurück.

Die Welt der Überwacher

In der Unternehmenspraxis existiert eine Vielzahl interner und externer Prüfungs/Überwachungs-/Audit-/Konformitätsbewertungs- Funktionen:[52]

- 1st line of defense: Mitarbeiter und Kollegen, Vorgesetzte, Vorstand/Geschäftsführer.
- 2nd line of defense: Controlling, IKS, Risikomanagement, Compliance, Qualitätsmanagement sowie weitere Funktionen, ***Interne Auditoren und Managementsysteme***
- 3rd line of defense: Revision, Assurance/Internal Investigation.
- 4th line of defense: Aufsichtsrat, Medien, Third parties (audits), ***Zertifizierungsstellen,*** Staatsanwälte, Behörden, Politik, Banken, Gerichte (Straf-, Zivil-, Verwaltungsgerichte) etc.

Diese „Überwacher" gehen leider in der Praxis nicht konzertiert, sondern nebeneinander agierend vor, obwohl sie alle im Wesentlichen die gleichen Ziele verfolgen:

Transparenz über die Anforderungen, um die Unternehmensziele zu erreichen sowie adäquate, auf diese Ziele abgestimmte Kennzahlen und gelebte Prozesse, die mit den diversen Muss- und Soll-Anforderungen angereichert sind, um den beabsichtigten Output zu gewährleisten. Flankiert wird dies durch ein angemessenes und wirksames Steuerungs- und Überwachungssystem.

Die in der Praxis feststellbaren unzähligen – redundanten – Aktionen kosten erhebliche Ressourcen. Die „Welt der Überwacher“[53] schafft es offenbar trotz des hohen Ressourceneinsatzes nicht, die wirklich wichtigen Dinge effektiv zu steuern und zu überwachen.

[51] 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/

[52] Vgl. *Scherer*, Die Welt(en) der Überwacher, FIRM Jahrbuch 2017, 2017, S. 79-81, abrufbar unter: https://www.gmrc.de/images/Docs/Publikationen/Scherer_Die_Welt_en_der_Ueberwacher.pdf

[53] 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

10. 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 KI „Desinformation und Manipulation“.[54]

Zu den größten Sorgen der CEOs weltweit gehörten auf Platz 1 die Cyber Risks.[55] Auch 2025 haben sich diese Risikoeinschätzungen kaum verändert.[56]

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.[57]

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*“[58].

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.

Zwischenfazit:

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

---

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

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

[56] 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

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

[58] 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.

11. 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.

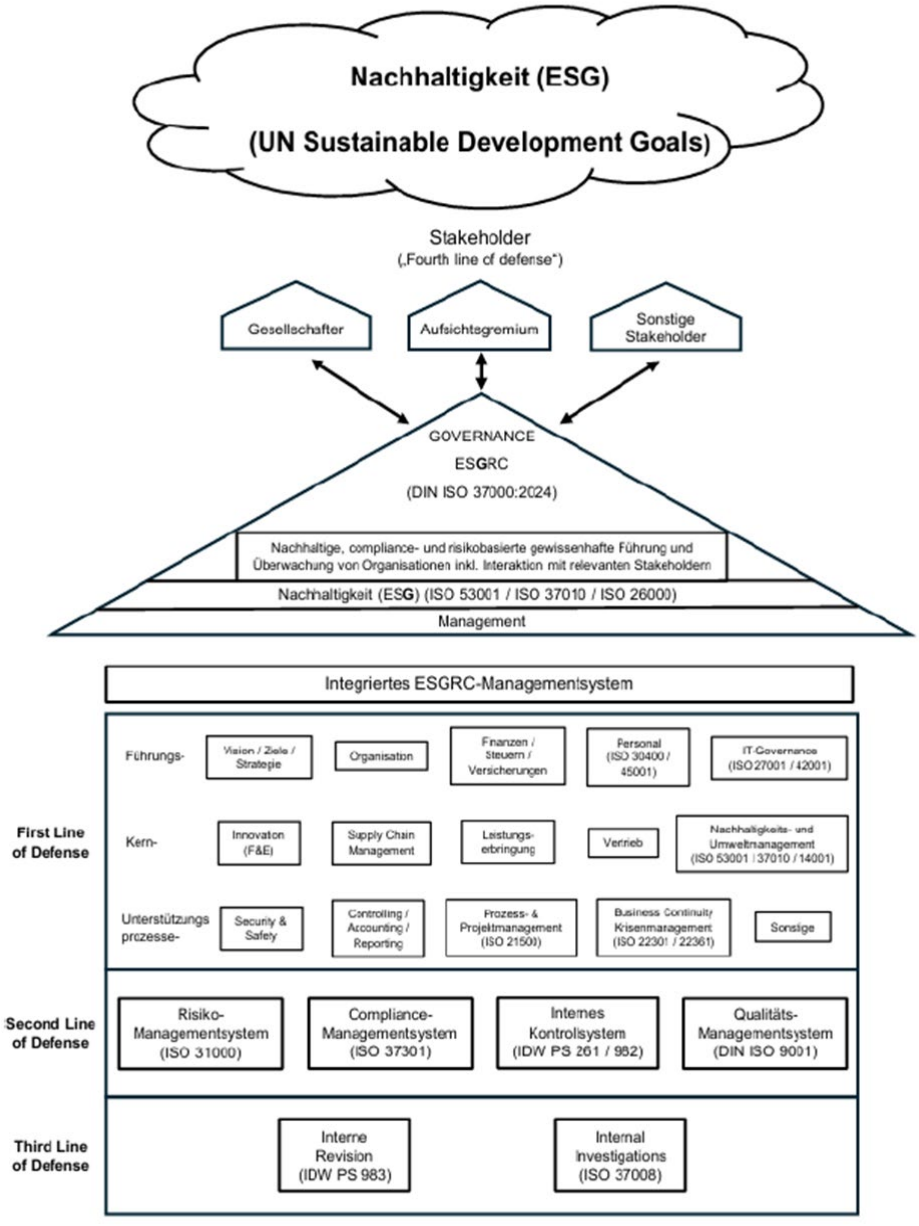


ABBILDUNG 2: DAS „ESGRC-HAUS“, EIGENE DARSTELLUNG AUS SCHERER, NACHHALTIGE FÜHRUNG UND ÜBERWACHUNG VON ORGANISATIONEN (GOVERNANCE) NACH DIN ISO 37000 - ERFOLGREICH UMSETZEN, AUDITIEREN UND REPORTEN, DIN MEDIA, 2025

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[59]) 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[60] *(…)“*
Dazu gehört mittlerweile auch KI.[61]

[59] 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.
[60] Vgl. *BGH*, Urteil vom 12.10.2016, Az. 5 StR 134 / 15 „HSH Nordbank“.
[61] 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.

12. 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 Business Continuity- und Krisenmanagement (vgl. IDW ES 16[62], IDW PS 340 und DIIR 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.[63]

Ebenso entschied das OLG Nürnberg[64] 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*.[65]

---

[62] 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/

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

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

[65] 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

13. 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 10-Jahreszeitraum von 1986 bis 1995 gab es genauso viele Verurteilungen zur Managerhaftung, wie in den letzten 100 Jahren zuvor. Für die nachfolgenden 10-Jahreszeiträume von 1996 bis 2005 und 2006 bis 2015 wurde eine nochmalige Verdoppelung gemessen bzw. geschätzt.
Die durchschnittliche Vergleichssumme der 50 größten US-Haftungs-Gerichtsurteile von 2014 bis 2018 von 28 auf 54 Millionen US-Dollar fast verdoppelt.[66]

„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.“[67]

„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. *(…)“*[68]

Der Bundesfinanzhof statuierte eine „Geschäftsführerhaftung wegen Unfähigkeit“:

---

[66] 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
[67] Zitat aus beck-aktuell, Allianz: Chefposten werden riskanter - mehr Klagen erwartet, vom 05.12.2024.
[68] Zitat aus Gesamtverband der Deutschen Versicherer, D&O-Versicherung: Manager werden öfter zur Kasse gebeten, 1.10.2024.

„[…] wer den Anforderungen an einen gewissenhaften Geschäftsführer nicht entsprechen kann, muss von der Übernahme des Geschäftsführeramtes absehen, bzw. dieses Amt niederlegen. […]“[69]

Hinweis:

Die neue DIN ISO 37301:2021(CMS) enthält ca. 60 BGH-Entscheidungen zur rechtssicheren Organisation.[70]

Haftungsverschärfung durch jüngste „Kardinalpflicht“-Rechtsprechung: „Blind in Haftung und Versicherungsverlust segeln“

Neben des nachgewiesen drastisch steigenden Risikos der persönlichen Haftung droht aufgrund des von aktueller Rechtsprechung des OLG Frankfurt am Main[71] 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[72]:

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

---

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

[70] 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.

[71] 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.**

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

- *weder sich noch Dritten aus dem Unternehmensvermögen Vorteile zu gewähren, auf die kein Anspruch besteht*[73]*,*
- *das Unternehmensvermögen nicht für unternehmensfremde Zwecke zu verwenden*[74]*,*
- *bei Insolvenzreife rechtzeitig Insolvenzantrag zu stellen,*
- *sich jederzeit über die wirtschaftliche Lage der Gesellschaft zu vergewissern*[75] *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[76]:

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

---

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

[74] 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.

[75] 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".

[76] 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."

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 wurde bereits 1998 mit dem KonTraG in § 91 AktG als gesetzliche Pflicht für Aktiengesellschaften und (analog) für große GmbHs statuiert.
Die Rechtsprechung zog schnell nach und erweiterte die Pflicht auf nicht bestandsgefährdende Risiken:[77]

Nichtige Vorstandsentlastung wegen nicht angemessenen Risiko-Managementsystems
Das *Landgericht München I*[78] 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.[79] 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".

---

[77] 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.

[78] 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.

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

Da zumeist nicht ein einziges Risiko sich als bestandsgefährdend auswirkt, sondern viele sich aggregierende Einzelrisiken, ist auch im Rahmen der Krisenfrüherkennung zunächst auf Risikofrüherkennung mit Quantifizierung und Aggregation und Abgleich mit der Risikotragfähigkeit zu achten:[80]

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.“[81]

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.

Gewissenhafte Geschäftsführung als Kardinalpflicht

Die aktuelle Entscheidung des OLG Frankfurt vom 5.3.2025 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*[82] 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

---

[80] 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

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

[82] 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.

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[83] 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[84], bzw. die Pflicht zur Compliance, also die Pflicht aller, sich an verbindliche Regeln, wie Gesetze oder Rechtsprechung zu halten, hat sich in den letzten Jahren auch in der Rechtsprechung manifestiert:
Beginnend mit dem „berühmten" „Neubürger"-Urteil des LG München vom 10.12.2013 im Siemens-Compliance-Skandal, führten das LAG Düsseldorf[85], das ArbG Frankfurt[86], der BGH[87] und aktuell das OLG Nürnberg[88] aus, das es Obliegenheit des Geschäftsführers oder Vorstands sei, ein angemessenes und wirksames Compliance-Managementsystem einzurichten.[89]
Flankierend dazu entschied der BGH im „Buchhändler-Urteil"[90], 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.[91]
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.

---

[83] Vgl. DIN ISO 37301 Normabschnitt 4.6 Compliance-Riskoanalyse und ISO IEC 31010 Risk Assessment.
[84] 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.
[85] Urteil vom 27.11.2015 („Schienenkartell").
[86] Urteil vom 11.9.2013 („Libor-Manipulation").
[87] Urteil vom 15.1.2013 („unternehmenszweckwidrige Derivate") und vom 9.5.2017 („Panzerhaubitzenfall").
[88] *OLG Nürnberg*, Urteil vom 30.3.2022, Az. 12 U 1520 / 19 („Tankstellenpächter").
[89] Vgl. *Scherer*, Compliance-Managementsystem nach DIN / ISO 37301 erfolgreich, implementieren, integrieren, auditieren, zertifizieren, DIN Media Verlag, 2022, S. 39.
[90] BGH, Urteil vom 18.11.2020, Az. 2 StR 246 /20.
[91] Vgl. *Scherer*, Compliance-Managementsystem nach DIN / ISO 37301 erfolgreich, implementieren, integrieren, auditieren, zertifizieren, DIN Media Verlag, 2022, S. 233: „Wer soll das alles wissen?".

Dass vorsätzliche Gesetzesverstöße in nahezu allen Rechtsgebieten (Strafrecht, Versicherungsrecht, Vertragsrecht etc.) streng sanktioniert werden, dürfte nicht überraschen.
Gegenmeinungen[92], 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. […]“[93]
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[94] 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.

[92] Vgl. Herdter, Die Versicherungspraxis, 6 / 2020.
[93] Vgl. Bundesfinanzhof, Beschluss vom 15.11.2022, VIII R 23/19 und *Dürr*, „Geschäftsführerhaftung wegen Unfähigkeit“, 20.03.2023.
[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 2025: („Mitarbeiter-Exzess“), Beschluss vom 25.2.2025.

14. Neue Ansätze für „Ratings“ / Bewertungen aufgrund von Angaben in Nachhaltigkeits-, Governance- oder Geschäftsberichten[95]

Ansätze zur Bewertung von Insolvenzwahrscheinlichkeit, Resilienz, Zukunftsfähigkeit u.v.m. finden sich in den Z-, O-, und Q-Score-Konzepten der Wissenschaft.[96]
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.

Obgleich zahlreiche deutsche Hochschulen in den vergangenen Jahren freiwillig Nachhaltigkeits- bzw. Umweltberichte nach EMAS, DNK oder GRI veröffentlichten, etwa die Freie Universität Berlin (vierter Nachhaltigkeitsbericht 2024[97]), die Universität Passau („Nachhaltigkeitsbericht 2024“[98]) oder die Universität Oldenburg („Nachhaltigkeitsbericht 2024“[99]), unterliegen klassische Geschäfts- bzw. Lageberichte nach betriebswirtschaftlichem Vorbild an Hochschulen bislang keiner breiten Praxis.
Die meisten Einrichtungen beschränken sich auf den nach Landesrecht vorgeschriebenen kaufmännischen Jahresabschluss mit Lagebericht (z. B. Hochschule Hannover, gem. § 49 LHO Nds. i. V. m. § 325 HGB[100]) oder auf einen narrativen „Jahresbericht“ ohne umfassende finanzielle Offenlegung. Die Rechnungslegung folgt dabei spezialgesetzlichen Vorgaben der Länder und unterscheidet sich strukturell von unternehmerischen Geschäftsberichten.[101]

Aus Compliance-Sicht empfiehlt es sich daher, hausintern zu klären, in welchem Format die Hochschule ihre unternehmerischen Aktivitäten (z. B. Weiterbildungs- und Transfergesellschaften, Vermietungen, Beteiligungen) dokumentiert:

- Werden diese bereits im Anhang des Jahresabschlusses, in separaten Spartenrechnungen oder in Nachhaltigkeitsberichten dargestellt?

---

[95] Vgl. *Gleissner, Wolfrum, Moecke*, Risikomanagement nach StaRUG und FISG, Der Aufsichtsrat, 2024, S. 110-112.
[96] 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.
[97] Vgl. *Freie Universität Berlin*, Nachhaltigkeitsbericht 2024, abrufbar unter: https://www.fu-berlin.de/sites/nachhaltigkeit/stabsstelle/kommunikation/aktuelles/241001_nachhaltigkeitsbericht.html
[98] Vgl. *Universität Passau,* Nachhaltigkeitsbericht 2024, abrufbar unter: https://www.uni-passau.de/fileadmin/dokumente/universitaet/Nachhaltigkeit/Berichte/Nachhaltigkeitsbericht_2024.pdf
[99] Vgl. *Universität Oldenburg,* Nachhaltigkeitsbericht 2024, abrufbar unter: https://uol.de/fileadmin/uni/profil/klima/Governance/Controlling/Nachhaltigkeitsberichterstattung/UOL_Nachhaltigkeitsbericht_2024.pdf
[100] Vgl. *Hochschule Hannover,* Veröffentlichungen, abrufbar unter: https://www.hs-hannover.de/ueber-uns/organisation/finanzmanagement/veroeffentlichungen
[101] Vgl. *Waltenberger*, Rechnungslegung staatlicher Hochschulen, 2006, abrufbar unter: https://www.ihf.bayern.de/uploads/media/ihf_studien_hochschulforschung-73.pdf

- Bedarf es, angesichts steigender Transparenzanforderungen mittelfristig eines integrierten Geschäfts- und Nachhaltigkeitsberichts?

Die Beantwortung dieser Fragen legt Verantwortlichkeiten fest, minimiert Haftungsrisiken und erhöht die Transparenz gegenüber Mittelgebern, Studierenden und Öffentlichkeit.

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

Für ein Governance-Scoring sollten quantitative Bewertungen – auch der Geschäftsberichte der Geschäftspartner - gegenüber qualitativen Ausführungen bevorzugt werden: *„If you can`t meassure it, you can`t manage it.“*

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 Nachhaltigkeitsberichten
Dabei sind an die Wahrheit der Nachhaltigkeitsberichte 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.[102]

In Lageberichten wird häufig sinngemäß ausgeführt:

[102] 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

„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.
Auch dies angemessen zu hinterfragen, gehört nach Ansicht des Autors zu den Aufgaben der vielen Überwachungsfunktionen *von Governance-Compliance*.[103]

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.

15. Das Wichtige richtig fragen

Für Auditoren und Zertifizierungsstellen geben die noch sehr neuen Standards DIN ISO 17021-13 und ISO 37304 wertvolle Hinweise an die erforderlichen Kompetenzen, die wiederum von der Deutschen Akkreditierungsstelle DAkkS überprüft werden.
Unabhängig davon sollte intensiv diskutiert werden, wie moderne Audits oder sonstige Überwachungsmaßnahmen durchgeführt werden sollten, um echte Wertbeiträge anstelle einer Scheinsicherheit zu kreieren.

Ein aufschlussreiches Gedankenexperiment formulierte kürzlich Mike Emerato[104] im Kontext der digitalen Transformation von Governance- und Kontrollsystemen: *„Kann eine künstliche Intelligenz künftig die Rolle des Auditors übernehmen, objektiver, schneller, umfassender als der Mensch?"* Diese Fragestellung berührt nicht nur technologische Möglichkeiten, sondern auch normative Grenzen: Wie verlässlich ist algorithmisch generierte Prüfung, wenn ethische Wertungen, Kontextwissen oder diskretionäre Abwägungen erforderlich sind? Hochschulen, die zunehmend unternehmerisch agieren, sehen sich mit der Herausforderung konfrontiert, ihre Controlling- und Berichtssysteme so

[103] 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/
[104] Vgl. *Internal Auditor*, Aufbau eines besseren Auditors: Was KI nicht kann, 06/2024, abrufbar unter: https://internalauditor.theiia.org/en/voices/2024/june/building-a-better-auditor-what-ai-cant-do

weiterzuentwickeln, dass sie auch digital-gestützten Revisions- und Compliance-Prüfungen standhalten, ohne jedoch die Verantwortung menschlicher Aufsicht vollständig zu delegieren.

Vorschlag einer Auditmethodik entlang der ISO Harmonized Structure (HS)

Die Auditcheckliste basiert auf der ISO Harmonized Structure und ordnet die relevanten Elemente systematisch den Funktionsbereichen der Organisation zu (vgl. ESGRC-Haus oder Prozessthemenfelder). Dadurch entsteht eine Auditmatrix, die eine strukturierte Prüfung ermöglicht.

I. Ablauf des Audits:

1. **Dokumentenprüfung**

- Zunächst erfolgt in „Phase 1“ (remote) eine Analyse der relevanten Dokumente. Dabei kann mithilfe von Datenanalyse und KI bereits viel Relevantes im Vorfeld eruiert werden: Internetrecherche über Berichte mit Auffälligkeiten bzgl. der zu auditierenden Organisation, Auswertung von Berichten der einzelnen Bereiche, der Internen Revision, des Ombudsmannes, von Compliance und Risk und eben auch *ehrliche und relevante Managementreviews oder Interne Auditberichte* u.v. m. bilden die Grundlage für eine KI-gestützte SWOT-Analyse.
- Auch in der Haupt-Auditphase können Dokumente, Prozessbeschreibungen, Systeme etc. mithilfe von KI ausgewertet werden.

2. **Interviews mit Funktionsbereichen**
    - Befragung risikobasiert ausgewählter verschiedener Funktionen, idealerweise in einer Kombination aus:
    - Leitungsebene als Accountable (als mögliche Prozessverantwortliche und Prozessrisikoeigner)
    - Eine niedrigere Hierarchiestufe als Responsible (als Prozessausführungsverantwortliche und mögliche Prozessrisikomelder).

II. Kernfragen im Auditprozess:

Während des Audits werden gezielt folgende Fragen gestellt:

- **Tätigkeitsbereich:** Was sind Ihre Aufgaben?
- **Organisatorische Einordnung:** Wo sind Sie im Organigramm verortet?
- **Rollen, Aufgaben, Verantwortung, Pflichten und Rechte:** Gibt es eine Stellenbeschreibung?
- **Prozessabläufe:** Gibt es für die zu verantwortenden Tätigkeiten *definierte Prozesse*?

Beispiel Einkauf: Hier sollten angemessene Haupt- und Teil-Prozesse für den strategischen und operativen Einkauf existieren: Z.B. Bedarfsanalyse, Bedarfsmeldung, Sourcing, Lieferantenmanagement, Lieferantenauswahl, Vertragsmanagement, Bestellwesen, Wareneingangslogistik etc.

In der Praxis fällt auf, dass in den meisten Organisationen der für Governance, Compliance und Digitalisierung unverzichtbare Bereich Prozessmanagement gar nicht oder nur als wenig beachtete Annexfunktion zum Qualitätsmanagement existiert: Da besteht dann dringender Nachholbedarf.
Auditoren müssen daher, um angemessen prüfen zu können, angemessene Kenntnisse im Prozessmanagement nach Stand der Technik aufweisen.[105]

- **Mitgeltende Dokumente:** Sind die genannten Nachweise zur Erfüllung der relevanten Anforderungen revisionssicher dokumentiert?
- **Nachweise:** Dokumente, Ablageorte (auch in IT-Systemen), Tools sowie Versionsstände mit Datum werden seitens der Auditoren identifiziert und dokumentiert.

Zusätzlich werden folgende Punkte geprüft:

- **Identifizierte Risiken?**
- **Einhaltung von Compliance-Anforderungen?**
- **Nutzung von unterstützenden Tools?**
- **KI-Unterstützung vorhanden?**

16. Governance-Compliance-Audits und Resilienz-Score: Erst recht in Krisenzeiten - Eine *Auswahl* von Audit-Checkfragen zum Thema „Governance-Compliance", Resilienz und Kapitalmarktfähigkeit[106]:

Verständnis der (Legal-) Definitionen im Bereich Governance[107]

- 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?[108]

---

[105] Vgl. *Scherer*, Compliance-Managementsystem nach DIN / ISO 37301 erfolgreich, implementieren, integrieren, auditieren, zertifizieren, Din Media Verlag, 2022, Kapitel 8.1: Die Evolution des Prozessmanagements mit Pflichtenheft für ein Prozessmanagment-Tool.

[106] 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.

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

[108] 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.

Rechtliche Grundlagen (Compliance) für Governance[109]

- Sind die rechtlichen Grundlagen für Governance (Führung und Überwachung von Organisationen), Digitalisierung und Nachhaltigkeit bekannt und ist deren Einhaltung sichergestellt?[110]

- 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?

Relevante Referenzgrößen inkl. Standards für Governance[111]

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

Organe[112]

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?

---

[109] Vgl. DIN ISO 37000, Normabschnitt 1.
[110] 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.
[111] Vgl. DIN ISO 37000, Normabschnitt 2.
[112] Vgl. DIN ISO 37000, Normabschnitt 4.3.

- 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.

17. 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.
Deutschlandweit wurden bisher sieben Unternehmen von der einzigen[113] für ISO 37301- (CMS) bzw. 37001 (Antikorruption)-akkreditierten Zertifizierungsstelle zertifiziert:
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 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.“

[113] Stand 05/2025.

– Zitat von André Karl, Geschäftsleitung Karl-Gruppe

„Das von der Beratungsgesellschaft 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

18. Wertbeiträge

Investitionen in Digitalisierung mit KI, Governance, Risk und Compliance kosten zunächst Geld. Aber sie verstärken Resilienz und bedeuten nachhaltige Unternehmenswertsteigerung und Zukunftsfähigkeit.

Ein weiterer derzeit unverzichtbarer Wertbeitrag eines Governance-Compliance-Managementsystems ist die – gemäß ständiger höchstrichterlicher Rechtsprechung[114] - *enthaftende Wirkung für Geschäftsführung, Aufsichtsrat, Management, Abteilungsleiter, Compliance- und Risikomanager und sonstige Beschäftigte*.[115]

[114] 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")

[115] 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.

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.

Gülsah Atay, B.A.

Gülsah Atay studierte bis 2023 Betriebswirtschaft an der Technischen Hochschule Deggendorf. Seit 2022 ist sie im Bereich GRC als Consultant tätig. 2023 erfolgte die zusätzliche Verankerung in der Stabsstelle ESGRC der Technischen Hochschule Deggendorf. Sie ist als Lehrbeauftrage an der Technischen Hochschule Deggendorf in den Studiengängen Wirtschaftsinformatik und Soziale Arbeit eingesetzt. Kürzlich absolvierte sie zudem ihre Zertifizierung zur Qualitätsmanagementbeauftragten (QMB) beim TÜV Süd. Aktuell absolviert sie nebenberuflich den Masterstudiengang Risiko- und Compliancemanagement.

Anna Klinger, B.A.

Anna Klinger studierte von 2020-2024 Betriebswirtschaft an der Technischen Hochschule Deggendorf. Seit Beginn des Studiums war sie beruflich im Bereich GRC, unteranderem im Consulting tätig. Seit 2023 ist sie in der Stabsstelle ESGRC der Technischen Hochschule Deggendorf verankert. 2024 erfolgte die zusätzliche Beschäftigung im Referat Compliance an der Technischen Hochschule Deggendorf wo sie sich mit der Konzeptionierung und Implementierung eines CMS beschäftigt. Kürzlich absolvierte sie zudem ihre Zertifizierung zur Qualitätsmanagementbeauftragten (QMB) beim TÜV Süd. Aktuell absolviert sie zusätzlich nebenberuflich den Masterstudiengang Risiko- und Compliancemanagement.